Master Thesis

Thorvald Demuth Jørgensen

Provability Logic

An Investigation of the Relationship Between Modal Logic and Arithmetics

Date: December 14, 2022

Advisor: Asger Dag Törnquist & Rasmus Kræmmer Rendsvig

Abstract

This project is about the subject provability logic from mathematical logic, and the main result will be to prove Solovay's completeness theorems. These theorems state that the $\Box$-operator in the modal logic **GL** axiomatizes the proof predicate $\mathrm{Pr}(\cdot)$ from a wide range of fragments of arithmetic, and that the modal logic **GLS** axiomatizes the proof predicate of true arithmetics; i.e the standard model $\mathcal{N}$ of arithmetic We will proof the first completeness theorem for the arithmetical theory known as primitive recursive arithmetic. To prove these theorems we will need some results from recursion theory, general knowledge about fragments of arithmetics and the modal logics **GL** and **GLS**. We will further prove the fixed point theorem for **GL**. Lastly we will state some theorems about provability logic with more $\Box$-operators and with quantiferes.

Abstrakt

Dette projekt omhander emnet bevislighedsloigk fra matemateisk logik, og hovedresultatet will være at bevise Solovays fuldstændighedssætninger. Disse sætninger siger, at $\Box$-operatoren fra modal logikken **GL** aksiomesere bevisprædikatet $\mathrm{Bev}(\cdot)$ fra en masse forskellige fragmenter af arimetik, og at modal logikken **GLS** aksiomesere bevisprædikatet fra sand arimetik; også kendt som standard model $\mathcal{N}$ for arimetik. Til at starte med beviser vi den Solovays første fuldstændighedssætning for den aritmatiske teori kendt som primitive rekursiv aritmetik. For at bevise disse sætninger vil der være brug for nogle resultater fra rekursion teori, general viden omkring fragmenter af arimetik og modal logikkerne **GL** og **GLS**. Fikspunkts sætningen for **GL** vil også blive bevist. Slutteligt vil vi kommentere på nogle resultater for bevisligheds logik med flere $\Box$-operatorere og med kvantorer.

Contents

0 Introduction

> If modern modal logic was conceived in sin, then it has been redeemed through Gödliness.
>
> (George. S. Boolos 1979, Page 1)

{chap:intro}

This project is about the subject provability logic from mathematical logic, and the main result will be Solovay's completeness theorems. These theorems state that the $\Box$-operator in the modal logic **GL** axiomatizes the proof predicate $\mathrm{Pr}(\cdot)$ from a wide range of fragments of arithmetics, and that the modal logic **GLS** axiomatizes the proof predicate of true arithmetics. We will proof the first completeness theorem for the arithmetical theory known as primitive recursive arithmetic. To prove these theorems we will need some results from recursion theory and general knowledge about fragments of arithmetics and the modal logics **GL** and **GLS**. We will further prove the fixed point theorem for **GL**. The project has the following structure:

Chapter 1: This chapter will list some prerequisite results and definitions about the modal logic **GL** and the arithmetical theory *primitive recursive arithmetic*.

Chapter 2: In this chapter there will be a short introduction to recursion theory, and the main goal is to show Kleene's recursion theorem.

Chapter 3: Here we will introduce the arithmetical hierarchy and fragments of arithmetics. We will further comment on the amount of induction we have available in primitive recursive arithmetics

Chapter 4: We will start out by strengthening the completeness theorem for **GL**, with the finite tree completeness theorem. Further, we will look at an expansion of **GL** known as **GLS**, which we will later use for proving and state Solovay's second completeness theorem.

Chapter 5: The main goal of this chapter is to state and prove the fixed point theorem. We will also use it to calculate a few fixed points.

Chapter 6: In this chapter, we will prove both of Solovay's completeness theorems. Next will look at applications of these theorem, and how they can be used together with the fixed point theorem.

Chapter 7: Here we will round up the project with some perspective to further results in provability logic.

In the rest of this introduction we will introduce some notational conventions and give a short historical overview of the different logical fields, that will play a role in the project.

The bibliography of this project consists of a wide range of logical, mathematical and philosophical texts that are, in one way or another, connected to or referenced in the project. The main sources for this project are (Smorynski 1985), (George S. Boolos 1993) and (Soare 1987). A few minor sources are also used through the project, and they will be stated explicitly when used.

0.1 Notation

We denote the non-negative integers with ω; i.e $\omega = \{0, 1, 2, 3, \ldots\}$, and $\omega \times \omega = \omega^2$ and so on. Subsets of ω will be denoted by $A, B, C \ldots$ and arbitrary sets will be denoted by $\Gamma, \Xi, \Theta \ldots$. Lower case Latin letter a, b, c and x, y, z will denote integers, and $\vec{x}$ will be shorthand for a finite sequences e.g.$x_1, \ldots, x_n$. We will let $\omega^{<\omega}$ denote the finite sequences over ω. Further, recursive functions will be denoted by $\varphi, \psi, \vartheta, \ldots$, the graphs of recursive functions will be denoted by τ, ξ and ζ . Functions that are primitive recursive will be denoted by $f, g, h, \ldots$.

Additionally, we will introduce a system of arithmetic called *primitive recursive arithmetic* (**PRA**, for short) and the formulas of this system will be denoted with F, G and G.

For a partial function $\varphi(x) \downarrow$ will denote that $\varphi(x)$ is defined and $\varphi(x) \downarrow= y$ denotes that $\varphi(x)$ is defined and has value y. $\mathrm{dom}(\varphi)$ and $\mathrm{im}(\varphi)$ denotes the domain and image of $\varphi(x)$. A few special functions have their own symbols: S for the successor function, Z for the zero function and P for the projection. The formulae of the language **PRA** and languages for other arithmetical theories will be denoted by F, G and H.

Relations will be denoted by R, and $<, >, \leq, \geq$ will be used in the usual sense on integers. For a binary relation R, we will write that x is related to y as xRy or $(x, y) \in R$, and if $\vec{x}$ is related to each other, we will write $R(\vec{x})$.

We will use the standard symbols of propositional logic $\wedge, \vee, \rightarrow, \neg$. Further, we will sometimes use $\exists$ and $\forall$ in the metalanguage of modal logic and use them in the language of first-order arithmetics. The differences of these two usages should be clear from the context. We will augment the propositional logic with the modal unary connective $\Box$ and its dual $\Diamond := \neg\Box\neg$. We will denote modal formulas by the Greek letters $\alpha, \beta, \gamma, \sigma$. The symbol $\mathcal{H}$ will denote a Hintikka frame, which is a tuple $\langle W, R\rangle$ where W is a set of "nodes" and R is a relation on W, and $\mathcal{K}$ will denote a Kripke model, which is a Hintikka frame with a valuation ϕ on. We will use superscript to distinguish different frames and models for each other. A tree will be denoted by $\mathcal{T}$.

That α is a theorem of a modal logic Λ will be denoted by $\vdash_\Lambda \alpha$ and that F is a theorem of **PRA** will be denoted by $\mathbf{PRA} \vdash F$. We will later define a special modal logic called **GL** and for this modal logic will define an interpretation of its formulae into **PRA** by *. With this notation we can state Solovay's first completeness theorem:

$$\vdash_{\mathbf{GL}} \alpha \Leftrightarrow \forall^*(\mathbf{PRA} \vdash \alpha^*)$$

I.e a formula α is a theorem of **GL** if and only if for all interpretations * we have that α^* is a theorem of **PRA**.

0.2 Historical Introduction

Humans have been interested in numbers and calculation with these since before the beginning of history; i.e arithmetic. Another thing that have interested human since antiquity is the notions of necessity and possibility, which can be studied through modal logic. These two concepts do not have much in common, but through the development of Kripke semantics for modal logic, it became clear that it was possible to make a connection between these two seemingly different areas of mathematics.

0.2.1 Modal Logic

For most of the development of modal logic, philosophers and logicians tried to find a clear semantic for the notions possibility and necessity. These are not the only modalities that exists; the one we will look at in this project will be provability in a given arithmetical system. But the theory of modal logic will be a useful framework to work with.

The Greek philosopher Aristotle did try to develop some kind of modal logic about necessary and possibility in both his logical work *De Interpretatione* and in his *Metaphysic*.

With our modern eyes his thoughts about necessity and possibility seems a bit confusing. But he gets some implications about these notions right. A good overview of this part of his logical work can be found in (Lemmon 1977) and in (Łukasiewicz 1957). In the late antiquity and the middle ages there was done some work building on Aristotle earlier work.

The next big step for modal logic came in the enlightenment when the rationalist philosopher Gottfried W. Leibniz came up with the idea of possible worlds. Leibniz thought that we live in the best possible world, since it is this world God has chosen to create. With this idea of a metaphysical possible worlds, it was possible to make a clear definition of when a proposition is necessary true; and a proposition is necessary true, if it is true in all possible worlds. But Leibniz did not any further works on modal logic as a whole.

Modern modal logic is said to be started by Clarence Irving Lewis. He set out to develop a formal system without the paradoxes of materiel implication. This led to his development of a wide range of different modal logical system in the first part of the 20th century. His method was syntactical, since there were yet to be develop a ”smart” semantic for modal logic. But in the start of the 20th century, C. I. Lewis had started the modern modal logic, and a lot of other philosophers and logicians began to take an interest in the subject.

In the 1950s there had been a lot of research into the syntax of modal logic. But there was still not a clear definition of the semantics of modal logic, even though philosophers and logicians still had the intuitive definition of necessary truth from Leibniz. The answer came in the late 1950s, when the philosophers and logicians Jaako Hintikka and Saul Kripke developed the concept of a Kripke model.[1] This concept is crucial in this project, since it Robert Solovay showed that it was possible to embed Kripke models into arithmetic, in such a way that the Kripke model modeled some important features of arithmetic. Hintikka came up with the idea of a frame; i.e a pair $\langle W, R\rangle$ where W is a set of worlds and R is an arbitrary relation on these. With this construction it was possible to explain for a given world, what other worlds was accessible to it; i.e possible worlds for it. Kripke came up with the same idea, but added a valuation function to the frame, which to each formula of the language ascribed a set of worlds in which it was true. This construction made it possible for Kripke to prove some completeness results about modal logics.

When the concept of the Kripke model became wider known, it started a *Golden age* of research in modal logic. A lot of completeness results about different modal logics was proven in the 1960s and early 1970s; including the weak completeness theorem for the logic that would later be known as provability logic; this was done by Krister Segerberg without him having knowledge of what the interpretation of this logic could be.

In this short period of time, modal logic became a rigorous part of philosophical logic, but it had not been used in mathematical logic yet. This changed in the 1970s when the subfield known as provability logic was created. Here modal logic was used to gain more mathematical knowledge, by showing that it could axiomatize

[1] They were not alone in this development.

the notion of provability in the arithmetical theory known as Peano Arithmetic. So even though modal logic in its early development was mostly used to help philosophers to gain knowledge about philosophical concepts like ethics, knowledge and metaphysics, the power of modal logic was also useful outside of philosophy.

A deeper look into the development of modal logic can be found in (Goldblatt 2003).

0.2.2 Arithmetics and Recursion Theory

A natural question to ask about a given mathematical theory is which properties the notion of provability in the theory have. In this project it will be shown that provability in different arithmetical theories can be seen as a modality, which we can modeled in a specific modal logic. But first we will introduce how it became clear how this was a possibility.

Even though humans have been using arithmetics for millennials, it had not been axiomatized.

It was first in the second half of the 1800s there was a development in the axiomatization of arithmetics. Richard Dedekind and Giuseppe Peano developed axioms system for arithmetics, these was later evolved into was today is known as the Peano axioms for arithmetics.

Another important achievement at the turn of the century, was David Hilbert's proof that the consistency of Euclidean geometry could be proven by proving that arithmetics was consistent in his work *Grundlagen der Geometrie* This was one of the first steps in what later would be known as the Hilbert program. The Hilbert program was not really a program until the end of 1920, where it became clear that its goal was to prove that the *ideal* transfinite mathematics was consistent, and that the proof of this should be conducted in a *real* finite mathematics system.

An example of such a finite system could be the *Primitive recursive arithmetics* that was developed by Toralf Skolem; the definition of this system will be given in the next chapter. This system can be seen as a (induction-wise) weaker version of Peano aritmetics. Tait argues that such a system fulfills the finitist conditions of the Hilbert program. This system will be the main system of this project and the definition of it will come in the next chapter.

Another important mathematical system of arithmetics was the one developed by Bertrand Russell and Alfred North Whitehead in their work: *Principia Mathematica*. The goal of this work was somewhat different than the one of the Hilbert program. Russell had a thesis that shortly (and not the most precis) says that all of mathematics could be reduce to logic. In Kantian terms he thought that mathematics was analytical *a priori*.

In 1931 Kurt Gödel's paper: *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I* it was shown that the system of Russell and Whitehead was not complete, and under the assumption that the system was consistent that it could not prove its own consistency. This result can be generalized to systems strong enough to do simple arithmetic. This was made possible by Gödel by defining a predicate inside of the mathematical system, which could state that if a given formula of the language of had a proof or not. The original proof was build on the system of Russel and Whitehead and had a assumption of ω-consistency. This was a blow to the Hilbert program, since the result showed that the goal of it could not be fulfilled. Later on John Barkley Rosser in his article (Rosser 1936) improved the result so that normal consistency was enough.

Later on in the 1930s Gödel extended the primitive recursive function to the recursive functions. A few different definitions of intuitively computable functions was set forward by Kleene, Turing and Church and it was shown that all these different notions of intuitively computable functions gave rise to the same class of functions.

This lead Church to state the so called *Church-Turing Thesis*, that states that this class of functions are the computable functions.

In 1955 Martin Löb showed that the proof predicate that Gödel had created fulfilled some simple conditions that now is known as Löb's derivability conditions. In the late 1960s and early 1970s it became clear that these conditions made an interpretation of the proof predicate possible in modal logic.

0.2.3 Provability Logic

The first time that someone made a connection between modal logic and the proof predicate of some form of arithmetic, was in 1933 when Kurt Gödel published his very short paper: *Eine Interpretation des intuitionistischen Aussagenkalkuls*. Here, Gödel stated as a hypothesis that it was possible to axiomatize what the intuitionist meant by a proof in a version of modal logic.

After Löb's derivability conditions was found and after the development of the semantics of modal in the 1960s, it became clear that there was a connection between the logic that Segerberg had proven to be weakly complete and the proof predicate from arithmetics.

This lead to research done in different places around the world, from The Netherlands, Italy and the United States. It was clear early on that if α was a theorem of provability logic, then for all interpretations of α in a fragment of arithmetics it was also a theorem of this fragment; but the other way was harder to show. In the same time there was proven a number of important theorems about provability; one of these, called the Fixed Point Theorem, will be proven in chapter 5. A short overview of this early development can be found in (George S. Boolos and Sambin 1991).

It was proven in 1976 by Solovay that the modal logic now known as provability logic, is the logic of the provability predicate in Peano Arithemic; i.e if for all interpretations of a formula α, if this interpretation was a theorem of Peano arithmetics, then the formula α was a theorem of provability logic. This also means that provability logic can be seen as an axiomataxion of the proof predicate. Solovay's result will be the main result in this project; it will be stated precisely and proven in Chapter 6.

After Solovay's article was published, the research focus of provability logic was to generalize Solovay's result to other fragments of arithmetics and if it did also hold for multi-modal provability logic and quantified provability logic. The results of these results will be commented on in the last part of chapter 6 and in chapter 7

The majority of the main results about provability logic were proven in the late 70s, 80s and early 90s. This project will not go beyond these early results.

1 Preliminary

{chap:Pre}

In this section, I will state a few results and definitions from two projects that I have written; one about modal logic and one about Gödel's incompleteness theorems. These results will be given without proof. The proofs can be found in the original two projects (Jørgensen 2021) and (Jørgensen 2022).

The main points of this section will be the definition of the predicate $\mathrm{Pr}(\cdot)$ which is constructed in the proof of Gödel's Incompleteness Theorems, and the definition of the modal logic **GL** (the name comes from Gödel and Löb) and a few of the properties of this modal logic. The main result of this project will be Solovay's arithmetic completeness theorem, which simply put states that these two predicates (from different mathematical systems) "behave" in the same way.

The most definitions and results from this section will be used in the rest of the project.

1.1 Modal Logic

Modal logic will play an important role in this project. The main point here, is that provability can be seen as modality. This will be shown later on in the project. This section will introduce a lot of basic definitions and results about modal logic. The most important of these being the Kripke model, the modal logic **GL** and the weak completeness theorem for this modal logic.

1.1.1 The language of modal logic

In this subsection we will define our language $\mathcal{L}_\Box$ of modal logic. We will start off with a set called Φ, which consists of propositional letters $p, q, \ldots$. We can further define the primitive symbols of our modal language $\mathcal{L}_\Box$:

Definition 1.1 The following symbols are the primitive in our language $\mathcal{L}_\Box$

1. Every letter from the set Φ.
2. The logical constants $\bot$ (zero-ary) and $\to$ (binary).
3. The modal operator $\Box$ (unary).

$\dashv$

We can now define the well-formed formulas of $\mathcal{L}_\Box$, or as we will call them: *modal formulas*.

Definition 1.2 We define a *modal formula* recursively in the following way:

i. Each $p \in \Phi$ is a modal formula

ii. $\perp$ is a modal formula

iii. If α and β are modal formulas then so is $\alpha \to \beta$.

iv. If α is a modal formula then so is $\Box\alpha$

v. Nothing is a modal formula except as prescribed by (i)-(iv)

$\dashv$

Further we will define the connectives $\wedge, \neg, \vee, \leftrightarrow, \Diamond, \Box^n, \Diamond^n$ and $\top$ in the usual way. We will read $\Box\alpha$ as "α is provable". Normally in the alethic modal logic the $\Box\alpha$ reads "α is necessarily true". Further the symbol $\perp$ stands for falsehood. We will read $\Diamond\alpha$ as "α is consistent".

1.1.2 Semantics

In this section we will define the notation of truth for our modal logic. We will begin by defining a Hintikka frame and a Kripke model.

Definition 1.3 (Hintikka frame) A *Hintikka frame* is a tuple $\mathcal{H} = \langle W, R\rangle$ where W is a non-empty set (we will call its members for nodes[1]) and where $R \subset W \times W$ is a relation that we will call the accessibility relation. We will use the notation wRv to denote that the note w sees the note v; i.e $(w, v) \in R$. $\dashv$

We do not at this time give the relation R any properties. It could be reflexive, transitive, anti-symmetric or have any other properties that a relation can have.

Definition 1.4 (Kripke model) A *Kripke model* is a tuple $\mathcal{K} = \langle \mathcal{H}, \phi\rangle$ where $\mathcal{H}$ is a Hintikka frame and ϕ is a valuation function that to each proportional letter $p \in \Phi$ assigns a subset $\phi(p)$ of W. Formally:

$$\phi : \Phi \to \mathcal{P}(W)$$

$\dashv$

[1] Normally the members of this set will be called worlds, but this interpretation does not make senses in provability logic

We can now define the notion of truth in a given Kripke model $\mathcal{K} = \langle \mathcal{H}, \phi \rangle$. If a modal formula α is true at a node w in a Kripke model $\mathcal{K} = \langle \mathcal{H}, \phi \rangle$, we will write:

$$\vDash^{\mathcal{K}}_{w} \alpha$$

This notation is taken from (Lemmon 1977). An alternative notation for $\vDash^{\mathcal{K}}_{w} \alpha$ is $\mathcal{K}, w \vDash \alpha$. This notation is more used today than the one that will be used in this project.

Definition 1.5 (Truth definition) We define the notion of *truth* in a Kripke model $\mathcal{K} = \langle \mathcal{H}, \phi \rangle$ in the following way:

1. If α is propositional p then:

$$\vDash^{\mathcal{K}}_{w} \alpha \text{ iff } w \in \phi(p)$$

2. If α is $\perp$ then:

$$\vDash^{\mathcal{K}}_{w} \alpha \text{ iff never}$$

3. If α is $\beta \to \gamma$ then:

$$\vDash^{\mathcal{K}}_{w} \alpha \text{ iff if} \vDash^{\mathcal{K}}_{w} \beta \text{ then } \vDash^{\mathcal{K}}_{w} \gamma$$

4. if α is $\Box\beta$ then:

$$\vDash^{\mathcal{K}}_{w} \alpha \text{ iff for all } v \text{ such that } wRv \text{ we have } \vDash^{\mathcal{K}}_{v} \beta$$

$\dashv$

We will end this section with definitions of a *valid* and *satisfiable* formula.

Definition 1.6 For a given Hintikka frame $\mathcal{H} = \langle W, R \rangle$, we say that α is *valid* in $\mathcal{H}$ and write $\vDash^{\mathcal{H}} \alpha$ if and only if $\vDash^{\mathcal{K}}_{w} \alpha$ for all Kripke models on our frame $\mathcal{H}$ and all notes $w \in W$. Further we say that α is *satisfiable* in $\mathcal{H}$ if and only if $\vDash^{\mathcal{K}}_{w} \alpha$ for some Kripke model $\mathcal{K}$ on the frame $\mathcal{H}$ and some note $w \in W$.

α is called *valid* if and only if α is valid in all frames $\mathcal{H}$, if this is the case we simply write $\vDash \alpha$. α is called *satisfiable* if and only if α is satisfiable on all frames $\mathcal{H}$.

A formula α is called valid on a class of frames $\mathcal{C}$, if for all $\mathcal{H} \in \mathcal{C}$ we have that $\vDash^{\mathcal{H}} \alpha$. We write this as $\vDash^{\mathcal{C}} \alpha$.

A formula α is *valid* in a Kripke model $\mathcal{K} = \langle W, R, \phi \rangle$ if and only if $\vDash^{\mathcal{K}}_{w} \alpha$ for all notes $w \in W$. We write this as $\vDash^{\mathcal{K}} \alpha$.

If a Kripke model $\mathcal{K}$ has a *minimal node* w_0, i.e a node such that for all $v \in W$ we have $w_0 Rv$, then a modal formula α is called *true* in $\mathcal{K}$ if we have that $\vDash^{\mathcal{K}}_{w_0} \alpha$. $\dashv$

1.1.3 The modal logic GL

In this section, we will define the notion of a modal logic and define the modal logic **GL**, which will be our base modal logic in this project.

Definition 1.7 A *modal logic* Λ is a set of modal formulas that contains all propositional tautologies, and is closed under *modus ponens* (MP) and uniform substitution. If $\alpha \in \Lambda$ we say that α is a theorem of Λ and write $\vdash_\Lambda \alpha$, else we write $\nvdash_\Lambda \alpha$.

We will also define the set $\Lambda_S = \{\alpha \vDash^{\mathcal{S}} \alpha, \text{ for all structures } \mathcal{S} \in S\}$. Where S is any class of frames. ⊣

We will further define when a given modal formula is deducible in a modal logic:

Definition 1.8 Let Λ be a modal logic, let $\beta_1, \ldots, \beta_n$ be modal formulas in Λ and let α be a modal formula. We say that α is *deducible* from $\beta_1, \ldots, \beta_n$ if $(\beta_1 \wedge \cdots \wedge \beta_n) \to \alpha$ is a tautology.

If $\Gamma \cup \{\alpha\}$ is a set of modal formulas, then α is *deducible* in Λ from Γ if $\vdash_\Lambda \alpha$ or if there are formulas $\beta_1, \ldots, \beta_n \in \Gamma$ such that:

$$\vdash_\Lambda (\beta_1 \wedge \cdots \wedge \beta_n) \to \alpha$$

In this case we write $\Gamma \vdash_\Lambda \alpha$, else we write $\Gamma \nvdash_\Lambda \alpha$. ⊣

We will now define what a *normal modal logic* is. We will later look at a modal logic that is not normal. But the modal logic **GL** is a normal one.

Definition 1.9 A modal logic Λ is called *normal* if it has the following axioms and deduction rules:

Tau All propositional tautologies.

K $\Box(p \to q) \to (\Box p \to \Box q)$.

MP $p,\ p \to q \vdash_\Lambda q$ (*modus ponens*.

Nec $p \vdash_\Lambda \Box p$ (*necessitation*).

If Γ is a set of modal formulas we call the smallest normal logic containing Γ the normal modal logic axiomatized by Γ. The normal modal logic axiomatized by the empty-set is called **K**, and this is the smallest normal modal logic.[2] ⊣

A few standard results follow from these definitions:

[2]Here **K** stands for Kripke.

Proposition 1.10 If Λ is a normal modal logic then:

1. If $\vdash_\Lambda \alpha \to \beta$ then $\vdash_\Lambda \Box\alpha \to \Box\beta$.

2. $\vdash_\Lambda \Box(\alpha \wedge \beta) \leftrightarrow \Box\alpha \wedge \Box\beta$.

3. $\vdash_\Lambda \Box(\alpha_1 \wedge \cdots \wedge \alpha_n) \leftrightarrow \Box\alpha_1 \wedge \cdots \wedge \Box\alpha_n$ for $n \geq 2$.

4. If $\vdash_\Lambda \beta_1 \wedge \cdots \wedge \beta_n \to \alpha$ then $\vdash_\Lambda \Box\beta_1 \wedge \cdots \wedge \beta_n \to \Box\alpha$, for $n \geq 0$.

It should further be noted that the axiom **K** is equivalent to the following formula:

$$\Box p \wedge \Box(p \to q) \to q$$

Smorynski uses this formula as an axiom instead of the axiom **K**. We can extend the logic **K** in the following way, to get the logic **GL** and the logic **4**.

Definition 1.11 **K4** is the modal logic that extends **K** by adding the following axiom:

4 $\Box p \to \Box\Box p$.

GL is the modal logic extending **K** by adding the two following axioms:

4 $\Box p \to \Box\Box p$.

L $\Box(\Box p \to p) \to \Box p$.

$\dashv$

Remark 1.12 Smorynski calls the modal logic **K4** for **BML** (Basic modal logic).

It can be shown that the axiom **4** is redundant. It is now possible to define the notions of soundness, strong completeness and weak completeness.

Definition 1.13 Let S be a class of frames or models.

1. A normal modal logic Λ is sound with respect to S if $\Lambda \subseteq \Lambda_S$, i.e if $\vdash_\Lambda \alpha$ implies $\vDash^{\mathcal{S}} \alpha$ for all $\mathcal{S} \in S$.

2. A modal logic Λ is strongly complete with respect to S if for any set of formulas $\Gamma \cup \{\alpha\}$, if $\Gamma \vDash^{\mathcal{S}} \alpha$ then $\Gamma \vdash_\Lambda \alpha$ for all $\mathcal{S} \in S$ and it is weakly complete with respect to S if for any formula α if $\vDash^{\mathcal{S}} \alpha$ then $\vdash_\Lambda \alpha$ for all $\mathcal{S} \in S$.

$\dashv$

To show completeness results you often have to create a *canonical model* and then show that the given modal logic is complete with respect to this model. It can be shown that **K** is sound and strongly complete with respect to the class of all frames. A lot of different completeness results can be found in (Lemmon 1977) and (Blackburn 2002). Here we will just state a few of the results about **GL**.

Theorem 1.14 **GL** is not sound and strongly complete with respect to any class of frames.

There is another result concerning the completeness and soundness of **GL**. To state this, we first need some definitions concerning relations:

Definition 1.15 A relation R on frame $\mathcal{H} = \langle W, R \rangle$ is said to be *transitive* if for all $w_1, w_2, w_3 \in W$, whenever $w_1 R w_2$ and $w_2 R w_3$ then $w_1 R w_3$.

The relation R is said to be *well-founded* on $\mathcal{H}$ if every non-empty subset $V \subseteq W$ has a minimal element with respect to R. In other words R is well-founded if there is no infinite sequence $\ldots R w_2 R w_1 R w_0$

Further the relation R is said to be *conversely well-founded* on $\mathcal{H}$ if the converse R^{-1} of R is well-founded; i.e if there is no infinite sequence such that $w_0 R w_1 R w_2 R \ldots$ $\dashv$

We can now state the following theorem:

{thm:GLcomplete}

Theorem 1.16 **GL** is sound and weakly complete with respect to the class of transitive and conversely well-founded frames.

In chapter 4 we will show some further results about **GL** and in chapter 5 we will show a fixed point theorem about **GL**. We will end this section with the following proposition that will be needed later:

{prop:GL}

Proposition 1.17 $\vdash_{\mathbf{GL}} \Box(\alpha \leftrightarrow \beta) \rightarrow (\Box\alpha \leftrightarrow \Box\beta)$

1.2 Gödel's Incompleteness Theorems

In this section we will state and sketch the proof of Gödel's incompleteness theorems. In this sketch we will define a predicate $\mathrm{Pr}(\cdot)$ that says a given formula has a proof in arithmetic. We will also introduce the class of primitive recursive functions, the arithmetical theory known as primitive recursive arithmetic and the notion of Gödel numbering.

1.2.1 Primitive Recursive Functions

We will begin by defining a class of functions that will both play a crucial role in the proof of Gödel's Incompleteness Theorems and in the rest of this project.

{def:Recur}

Definition 1.18 The class of primitive recursive functions is the smallest class closed under the following schemata:

I. $S(x) = x + 1$ is primitive recursive.

II. $Z(x) = 0$ is primitive recursive.

III. $P_i^n(x_1, \ldots, x_n) = x_i$ is primitive recursive.

IV. If $g, h_1, \ldots h_m$ are primitive recursive then so is

$$f(x_1, \ldots, x_n) = g(h_1(x_1, \ldots, x_n), \ldots, h_m(x_1, \ldots, x_n))$$

V. If g and h are primitive recursive and $n \geq 1$ then f is also primitive recursive where:

$$\begin{aligned} f(0, x_1, \ldots, x_n) &= g(x_1, \ldots, x_n) \\ f(x_1 + 1, x_2, \ldots, x_n) &= h(x_1, f(x_1, \ldots, x_n), x_2, \ldots, x_n) \end{aligned}$$

$\dashv$

We can also define relations as being primitive recursive:

Definition 1.19 A relation $R \subseteq \omega^n$ is primitive recursive if its characteristic function is:

$$\chi_R(\vec{x}) = \begin{cases} 0 & \text{if } R(\vec{x}) \\ 1 & \text{if } \neg R(\vec{x}) \end{cases}$$

$\dashv$

So with these definitions we can show that some well known functions are primitive recursive. The proofs of these can be rather tiresome and have therefor been left out.

Proposition 1.20 The following list of functions are all primitive recursive:

1.	$K^n_k(x_1, \ldots, x_n) = k$	Constant
2.	$A(x, y) = x + y$	Addition
3.	$M(x, y) = x \cdots y$	Multiplication
4.	$E(x, y) = x^y$	Exponentiation
5.	$pd(x) = \begin{cases} x - 1, & x > 0 \\ 0, & x = 0 \end{cases}$	Predecessor
6.	$x \dot{-} y = \begin{cases} x - y & x, \geq y \\ 0, & x < y \end{cases}$	Cut-off subtraction
7.	$sg(x) = \begin{cases} 0, & x = 0 \\ 1, & x > 0 \end{cases}$	Signum
8.	$\overline{sg}(x) = \begin{cases} 1, & x = 0 \\ 0, & x > 0 \end{cases}$	Signum complement
9.	$\lvert x - y \rvert = \begin{cases} x - y, & x \geq y \\ y - x, & x < y \end{cases}$	Absolute value

1.2.2 PRA

In this section we will specify the rules and language of the arithmetical theory **PRA**. This theory will be the one we will state Gödel's incompleteness theorems for, and later will prove Solovay's completeness theorems for it. We could have picked a different theory like *Peano Arithmetic*, but the axioms of **PRA** makes it a lot easier to show that the theory can compute the functions known as primitive functions, which are crucial for the proof of Gödel's completeness theorems. First, we will define the language $\mathcal{L}_{\mathbf{PRA}}$ of **PRA**.

Definition 1.21 The language $\mathcal{L}_{\mathbf{PRA}}$ consists of the following symbols:

$$\begin{aligned} \text{Variables} &: v_0, v_1, \ldots \\ \text{Constants} &: \overline{0} \\ \text{Function symbols} &: \overline{f} \text{ for each primitive recursive function } f \\ \text{Relation symbols} &: = \\ \text{Propositional connectives:} &: \neg, \wedge, \vee, \rightarrow \\ \text{Quantifiers} &: \forall, \exists \end{aligned}$$

⊣

We will now define the notions of terms and formulae of **PRA**. This part is mostly done to settle notations.

Definition 1.22
1. The set of *terms* of the language of **PRA** is defined inductively by:
   a) $\overline{0}$ is a term and each v_i is a term.
   b) If f is an n-ary function symbol and $t_1, \dots t_n$ are terms then $\overline{f}t_1 \dots t_n$ is a term.
2. The set of *formulae* of the language of **PRA** is defined inductively by:
   a) If t_1 and t_2 are terms then $= t_1 t_2$ is a formula.
   b) If F and G are formulae, so are $\neg F, \wedge FG, \vee FG$ and $\rightarrow FG$.
   c) If F is a formula and v is a variable, then $\exists v F$ and $\forall v F$ are also formulae.

$\dashv$

We use Polish notation so we do not have parentheses in our language. In practice we will use parentheses and infix notation, by defining the connectives in the classic way. We leave out parentheses to make the Gödel numbering of **PRA** easier to do. We will also need the definition of a *sentence*.

Definition 1.23 A formula F of **PRA** is called a *sentence* if it has no free variables; i.e if all variables v that occur in F are bound. $\dashv$

Having defined the language of **PRA** we can now state the different axioms of **PRA**:

Definition 1.24 The axioms **PRA** are the following:

1. Propositional axioms
   a) $F \rightarrow (G \rightarrow F)$
   b) $(F \rightarrow (G \rightarrow H)) \rightarrow ((F \rightarrow G) \rightarrow (F \rightarrow H))$
   c) $F \wedge G \rightarrow F$
   d) $F \wedge G \rightarrow G$
   e) $F \rightarrow (G \rightarrow F \wedge G)$
   f) $F \rightarrow F \vee G$
   g) $G \rightarrow F \vee G$
   h) $(F \rightarrow H) \rightarrow ((G \rightarrow H) \rightarrow (F \vee G \rightarrow H))$

i) $(F \to G) \to ((F \to \neg G) \to \neg F)$

j) $\neg\neg F \to F$

2. Quantifier axioms

   a) $\forall v F v \to F t$

   b) $F t \to \exists v F v$

   Where t is substitutable for v in Fv in both cases.

3. Equality axioms

   a) $v_0 = v_0$

   b) $v_0 = v_1 \to v_1 = v_0$

   c) $v_0 = v_1 \wedge v_1 = v_2 \to v_0 = v_2$

   d) $v_i = w \to \bar{f}(v_1, \ldots, v_i, \ldots, v_n) = \bar{f}(v_1, \ldots, w, \ldots, v_n)$

   Where $1 \leq i \leq n$ and $\overline{f}$ is an n.ary function symbol.

4. Non-logical axioms

   a) Initial functions

      i. $\overline{Z}(v_0) = \overline{0}$

      ii. $\neg(\overline{0} = \overline{S}(v_0))$

      iii. $\overline{S}(v_0) = \overline{S}(v_1) \to v_0 = v_1$

      iv. $\overline{P}_i^n(v_1, \ldots, v_n) = v_1$ for $1 \leq i \leq n$

   b) Derived functions

      i. $\overline{f}(v_1, \ldots, v_n) = \overline{g}(\overline{h}_1(v_1, \ldots, v_n), \ldots, \overline{h}_m(v_1, \ldots v_n)$. Here f is defined by composition of $g, h_1, \ldots, h_m$

      ii. Let f be defined by primitive recursion from the primitive recursive function g and h, then the following to things holds:
      $\overline{f}(\overline{0}, v_1, \ldots, v_n) = \overline{g}(v_1, \ldots, v_n)$ and
      $\overline{f}(\overline{S}v_0, v_1, \ldots, v_n) = \overline{h}(\overline{f}(v_0 1, v_1, \ldots, v_n), v_0, v_1, \ldots, v_n)$

   c) Induction
      $F(\overline{0}) \wedge \forall v(Fv \to F(\overline{S}v)) \to \forall v F(v)$ where $F(v)$ is

$$\exists v_n(\overline{f}(v, v_0, v_1, \ldots, v_n) = \overline{0})$$

$\dashv$

The only of these axioms that are a bit strange is the induction one. The axiom gives a bit more induction than necessary for the proof of Gödel's incompleteness theorem; but we will need a bit more induction for the proof of Solovay's completeness theorems. On the other hand, if we had allowed full induction; i.e induction on every formula, the system we would have defined would be known as **PA**; Peano Arithmetics, and this system is a lot stronger than what is needed for the proof of Gödel's incompleteness theorems and Solovay's completeness theorems. We will in Chapter 3 comment a bit more about different arithmetical theories and the amount of induction in them. Having written down the axioms, we will move on to the inference rules of **PRA**.

Definition 1.25 The *inference rules* of **PRA** are the following:

1. From $F, F \to G$, derive G (modus ponens).
2. From $Fv \to G$ derive $\exists vFv \to G$, under the assumption that no v occurs free in G.
3. From $G \to Fv$ derive $G \to \forall vFv$, under the assumption that no v occurs free in G.

A *formal derivation* in **PRA** is a sequence of formulas of **PRA** $F_0, F_1, \ldots, F_k$ such that each F_i is either an axiom of **PRA** or follows from two other formulas F_j, F_l where $j, l < i$ by one of the three inferences rules. ⊣

We will end this section with a theorem that states that **PRA** can compute the primitive recursive functions.

Theorem 1.26 Let f be an n-ary primitive recursive function and let $\overline{f}$ be the function symbol representing it in **PRA**. Then for all $n_1, \ldots, n_m, n \in \omega$ we have:

$$f(n_1, \ldots, n_m) = n \Rightarrow \mathbf{PRA} \vdash \overline{f}(\overline{n_1}, \ldots, \overline{n_m}) = \overline{n}$$

That **PRA** can compute the primitive recursive functions makes it possible to encode the syntax of **PRA**. This will be explained in the next section.

1.2.3 Arithmetization of the syntax

In this section we will discus how each expression ρ in the language of **PRA** can be given a unique code-number $\ulcorner \rho \urcorner$ called the Gödel number. This makes it possible for **PRA** to express things about itself. For this encoding to work we will need the fundamental theorem of arithmetic that states that every natural number $a \geq 2$ has a unique representation:

$$a = p_{i_0}^{n_0} \cdots p_{i_k}^{n_k}$$

Where each p is a distinct prime and all the n_i are positive. If given a sequence of natural numbers $(j_0, \ldots j_t)$ we can encode it with a unique code in the following way:

$$c = 2^{j_0+1}3^{j_1+1} \cdots p^{j_t+1}$$

By encoding them like this it is possible to give each string of symbols of **PRA** a unique code. We will begin by listing the codes for some of our symbols of **PRA**:

1. $\ulcorner \overline{0} \urcorner$ is (0).
2. $\ulcorner = \urcorner$ is (1).
3. $\ulcorner \neg \urcorner$ is (2); $\ulcorner \wedge \urcorner$ is (3); $\ulcorner \vee \urcorner$ is (4) and $\ulcorner \rightarrow \urcorner$ is (5).
4. $\ulcorner \forall \urcorner$ is (6) and $\ulcorner \exists \urcorner$ is (7).
5. $\ulcorner v_i \urcorner$ is $(8, i)$.

These are the easy one to gives. The hard ones are the codes for the function symbols. We will define the codes for these inductively as seen in the following table:

Function	Index
$Z(x) = 0$	$(9, 1, 1)$
$S(x) = x + 1$	$(9, 2, 1)$
$P_i^n(x_1, \ldots, x_n) = x_i$	$(9, 3, n, i)$
$f(\vec{x}) = g(h_1(\vec{x}), \ldots, h_m(\vec{x}))$	$(9, 4, n, m, (g^*, h_1^*, \ldots, , h_m^*)$
$f(0, x_1, \vec{x}) = g(\vec{x})$ $f(x + 1, \vec{x}) = h(f(x, \vec{x}), x, \vec{x})$	$(9, 5, n + 1, g^*, h^*)$

Table 1.1: The Codes for the Function Symbols

This encoding is primitive recursive so **PRA**, can do this encoding. But the proof of that is very tedious, so it will be left out. A lot of different relations and functions can be shown to be primitive recursive, one of the important ones is the function $subst(x; y, z)$, which substitutes z for y in the formula x. With this, it is possible to show that we can primitive recursively define our axioms of **PRA**. This means that **PRA** is capable of identifying its own axioms. Further it can also identify that if a given sequence of formulas is a proof of another given formula; i.e the relation that says "y codes a derivation of the formula with code x". We shorten this as $\mathrm{Prov}(x, y)$ and we further define the non primitive recursive predicate "x codes a provable formula" as: $\mathrm{Pr}(x) \leftrightarrow \exists y(\mathrm{Prov}(y, x))$. This predicate is the one known as the proof predicate.

1.2.4 The Proof Predicate and the Theorems

The predicate $\mathrm{Pr}(x)$ can been shown to having the following properties called Löb's derivability conditions:

D1: $\mathbf{PRA} \vdash F \Rightarrow \ \mathbf{PRA} \vdash \mathrm{Pr}(\ulcorner F \urcorner)$.

D2: $\mathbf{PRA} \vdash \mathrm{Pr}(\ulcorner F \to G \urcorner) \to (\mathrm{Pr}(\ulcorner F \urcorner) \to \mathrm{Pr}(\ulcorner G \urcorner))$.

D3: $\mathbf{PRA} \vdash \mathrm{Pr}(\ulcorner F \urcorner) \to \mathrm{Pr}(\ulcorner \mathrm{Pr}(\ulcorner F \urcorner) \urcorner)$.

It is also clear that $\neg \mathrm{Pr}(\perp)$, where $\perp$ is some false statement, expresses consistence of **PRA**. We will denote this by Con. With the use of the *subst* function, we can further prove the following important lemma:

Lemma 1.27 (The Fixed Point Lemma) Given any formula G where the only free variable is v, we can find a sentence F such that:

$$\mathbf{PRA} \vdash F \leftrightarrow G(\ulcorner F \urcorner)$$

This lemma makes it possible for us to show the first incompleteness theorem:

Theorem 1.28 (The First Incompleteness Theorem) The predicate $\mathrm{Pr}(\cdot)$ have the following properties for all formulas G:

1. $\mathbf{PRA} \vdash G \Rightarrow \ \mathbf{PRA} \vdash \mathrm{Pr}(\ulcorner G \urcorner)$

2. $\mathbf{PRA} \vdash \mathrm{Pr}(\ulcorner G \urcorner) \Rightarrow \ \mathbf{PRA} \vdash G$

If we let F be as follows, by the fixed point lemma: $\mathbf{PRA} \vdash \ F \leftrightarrow \neg \mathrm{Pr}(\ulcorner F \urcorner)$, we then have:

1. $\mathbf{PRA} \nvdash F$

2. $\mathbf{PRA} \nvdash \neg F$

I.e we have a sentence where neither it or its negation can be proven. So our system is incomplete.

Since $\mathrm{Pr}(\cdot)$ fulfills the derivability conditions, the second theorem can also be proven.

Theorem 1.29 (The Second Incompleteness Theorem) Under the assumption that **PRA** is consistent we have that $\mathbf{PRA} \nvdash \mathrm{Con}$.

The main goal for the rest of this project is now to prove that the $\Box$ in **GL**"behaves" in the same way as the $\mathrm{Pr}(\cdot)$ predicate from **PRA**. How this should be understood will be explained latter on. To prove this theorem, we will first need a main result from Recursion Theory called the recursion theorem, which will be introduced in Chapter 2.

We will need one more result about the proof predicate in the project. It is called the formalized Löb's theorem, and this theorem together with the derivability conditions tells the full story about the predicate $\mathrm{Pr}(\cdot)$.

Theorem 1.30 (Formalized Löb's Theorem) Let F be any sentence of **PRA**. Then:

$$\mathbf{PRA} \vdash \mathrm{Pr}(\ulcorner \mathrm{Pr}(\ulcorner F \urcorner) \to F \urcorner) \to \mathrm{Pr}(\ulcorner F \urcorner)$$

This theorem was an original an answer to a question asked by Leon Henkin: "If **PRA** proves that $G \leftrightarrow \mathrm{Pr}(\ulcorner G \urcorner)$ what does this say about G? Löb's answer is then that **PRA** can only prove that $\mathrm{Pr}(\ulcorner G \urcorner) \to G$ in the case where **PRA** proves G itself.

We will in a later chapter need the following lemma:

{lem:Prov}

Lemma 1.31 Let $\overline{f}$ be an n-ary primitive recursive function symbol. There is a function g depending on f, such that:

$$\mathbf{PRA} \vdash \overline{f} v_0 \dots v_{n-1} = v \to \mathrm{Prov}(\overline{g} v_0 \dots v_{n-1}, \ulcorner f \dot{v}_0 \dots \dot{v}_{n-1} = \dot{v}_n \urcorner)$$

Where $\ulcorner f \dot{v}_0 \dots \dot{v}_{n-1} = \dot{v}_n \urcorner$ denotes the code of the formula where we have substituted the variables with the nummerals: $\overline{v}_0, \dots, \overline{v}_{n-1}$.

The Formalized Löb's Theorem and the derivability conditions can be shown to hold for a wide range of arithmetical systems. A short overview of this subject will be given in Chapter 3.

Remark 1.32 If we write $\vdash F$ instead of $\mathbf{PRA} \vdash F$, it means we have not specified the arithmetical system we are looking at.

If we compare the properties of $\mathrm{Pr}(\cdot)$ with the properties of the $\Box$-operator of **GL**, we get the following table:

$\vdash_{\mathbf{GL}} \alpha \Rightarrow \vdash_{\mathbf{GL}} \Box\alpha$	$\vdash F \Rightarrow \vdash \mathrm{Pr}(\ulcorner F \urcorner)$
$\vdash_{\mathbf{GL}} \Box(\alpha \to \beta) \to (\Box\alpha \to \Box\beta)$	$\vdash \mathrm{Pr}(\ulcorner F \to G \urcorner) \to (\mathrm{Pr}(\ulcorner F \urcorner) \to \mathrm{Pr}(\ulcorner G \urcorner))$
$\vdash_{\mathbf{GL}} \Box\alpha \to \Box\Box\alpha$	$\vdash \mathrm{Pr}(\ulcorner F \urcorner) \to \mathrm{Pr}(\ulcorner \mathrm{Pr}(\ulcorner F \urcorner) \urcorner)$
$\vdash_{\mathbf{GL}} \Box(\Box\alpha \to \alpha) \to \Box\alpha$	$\vdash \mathrm{Pr}(\ulcorner \mathrm{Pr}(\ulcorner F \urcorner) \to F \urcorner) \to \mathrm{Pr}(\ulcorner F \urcorner)$

Table 1.2: The properties of $\Box$ and the predicate $\mathrm{Pr}(\cdot)$

It is clear from this table that the predicate $\mathrm{Pr}(\cdot)$ and the $\Box$-operator of **GL** have a lot of the same properties in common. Solovay's completeness theorems show that the modal logic **GL** in some way axiomatizes the proof predicate of a wide range of different arithmetical systems. A somewhat fun fact is, that the first time the principle $\Box(\Box\alpha \to \alpha) \to \Box\alpha$ was used in modal logic, was in 1963 in a paper by Timothy John Smiley about the logic basis of ethic (Smiley 1963). Further the modal logic now known as **GL** was considered before the arithmetical interpretations of it was conjectured. Segerberg actually proved that it was completeness with respect to the conversely well-founded frames before he knew about its importance in arithmetic.

2 Recursion Theory

{chap:Recur}

We will begin this section by defining two classes of functions; the *Partial Recursive Functions* and the *Turing Computable Functions*. These two classes of functions give rise to the same class of functions. The idea behind these two classes of functions is to define what we intuitively mean with a computable function. The proofs in this section will be rather informal. The goal of this section will be to state and prove Kleene's recursion theorem, which will play a crucial role in our proof of Solovay's two completeness theorems.

The topic I have chosen to call *recursion theory* is today often known as *computability theory*. In his book (Soare 2016), Robert Soares has put forth, some arguments for why this named is better suited for the discipline than recursion theory.

This chapter will follow (Soare 1987), unless stated otherwise.

2.1 Partial Recursive Functions and Recursive Functions

The class of partial recursive functions is an enlargement of the primitive recursive functions. The class of primitive recursive functions captures a lot of the functions we intuitively see as computable. It does not contain any functions that we would say was incomputable.

But the primitive recursive functions do not include all intuitively computable functions. For example the following function, called the Ackermann function, which is clearly computable, is not in the class of primitive recursive functions:

$$\begin{aligned}
Ack(0, n) &= n + 1 \\
Ack(m + 1, 0) &= A(m, 1) \\
Ack(m + 1, n + 1) &= A(m, A(m + 1, n))
\end{aligned}$$

This function grows too fast to be a primitive recursive function, i.e we have for all primitive recursive functions $f(x)$ that for some y that $Ack(x, y) > f(x)$ for all $x \in \omega$. proof of this fact can be found in (Kleene 1952)

So we will need to expand our class of functions, if we want to *capture* all intuitively computable functions. We will expand them in the following way:

Definition 2.1 The class of *partial recursive* (from now on some times called (p.r) functions is the least class closed under schemata I through V from the definition of primitive recursive (definition 1.18) functions and the following VI schema.

VI. If $\theta(x_1, \ldots, x_n, y)$ is a partial recursive function of $n+1$ variables and

$$\begin{aligned}\psi(x_1, \ldots, x_n) = \mu y[\theta(x_1, \ldots, x_n, y) \downarrow = 0 \\ \wedge \forall z \leq y[\theta(x_1, \ldots, x_n, z) \downarrow]\end{aligned}$$

Then ψ is a partial recursive function of n variables.

A partial recursive function that is total (define on all of ω) is called a total recursive function; abbreviated to recursive function. ⊣

This is one way in which one can define what the computable functions are. In the next section we will present another definition of a type of functions, and it will be shown that these lead to the same class of functions.

We will end this section with the following definition:

Definition 2.2 A relation $R \subset \omega^n$ where $n \geq 1$ is recursive (primitive recursive) if its characteristic function χ_R is recursive (primitive recursive). The case where $n = 1$ is the case where R is a set $A \subset \omega$, so we also have the definition of a set being recursive. ⊣

2.2 Turing Computable Functions

Another way to describe the intuitively computable functions is via a Turing machine.

Definition 2.3 A *Turing machine* M consists of a two-way infinite tape that is divided into different cells and a finite set of internal states $Q = \{q_0, \ldots, g_n\}$, $n \geq 1$. Each cell is either blank: B or has value 1. The following three things can happen simultaneously in a single step:

1. Change from one state to another.

2. Change the scanned symbol s to another symbol $s' \in S = \{1, B\}$

3. Move the reading head one cell to the right R or the left L.

The operation of M is controlled by a partial map:

$$\delta : Q \times S \to Q \times S \times \{R, L\}$$

Which may not be defined for all arguments. $\dashv$

The situation can be seen in the following figure:

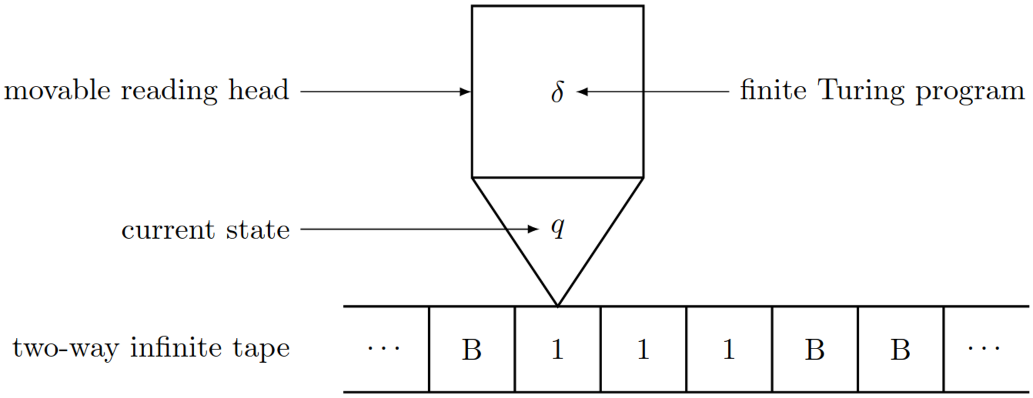


Figure 2.1: A Turing Machine[1]

The way to understand this definition is the following: if $(q, s, q', s', X) \in \delta$, it means that the machine M is in stage q where it scans symbol s then changes to state q' and replaces s by s'. Lastly it moves to the right if $X = R$ and the left if $X = L$. The map δ is called a Turing program if it can be viewed as a finite set of quintuples. If the input integer is x then it will be represented by a string of $x + 1$ consecutive $1's$, where all other cells are blank.

Further the machine M starts in the state q_1 by scanning the leftmost cell that contains a 1. The machine stops if it reaches the halting state q_0, and it will then output the number y, which is the total number of 1's on the tape in this state. If M with input x halts and outputs y we, say that M computes the partial function $\psi(x) = y$.

The conditions at M for each step of a Turing calculation is determined by the following:

1. The current state q_i.

[1]This picture is taken from (Soare 1987)

2. The symbol s_0 that is being scanned.
3. The symbols on the tape to the right of s_0 up to the last 1. Denote this sequence by $s_1, s_2, \dots s_n$
4. The symbols on the tape to the left of s_0 op to the first 1. Denote this sequence by $s_{-1}, s_{-2}, \dots s_{-m}$.

This is called the configuration of the machine and we can write it as follows:

$$s_{-m} \cdots s_{-1} q_0 s_0 s_1 \cdots c_n$$

Definition 2.4 A *Turing computation* according to the Turing program P with input x is a sequence of configurations $c_0, c_1, \dots, c_n$ such that c_0 represents the machine in the halting state q_0, and the transition $c_i \to c_{i+1}$ for all $i < n$ is given by the Turing program P. ⊣

These definitions makes it possible to list all the Turing programs, by giving them a Gödel number. This is because each Turing program is a finite set of quintuples, and thus we can effectively find its Gödel number on a list. We will now show how to give each Turing program a Gödel number:

Proposition 2.5 Each Turing program P_e can be assigned a Gödel number e.

Proof. We will use the fact that each $x \in \omega$ has a unique prime decomposition:

$$x = p_0^{x_0} \cdots p_n^{x_n} \cdots$$

We can assign a number to each quintuple $(q_{i,j}, q_k, s_l, r_m)$ in a Turing program P in the following way:

$$p_0^{1+i} p_1^{1+j} p_2^{1+k} p_3^{1+l} p_4^{1+m}$$

Where we have that $r_0 = R$ and $r_1 = L$.

Since the prime decomposition is unique, each different state of the program has a unique code. Each Turing is a sequence of different states and we can thus for an arbitrary Turing program P_e let $e_0, \dots e_n$ denote the Gödel number of each different state and set:

$$e = p_0^{e_0} \cdots p_n^{e_n}$$

Thus each Turing program P_e has a unique Gödel number e. ⊣

Since each Turing program has a unique code we can list them and be able to find any program P_e by its code e. This gives the following definition:

Definition 2.6 Let P_e be the Turing program with Gödel number e in the list and let $\varphi_e^{(n)}$ be the function of n variables computed by P_e. Further let φ_e abbreviate $\varphi_e^{(1)}$. ⊣

2.3 The *s-m-n*-Theorem

It can be proven that the two classes of functions; partial recursive and Turing computable functions give rise to the same class of partial functions. This can be seen as evidence for *Church's Thesis*, which states that this class of functions coincides with the function that we see as intuitively computable. In the rest of this project we will assume that Church's Thesis is true. There are some other definitions of computable functions that gives rise to exactly the same class of functions; a list of these can be found in (Cutland 1980)

We will begin by proving the padding lemma, which states that each partial function φ_x has an infinite amount of indices.

Lemma 2.7 (The Padding Lemma) Each partial recursive function φ_x has $\aleph_0$ indicies, and for each x we can *effectively* find an infinite set A_x of indices for the same partial function.

Proof. For any program P_x that has internal states: $\{q_0, \dots, q_n\}$ we can add extra instructions $q_{n+1}B\ R, q_{n+2}B\ R, \dots$ such that we get a new program for the same computation. $\dashv$

The following theorem will show that each Turing computable function is in fact partial recursive. The converse also holds, and the proof of this fact can be found in (Kleene 1952). The proof of that fact is left out since it is very tedious.

{thm:Normalform}

Theorem 2.8 (The Normal Form Theorem) There exists a predicate $T(e,x,y)$ and a function $U(y)$ that are primitive recursive such that:

$$\varphi_e(x) = U(\mu y T(e,x,y))$$

The proof will not be fully rigorous.

Proof. It can be shown that the predicate $T(e,x,y)$ exists and is primitive recursive, we will only do a bit of this work. This predicate informally states that y is the code of Turing program P_e with input x. For each possible configuration c, we can assign a code:

$$\ulcorner c \urcorner = 2^{1+i} \cdot 3^{1+\ulcorner s_0 \urcorner} \cdot 5^r \cdot 7^l$$

Where $\ulcorner s \urcorner = 0$ if $s = B$ and is equal to 1 otherwise, $r = \prod_{j\geq 1} p_j^{\ulcorner s_j \urcorner}$ and $l = \prod_{j\leq -1} p_j^{\ulcorner s_j \urcorner}$.

We can now define the code of a Turing computation $c_0, c_1, \dots c_n$ according to P_e to be:

$$y = 2^e \prod_{i\leq n} p_{i+1}^{\ulcorner s_i \urcorner}$$

From this it follows that $T(e,x,y)$ is computable in the intuitive sense.

Having defined the predicate T we can check if it holds. By proposition 2.1 we can "recover" the program P_e from e. Then we can recover the computation $c_0, c_1, \dots c_n$ from y, if y codes such a thing. We can now check if $c_0, c_1, \dots, c_n$ is a computation according to P_e with x as the input in the first configuration c_0. If this is true, then $U(y)$ just outputs the number of 1's in the final configuration c_n.

Further the encoding we have made makes it so that T and U are primitive recursive. This is shown in (Kleene 1952, p. 376). ⊣

This theorem also gives us that each partial recursive function can be created by two primitive recursive functions, with a single application of the μ-operator.

{thm:Emu}

Theorem 2.9 (Enumeration Theorem) There is a partial recursive function of 2 variables $\varphi_z^{(2)}(e,x)$ such that $\varphi_z^{(2)}(e,x) = \varphi_e(x)$.

Proof. By Theorem 2.8 we will define $\varphi_z^{(2)}(e,x) = U(\mu y T(e,x,y)) = \varphi_e(x)$ ⊣

We will need the following notation in the next proof:

Definition 2.10 Set $\langle x,y\rangle$ to be the image of (x,y) under the injective recursive pairing function:

$$\frac{1}{2}(x^2 + 2xy + y^2 + 3x + y)$$

This function is from $\omega \times \omega$ onto ω. ⊣

Theorem 2.11 (s-m-n theorem) For every $m, n \geq 1$ there exists an injective recursive function s_n^m of $m+1$ variable such that for all $x, y_1, \dots, y_m$

$$\varphi^{(n)}_{s_n^m(x,y_1,\dots,y_m)}(z_1, \dots z_n) = \varphi_x^{(m+n)}(y_1, \dots, y_m, z_1, \dots, z_n)$$

Proof. I will follow Soare and only prove the case where $m = n = 1$. I.e the case where we have to prove:

$$\varphi_{s_1^1(x,y)}(z) = [\varphi_x^2(y,z)]$$

Let x and y be given. Then $s_1^1(x,y)$ can be described as follows:

1. Let P_x be the Turing program with code x.
2. Change P_x into another Turing program $P_{x'}$ such that: $P_{x'}$ writes $y+1$ "1" left of the input, such that there is a B between these 1 and the other input. Further i places the head to the left of the new input and proceeds to *run* P_x.
3. outputs x'

it is clear that $P_{x'}$ on input z compute the same as p_e would on input (x, y); i.e $\varphi_{x'} = \varphi_x^{(2)}(y, z)$. Further we have that $x' = s_s^1(x, y)$. By Church's Thesis the function $s = s_1^1$ is recursive, since it can be computed effectively. If it is not injective it can be replaced by an injective recursive function s' such that $\varphi_{s(x,y)} = \varphi_{s'(x,y)}$ by using the padding lemma and by defining $s'(x, y)$ in increasing order of $\langle x, y\rangle$. ⊣

A full proof of this statement can be found in Kleene. The $s - m - n$ theorem plays a crucial role in both the proof and the use of the recursion theorem. The theorem is not the most intuitive to use, and takes a bit of work to get used to. Therefore we will use the $s - m - n$ theorem to prove the following proposition:

Proposition 2.12 There is a recursive function g of two variables such that for all x, y:

$$\varphi_{g(x,y)} = \varphi_x \varphi_y$$

Proof. By Church's Thesis it is clear that $\eta = \varphi_x \varphi_y$ is a partial recursive function since it is the product of two partial recursive functions.

To end the proof we must show that we can the find Gödel number for η in an uniform effective way from x and y as x and y vary. We will begin by defining:

$$\theta(x, y, z) = \varphi_x(\varphi_y(z)) = \varphi_{x_1}(x, \varphi_{x_1}(y, z))$$

Where φ_{x_1} is the function $\varphi_z^{(2)}$ from Theorem 2.9.

By the church thesis this function is partial recursive and has an index e. So by applying the $s - m - n$ Theorem we get:

$$\varphi_x \varphi_y(z) = \varphi_e(x, y, z) = \varphi_{s_1^2(e,x,y)}$$

And thus $s_1^2(e, x, y)$ is our g. ⊣

2.4 Recursively Enumerable sets and the Graph of a function

In this section we will introduce the two concepts *recursive enumerable* sets and the *graph* of a function. We will further show that there is a connection between these two concepts.

The idea behind a recursively enumerable set is that we can have an algorithm that can enumerate the members of the set.

Definition 2.13 A set A is *recursively enumerable* (r.e.) if A is the domain of some primitive recursive function. Further we define the following two sets:

1. We let the eth r.e set be denoted by:

$$E_e = \text{dom } (\varphi_e) = \{x : f(x) \downarrow\} = \{x : \exists y T(e, x, y)\}$$

2.

$$E_{e,s} = \text{dom}(\varphi_{e,s})$$

⊣

A set can be recursively enumerable without being recursive, which the following two propositions shows:

Proposition 2.14 Let $K = \{x : \varphi_x(x) \text{ converges}\} = \{x : x \in E_x\}$, then K is r.e.

Proof. We have that K is the domain of the following primitive recursive function:

$$\psi(x) = \begin{cases} x & \text{if } \varphi_x(x) \text{ converges} \\ \text{undefined} & \text{otherwise.} \end{cases}$$

This function is primitive recursive by Church's Thesis, since $\psi(x)$ can be computed by program P_x on input x, which outputs x only if $\varphi_x(x)$ converges. ⊣

Proposition 2.15 K is not recursive.

Proof. If K was recursive we would have that it had a recursive characteristic function K_χ, and thus the following would be recursive:

$$f(x) = \begin{cases} \varphi_x(x) + 1 & \text{if } x \in K \\ 0 & \text{if } x \notin K \end{cases}$$

But this f can not be recursive, since for all x we have $f \neq \varphi_x$. ⊣

So even though we have a algorithm that can enumerate all the members of the set K, we can not for a given x decide whether $x \in K$, so we can not solve for a given x that $\varphi_x(x)$ converges or not.

Next goal is to show that the definition of a r.e sets is equivalent to the definition that there is an algorithm that enumerates the members of it. We will further also show that the definition of a r.e set is equivalent to the set being Σ_1, which is a concepts that will play a bigger role later on in this project.

Definition 2.16 A set A is the *projection* of some relation $R \subseteq \omega \times \omega$ if $A = \{x : \exists y : R(x, y)\}$. We further say that a set A is in Σ_1 form, if A is the projection of some recursive relation $R \subseteq \omega \times \omega$. ⊣

We can now show the following theorem:

Theorem 2.17 (Normal Form Theorem for r.e sets) A set A is r.e iff A is Σ_1.

Proof. ($\Rightarrow$) Since A is r.e we have that $A = W_e = \mathrm{dom} f_e$ for some e. This means that:

$$x \in W_e \Leftrightarrow \exists s(x \in W_{e,s}) \Leftrightarrow \exists s(T(e,x,s))$$

Since the relation T is primitive recursive and we have that the set A is the projection a recursive relation.

($\Leftarrow$) Let $A = \{x : \exists y(Rx, y)\}$ where R is recursive. We then have that $A = \mathrm{dom} f$ where $f(x) = \mu y(R(x,y))$ and thus A is r.e $\dashv$

This theorem is equivalent to the normal form theorem for partial recursive functions. The next theorem shows a way to determine whether a given set is Σ_1.

{thm:RecSigma}

Theorem 2.18 (Qunatifier Contraction Theorem) If there is a recursive relation $R \subseteq \omega^{n+1}$ and if we have the following set:

$$A = \{x | \exists y_1 \ldots \exists y_n R(x, y_1, \ldots, y_n)\}$$

Then the set A is Σ_1.

Proof. We will start of by defining the relation $S \subseteq \omega^2$ as follows:

$$S(x,z) \Leftrightarrow R(x,(z)_1,\ldots,(z)_n)$$

Where we have the following prime decomposition of z:

$$z = p_1^{(z)_1} \cdots p_k^{(z)_k}$$

Then the following equivalences hold:

$$\begin{aligned}\exists z S(x,z) &\Leftrightarrow \exists z R(x,(z)_1,\ldots (z)_n)\\ &\Leftrightarrow \exists y_1 \cdots \exists y_n R(x, y_1, \ldots, y_n)\end{aligned}$$

And thus the set A is clearly Σ_1. $\dashv$

From this theorem, we can easily get the following corollary:

Corollary 2.19 The projection of an r.e relation is r.e.

The next definition will also play a role in our proof of Solovay's completeness theorems.

Definition 2.20 The graph of a (partial) function φ is the relation:

$$(x, y) \in \text{ graph}(\varphi) \Leftrightarrow f(x) = y$$

$\dashv$

The relation of a graph can also be seen as a function in the language of **PRA**; so we will often denote the graph of a function $\varphi(x) = y$ with the following notation: τxy, and say that $(x, y) \in \text{ graph}(\varphi)$ if and only if τxy is true. We will use this notation in chapter 6, since Smorinsky uses this notation, and we will follow his book (Smorynski 1985) in that chapter.

Theorem 2.21 (Uniformaization Theorem) If $R \subseteq \omega^2$ is an r.e relation, then there is a p.r function sel called the selector function for R such that:

$$\text{sel}(x) \text{ is defined } \Leftrightarrow \exists y(R(x, y))$$

and if this is the case we have that $(x, f(x)) \in R$

Proof. Since R is r.e it is Σ_1. This means that there is a recursive relation S such that $R(x, y)$ holds iff $\exists z(S(x, y, z))$. Thus we can define the following p.r function:

$$g(x) = \mu u(S(x, (u)_1, (u)_2))$$

And now we put $f(x) = (g(x))_1$ $\dashv$

It will be the following theorem we will use in our proof later on.

Theorem 2.22 (Graph Theorem) A partial function φ is partial recursive iff its graph is recursive enumerable.

Proof. ($\Rightarrow$) The graph of φ_e is r.e by theorem 2.18 and the definition of a graph.

($\Leftarrow$) Since the graph of φ is assumed to be r.e we can conclude that φ is its own primitive recursive selector function. This is that $R = \text{graph}\varphi$ can only have φ as its selector function. $\dashv$

We will end this section with the next theorem. It justifies the notion of a r.e set A as one where we can effectively enumerate its members; $A = \{a_0, a_1, a_2, \ldots\}$

Theorem 2.23 (Listning Theorem) A set A is r.e if and only if $A = \emptyset$ or A is in the range of a total recursive function f.

Proof. ($\Leftarrow$) If $A = \emptyset$ then A is clearly r.e. Now assume that $A = im(f)$, where f is a total recursive function. Then A is r.e by corollary 2.1

($\Rightarrow$) Let $A = E_e = \emptyset$. We will find the least integer $\langle a, t \rangle$ such that $a \in E_{e,t}$. We will now define the following recursive function f as:

$$f(\langle s, x \rangle) = \begin{cases} x & \text{if } x \in E_{e,s-1} \setminus E_{e,s} \\ a & \text{otherwise} \end{cases}$$

WE have that $A = im(f)$, since if $x \in E_e$, we can choose the least s such that $x \in E_{e,s+1}$, and thus $f(\langle s, x \rangle) = x$ and hence $x \in im(f)$ $\dashv$

2.5 The Recursion Theorem

In this section we will state and prove the recursion theorem. It will be crucial in chapter 6, since we will need it to define a function, which will be used to embed a Kripke model in **PRA**.

Theorem 2.24 (The Recursion Theorem) For every recursive function f there exists a fixed point n such that $\varphi_n = \varphi_{f(x)}$

Proof. We will start of be defining the following *diagonal* function $d(u)$ as:

$$\varphi_{d(u)}(z) = \begin{cases} \varphi_{\varphi_u(u)}(z) & \text{if } \varphi_u(u) \text{ converges} \\ \text{undefined} & \text{else} \end{cases} \tag{2.1}$$ {eq:du}

By the $s-m-n$ theorem we have that the function d is injective and total. Further it is clearly seen that d is independent of f.

Given an arbitrary f we will choose an index v such that:

$$\varphi_v = f \circ d \tag{2.2}$$ {eq:fd}

Now set $n = d(v)$. We will show that this is a fixed point for the function f. Since f is total we also have that $f \circ d$ is total. This means that $\varphi_v(v)$ converges and that $\varphi_{d(v)} = \varphi_{\varphi_v(v)}$. Thus we have:

$$\varphi_n = \varphi_{d(v)} = \varphi_{\varphi_v(v)} = \varphi_{f \circ d(v)} = \varphi_{f(n)}$$

The second equality sign follows from 2.1 and the third follows from 2.2. $\dashv$

Following (Owens 1973), the argument in the proof can be seen as a digitalization argument that fails. Commonly when we apply a digitalization argument, we have a class of sequences, with terms from a set A, that we arrange as the rows in a square matrix. We then have a map $h : A \to A$ that induces an operation h^* on the set of sequences such that if $\langle s(i), i \in I\rangle$ is a sequence in our matrix then

$$h^*(\langle s(i), i \in I\rangle) = \langle h(s(i)), i \in I\rangle$$

After having defined this map we will use it on the sequences that consist of the elements of the diagonal of the matrix and show that the resulting sequence is not one of the original sequences.

The digitalization argument "fails" in our case, since the sequences of the diagonal is already one of the rows and thus the image h^* of this sequences will also be one of the rows; i.e the h has a fixed point.

The start of the proof can be seen as the following lemma:

Lemma 2.25 There is a diaognal function $d(u)$ such that:

$$\varphi_{d(u)}(z) = \begin{cases} \varphi_{\varphi_u(u)}(z) & \text{if } \varphi_u(u) \text{ converges} \\ \text{undefined} & \text{else} \end{cases} \tag{2.3}$$

Most of the time where one uses the Recursion Theorem, one actually uses this lemma to construct the given function.

2.5.1 Application of the Recursion Theorem

The recursion theorem is a "powerful" tool. It enables us to define a partial recursive function, which uses its own index as part of its definition. The recursion theorem overrides this "self-reference", because we are using the $s-m-n$ theorem to define a function $f(x)$ and $\varphi_{f(x)}(z) = (\ldots, x \ldots)$ and then taking a fixed point: $\varphi_n = \varphi_{f(n)}$. When we are making constructions like this, the only thing we cannot do is use specific properties of the function φ_n. We will use the theorem in this way in our proof of Solovay's Completeness Theorems to define a function with the help of the function own Gödel number; and the recursion theorem makes this a viable tactic.

The following examples will show a few uses of this theorem.

Example 2.26 We will show that there is an n such that:

$$W_n = \{n\}$$

We start of by using the $s-m-n$ theorem to define $W_{f(x)} = \{x\}$, then by the recursion theorem we can choose n such that we have:

$$W_n = W_{f(n)} = \{n\}$$

$\dashv$

The next example will be an application of the Recursion Theorem that is in the same vein as the one we will use proving Solovay's completeness theorems.

Example 2.27 Let $\psi : \omega^2 \to \omega$ and $\theta : \omega^3 \to \omega$ be recursive functions and define the function $\varphi : \omega^2 \to \omega$ by:

$$\begin{aligned} \varphi(0, y) &= \psi(y) \\ \varphi(x+1, y) &= \theta(\varphi(x, y), x, y) \end{aligned}$$

We will now show that φ is recursive by using the recursion theorem.

Let $\tau_0 v_0 v_1$ be an arbitrary graph and let $\tau_1 v_0 v_1$ be the graph of ψ and $\zeta v_0 v_1 v_2$ be the graph of θ. We will now look at the following formula:

$$\Xi(\tau_0) : \ (v_0 = \overline{0} \wedge \tau_1 v_0 v_1) \vee (v_0 > \overline{0} \wedge \exists v(\tau_0(v_+ - 1, v) \wedge \zeta v v_0 v_1))$$

We can see $\ulcorner \Xi(\tau_0) \urcorner$ as a primitive recursive function of $\ulcorner \tau_0 \urcorner$. I.e we have:

$$\ulcorner \Xi(\tau_0) \urcorner = \eta(\ulcorner \tau_0 \urcorner)$$

We can now use the Recursion Theorem to chose an n such that we have: $\varphi^{(2)}_{\eta(n)} = \varphi^{(2)}_n$ and for $\varphi = \varphi^{(2)}_n$ we have:

$$\varphi(x, y) = z \leftrightarrow (x = 0 \wedge \psi(y) = z = \vee(x > 0 \wedge \theta(\varphi(x-1, y), x, y) = z)$$

I.e φ does exactly what we want it to do. We just need to define φ and this can be done by a Σ_1 induction. $\dashv$

This end our discussion about recursion theory. In the next chapter, we will generalize the notion of Σ_1 sets and in chapter 6 we will use the recursion theorem to define an important function.

3 The Arithmetical Hierarchy and Fragments of Arithmetic

{chap:PRA}

In this section we will generalize the class of σ_1 sets to the classes of σ_n, π_n and δ_n sets. We will use these sets in later chapters, since they make it possible for us to classify different arithmetical formulas. These definitions will make it possible for us to look at different fragments of arithmetic, since we can distinguish these fragments by which class of sets they allow induction on. We will start off by defining a "base" fragment called **Q** and then augment it with stronger inductions axioms. This means that some of these fragments contains the other fragments. With this knowledge it will be possible for us to place **PRA** in this hierarchy.

We will further look at how much induction we have in **PRA**; i.e which class of formulae from the arithmetical hierarchy we can perform induction on in **PRA**.

We will also introduce two other ways to augment the different fragments without the adding more induction. These will play a role in the generalization of Solovay's completeness theorems to other fragments than **PRA**.

Lastly we will prove a generalization of Löb's third derivability condition for **PRA**.

This chapter should be seen as an overview of the subject, and a lot of statements will be left unproven; since they will not play a major role in what is to come.

3.1 The Arithmetical Hierarchy

In this section we will introduce the so-called arithmetical hierarchy. Parts of it has already be defined; i.e the sets Σ_1. In the arithmetical hierarchy, we can classify sets with respect to their quantifier complexity in their syntactical definition.

In the next section concerning the fragments of arithmetics, we will use the arithmetical hierarchy as a tool to determine the amount of induction we will have in a given fragment.

The goal of this section is to introduce the arithmetical hierarchy and prove some results concerning it. Most of these results might not be used going forward.

Definition 3.1 We define the sets Σ_n and Π_n in the following way:

1. A set A is in Σ_0 (Π_0) if and only if A is recursive.

2. For $n \geq 1$ the set A is in Σ_n if there is a recursive relation $R(x, y_1, \ldots, y_n)$ such that:
$$x \in A \text{ iff } \exists y_1 \forall y_2 \exists y_3 \cdots Q y_n R(x, y_1, \ldots, y_n)$$
Here Q is $\exists$ if n is odd and Q is $\forall$ if n is even. We define A being in Π_n in a similar way. A is in Π_n if:
$$x \in A \text{ iff } \forall y_1 \exists y_2 \forall y_3 \cdots Q y_n R(x, y_1, \ldots, y_n)$$
3. A is in Δ_n if $A \in \Sigma_n \cap \Pi_n$

We further say that a formula F is Σ_n (Π_n) if it is Σ_n (Π_n) as a relation of the variables that are free in it. $\dashv$

In the rest of this project, we will mostly look at formulae that are either Σ_n or Π_n and not the sets of these classes. Furthermore we have that $\Sigma_0 = \Pi_0 = \Delta_0$, and a formula F that is Δ_0 is also called a bounded formula.

We can show a few properties of these sets.

Proposition 3.2 1. $A \in \Sigma_n \Leftrightarrow \overline{A} \in \Pi_n$

2. $A \in \Sigma_n(\Pi_n) \Rightarrow (\forall m > n)(A \in \Sigma_m \cap \Pi_m)$

3. $A, B \in \Sigma_n(\Pi_n) \Rightarrow A \cup B, A \cap B \in \Sigma_n(\Pi_n)$

4. $(R \in \Sigma_n \wedge n > 0 \wedge A = \{x : \exists y R(x, y)\}) \Rightarrow A \in \Sigma_n$

5. If $R \in \Sigma_n(\Pi_n)$ and A and B are defined by:
$$\langle x, y \rangle \in A \Leftrightarrow \forall z < y R(x, y, z)$$
and
$$\langle x, y \rangle \in B \Leftrightarrow \exists z < y R(x, y, z)$$
Then we have $A, B \in \Sigma_n(\Pi_n)$

Proof. 1. If we have that:
$$A = \{x : \exists y_1 \forall y_2 \cdots R(x, y_1, \ldots)\}$$
Then we have:
$$\overline{A} = \{x : \forall y_1 \exists y_2 \cdots \neg R(x, y_1, \ldots)\}$$
Which is clearly Π_n.

2. If for example $A = \{x : \exists y_1 \forall y_2 R(x, y_1, y_2)\}$, then we can make the following reformulation of A:

$$A = \{x : \exists y_1 \forall y_2 \exists y_3 (Rx, y_1, y_2) \wedge y_3 = y_3)\}$$

   This kind of reformulation can be done for any set in Σ_n (Π_n)

3. Let the following two sets be defined:

$$A = \{x : \exists y_1 \forall y_2 \cdots R(x, y_1, y_2, \ldots)\}$$

$$B = \{x : \exists z_1 \forall z_2 \cdots S(x, z_1, z_2, \ldots)\}$$

   Then we have:

$$\begin{aligned} x \in A \cup B &\Leftrightarrow \exists y_1 \forall y_2 \cdots R(x, y_1, y_2, \ldots) \vee \exists z_1 \forall y_2 \cdots S(x, z_1, z_2 \ldots) \\ &\Leftrightarrow \exists y_1 \exists z_1 \forall y_2 \forall z_2 \cdots (R(x, y_1, y_2, \ldots) \vee S(x, z_1, z_2, \ldots)) \\ &\Leftrightarrow \exists u_1 \forall u_2 \cdots (R, (u_1)_0, (u_2)_0, \ldots) \vee S(x, (u_1)_1, (u_2)_1, \ldots)) \end{aligned}$$

   Which is clearly Σ_n. The same argument can be made for $A \cap B$ and for Π_n sets.

4. This follows by quantifier contraction, in the same way as (3)

5. We will prove this by induction on n.

   Base case: Let $n = 0$. Then A and B are clearly recursive.

   Induction step: Now assume that $n > 0$ and suppose that $R \in \Sigma_n$. Our induction hypothesis says that (6) is true for all $m < n$. Then by (4) we have that $B \in \Sigma_n$. Further we have $S \in \Pi_{n+1}$ such that the following holds:

$$\begin{aligned} \langle x, y \rangle \in A &\Leftrightarrow (\forall z < y) R(x, y, z) \\ &\Leftrightarrow (\forall z < y) \exists u S(x, y, z, u) \\ &\Leftrightarrow \exists \sigma (\forall z < y) S(x, y, z, \sigma(z)) \end{aligned}$$

   We have that σ range is in $\omega^{<\omega}$. By the induction hypothesis we have that $(\forall z < y) S \Pi_{n+1}$ but by the above deduction we must then have that $A \in \Sigma_n$. $\dashv$

3.2 Fragments of arithmetic

In this section we will use the previous section to look at different fragments of arithmetic. These can be seen as different sub-theories of *Peano Arithemtics*.

These different fragments are important, since a natural question to ask is; "which axioms of arithmetic do we need for proving Gödel's incompleteness theorems and Solovay's completeness theorems for the proof predicate of the given theory?" We will comment on the bit about Solovay's completeness theorem going forward.

We will split the different fragments up in two categories:[1]

Strong fragments: The fragments that contain some induction axiom.

Weak fragments: The fragments which do not contain any induction axioms.

We will start of by defining a very weak fragment called Robinson's theory. This fragment was first considered in (Robinson 1950). We will denote this theory with **Q**. This theory has the following axioms:

$$\begin{aligned}
&\forall x(\neg Sx \neq 0)\\
&\forall x\forall y(Sx = Sy \to x = y)\\
&\forall x(x \neq 0 \to \exists y(Sy = x)\\
&\forall x(x + 0 = x)\\
&\forall x\forall y(x + Sy = S(x + y)\\
&\forall x(x \cdot 0 = 0)\\
&\forall(x \cdot Sy = x \cdot y + x)
\end{aligned}$$

This theory dose not have the inequality symbol. We will extend **Q** with the following axiom:

$$x \leq y \leftrightarrow \exists z(x + z = y)$$

This extension of **Q** is denoted by $\mathbf{Q}_{\leq}$. Both **Q** and $\mathbf{Q}_{\leq}$ are very weak fragments since they do not contain any induction schemas.

Definition 3.3 Giving a class Γ of either Σ_n or Π_n formulae we define Γ-*induction* (Γ-*IND*) to be the following schema:

$$\varphi(0) \wedge \forall v(\varphi(x) \to \varphi(Sx)) \to \forall v\varphi(v)$$

for $\varphi \in \Gamma$. Further we define Γ-*Least Number Principle* (Γ-*LNP*) to be the following schema:

$$\exists x\varphi(x) \to \exists(\varphi(x) \wedge \neg\exists y(y < x \wedge \varphi(y)))$$

For $\varphi \in \Gamma$. Lastly we define the replacement axioms for Γ, (Γ-REPL) as the following formulas:

$$(\forall x \leq t)\exists y\varphi(x, y) \to \exists z(\forall x \leq t)(\exists y \leq z)\varphi(x, y)$$

[1] These definitions are not canonocal. Buss splits them up in three: strong fragments, weak fragments and very weak fragments. But for the scope of this project, we will only need two categories.

⊣

From the above axioms we can create a hierarchy of different strong fragments of arithmetics. We will define the following theories:

Definition 3.4 We define the following strong fragments:

1. The theory **EA** is the theory axiomatized by the axioms of $\mathbf{Q}_{\leq}$ and the induction over bounded formulas $F(x, \vec{a})$.
2. The theory $I\Sigma_n$ $[I\Pi_n]$ is the theory that is axiomatized by the axioms of $Q_{\leq}$ and the Σ_n $[\Pi_n]$-IND axioms.
3. The theory $I\Delta_0$ is $Q_{\leq}$ plus the Δ_0-IND axioms.
4. The theory $L\Sigma_n$ is defined by the theory $I\Delta_0$ plus the Σ_n-LNP axioms.
5. The theory $B\Sigma_n$ is defined by the theory $I\Delta_0$ plus the Σ_n-REPL axioms.
6. The theory $I\Sigma_n^R$ is defined as the closure of $\mathbf{Q}_{\leq}$ under the Σ_n induction rule:
$$\frac{F(0),\ \forall x(F(x) \to \varphi(x+1))}{\forall x F(x)}$$
7. The theory $I\Sigma_n^-$ $[\Pi_n^-]$ is the theory axiomatized by the axioms of $\mathbf{Q}_{\leq}$ and the schema of induction of Σ_n $[\Pi_n]$ functions $f(x)$, which only has x as a free variable.
8. The theory Peano arithmetics is defined as the theory $\mathbf{Q}_{\leq}$ plus induction for all first order formulae.

⊣

Going forward the most important of these theories is $I\delta_0$, since we will later augment and for this agumention it can be shown that Solovay's completeness theorems holds. It can be shown that in $\mathbf{Q}Q$ a lot of the basic facts about arithmetic can be shown, and these facts holds in all the exetions of **Q**. These facts will not be shown here, but a list of them can be found in (Buss 1998b).

3.3 PRA's and the other fragments of Arithmetics

Having introduced the arithmetical hierarchy in the previous section, it is not obvious where to place **PRA** in this hierarchy. We know that **PRA** has Σ_1 induction by axiom 1.18.2.c, so it is natural to ask whether **PRA** has induction on other sets. But the following theorem can be shown.

Proposition 3.5 **PRA** is the equivalent to the theory $I\Sigma_1^R$

The proof of this is non-trivial and would go much beyond the scope of this project. The statement will not be used going forward, and it is just included to give some intuition concerning the placement of **PRA** in the arithmetical hierarchy. The proof can be found in (S. N. Artemov and Beklemishev 2005). This makes it possible to place **PRA** in the arithmetical hierarchy. We can make a visualization of how all the different fragments relate to each other:

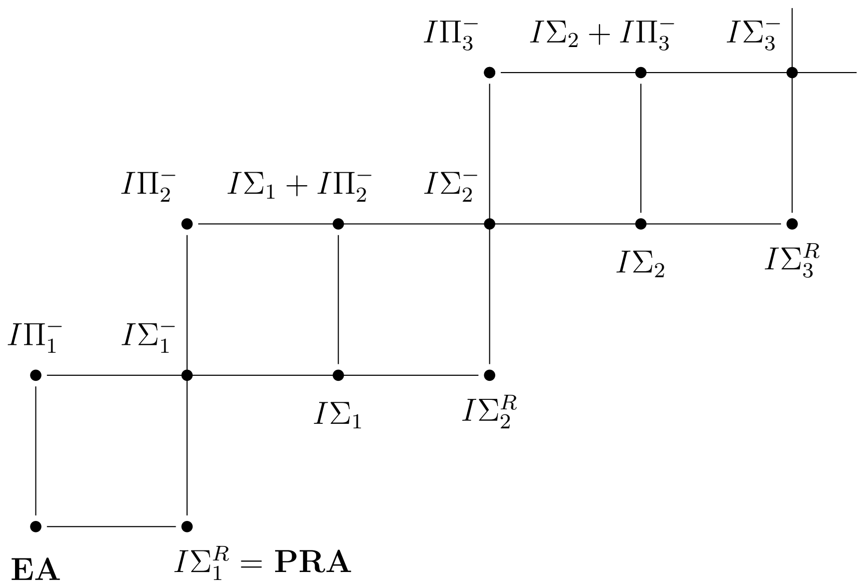


Figure 3.1: How the fragments relate to each other.

The figure shows how the other fragments relate to each other, this will not be shown.

We will now turn to another version of the Selection Theorem.

{thm:sel}

Theorem 3.6 Let $\tau v_0 \dots v_{n-1} v_n$ be Σ_1. There is then a Σ_1-formula $\mathrm{Sel}(\tau)$ with exactly the same free variables such that:

1. $\mathrm{Sel}(\tau) v_0 \dots v_n \to \tau v_0 \dots v_n$
2. $\mathrm{Sel}(\tau) v_0 \dots v_{n-1} v_n \wedge \mathrm{Sel}(\tau) v_0 \dots v_{n-1} v^* \to v_n = v^*$
3. $\exists v_n \tau v_0 \dots v_{n-1} v_n \to \exists v_n \mathrm{Sel}(\tau v_0 \dots v_{n-1} v_n$

Further this can be proven in **PRA**.

Proof. Since τ is Σ_1 it is recursively enumerable. So we have that:

$$\tau v_0 \dots v_n : \ \exists v(f v v_0 \dots v_n = \overline{0})$$

We will want to set $\mathrm{Sel}(\tau)$ to be the function that chooses the least v_n:

$$\exists v(f v v_0 \dots v_n = \overline{0}) \land \forall v_{n+1} \leq v_n \neg \exists v(f v v_0 \dots v_{n-1} v_{n+1} = \overline{0})$$

This formula is not Σ_1.

We can get a Σ_1 formula, if we minimise the pair (v, v_n). For this end we will first define τ^*:

$$\tau^* v v_0 \dots v_{n-1} : \ f((v)_0, v_0, \dots v_{n-1}, (v)_1 = \overline{0}$$

We can then minimise v in τ^*:

$$\tau^{**} v v_0 \dots v_{n-1} : \ \tau^* v v_0 \dots v_{n-1} \land \forall v^* \leq v \neg \tau^* v^* v_0 \dots v_{n-1}$$

We can then define $\mathrm{Sel}(\tau)$ by τ^{**} in the following way:

$$\mathrm{Sel}(\tau) v_0 \dots v_{n-1} v_n : \ \exists v(\tau^{**} v v_0 \dots v_{n-1} \land (v)_1 = v_n)$$

$\mathrm{Sel}(\tau)$ is then Σ_1. The next goal is the show that it ratifies 1-3. The least number principle gives us that there exists a unique least $v = ((v)_0, v_n)$ that satisfies τ^*, for any given $v_0, \dots, v_{n-1}$.

Further this can be done with the amount of induction of **PRA**. The least number principle applied to ζv is the same as the strong form of induction applied to $\neg\zeta$:

$$\forall v(\forall v^* < v \neg \zeta v^* \to \neg \zeta v) \to v \neg \zeta v$$

And this principle follows form ordinary induction applied to $\forall v^* < v \neg \zeta v^*$:

$$\forall v^* < \overline{0} \neg \zeta v^* \land \forall v(\forall v^* < v \neg \zeta v^* \to \forall v^* < v + 1 \neg \zeta v^*) \to \forall v \forall v^* < v \neg \zeta v^*$$

Thus for a p.r relation ζ we have that $\forall v^* < v \neg \zeta v^*$ is also p.r, and thus since **PRA** has Σ_1-induction we have the least number principle for ζ. ⊣

3.3.1 Induction in PRA

We know that we can de induction on Σ_1 formulae in **PRA**. A natural question to ask is then what other kinds of formulae can we do induction on in **PRA**? We will define $\mathbf{PRA}^-$ as the sub-theory of **PRA**obtained by restricting induction PR-formulae. The following proposition will give an answer to this question:

{prop:indu}

Proposition 3.7 Over $\mathbf{PRA}^-$ the following schemata are equivalent:

1. Σ_n-*Ind*
2. Π_n-*Ind*
3. Σ_n-*LNP*
4. Π_n-*LNP*

It shall be noted that we will only use the case of $n = 1$ going forward.

Proof. The implications (1) $\Rightarrow$ (4) and (2) $\Rightarrow$ (3) was proven in proof of theorem 3.6. The converse of these are done in the same way.

We will now show that (1) $\Rightarrow$ (2). The (2) $\Rightarrow$ (1) is similar. We will prove the case where $n = 1$, and the cases where $n > 1$ are identical, *modulo* the closure of Σ_n under bounded quantification.

So assume Σ_1-IND and suppose for $Fv \in \Sigma_1$ that the following instance of Π_1-IND fails:

$$(\neg F(\overline{0}) \wedge \forall v(\neg F(v) \to \neg F(Sv))) \to \forall v \neg F(v)$$

This means that we have $\neg F(\overline{0})$, $\forall v(\neg F(v) \to \neg F(Sv)$ and $\exists v F(v)$. We chose v_0 such that $F(v_0)$. We will use Σ_1 induction on the variable v in $F(v_0 \dot{-} v)$ to prove that $F(\overline{0})$ and get a contradiction.

Base step: It is clear that $F(v_0 \dot{-} \overline{0})$, since this is just $F(v_0)$.

Induction step: Assume that $F(v_0 \dot{-} v)$ is true. We have that $S(v_0 \dot{-} S(v)) = v_0 \dot{-} v$ unless we already have that $v = v_0$, in which case we have that $v_0 \dot{-} S(v) = v_0 - v$. So we can conclude that $\forall v F(v_0 \dot{-} v)$ and thus we have $F(\overline{0})$ and get our contradiction.

The converse of i.e. (2) $\Rightarrow$ (1) is done in a similar way. ⊣

This means that **PRA** can do induction on Π_1 formulas, since it has induction for Σ_1 induction. It also tells us that **PRA** has the least number principle for Σ_1 and Π_1 formulas. For **PRA** the following theorem can be proven, though the proof will not be given here. But we will use the theorem.

Theorem 3.8 **PRA** $\vdash$ $\mathrm{Bool}(\Sigma_1) - \mathit{Ind}$ where $\mathrm{Bool}(\Sigma_1)$ is the class of combinations of Σ_1 formulae.

We will use these results in chapter 6, since we will need to do induction on a few complicated formulae inside of **PRA**.

3.4 Further extensions of the arithmetical hierarchy

If we have that $I\Gamma$ is a fragment of Peano Arithmetics, then we can look at the fragment $I\Gamma + \text{EXP}$ which proves induction over Γ-formulas and proves that for all x the power 2^x exists. We can also look at $I\Gamma + \Omega_1$ which is a weaker theory than $I\Gamma + \text{EXP}$. Here Ω_1 is an axiom that asserts that for all x, its power $x^{\log(x)}$ exists. It is also clear that since $\mathbf{PRA} = I\Sigma_1^R$ the two fragments $I\sigma_1 + \text{EXO}$ and $I\sigma_1 + \Omega_1$ are weaker than $\mathbf{PRA}$. We will return to these two fragments later on in chapter 6.

It should here be stated that if look at theories T such that $\mathbf{EA} \subseteq T$, then it will be possible to encode the syntax of that theory in a similar way to what we have done with $\mathbf{PRA}$; i.e in a way such that the proof predicate of that theory $\text{PR}_T(x)$ is a Σ_1 formula. We will call such a theory for a *RE*-theory. We can then derive all the incompleteness results that we have obtained for $\mathbf{PRA}$ in that theory. Sometimes a little *tweaking* of the encode should be made, but we can get the following result that will not be proven here:

Theorem 3.9 Let T be a *RE*-theory such that $\mathbf{PRA} \subseteq T$. Then the following holds:

1. For any sentences F and G we get Löbs derivability conditions.
2. Gödel's incompleteness theorems for any sentence such that $\mathbf{PRA} \vdash F \leftrightarrow \neg\text{Pr}_T(\ulcorner F \urcorner)$.
3. Löb's theorem for any sentence F.

This shows that the provability predicate of such fragments T behaves in the same way as the one from $\mathbf{PRA}$.

3.5 Sigma Completeness

We can make a generalization of $D3$. We use this generalization in some of our proofs later on. We will first need the following lemma which will not be proven:

Lemma 3.10 Let $Fv_0 \dots v_{n-1}$ be a Σ_1. Then there is a recursively enumerable formula such that

$$\mathbf{PRA} \vdash Fv_0 \dots v_{-n1} \leftrightarrow \exists v(fvv_0 \dots v_{n-1} = \overline{0})$$

Theorem 3.11 (Demonstrable Σ_1 completeness) Let $Fv_0 \dots v_{n-1}$ be a Σ_1 formula with free variables. Then: {thm:DemoSiga}

$$\mathbf{PRA} \vdash Fv_0 \dots v_{n-1} \to \text{Pr}(\ulcorner f\dot{v}_0 \dots \dot{v}_{n-1} \urcorner)$$

This theorem states that if a Σ_1 formula F is true, then it can be proven to be true in **PRA** i.e **PRA** is complete with respect to Σ_1 formulae.

Proof. By the lemma we have that there is a Σ_1 formula $\exists v(gvv_0 \dots v_{n-1} = \overline{0}$ such that we have:

{eq:Com1}
$$\mathbf{PRA} \vdash Fv_0 \dots v_{n-1} \leftrightarrow \exists v(fvv_0 \dots v_{n-1} = \overline{0}) \tag{3.1}$$

and by $D1$ we have:

{eq:Com2}
$$\mathbf{PRA} \vdash \mathrm{Pr}(\ulcorner F\dot{v}_0 \dots \dot{v}_{n-1} \leftrightarrow \exists v(f\dot{v}\dot{v}_0 \dots \dot{v}_{n-1} = \overline{0})\urcorner) \tag{3.2}$$

We can now make the following deductions:

$$\begin{aligned}
\mathbf{PRA} \vdash fv_0 \dots v_{n-1} &\to \exists v(fvv_0 \dots v_{n-1} = \overline{0}) && \text{By 3.1} \\
&\to \exists v \mathrm{Pr}(\ulcorner f\dot{v}\dot{v}_0 \dots \dot{v}_{n-1} = \overline{0}\urcorner && \text{1.31} \\
&\to \mathrm{Pr}(\ulcorner \exists v(f\dot{v}\dot{v}_0 \dots \dot{v}_{n-1} = \overline{0})\urcorner) && \text{By D1 and D2} \\
&\to \mathrm{Pr}(\ulcorner F\dot{v}_0 \dots \dot{v}_{n-1}\urcorner) && \text{By 3.2}
\end{aligned}$$

$\dashv$

This theorem gives a difference between Σ_1 and Π_1 sentences in **PRA**. If F is Π_1 we can have that both $F + \mathrm{Con}(\mathbf{PRA} + F)$ and $F + \mathrm{Con}(\mathbf{PRA} + \neg F)$ are consistent, but if F is Σ_1 we get that $F + \mathrm{Con}(\mathbf{PRA} + \neg F)$ is inconsistent.

In the next two chapter we will turn to prove some results about the modal logic **GL**. The next results in chapter 4 will be important for the proof of Solovay's completeness theorems, while the results in chapter 5 will important for using Solovay's completeness theorems to gain results about formulae of arithmetic. This means that the results from chapter 2 and 3 will first be used in chapter 6, where they will be crucial in the proof of Solovay's theorems, but they do not play any role for the "pure" modal logic side of things.

4 General Results on GL

{chap:GL}

In this section we will prove some different properties about the modal logic **GL**, that was introduced in Chapter 1. These properties will be used in the following chapters. Some of these properties might not hold in other modal logics, but we will look at **GL** as our base logic, instead of a more common modal logic like **K**. Further, in the end we will introduce the system **GLS** (the "**S**" stands for Solovay).

This section will follow (Smorynski 1985), but there will be a some small differences. Smorynski calls the logic **GL** for **PRL** which stands for *Pr*ovability *L*ogic, and he denotes the logic we have called **GLS** by $\mathbf{PRL}^{\omega}$.[1]

We start of by proving the finite tree theorem for **GL**. This theorem makes it possible for us to assume that for a Kripke model $\mathcal{K} = \langle W, R, \phi \rangle$ of **GL**, that the set W is finite. For proving this theorem we will first need the need some knowledge about trees and prove König's lemma.

After this we will prove the continuity theorem which we will use a lot in chapter 5, for the proof of the fixed point theorem.

We will end this chapter by defining the logic **GLS** and show some few results about this logic.

This chapter (and the following one) does not use the preceding sections about recursive theory and the arithmetical hierarchy. We will only focus on modal logic and not anything that has to do with arithmetic. In chapter 6 we will combine all three parts; the recursion theory, the arithmetic and the modal logic.

4.1 Trees and GL

It is known that **GL** is weakly complete with respect to conversely well-founded transitive frames. There is another result that is in the same vein; **GL** is complete with respect to finite trees. The goal of this section is to prove this result. We will first start out by defining the notion of a tree and a few results about these.

4.1.1 Trees

In this subsection the notion of a special type of graphs called trees will be introduced. The goal of this section is to prove König's lemma about trees. We will

[1]Smorinsky also has a slightly different definition of a Kripke model.

start of by defining the notion of a tree.

Definition 4.1 A *tree* is a tuple $\mathcal{T} = \langle W, <, w_0 \rangle$ where $(W, <)$ where:

1. $<$ is transitive and asymmetric.
2. w_0 is the minimal element of $<$. I.e $w_0 < w$ for all $w \in W$.
3. The set of predecessors of any element is finite and linearly ordered by $<$.

A tree is *infinite* if the set W is infinite. $\dashv$

It is clear that trees can be seen as a special form of frames.

We will state some immediate definitions that should be known from the course *Diskret matematik*:

Definition 4.2 The *nodes* of a tree $\mathcal{T} = \langle W, R, w_0 \rangle$ are the elements of the set W.

If $w, v \in W$ are nodes and wRv then we say that they are joined by an *edge*.

A *walk* is an altering series of vertices and edges in which for each v we have that wRv for the w immediately before it . We call a walk for a *trail*, if all the edges of the walk are distinct. A *path*, is trail in which all the nodes are different. $\dashv$

It is known from the course *Diskret matematik* that between any two vertices there is exactly one path in a tree. As the concept of a tree is assumed to be known, we will not look at any concrete examples. We will need some further definitions to state and prove König's lemma:

Definition 4.3 Let $w \in W$. The *degree* of of w in $\mathcal{T}$ is the number of edges incident to it. $\dashv$

Definition 4.4 Let w be a node of a tree $\mathcal{T}$, we then define the map $\pi : \mathcal{T} \backslash \{w_0\} \to \mathcal{T}$ in the following way:

$$\pi(w) = \text{The node adjacent to } w \text{ on the path to } w_0$$

We call $\pi(w)$ the *parent node* of w.

The *child nodes* of w are the elements of the set $\{v\mathcal{T} : \pi(v) = w\}$, i.e the child nodes of w are all the nodes of $\mathcal{T}$ to which w is the parent. If w has no child nodes it is called a *leaf node*. $\dashv$

It is clear that if w is a leaf node, then the degree of w is 1.

Definition 4.5 A subset Γ of a tree $\mathcal{T}$ is called a *branch* if and only if all the following conditions hold:

1. $w_0 \in \Gamma$.

2. The parent node of each $w \in \Gamma \setminus \{w_0\}$ is in Γ.

3. Each node in Γ is either a leaf node in $\mathcal{T}$ or has exactly one child node in Γ.

A branch Γ is called *infinite* if and only if it has no leaf node at the end. ⊣

Definition 4.6 A *fork* of a $\mathcal{T}$ is a node of $\mathcal{T}$ which is the end point of two or more branches. ⊣

Definition 4.7 A tree $\mathcal{T}$ is called a *finitely branching tree* if every node of $\mathcal{T}$ has finitely many child nodes. ⊣

The proof of König's lemma will depend on the following axiom:

Axiom 4.8 (Axiom of Dependent Choice) Let R be a relation on a set W and suppose that:

$$\forall w \in W \exists v \in W : wRv$$

Then there exists a sequence $(w_n)_{n\in\omega} \in W$ such that

$$\forall n \in \omega : w_n R w_{n+1}$$

This axiom is a weak form of the axiom of choice. So it there might be some controversies about the use of it. These will not be commented on here.

In the proof of König's, lemma we will look at the subset of all nodes with infinitely many descendants and the relation R where we have that for nodes $w, v \in W$: wRv if and only if v is a child of w. This relation and set fulfills the conditions of the axiom and we can thus create the sequence $(w_n)_{n\in\omega}$.

We can now state König's lemma:

{lem:kong}

Lemma 4.9 (König's lemma) Let $\mathcal{T}$ be a finitely branching tree. Then it is infinite if and only if has an infinite path.

Proof. ($\Leftarrow$) If $\mathcal{T}$ has an infinite path, then it is trivially true that $\mathcal{T}$ is infinite.

($\Rightarrow$) Assume that $\mathcal{T}$ is infinite. To show that $\mathcal{T}$ has an infinite path is the same as showing that it has an infinite branch. We will show that there is a sequence of nodes $w = (w_0, w_1, w_2, \ldots)$ in $\mathcal{T}$ such that the following holds:

1. w_0 is the root node.

2. w_{n+1} is a child node of w_n.

3. each w_n has infinitely many descendants i.e. that the set $\{v \in W : w_n R v\}$ is a infinite set.

Then w is a branch of infinite length, and thus $\mathcal{T}$ has an infinite path.

We start with the root node w_0. It has a finite number of child nodes. Suppose for contradiction that each of these child nodes had a finite number of descendants, but this would mean that w_0 would have a finite number of descendants, and thus that $\mathcal{T}$ would be finite. Therefore w_0 has a child node with infinitely many descendants; let w_1 be one of those.

Now suppose that node w_k has infinitely many descendants. By the same argument as before, we get that w_k has at least one child node with infinitely many descendants. Let w_{k+1} be one of these. We have thus shown how the sequence w can be constructed, and the lemma follows by the axiom of dependent choice. $\dashv$

It is clear that finite trees are conversely well-founded frames. This fact is crucial in the proof of the theorem in the next subsection, which can be seen as strengthening the weak completeness theorem of chapter 1.

4.1.2 The Finite Tree Theorem

The following theorem is a strengthening of the weak completeness theorem for **GL**, since trees are a subset of the transitive conversely well-founded models . Due to this theorem we get that we can without loss of generality assume that our model is finite. This last feature will be crucial in the proof of main theorems of the next chapter.

Theorem 4.10 (The Finite Tree Theorem) Let α be a modal formula. Then the following are equivalent:

1. $\vdash_{\mathbf{GL}} \alpha$.

2. α is true in all models on finite trees.

3. α is valid in all models on finite trees.

With this theorem, it is possible to only consider finite frames. This will make the proof of our main theorem of chapter 6 possible. We will call the class of finite trees for FT, and call a formula valid in this class of models for FT-valid.

Proof. The implications (1) $\Rightarrow$ (2) and (1) $\Rightarrow$ (3) follow by the completeness theorem 1.16. We also have that (2) $\Leftrightarrow$ (3) is true since (3) $\Rightarrow$ (2) is trivial and (2) $\Rightarrow$ (3) follows since finite trees are transitive.. Thus we will just have to show (2) $\Rightarrow$ (1)

We will show this by contraposition, i.e $\neg(1) \Rightarrow \neg(2)$. Assume that $\nvdash_{\mathbf{GL}} \alpha$ and let $\mathcal{K}$ be the following model $\mathcal{K} = \langle W, R, w_0, \phi \rangle$ which we assume to be a counter model i.e $\nVdash^{K}_{w_0} \alpha$. We know that such a counter-model exists by the completeness theorem for **GL**. Let S be the set of subformulae of α The goal is now to define a finite tree model: $\mathcal{K}_{\mathcal{T}} = \langle W_T, <_{\mathcal{T}}, \phi_{\mathcal{T}} \rangle$. We will do this be letting W_T consist of finite R-increasing sequences from K.

Stage 0: Let the sequence (w_0) be a part of $K_{\mathcal{T}}$.

Stage $n+1$**:** For each sequence $(w_0, \ldots w_n) \in W_{\mathcal{T}}$ we will look at $\Gamma = \{\Box\beta \in S(\alpha) : \ w_n \in \phi(\Box\beta)\}$. If $\Gamma = \emptyset$ then we do not extend the sequence $(w_0, \ldots w_n)$. Otherwise we will for each $\Box\beta \in \Gamma$ choose a node $v \in W$ such that $w_0 R v$, and such that we have:

$$v \in \phi(\Box\beta),\ v \notin \phi(\beta)$$

We can do this because of axiom **L**. We will then add the sequence $(w_0, \ldots w_n, v)$ to the set $W_{\mathcal{T}}$.

The model $\mathcal{K}_{\mathcal{T}}$ then further consists of:

1. The relation $<_{\mathcal{T}}$ which is the usual strict ordering by extension of finite sequences.

2. The world w_0 which is the root node.

3. The valuation$\phi_{\mathcal{T}}$ that is the defined in the following way:

$$(w_0, \ldots, w_n) \in \phi_{\mathcal{T}}(p) \Leftrightarrow w_n \in \phi(p)$$

This leads to the following notation that we will use for the rest of the proof:

$$\vDash^{\mathcal{K}_{\mathcal{T}}}_{(w_0,\ldots,w_n)} p \Leftrightarrow \vDash^{\mathcal{K}}_{w_n} p$$

We will now prove two claims, by which the theorem will follow:

Claim 1: $\mathcal{T} = (W_{\mathcal{T}}, <_{\mathcal{T}}, w_0)$ is a finite tree with origin (w_0) Finiteness follows from Lemma 4.9, since the tree $\mathcal{T}$ is finitely branching as the branches correlate with the elements of S. Further there is no infinite paths in $\mathcal{T}$, since when we go from $(w_0, \ldots w_n)$ to $(w_0, \ldots, w_n, w_{n+1})$ one sentence from $\Box\beta \in S$ gets forced by w_{n+1} and since these are finite, the process will stop at some point, and thus the path will be finite.

Claim 2: For all $\beta \in S(\alpha)$ and for all $(w_0, \ldots w_n) \in W_{\mathcal{T}}$ we have:

$$\vDash^{\mathcal{K}_T}_{(w_0,\ldots,w_n)} \beta \Leftrightarrow \vDash^{\mathcal{K}}_{w_n} \beta$$

This proof is done by induction on the complexity of β. We will only look at the case $\beta = \Box\gamma$. So, by the induction hypothesis we have:

$$\begin{aligned}\vDash^{\mathcal{K}}_{w_0} \Box\gamma &\Rightarrow \forall v(w_0Rv \Rightarrow \vDash^{\mathcal{K}}_{v} \gamma)\\ &\Rightarrow \forall v((w_0,\dots w_n,v) \in W_{\mathcal{T}} \Rightarrow \vDash^{\mathcal{K}}_{v} \gamma)\\ &\Rightarrow \forall v((w_0,\dots w_n,v) \in W_{\mathcal{T}} \Rightarrow \vDash^{\mathcal{K}_{\mathcal{T}}}_{(w_0,\dots w_n,v)} \gamma)\end{aligned}$$

And the last line is the same as $\vDash^{\mathcal{K}_{\mathcal{T}}}_{(w_0,\dots,w_n)} \Box\gamma$. For the other way, we will use contraposition:

$$\begin{aligned}\nvDash^{\mathcal{K}}_{w_0} \Box\gamma &\Rightarrow \exists v(w_0Rv \;\&\; \nvDash^{\mathcal{K}}_{v} \gamma)\\ &\Rightarrow \exists v((w_0,\dots w_n,v) \in W_{\mathcal{T}} \;\&\; \nvDash^{\mathcal{K}}_{v} \gamma)\\ &\Rightarrow \exists v((w_0,\dots w_n,v) \in W_{\mathcal{T}} \;\&\; \nvDash^{\mathcal{K}_{\mathcal{T}}}_{(w_0,\dots,w_n,v)} \gamma)\end{aligned}$$

And the last line is the same as $\nvDash^{\mathcal{K}_{\mathcal{T}}}_{(w_0,\dots,w_n)} \Box\gamma$.
The theorem now follows since we have:

$$\nvDash_{w_0} \alpha \Rightarrow \nvDash^{\mathcal{K}_{\mathcal{T}}}_{(w_0)} \alpha$$

$\dashv$

From this theorem a number of intereseting corroloais follows:

Corollary 4.11 **GL** is decidable, i.e there is an effective procedure for each modal formula α that detemines if $\vdash_{\mathbf{GL}} \alpha$ or $\nvdash_{\mathbf{GL}} \alpha$.

{cor:Nec}

Corollary 4.12 For all formulas α we have:

$$\vdash_{\mathbf{GL}} \alpha \Leftrightarrow \vdash_{\mathbf{GL}} \Box\alpha$$

From this theorem, we can also find the minimum element of a Kripke model of **GL**. This leads to the following definition:

Definition 4.13 Let $\mathcal{K} = \langle W, R, \phi\rangle$ be a Kripke model. A *pointed Kripke model* is a pair $\langle \mathcal{K}, w_0\rangle$ where w_0 is a node of W. In the rest of this, project we will have that w_0 is the minimum node of the tree of **GL**. We will often just define a pointed Kripke model, as $\mathcal{K} = \langle W, R, \phi, w_0\rangle$. $\dashv$

4.2 The Continuity Theorem

In this section the continuity theorem and a corollary of it will be stated and proven. This section applies to all Kripke model, and thus is not only about **GL**.

The name of this theorem comes from (George S. Boolos 1993), he does not give any deeper explanation for the name.

We will first need two definitions:

Definition 4.14 We define $d(\alpha)$ in the following way: $d(p) = d(\bot) = 0$, $d(\alpha \to \beta) = \max(d(\alpha), d(\beta))$ and $d(\Box(\alpha) = d(\alpha) + 1$. So $d(\alpha)$ is the maximal number of nested occurrences of $\Box$ in α. We call $d(\alpha)$ the *modal degree* of α. $\dashv$

Definition 4.15 Let R be a relation on a set W. For each $i \in \omega$ define R^i as follows: R^0 is the identity relation on W. $R^{i+1} = \{\langle w, v\rangle : \exists v'(wR^iv' \wedge v'Rv\}$. Thus $R^1 = R$ and wR^nv if and only if $\exists v_0, \ldots v_n(w = v_0R \ldots Rv_n = v)$. $\dashv$

{thm:conti}

Theorem 4.16 (The Continuity Theorem) Let $\mathcal{K} = \langle W, R, \phi\rangle$ and $\mathcal{K}' = \langle V, R', \phi'\rangle$ be models and let $w \in W$. Let $P \subseteq \Phi$ be a set of proportional letters. Suppose that $d(\alpha) = n$, that all proportional letters that occur in α are in P, $\{v : \exists i \leq n\ wR^iv\} \subseteq V$, $R' = \{\langle v, v'\rangle : v, v' \in V \wedge vRv'\}$, and $p \in \phi'(v)$ if and only if $p \in \phi(v)$ for all $v \in V$ and all proportional letters in P. Then $\vDash^{\mathcal{K}}_w \alpha$ if and only if $\vDash^{\mathcal{K}'}_w \alpha$.

Proof. We will show that for all subformulae β of α, if we for some i have that wR^iv and $d(\beta) + i \leq n$ such that $i \leq n$ and $v \in V$, then $\vDash^{\mathcal{K}}_v \beta$ if and only if $\vDash^{\mathcal{K}'}_v \beta$. Since wR^0w and $d(\alpha) = n$ the theorem will follow.

The proof will be induction on the complexity if β. The cases where β is $\bot$ or a $p \in P$ is trivial. If β is $\gamma \to \sigma$ then $d(\gamma), d(\sigma) \leq d(\beta)$ and the result follows the induction hypothesis. If β is , wR^iv and $d(\beta) + i \leq n$. Then $v \in V$ and $d(\beta) = d(\gamma) + 1$. If vRv' then $wR^{i+1}v'$, $d(\gamma) + i + 1 \leq n$, $v' \in V$ and therefore vSv' and by the induction hypothesis we get $\vDash^{\mathcal{K}}_{v'} \Gamma$ if and only if $\vDash^{\mathcal{K}'}_{v'} \gamma$, since we have that $S \subseteq R$, vRv' if vSv'. But this means that $\vDash^{\mathcal{K}}_v \beta$ if and only if for all v' such that vRv' we have that $\vDash^{\mathcal{K}'}_{v'} \gamma$; if and only if for all v' such that vSv': $\vDash^{\mathcal{K}}_{v'} \gamma$ if and only if by the induction hypothesis for all v' such that vSv'; $\vDash^{\mathcal{K}'}_{v'} \gamma$ if and only if $\vDash^{\mathcal{K}'}_v \beta$. $\dashv$

From this theorem the following corollary is a immediate consequence and we will use it to prove parts of the main theorem of the next chapter:

{cor:conti}

Corollary 4.17 Let α be a formula. Let $\mathcal{K} = \langle W, R, \phi\rangle$ and $\mathcal{K}' = \langle W, R, \phi'\rangle$ be models, and $p \in \phi(w)$ if and only if $p \in \phi'(w)$ for all $w \in W$ and all p contained in α. Then $\vDash^{\mathcal{K}}_w \alpha$ if and only if $\vDash^{\mathcal{K}'}_w \alpha$.

4.3 The Modal Logic GLS

In this section we will define the modal logic **GLS** (The "S" is for Solovay). This logic is an extension of **GL**, but it is not as well behaved as **GL**. It is this logic we will use in the statement of Solovay's second completeness theorem, so it is important to know a few basic results about it.

Further, this section will follow (Lindström 1997), since the version of the main theorem found in that work is a bit better stated than the one found in (Smorynski 1985).

Definition 4.18 The modal logic **GLS** is the logic which has the following axioms

GL All theorems of **GL**.

Refl $\Box p \to p$

and which sole rule of inference is modus ponens. $\dashv$

The axiom Refl is added since we for **PRA** can add the following principle called *local reflexion principle* (Rfn) for any formula:

$$\mathrm{Pr}(\ulcorner F \urcorner) \to F$$

We will further define Con^n for $n > 0$ in the following way: $\mathrm{Con}^1 = \mathrm{Con}$, $\mathrm{Con}^{n+1} = \mathrm{Con}_{\mathbf{PRA}+\mathrm{Con}^n}$, where $\mathrm{Con}_{\mathbf{PRA}+textCon^n}$ is the consistent of **PRA** with Con^n added. It can then be shown that **PRA** + Rfn is a proper extension of **PRA** + $\{\mathrm{Con}^n, n \in \omega\}$. So we add the axiom Refl to simulate the local reflexion principle in **GLS**. Another more cumbersome definition of this modal logic can be found in (Smorynski 1985). We follow the definition form (George S. Boolos 1993) and (Lindström 1997) since it is a lot easier to understand and work with. It is also the original definition from (Solovay 1976)

It should be noted that this modal logic is not a *normal* one, since it do not have necessitation as a rule of inference. If a modal logic just extended **GL** with the axiom *Refl* then this logic would prove both $\neg\Box\bot$ and $\Box\bot$ and thus be inconsistent; this is why we have not included it as rule.

There is no completeness theorem for **GLS** in the same vein as the finite tree theorem for **GL**. But there is another similar result we will now state and prove (This theorem is found in (Lindström 1997)).

Definition 4.19 Let α be any modal formula, let $\mathcal{K} = \langle W, R, \phi, w_0 \rangle$ be a pointed Kripke model and suppose that $w \in W$. Then w is α-*reflexive* in $\mathcal{K}$ if $\Box\beta \to \beta \in \phi(w)$ for all $\Box\beta \in S(\alpha)$. $\mathcal{K}$ is α-reflexive if w_0 is α-reflexive. Let $\mathcal{F}$ be a class of Kripke models; a formula α is *r-valid* in $\mathcal{F}$ if $\vDash^{\mathcal{K}} \alpha$ for all α-reflexive $\mathcal{K} \in \mathcal{F}$. $\dashv$

If we want to show that a formula α is not r-valid in the class of finite tree Kripke models, it is enough to find a $\mathcal{K}$ in this class and a α-reflexive $w \in W$ such that $\alpha \notin \phi(w)$.

The main theorem about **GLS** is the following, which gives a sort of model theory for this modal logic.

m:MainGLS}

Theorem 4.20 Let α be a modal formula. Define the following set: $S_\Box(\alpha) = \{\Box\beta : \Box\beta$ is a subformula of $\alpha\}$ the set of subformulae of α that is boxed. Then the following three statements are equivalent:

1. $\vdash_{\mathbf{GLS}} \alpha$
2. $\vdash_{\mathbf{GL}} \bigwedge_{\Box\beta\in S_\Box(\alpha)}(\Box\beta \to \beta) \to \alpha$
3. α is r-valid in the class of FT Kripke models

The equivalences of (1) and (2) makes since we have added the axiom Refl; i.e. the r-valid class of finite tree Kripke models are the models where the local reflexion principle is true.

This theorem reduces the decidability of **GLS** to the decidability of **GL** and describes a model theory for **GLS**.

We have that (2) $\Leftrightarrow$ (3) by the finite tree theorem, and that (2) $\Rightarrow$ (1) is follows by the definitions of **GLS**.

The proof that (1) $\Rightarrow$ (2) is non trivial, and for this proof we need the following lemma:

{lem:hvad}

Lemma 4.21 Let $\mathcal{K} = \langle W, R, \phi, w_0\rangle$ and suppose that $w_0Rw_1R\dots Rw_{n+1}$. Let ϑ_n be the following formulas:

$$(\Box p_1 \to p_1) \wedge \cdots \wedge (\Box p_n \to p_n)$$

Then there is an i; $1 \le i \le n+1$, such that $\vartheta_n \in \phi(w_i)$, and thus $\vDash^{\mathcal{K}} \vartheta_n$.

Proof. The lemma follows from the fact that for each k; $1 \le k \le n$, there is at most one j; $1 \le j \le n+1$, such that $\neg(\Box p_k \to p_k) \in \phi(w_j)$ $\dashv$

Further for the proof we will make use of the following operation on Kripke models:

Definition 4.22 Let $\mathcal{K} = \langle W, R, \phi\rangle$ be a Kripke Model. The derived model $\mathcal{K}'$ is defined as follows: $W' = W \cup \{w'\}$, where $w' \notin W$. We further have that R' is defined as $wR'v$ iff wRv for $w, v \in W$; w' is the new minimum element. Further we have that $w \in \phi'(p)$ iff $w \in \phi(p)$ for $w \in K$, where p is any atomic formula. Lastly we have that $w' \in \phi'(p)$ iff $w_0 \in \phi(p)$. $\dashv$

We can further define the notion of a sequences of successive derived models: $\mathcal{K}^{(1)}, \mathcal{K}^{(2)}, \dots$ that have $w_1, w_2, \dots$ as their minima. We define $\mathcal{K}^{(1)} = \mathcal{K}$ and $\mathcal{K}^{(n+1)} = (\mathcal{K}^{(n)})'$ and let w_n denote the minimum of $\mathcal{K}^{(n)}$. This can graphically been seen by adding a tail of n nodes below w_0, as seen in the following graphs:

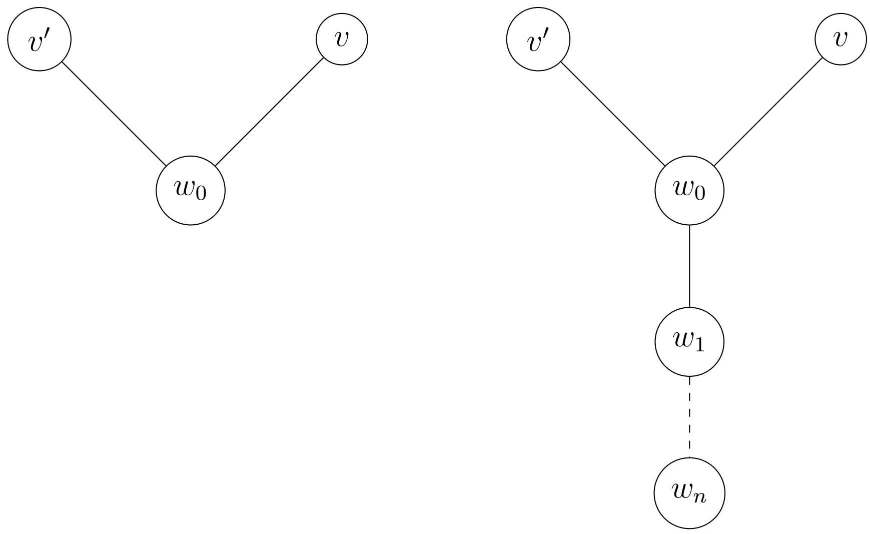


Figure 4.1: The visualization of the models $\mathcal{K}$ (left) and $\mathcal{K}^{(n)}$ (right)

Remark 4.23 We have for $w \in W$ and for any formula γ that:

$$\vDash^{\mathcal{K}} \gamma \text{ iff } \vDash^{\mathcal{K}^{(n)}} \gamma$$

So we can remove the superscript without consequences for the understanding. We will do so going forward.

The following lemma will explain a bit deeper how these derived models works, and will be used in the proof of theorem and later on in the proof of Solovay's second completeness theorem.

{lem:GLS}

Lemma 4.24 Let $\mathcal{K}$ be a α-reflexive model, $S(\alpha)$ the set of subformulas of α and $\mathcal{K}^{(n)}$ be the n-derived model. Then for all $\beta \in S(\alpha)$ we have:

$$\vDash_{w_0} \beta \Leftrightarrow \vDash_{w_n} \beta$$

Proof. We will prove this by induction on n. The lemma will follow from the case $n = 1$, since we can use that result n times to get the lemma, and this will be proven by induction om complexity of β. The only non trivial case is the case where $\beta = \Box\gamma$, so this is the only case that will be shown:

Let $\beta = \Box\gamma \in S(\alpha)$.

($\Rightarrow$) The following is clear for $\Box\gamma \in S(\alpha)$:

$$\vDash_{w_0} \Box\gamma \Rightarrow \vDash_{w_0} \gamma$$

This follows since our model is α-reflexive. Therefore we have: $\forall v : w_1 R v (\vDash_v \gamma)$ and thus $\vDash_{w_1} \Box\gamma$

($\Leftarrow$) Here we can make the following deduction:

$$\begin{aligned} \vDash_{w_1} \Box\gamma &\Rightarrow \forall v : w_1 R v (\vDash_v \gamma) \\ &\Rightarrow \forall v : w_0 R v (\vDash_v \gamma) \\ &\Rightarrow \vDash_{w_0} \Box\gamma \end{aligned}$$

$\dashv$

We can now return to our proof of the main theorem of this section by proving

Proof of 4.20. We will just have to show that (1) $\Rightarrow$ (2). Assume that α is not FT-r-valid, i.e we have that there is an α-reflexive $\mathcal{K} = \langle W, R, \phi, w_0 \rangle \in$ FT such that $\vDash^{\mathcal{K}} \neg\alpha$. Our goal is to show that $\nvdash_{\mathbf{GLS}} \alpha$.

If we have that $\vdash_{\mathbf{GLS}} \alpha$ there are formulas γ_i, $i < n$ such that if let σ be the following formula

$$\bigwedge\{\Box\gamma_i \to \gamma_i : i < n\} \to \alpha$$

is provable in **GL** and therefor σ is FT-valid. The theorem follows if we can show that σ is not FT-valid. We will look at the derived model $\mathcal{K}^{n+1}$, and by Lemma 4.21 there is a $j \leq n$ such that

$$w_{j+1} \in \phi^{n+1}(\bigwedge\{\Box\gamma_i \to \gamma_i : i < n\})$$

Since we have that $w_{j+1} \in \phi^{n+1}\neg\alpha$ and thus $a_{j+1} \in \phi(\neg\sigma)$ and thus σ is not FT-valid $\dashv$

Since the models used in this proof is finite and since **GL** is decidable we get the following corollary:

Corollary 4.25 **GLS** is decidable

In the chapter 6 it will be shown that **GL** axiomatise the provable schemata in **PRA** and **GLS** will axiomatise the *true* schemata of arithmetics; i.e truth in the standard model $\mathcal{N} = \langle \omega, +, \cdot \rangle$ of arithmetics.

5 Fixed Point Theorem

{chap:Fixed}

In this section we will prove the so called *fixed point theorem* for **GL**. This theorem says that there for some formulae α of **GL** exists fixed points σ, i.e that for these formulae:

$$\vdash_{\mathbf{GL}} \sigma \leftrightarrow \alpha(\sigma)$$

This theorem gives is one of the most striking applications of modal logic in the study of provability in arithmetic; it can be proven to say self-reference is not necessary in the proofs of Gödel's incompleteness theorems. There has been a lot of different ways to prove this theorem; Boolos list three different ways in his book (George S. Boolos 1993) and Per Lindström has another one in his paper (Lindström 1996). Here we will follow the proof from (Reidhaar-Olson 1990).

This proof of the theorem is a semantical proof; i.e it makes use of the Kripke semantics of the modal logic **GL**, and it further gives a simple procedure for "calculating" fixed points.

We will end this chapter with calculating some fixed points. This will be possible since the proof of the fixed point theorem contains a algorithm, which can be used to calculate these. In the next chapter we will use the soundness part of Solovay's completeness theorems and the fixed point theorem to conclude a few things about arithmetic with the help of modal logic. This is the *power* of the fixed point theorem; it makes it possible to study the proof predicate with the help of modal logic.

5.1 Prerequisite Results and Definitions

We will start of by make stating some definitions and results that are crucial in the proof of the fixed point theorem. We will also in this section define the special formulae for which the fixed point theorem holds.

Definition 5.1 We abbreviate $\Box\alpha \wedge \alpha$ as $\boxdot\alpha$ for every α in our language. $\dashv$

$\boxdot$ is called "strong box" and for a given model $\mathcal{K}$ we have that $\vDash_w^{\mathcal{K}} \boxdot\, \alpha$ states that α is both true and provable in node w. There are a few theorem about $\boxdot$ in the modal logic **K4** and logics which extends this, that will be important in the following. These results are syntactical. We will state these now, and more results can be found in (Smorynski 1985) and (George S. Boolos 1993)

{seet}

Theorem 5.2 Let α be a modal formula then:

1. $\vdash_{\mathbf{K4}} (\boxdot\Box\alpha \leftrightarrow \Box\alpha) \leftrightarrow \Box\boxdot\alpha$
2. $\vdash_{\mathbf{K4}} \boxdot\alpha \leftrightarrow \boxdot\boxdot\alpha$

The proof of this is syntactical and is left out.

{GLsæt}

Theorem 5.3 Suppose that $\mathbf{L}$ extends $\mathbf{K4}$, and we have that $\vdash_{\mathbf{L}} \boxdot\alpha \to \beta$. Then $\vdash_{\mathbf{L}} \Box\alpha \to \Box\beta$ and $\vdash_{\mathbf{L}} \boxdot\alpha \to \boxdot\beta$

This theorem clearly holds for **GL**, since it is an extension of **K4** and we will use it later in this chapter.

Proof. Since $\mathbf{L}$ extends $\mathbf{K4}$ we have that $\vdash_{\mathbf{L}} \Box\boxdot\alpha \to \Box\beta$ and thus by theorem 5.2 we have that $\vdash_{\mathbf{L}} \Box\alpha \to \Box\beta$ and by the definition of $\boxdot$ we get that $\vdash_{\mathbf{L}} \boxdot\alpha \to \boxdot\beta$ $\dashv$

Having shown a few results about the syntactical properties of $\boxdot$ we will now turn to some of the sementical properties about the relationship between $\Box$ and $\boxdot$

{rem:acc}

Remark 5.4 By our semantic of modal logic, we have that $\vDash_w \boxdot\alpha$ is true iff $\vDash_v \alpha$ for all $v \in \{w\} \cup \text{acc}(w)$, where $\text{acc}(w)$ is the collection of nodes that are accessible from w, i.e: $\text{acc}(w) = \{v \in W : wRv\}$.

This remark gives us an easy way to determine if $\boxdot\alpha$ is true.

Another useful definition that we can make, since we can without loss of generality assume that for the Kripke model $\mathcal{K} = \langle W, R, \phi\rangle$ of **GL** we look at that the set W is finite, is the following:

Definition 5.5 Let $\mathcal{K} = \langle W, R, \phi\rangle$ be a Kripke model of **GL**. The *rank* of the nodes $w \in W$ is defined in the following way: $\text{rank}(w) = 0$ iff there is no world v such that wRv. Otherwise we have that $\text{rank}(w) = 1 + \max\{\text{rank}(v) : wRv\}$. $\dashv$

So $\text{rank}(w)$ simple states how long the longest path from w is, and the rank is finite since W is finite. Further since W is finite and that R is irreflexive we have that the for each $w \in W$ the rank of w is unique.

We will need the following three lemmas in our proof of the Fixed Point Theorem. All three of these lemmas are sementical in nature.

{lem:acc}

Lemma 5.6 Given any Kripke model $\mathcal{K} = \langle W, R, \phi\rangle$ of **GL**, $w \in W$ and sentence α, we have that if $\vDash_w \Box\alpha$ then $\vDash_v \Box\alpha$ for any $v \in \text{acc}(w)$. Further we have that $\vDash_v \boxdot\alpha$ for all $v \in \text{acc}(w)$.

Proof. Assume that we have: $\vDash_w \Box\alpha$, w sees v and v sees v'. Since R is transitive we have that w also sees v' and thus we have that $\vDash_{v'} \alpha$. Since v' was chosen arbitrarily we have that $\vDash_v \Box\alpha$. We also have that $\vDash_v \alpha$ and thus we have $\vDash_v \boxdot \alpha$. ⊣

{lem:con}

Lemma 5.7 Given any Kripke model $\mathcal{K} = \langle W, R, \phi \rangle$ of **GL**, $w \in W$ and sentence α, if $\nvDash_w \Box\alpha$ then there is nodes v seen by w such that $\vDash_v \Box\alpha$ and $\nvDash_v \alpha$.

Proof. Assume that $\nvDash_w \Box\alpha$ then there is a node v that sees w such that $\nvDash_v \alpha$. Let v be the nodes with the least rank with this property and suppose that vRv'. Since v' is of less rank than v we have that $\vDash_{v'} \alpha$. Now since v' was chosen arbitrarily we have that $\vDash_v \Box\alpha$ and the lemma is proven. ⊣

The next lemma will be crucial in the proof of the fixed-point theorem; since it enable us to substitute two formulae into another formula.

{lem:sem}

Lemma 5.8 (Semantic Substitution Lemma) For any sentences α, β and γ we have that the following formula is valid in all models of **GL**:

$$\boxdot(\beta \leftrightarrow \gamma) \rightarrow (\alpha(\beta) \leftrightarrow \alpha(\gamma))$$

The meaning of $\alpha(\beta)$ is that we replace every occurrences of p in α with β; the meaning of $\alpha(\gamma)$ is similar.

Proof. We start of by fixing β and γ. The proof will be by induction on the complexity of α. We will only proof the part where α is $\Box\sigma$.

So suppose that α is $\Box\sigma$, where $\boxdot(\beta \leftrightarrow \gamma) \rightarrow (\sigma(\beta) \leftrightarrow \sigma(\gamma))$ is valid. Let $\mathcal{K}$ be any model of **GL** and let $w \in W$. Suppose that $\vDash_w \boxdot(\beta \leftrightarrow \gamma)$. Let v be any world seen by w. Then by lemma 5.6 we have $\vDash_v \boxdot(\beta \leftrightarrow \gamma)$. Since $\boxdot(\beta \leftrightarrow \gamma) \rightarrow (\sigma(\beta) \leftrightarrow \sigma(\gamma))$ is valid we get that $\vDash_v \sigma(\beta) \leftrightarrow \sigma(\gamma)$ and since v was chosen arbitrary we get $\vDash_w \Box(\sigma(\beta) \leftrightarrow \sigma(\gamma))$. By proposition 1.17 and weak completeness we can conclude $\vDash_w \Box\sigma(\beta) \leftrightarrow \Box\sigma(\gamma)$. ⊣

We are now almost ready to state state and prove the fixed-point theorem. We will just need the next two definitions:

Definition 5.9 A formula α is called *modalized in* p if every occurrence of p in α is under the scope of $\Box$. ⊣

That α is modalized in p will be a sufficient condition for α having a fixed point, but it is not a necessary condition for this. $\Box p \vee p$ is one example of a formula that has a fixed point, even though p is not modalized in this formula. This will be showed later.

We will also need the following definition, which in some way is a generalization of being modalized in p:

Definition 5.10 A sentence α is said to be *n-decomposable* iff for some sequence $q_1, \dots, q_n$ consisting of distinct senctence letters that do not occur in α we have some sentence $\beta(q_1, \dots, q_n)$ that do not contain p and another sequence of distinct sentences $\gamma_1(p), \dots, \gamma_n(p)$, which each contains p that we have

$$\alpha = \beta(\gamma_1(p), \dots, \gamma_n(p))$$

. $\dashv$

The following remark will be important in the proof of the fixed point theorem.

Remark 5.11 It should be noted that if α is modalized in p that we then have that α is n-decomposable for some n.

5.2 Proof of the Fixed Point Theorem

We can now state the fixed point theorem. But we will still need a few lemmas in our proof. These will be stated and proven when needed. The theorem we will start of by showing can be seen as a uniqueness theorem, we will after this theorem state and prove a theorem that can be seen as a existences theorem. Lastly we will prove a corollary that will show why the name fixed point theorem is appropriate; this is not clearly seen from the fixed point theorem itself.

{thm:Fixed}

Theorem 5.12 If α is modalized in p, then there exists a formula σ in which the only sentence letters that occurs are these other than p that occur in α, and such that:

$$\boxdot(p \leftrightarrow \alpha) \rightarrow (p \leftrightarrow \sigma)$$

The formula σ is called a *fixed-point* of α.

We will later on prove that $\vdash_{\mathbf{GL}} \sigma \leftrightarrow \alpha(\sigma)$ for such a σ and thus the name fixed point is appropriate.

Proof. We will prove this by showing that if α is n-decomposable then it has a fixed point. We will show this by induction on n.

Base case: Suppose that α is 0-decomposable. Then we have that p does not occur in α and it can thus itself be the sentence β.

Induction step: Assume that every sentence that is n-decomposable has a fixed point. We now have to show that every sentence that is $(n+1)$-decomposable also has a fixed point. To show this we will assume the following:

$$\alpha(p) = \beta(\Box\gamma_1(p), \dots, \Box_{n+1}(p))$$

Further for each i such that $1 \leq i \leq n+1$ let:

$$\alpha_i(p) = \beta(\Box\gamma_1(p), \ldots, \Box\gamma_{i-1}, \top, \Box\gamma_{i+1}, \ldots, \Box\gamma_{n+1}(p))$$

Thus we have that for each i such that $1 \leq i \leq n+1$ that $\alpha(p)$ is n-decomposable, so it has a fixed point, that we call σ_i. Lastly we define:

$$\sigma = \beta(\Box\gamma_1(\sigma_1), \ldots, \Box\gamma_{n+1}(\sigma_{n+1}))$$

Our goal is to show that σ is a fixed point of α, and for that we will need the following lemma:

{lem:fix}

Lemma 5.13 For each i such that $1 \leq i \leq n+1$ we have that:

$$\vdash_{\mathbf{GL}} \boxdot(p \leftrightarrow \alpha) \rightarrow \boxdot\Box\gamma_i(p) \leftrightarrow \gamma_i(\sigma_i))$$

Proof. Since we have that **GL** is complete, we just have to show that for any model $\mathcal{K} = \langle W, R, \phi\rangle$ and any $w \in W$ that:

$$\vDash^{\mathcal{K}} \boxdot(p \leftrightarrow \alpha) \rightarrow (\boxdot(\Box\gamma_i(p) \leftrightarrow \Box\gamma_i(\sigma_i)) \tag{5.1}$$ {eqn:1}

So we will start of by fixing i, $\mathcal{K}$ and $w \in W$. We will show 5.1 by assuming $\vDash_w \boxdot (p \leftrightarrow \alpha)$ and then deduce: $\vDash_w \boxdot (\Box\gamma_i(p) \leftrightarrow \Box\gamma_i(\sigma_i))$; this is equivalent to $\vDash_v \Box\gamma_i(p) \leftrightarrow \Box\gamma_i(\sigma_i)$ for all $v \in \{w\} \cup \mathrm{acc}(w)$ by remark 5.4. So let $v \in \{w\} \cup \mathrm{acc}(w)$ and assume that $\vDash \Box\gamma_i(p)$, i.e $\vDash_v \Box\gamma_i(p) \leftrightarrow \top$. By lemma 5.6 we have that for any $v' \in \mathrm{acc}(v)$ that $\vDash_{v'} \Box\gamma_i(p)$ and thus $\vDash_{v'} (\Box\gamma_i(p) \leftrightarrow \top)$. This means that we have:

$$\vDash_v \boxdot(\Box\gamma_i(p) \leftrightarrow \top)$$

And thus by lemma 5.8 we get that $\vDash_v \alpha_i \leftrightarrow \alpha$ and since our v was chosen arbitrarily we have that $\vDash_w \Box(\alpha_i \leftrightarrow \alpha)$ and thus by lemma 5.6 we get that: $\vDash_v \boxdot(\alpha_i \leftrightarrow \alpha)$. Since we have assumed that $\vDash_w \boxdot(p \leftrightarrow \alpha)$ we again have by lemma 5.6 that $\vDash_v \boxdot(p \leftrightarrow \alpha)$, and hence we have $\vDash_v \boxdot(p \leftrightarrow \alpha_i)$. Since our logic is complete and we have assumed by the induction hypothesis that α_i has a fixed point σ_i we have that $\vDash_v (p \leftrightarrow \gamma_i)$, and thus, since v was chosen arbitrarily we have that $\vDash_w \Box(p \leftrightarrow \gamma_i)$. So by using 5.6 again we get that $\vDash_v \boxdot(p \leftrightarrow \gamma_i)$. We will now use lemma 5.8 again and get that:

$$\vDash_v \gamma_i(p) \leftrightarrow \gamma_i(\sigma_i) \tag{5.2}$$ {eqn:sub1}

and

$$\vDash_v \Box\gamma_i(p) \leftrightarrow \Box\gamma_i(\sigma_i) \tag{5.3}$$ {eqn:sub2}

Notice that these two holds for any $v \in \{w\} \cup \mathrm{acc}(w)$ such that $\vDash_v \Box\gamma_i(p)$. Further by 5.3 we can deduce $\vDash_v \Box\gamma_i(p) \rightarrow \Box\gamma_i(\sigma_i)$

For the next step of the proof of this lemma we will assume that $\nvDash_v \Box\gamma_i(p)$. This means by lemma 5.7 that there is some world v' where $v' \in \mathrm{acc}(v)$, such that $\nvDash_{v'} \gamma_i(p)$ and $\vDash_{v'} \Box\gamma_i(p)$. 5.2 holds for v' since $v' \in \{w\} \cup \mathrm{acc}(w)$ and thus we have $\vDash_{v'} \gamma_i(p) \leftrightarrow \gamma_i(\sigma_i)$. This us gives that $\nvDash_{v'} \gamma_i(\sigma_i)$ and thus since vRv' we have that $\nvDash_v \Box\gamma_i(\sigma_i)$. By contraposition we then get: $\vDash_v \Box\gamma_i(\sigma_i) \rightarrow \Box\gamma_i(p)$, and thus we have shown that:

$$\vDash_v \Box\gamma_i(p) \leftrightarrow \Box\gamma_i(\sigma_i)$$

We can now shown the lemma. ⊣

We now go back and finish our proof of the fixed point theorem. Suppose that $\mathcal{K}$ is a model and that $w \in W$ such that $\vDash_w \boxdot (p \leftrightarrow \alpha)$. By lemma 5.13 and completeness we get $\vDash_w \boxdot (\Box\gamma_i(p) \leftrightarrow \Box\gamma_i(\sigma_i))$. By using lemma 5.8 $(n+1)$ times we can deduce that:

$$\vDash_w \beta(\Box\gamma_i(p), \ldots, \Box\gamma_{n+1}(p)) \leftrightarrow \beta(\Box\gamma_1(\sigma_1), \ldots, \Box\gamma_{n+1}(\sigma_{n+1}))$$

i.e $\vDash_w \alpha \leftrightarrow \sigma$.

Since we have $\vDash_w p \leftrightarrow \alpha$ we get $\vDash_w p \leftrightarrow \sigma$, we can obtain $\vDash_w \boxdot(p \leftrightarrow \alpha) \rightarrow (p \leftrightarrow \sigma)$. Since our $\mathcal{K}$ and w was chosen arbitrarily we have that $\boxdot(p \leftrightarrow \alpha) \rightarrow (p \leftrightarrow \sigma)$ is valid. By completeness we then have: $\vdash_{\mathbf{GL}} \boxdot(p \leftrightarrow \alpha) \rightarrow (p \leftrightarrow \sigma)$ ⊣

The following result follows from the fixed-point theorem.

{thm:exi}

Theorem 5.14 Let $\alpha(p)$ be modalized in p, and let σ be a fixed-point of α. Then:

$$\vdash_{\mathbf{GL}} \boxdot(p \leftrightarrow \sigma) \rightarrow (p \leftrightarrow \alpha)$$

Proof. Suppose that $\mathcal{K} = \langle W, R, \phi \rangle$ is a finite transitive and irreflexive model in which $\boxdot(p \leftrightarrow \sigma) \rightarrow (p \leftrightarrow \alpha)$ is invalid. This means that for some $w \in W$ of least rank that we have: $\vDash_w \boxdot(p \leftrightarrow \sigma)$ and thus $\vDash_w p \leftrightarrow \sigma$ and $\nvDash_w p \leftrightarrow \alpha$. If wRv then $\vDash_v \boxdot (p \leftrightarrow \sigma)$ and since x is of lower rank than w we also have $\vDash_v p \leftrightarrow \alpha$. Let ϕ' be like ϕ expect that $p \in \phi'(w)$ if and only if not $p \in \phi(w)$. Set $\mathcal{K}' = \langle W, R, \phi' \rangle$, and this model is clearly transitive and irreflexive.

In the rest of this proof we will use corollary to the continuity theorem; i.e corollary 4.17.

The formula α is a truth-functional compound of closed formulas $\Box\beta$ and proportional letters q such that each q is not p. We have that $\vDash^{\mathcal{K}}_w \Box\beta$ if and only if $\vDash^{\mathcal{K}}_v \beta$ for all v such that wRv, if and only if $\vDash^{\mathcal{K}'}_v$ for all v such that wRv (by continuity), if and only if $\vDash^{\mathcal{K}'}_w \Box\beta$. We further have by the definition of $\mathcal{K}'$ that $\vDash^{\mathcal{K}}_w \alpha$ if and only iff $\vDash^{\mathcal{K}'}_w$ and $\vDash^{\mathcal{K}}_w p$ if and only if not $\vDash^{\mathcal{K}'}_w p$. Thus we have $\vDash^{\mathcal{K}'}_w p \leftrightarrow \alpha$

and b the continuity theorem we again get $\vDash_v^{\mathcal{K}'} p \leftrightarrow \alpha$ for all v such that wRv. But this means that we get $\vDash_w^{\mathcal{K}'} \boxdot(p \leftrightarrow \alpha)$.

Since σ does not contain p we get by the Corollary 4.17 that $\vDash_w^{\mathcal{K}} \sigma$ if and only if $\vDash_w^{\mathcal{K}'} \sigma$. Since we have that $\vDash_w^{\mathcal{K}} p$ if and only if not $\vDash_w^{\mathcal{K}'} p$ we get $\nvDash_w^{\mathcal{K}'} p \leftrightarrow \sigma$ and thus $\boxdot(p \leftrightarrow \sigma) \to (p \leftrightarrow \sigma)$ is invalid.

By soundness and completeness of **GL** we thus get that if $\vdash_{\mathbf{GL}} \boxdot(p \leftrightarrow \alpha) \to (p \leftrightarrow \sigma)$ then $\vdash_{\mathbf{GL}} \boxdot(p \leftrightarrow \sigma) \to (p \leftrightarrow \alpha)$. ⊣

From this we can prove the following corollary that show that the name fixed-point is appropriate:

Corollary 5.15 Let $\alpha(p)$ be modalized in p and let σ be a fixed-point of α. Then:

$$\vdash_{\mathbf{GL}} \sigma \leftrightarrow \alpha(\sigma)$$

Proof. Since we have assumed uniform substitution and by theorem 5.14 the result of substituting σ for p in $\boxdot(p \leftrightarrow \sigma) \to (p \leftrightarrow \alpha)$ is a theorem of **GL**. This means that $\vdash_{\mathbf{GL}} \boxdot(\sigma \leftrightarrow \sigma) \to (\sigma \leftrightarrow \alpha(\sigma))$. $\boxdot(\sigma \leftrightarrow \sigma)$ is obviously a theorem of **GL** so we get:

$$\vdash_{\mathbf{GL}} \sigma \leftrightarrow \alpha(\sigma)$$

⊣

We can also state (by Theorem 5.14 and Theorem 5.12) the fixed point theorem in the following form:

{cor:Fixed}

Corollary 5.16 For every modal formula α modalized in p, there is a modal formula σ only containing proportional letters contained in α not containing p such that:

$$\vdash_{\mathbf{GL}} \boxdot(p \leftrightarrow \alpha) \leftrightarrow \boxdot(p \leftrightarrow \sigma)$$

5.3 Calculation of Fixed Points

The algorithm in the proof of the fixed theorem can be used to calculate specific fixed points for some given formula, that fulfills the conditions of the theorem.

When we have shown the soundness part of the first Solovay's completeness theorem, the fixed point theorem will then make it possible for us to determine the fixed point of a wide range of sentences of arithmetic. This is important because this way of finding these points are often a lot easier than finding the points only with the help of the arithmetical methods.

Below are a few example of how we can use this algorithm.

Example 5.17 Let $\alpha(p) = \Box\neg p$. We will calculate the fixed point for α. Let $\gamma_1(p) = p$ and $\beta(q_1) = q_1$. We then have that $\alpha(p) = \beta(\Box\gamma_1(p))$ and $\alpha_1(p) = \beta(\top) = \top$. The fixed point of σ_1 of α_1 is then $\top$, since p does not occur in α_1. We can thus conclude that the fixed point σ of α is the following:

$$\beta(\Box\gamma_1(\top)) = \beta(\Box\neg\top) = \Box\neg\top$$

this formula is equivalent to $\Box\bot$. ⊣

Example 5.18 Let $\alpha(p) = \Box p \to \Box\neg p$. To find the fixed point, let$\gamma_1(p) = p$,$\gamma_2(p) = \neg p$ and $\beta(q_1, q_2) = q_1 \to q_2$. Then clearly we have:

$$\alpha(p) = \beta(\Box\gamma_1(p), \Box\gamma_2(p))$$

$$\alpha_1(p) = \beta(\top, \Box\gamma_2(p)) = \top \to \Box\neg p$$

and

$$\alpha_2(p) = \beta(\Box\gamma_1(p), \top) = \Box p \to \top$$

It is clear that α_1 is equivalent to $\Box\neg p$ and that α_2 is equivalent top $\top$; thus they have fixed points $\sigma_1 = \Box\bot$ and $\sigma_2 = \top$. So the fixed point σ of α is the following:

$$\beta(\Box\gamma_1(\Box\bot), \Box\gamma_2(\top)) = \Box\Box\bot \to \Box\neg\top$$

or equivalent: $\Box\Box\bot \to \Box\bot$. ⊣

5.3.1 Calculation of a Non-Modalized Fixed Point

We will now show that $\Box p \vee p$ has a fixed point. It is clear that this formula is not modalized in p, but it can still be shown to have a fixed point.

For this end we will need the following theorem: We will start of by showing that no β modalized in p is equivalent to $\Box p \vee p$. This will the following two propositions show:

Proposition 5.19 Suppose that β is modalized in p. Then we have:

$$\vdash_{\mathbf{GL}} p \to \beta \Rightarrow \vdash_{\mathbf{GL}} \beta$$

Proof. Suppose that $\nvdash_{\mathbf{GL}} \beta$. This means that for some finite transitive and irreflexive model $\mathcal{K} = \langle W, R, \phi\rangle$ and some $w \in W$ that: $\nvDash_w \beta$. Let ϕ' be such that $w \in \phi'(p)$ and otherwise it is just ϕ and let $\mathcal{K}' = \langle W, R, \phi'\rangle$. We have that β is a truth-functional compound of formulae $\Box\gamma$ and proportional letters that are not p. By continuity we have that $\nvDash_w^{\mathcal{K}'} \beta$ but we have that $\vDash_w^{\mathcal{K}'} p$. Hence we have that $\vDash_w^{\mathcal{K}'} p \to \beta$ and the propositions follows. ⊣

The next proposition shows that no β equivalent to $\Box p \vee p$ is modalized in p.

Proposition 5.20 For no β modalized in p, we have that:

$$\vdash_{\mathbf{GL}} \beta \leftrightarrow (\Box p \vee p)$$

Proof. If there was such a β we would have that $\vdash_{\mathbf{GL}} p \to \beta$ and thus from the just shown proposition we would have that $\vdash_{\mathbf{GL}} \beta$ and $\vdash_{\mathbf{GL}} \Box p \vee p$. By substitution we would then have that $\vdash_{\mathbf{GL}} \Box\bot \vee \bot$ and this is clearly false. $\dashv$

So $\Box p \vee p$ is not equivalent to any formula modalized in p, but we can show that it has a fixed point in a another way:

Proposition 5.21

$$\vdash_{\mathbf{GL}} \boxdot(p \leftrightarrow \Box p \vee p) \leftrightarrow \boxdot(p \leftrightarrow \top)$$

Proof. The right to left implication is trivial. The other way will be shown by the following deduction:

$$\begin{aligned}
\vdash_{\mathbf{GL}} \boxdot(p \leftrightarrow \Box p \vee p) &\to \boxdot(\Box p \to p) \\
&\to \boxdot\boxdot(\Box p \to p) \text{ By theorem 5.2} \\
&\to \boxdot(\Box(\Box p \to p) \wedge (\Box p \to p)) \text{ By definition of } \boxdot \\
&\to \boxdot(\Box p \wedge (\Box p \to p)) \\
&\to \boxdot p \\
&\to (p \leftrightarrow \top)
\end{aligned}$$

$\dashv$

In figure 5.1 we can see some more fixed points. formula on the left is the formula $\alpha(p)$ and the formula on the right is the formula σ. Line (3) and (6) has already been shown.

1. $\neg\Box p$	$\neg\Box\bot$
2. $\Box p$	$\top$
3. $\Box\neg p$	$\Box\bot$
4. $\neg\Box\neg p$	$\neg\Box\bot$
5. $\neg\Box\Box\neg p$	$\neg\Box\Box\bot$
6. $\Box p \to \Box\neg p$	$\Box\Box\bot \to \Box\bot$
7. $\Box(\neg p \to \Box\bot) \to \Box(p \to \Box\bot)$	$\Box\Box\Box\bot \to \Box\Box\bot$
8. $\Box p \to q$	$\Box q \to q$
9. $\Box(p \to q)$	$\Box q$
10. $\Box p \wedge q$	$\Box q \wedge q$
11. $\Box(p \wedge q)$	$\Box q \wedge q$
12. $q \vee \Box p$	$\top$
13. $\neg\Box(q \to p)$	$\Diamond q$
14. $\Box(p \to q) \to \Box\neg p$	$\Box(\Box\bot \to q) \to \Box\bot$
15. $q \wedge (\Box(p \to q) \to \Box\neg p)$	$q \wedge \Box\neg q$
16. $\Diamond p \to (q \wedge \neg\Box(p \to q))$	$\Diamond\top \to (q \wedge \neg\Box(\Box\bot \to q))$
17. $\Box(\Box(p \wedge q) \wedge \Box(p \wedge r))$	$\Box(\Box q \wedge \Box r)$
18. $\Box p \vee p$	$\top$

{Fig} Figure 5.1: A Table of Fixed Points

We will after the proof of the soundness part of Solovay's Completeness Theorems come back to this table, and make some conclusions about the fixed points.

6 Solovays Completeness Theorems

{chap:Complete}

In this section we will prove Solovay's completeness theorems. The proof of these theorems follows a technique invented by Robert Solovay, which today is known as a *Solovay construction*. This technique is a way of embedding Kripke models into arithmetic. The first theorem show that the $\Box$-operator of the logic **GL** behaves like the proof predicate Pr from **PRA**. The second theorem shows that the modal logic **GLS**axiomatize the notion provability in the standard model of arithmetic $\mathcal{N}$.

Further these theorems shows that the proof predicate of arithmetics can be axiomatized, by the axioms of **GL** and **GLS**.

6.1 Soundness

For each formula in $\mathcal{L}_\Box$ we want to assign a sentence of $\mathcal{L}_{\mathbf{PRA}}$. This can be done in the following way.

Definition 6.1 An interpretation of $\mathcal{L}_\Box$ in **PRA** is a function that to each formula α of $\mathcal{L}_\Box$ assigns a sentence α^* of **PRA** which satisfies the following requirements:

1. For atomic p, p^* is a formula of the language of arithmetic
2. $(\bot)^* =$ "$0 = 1$"
3. $(\alpha \to \beta)^* =$ "$\alpha^* \to \beta^*$"
4. $(\Box\alpha)^* =$ " $\mathrm{Pr}(\ulcorner\alpha^*\urcorner)$"

We will further say that a modal formula α is **PRA**-valid if, in every interpretation *, α^* is a theorem of **PRA**. $\dashv$

The goal of the current section is to prove the that the set of **PRA**-valid formulas are the theorems of **GL**. I.e we want to prove the following bi-implication:

$$\mathbf{GL} \vdash \alpha \Leftrightarrow \forall^*(\mathbf{PRA} \vdash \alpha^*)$$

This statement says that **GL** completely captures what **PRA** can say about its own provability. This result can be expanded to other fragments of arithmetics.

So the modal logic **GL** is the modal logic that captures what a lot of different fragments of arithmetics can say about its own provability. Later on in the project it will be shown for which fragments this is the case.

In 6.4 we will show that **GLS** is the modal logic of the proof predicate of the standard modal $\mathcal{N}$. This is called Solovay's second completeness theorem.

We will start with proving the "$\Rightarrow$" implication; i.e that every theorem of **GL** is **PRA**-valid. The other way will be a bit harder to prove, and that is the part that is known as Solovay's first completeness theorem.

Theorem 6.2 (Soundness) For all modal sentences φ we have that :

$$\mathbf{GL} \vdash \alpha \Rightarrow \forall^*(\mathbf{PRA} \vdash \alpha^*)$$

Proof. The proof will be done as an induction proof on the number of axioms and rules of inference use in a **GL**-proof of a formula α. The proof will be done by looking at the last rule or axiom schema used in the proof of α.

The case of tautologies and modus are clear. We further have that the theorems of **PRA** are closed under modus ponens so axiom **K** is also clear.

Assume that the last step of the proof of α is an instance of necessitation. We have that $\mathrm{Pr}(x)$ is Σ_1 formula, so it is equivalent to some formula of the form $\exists y R(x, y)$, where R is a primitive recursive predicate. We know that if a Σ_1 sentences is true it is provably, so this shows the case of necessitation.

The axiom **4** can be derived from the others, so this case is redundant.

We will now just have to show the case of **L**. This case follows by Löb's theorem. $\dashv$

We can immediately use this theorem in conjecture with the fixed point theorem to deduce some things about formulae of **PRA**.

6.2 Solovay's Soundness Theorem and Fixed Points

We will now comment a bit about the implications of the soundness theorem and the fixed point theorem.

From table 5.1 and the arithmetical soundness theorem, we can conclude the following things:

1. From line 3, we have that $\vdash_{\mathbf{GL}} \boxdot(p \leftrightarrow \Box\neg p) \leftrightarrow \boxdot(p \leftrightarrow \Box\bot)$; i.e a sentence F of **PRA** is equivalent to its own unprovability if and only if F is equivalent to the assertion that **PRA**is inconsistent. For let * be such that $F = p^*$, then we if F is such that $\mathbf{PRA} \vdash F \leftrightarrow \mathrm{Pr}(\ulcorner \neg F \urcorner)$ which is the same as $\mathbf{PRA} \vdash (p \leftrightarrow \Box\neg p)^*$ and thus we have: $\mathbf{PRA} \vdash \Box(p \leftrightarrow \Box\neg p)^*$ and hence $\mathbf{PRA} \vdash \boxdot(p \leftrightarrow \Box\neg p)^*$. But by the soundness theorem we get that: $\mathbf{PRA} \vdash$

$(\boxdot(p \leftrightarrow \Box\neg p) \leftrightarrow \boxdot(p \leftrightarrow \Box\bot))^*$, and thus $\mathbf{PRA} \vdash \boxdot(p \leftrightarrow \Box\bot)^*$ whence $\mathbf{PRA} \vdash (p \leftrightarrow \Box\bot)^*$ and thus $\mathbf{PRA} \vdash F \leftrightarrow \mathrm{Pr}(\ulcorner\bot\urcorner)$. Which shows that F is equivalent to the inconsistency of **PRA**.

2. We can from line 1 and 6 infer that a sentence of **PRA** is equivalent to its own unprovability if and only if it is equivalent to the assertion that **PRA** is consistent and that a sentence of **PRA** that is equivalent to the assertion that it is unprovable if it is provable if and only if it is equivalent to the assertion that if the inconsistency of **PRA** is provable then **PRA** is provable.
3. From line 10 we can conclude that for arbitrary sentence F and G of **PRA** that: F is equivalent to the conduction of F is provable and G is true if and only if F is equivalent to the conduction of G is provable and true. Here we take * such that $p^* = F$ and $q^* = G$.
4. From line 6 again we can conclude that a fixed point may have a bigger modal degree, than formula of which it is a fixed point: the formula $\Box p \to \Box\neg p$ has modal degree 1 and the formula $\Box\Box\bot \to \Box\bot$ has degree 2. We can conclude the same for line 7, where the fixed point has modal degree 3 and the formula it is a fixed point for has degree 2.
5. The modal formula α has at most the same modal degree as the modal formula σ.
6. We can further see that line 1 gives that sentences of arithmetic that express their own unprovability are equivalent to the assertion arithmetic is consistent. Line 2 is the same as Löb's answer to Henkin's question, and line 4 gives that refutable sentences are those equivalent to their own consistency.

6.3 The First Theorem

Having shown soundness, we will now show the completeness theorem:

Theorem 6.3 (Solovay's first completeness theorem) For all modal sentences α we have that:

$$\forall^*(\mathbf{PRA} \vdash \alpha^*) \Rightarrow \mathbf{GL} \vdash \alpha$$

This theorem will be shown by contraposition. So we want to show the following: "If $\mathbf{GL} \nvdash \alpha$ then we have one * such that $\mathbf{PRA} \nvdash \alpha^*$". The start of the proof is the following: If $\mathbf{GL} \nvdash \alpha$ then $\mathbf{GL} \nvDash \alpha$ and thus there is a finite pointed Kripke model $\mathcal{K} = \langle W, R, \phi, w_0\rangle$ in which we have $w_0 \notin \phi(\alpha)$. The goal is then to find an interpretation * such that $\mathbf{PRA} \nvdash \alpha^*$.

The construction of this * is rather complex, and will take the rest of this subsection to prove. So for the rest of this subsection fix a modal formula α such that $\mathbf{GL} \nvdash \alpha$ and let $\mathcal{K} = \langle W, R, \phi, w_0 \rangle$ be a pointed Kripke model such that $w_0 \notin \phi(\alpha)$.

We will assume without loss of generality that $W = \{1, \dots, n\}$ for some finite n and that $w_0 = 1$. R can be extended by setting $0Ri$ for each i in W. Is shall be noted that 0 is not part of our Kripke model, but we will in section 6.4 create a model where it is a part of the model.

Further we will first intuitively define a function $\varphi : \omega \to \{0, \dots, n\}$ in the following way: Set $\varphi(0) = 0$. Further we define $\varphi(x+1)$ in the following way: If $x+1$ is the code of a proof that $\lim_{k\to\infty} \varphi(k) \neq z$ for some z accessible to $\varphi(x)$ we set $\varphi(x+1) = z$ otherwise we have that $\varphi(x+1) = \varphi(x)$.

The way this function works can be explained intuitively by the following quote:

> Imagine a refugee who is admitted from one country to another only if he/she provides a proof not to stay there forever. If the refugee is also never allowed to go to one of the previously visited countries, he/she must eventually stop somewhere. So, an honest refugee will never be able to leave his/her country of origin. (S. N. Artemov and Beklemishev 2005)

Before we can give a formal definition of the function φ, we will have to introduce some notation. First of we will let ψ be an arbitrary partial recursive function with the following Σ_1 graph: $\tau v_0 v_1$. From this graph we can obtain the following Σ_2 formula:

$$\exists v_0 \forall v_1 > v_0 : \tau v_1 v$$

Which says that ψ has limit v. We will abbreviate this as $L_\tau = L$. We will use this notation to define φ in the following way:

$$\varphi(v_0) = v_1 \leftrightarrow \begin{pmatrix} (v_0 = \overline{0} \wedge v_1 = \overline{0}) \vee \\ (v_0 > \overline{0} \wedge Prov(v_0, \ulcorner L \neq \dot{v}_1 \urcorner) \wedge \varphi(v_0 \dot{-} \overline{1}) \overline{R} v_2) \vee \\ (v_0 > \overline{0} \wedge \forall v_2 \leq v_0 \neg (Prov(v_0, \ulcorner L \neq v_2 \urcorner)) \wedge \overline{\varphi}(v_0 \dot{-} \overline{1}) \overline{R} v_2 \wedge \\ v_1 = \overline{\varphi}(v_0 - \overline{1})) \end{pmatrix}$$

We will define the graph $\tau v_0 v_1 = \exists v_3 \zeta v_3 v_0 v_1$ of the partial recursive function φ. Since we have that the graph of φ is Σ_1 we have that the graph τ is also Σ_1 and thus the graph ζ is Δ_0. We will define a formula $\Xi(\zeta)$ as the disjunction of the following three formulas:

1. $v_0 = \overline{0} \wedge v_1 = \overline{0}$
2. $v_0 > \overline{0} \wedge \mathrm{Prov}(v_0, \ulcorner L_\tau \neq v_1 \urcorner) \wedge \exists v_4 (\tau(v_0 \dot{-} \overline{1}, v_4) \wedge v_4 \overline{R} v_1)$

3. $v_0 > \overline{0} \wedge \exists v_3 v_4 \forall v_2 \leq v_0 \neq (\text{Prov}(v_0, \ulcorner L_\tau \neq v_2 \urcorner) \wedge \chi(v_3, v_0 - \overline{1}, v_4) \wedge v_4 \overline{R} v_1)$ $\wedge \tau(v_0 - \overline{1}, v_1)$

Thus we have that the set $\Xi(\zeta)$ can be seen as a primitive recursive function of $\ulcorner \zeta \urcorner$; i.e we have:

$$\ulcorner \Xi(\zeta) \urcorner = \vartheta(\ulcorner \zeta \urcorner)$$

Since primitive functions are recursive we have by the Recursion Theorem that we can pick an n such that $\varphi_{\vartheta(n)} = \varphi_n$. Now set $\varphi = \varphi_n$. This definition of φ is rather involved. But we have defined φ by its own graph, and avoided the imperant circularity by using the recursion theorem to not rely on the graph.

We further define the relation $\overline{R}$ by listing all pairs $(x, y) \in R$ (We can do this since the set R is finite) and then define:

$$v_0 \overline{R} v_1 : \bigvee_{(x,y) \in R} (v_0 = \overline{x} \wedge v_1 = \overline{y})$$

Thus we have that φ have the following properties:

1. $\varphi(0) = 0$
2. If $x + 1$ proves that $L \neq \overline{z}$ and we have that $\varphi(x) R z$, then $\varphi(x + 1) = z$
3. Else we have that $\varphi(x + 1) = \varphi(x)$

Further it is a total function since it is defined by recursion, and this can be proven in **PRA**.

Proposition 6.4 Let ξ be the Σ_1-formula that defines the graph of φ. Then:

$$\textbf{PRA} \vdash \forall v_0 \exists ! v_1 \xi v_0 v_1$$

Proof. The uniqueness of v_1 is given by the definition of φ. The existence of a value is given by induction on v_0 in the Σ_1 formula $\exists v_1 \xi v_0 v_1$ in **PRA**, and thus this induction is possible in **PRA**.

Base step: When $v_0 = 0$ we have that $\xi(0) = 0$ by definition of φ; i.e $\exists v_1 \xi v_0 v_1$, where $v_1 = 0$.

Induction step: Assume that $\exists v_1 \psi v_0 v_1$ holds for $v_0 = n$, i.e we have a $v_1 = m$ such that $\varphi(n) = m$. Look at $\varphi(n + 1)$, then if $n + 1$ proves that $L_\psi \neq \overline{z}$ and we have that $\varphi(n) R z$, then we will have that $\varphi(n + 1) = z$, i.e $v_1 = z$ otherwise we will have that $\varphi(n + 1) = \varphi(n) = m$, and the induction is done. ⊣

Further we will expand the langauge with a new function constant (This can be done, since ξ is the graph of a total function) $\overline{\varphi}$ with the following defining axiom:

$$\overline{\varphi}(v_0) = v_1 \leftrightarrow \xi(v_0) = v_1$$

We will now prove and state a few lemmas about the function φ and the limit of this function $L_\tau = L$. These will build up the proof of Solovay's First Completeness Theorem. Thus we will use the function φ and the limit L to deduce the theorem

{lem:2}

Lemma 6.5 The following three statements holds:

1. $\mathbf{PRA} \vdash \forall v_0(\overline{\varphi} v_0 \leq \overline{n})$

2. For all $x \in \omega$ we have that:

$$\mathbf{PRA} \vdash \forall v_o(\overline{\varphi} v_0 = \overline{x} \rightarrow \forall v_1 > v_0(\overline{\varphi} v_1 = \overline{x} \vee \overline{x}\overline{R}\overline{\varphi} v_1))$$

3. $\mathbf{PRA} \vdash \exists v_0 v_1 \forall v_2 > v_0(\overline{\varphi} v_2 = v_1)$.

Where (3) just means that $\mathbf{PRA} \vdash \exists v_1(L = v_1)$.

Proof. We will prove each part separately

1. We will prove this part by induction.

   Base case: $\varphi(0) = 0 \leq n$ is is clearly true.

   Induction step: Assume that $\varphi(x) \leq n$ is true.Then we have that $\varphi(x+1)$ is in the range of φ and this $\leq n$ or we have that $\varphi(x+1) \leq n$ so the induction is complete.

2. We will start of by write the formula we have to prove as the following equivalent formula:

$$\forall v_1 \forall v_0(\overline{\varphi} v_0 = \overline{x} \rightarrow \varphi(v_0 + v_1 + \overline{1}) = \overline{x} \vee \overline{x}\overline{R}\overline{\varphi}(v_0 + v_1 + 1))$$

   To prove this we will use induction on v_1. This is an induction on a Π_1 formula; which is a possible induction for **PRA** by Propostion 3.7

   Base case: if $v_1 = 0$ then clearly we have that $\varphi(v_0+1) = \overline{x}$ or $\overline{x}\overline{R}\overline{\varphi}(v_0+1)$ by the definition of φ.

   Induction step: Assume that it holds for $v_1 = n-1$, i.e that we for all v_0 have that:

$$\varphi(v_0 + \overline{n}) = \overline{x} \text{ or } \overline{x}\overline{R}\overline{\varphi}(v_0 + \overline{n})$$

   We will split the rest of this proof up in two parts; one where the first disjunct is true, and one where the second is true.

   The first disjunct is true:. Assume that both $v_0 + n + 1$ codes a proof that $L \neq z$ and $\varphi(v_0 + \overline{n})Rz$ is true. This means that $\varphi(v_0 + \overline{n} + 1) = z$. But this is just that $x\overline{R}\varphi(v_0 + \overline{n} + 1)$, and the lemma is true in this case. If these assumptions are not true, we will then have that $\varphi(v_0+\overline{n}+1)=\varphi(v_0+\overline{n})$. But then we have that $\varphi(v_0+\overline{n}+1)=\overline{x}$, and the lemma holds.

The second disjunct is true: We will again start of by assuming that $L\neq z$ and $\varphi(v_0+n)Rz$; i.e $\varphi(v_0+n+1)=z$. We then get that $\varphi(v_0+n)R\varphi(v_0+n+1)$ and by the transitivity of R we get: $x\overline{R}\varphi(v_0+n+1)$. If we otherwise have that $\varphi(v_0+n)=\varphi(v_0+n+1)$ we clearly have that $\overline{x}\overline{R}\varphi(v_0+n+1)$.

3. Here we will first prove the following:

$$\forall v_0(\exists v_1(\overline{F}v_1=v_0)\rightarrow\exists v_1(L=v_1))$$

This is clearly true for $v_0>n$. For $v_0\leq n$ we will use induction on the converse of R. By 2) from this lemma it holds for maximal nodes y in W. If y is not a maximal note and $\exists v_1(\overline{\varphi}(v_1)=\overline{x})$ then again by 2) we either get that $L=\overline{x}$ or that for some y such that xRy: $\exists v_1(\overline{\varphi}(v_1)=\overline{y})$, and the induction hypothesis gives us that $\exists v_1(L=v_1)$. But since the set W is finite we will end up with getting:

$$\mathbf{PRA}\vdash\exists v_1(\overline{\varphi}(v_1)=\overline{0})\rightarrow\exists v_1(L=v_1)$$

But we have that $\mathbf{PRA}\vdash\overline{\varphi}(\overline{0})=\overline{0}$ so clearly: $\mathbf{PRA}\vdash\exists v_1(L=v_1)$

$\dashv$

The induction in the above proof was not done inside of **PRA**, but was done as metamathematical induction outside of **PRA**. This done because the formula $\exists v_1(L=v_1)$ is Σ_2 and thus we can not use induction on this formula inside of **PRA**.

{cor:disjunct}

Corollary 6.6 $\mathbf{PRA}\vdash L\leq\overline{n}$, i.e $\mathbf{PRA}\vdash\bigvee_{x\leq n}L=\overline{x}$

Proof. By lemma 6.5 part 1) and 3) and the following implication:

$$\mathbf{PRA}\vdash v\leq\overline{n}\rightarrow\bigvee_{x\leq n}v=\overline{x}$$

The corollary follows. $\dashv$

Remark 6.7 In the rest of this section we will use the notation $\mathrm{Con}_{\mathbf{PRA}+F}$ where F is a formula of **PRA**. This notation is just shorthand for "**PRA** plus the formula F is consistent".

{lem:4}

Lemma 6.8 For all $x,y\leq n$ we have that:

1. $L = \overline{x} \wedge \overline{x}\overline{R}\overline{y} \to \mathrm{Con}_{\mathbf{PRA}+L=\overline{y}}$

2. $\mathbf{PRA} \vdash L = \overline{x} \wedge \overline{x} \neq \overline{y} \wedge \neg(\overline{x}\overline{R}\overline{y}) \to \neg\mathrm{Con}_{\mathbf{PRA}+L=\overline{y}}$

3. $\mathbf{PRA} \vdash L = \overline{x} \wedge \overline{x} > \overline{0} \to \mathrm{Pr}(\ulcorner L \neq \overline{x} \urcorner)$

Proof. We will prove each statement separately:

1) Let xRy and assume for contradiction that $L = \overline{x} \wedge \mathrm{Pr}(\ulcorner L \neq \overline{y} \urcorner)$. Since we have that $L = \overline{x}$ we can chose a v_0 such that $\forall v_2(v_2 > v_0 \to \overline{F}v_2 = \overline{x})$ and we can also chose $v_1 + \overline{1} > v_0$ such that $\mathrm{Prov}(v_1 + \overline{1}, \ulcorner L \neq \overline{y} \urcorner)$ But we also have the following:

$$\mathbf{PRA} \vdash \mathrm{Prov}(v_1 + \overline{1}, \ulcorner L \neq y \urcorner) \wedge \overline{F}v_1 = \overline{x_1, \ldots, x_n} \wedge \overline{x}\overline{R}\overline{y} \to \overline{F}(v_1 + \overline{1}) = \overline{y}$$

This contradicts with $\forall v_2 > v_0(\overline{F}v_0 = \overline{x})$ which came from the assumption that $L = \overline{x}$ so we con conclude:

$$\mathbf{PRA} \vdash L = \overline{x} \wedge \overline{x}\overline{R}\overline{y} \to \neg\mathrm{Pr}(\ulcorner L \neq \overline{y} \urcorner)$$

Where we have that $\neg\mathrm{Pr}(L \neq \overline{y})$ is equivalent to $\mathrm{Con}_{\mathbf{PRA}+L=\overline{y}}$ and 1) follows.

2) By demonstrable Σ_1 completeness 3.11 we can do the following deduction:

$$\mathbf{PRA} \vdash L = \overline{x} \to \exists v_0(\overline{F}v_0 = \overline{x}) \tag{6.1}$$

{eq:21}
$$\to \mathrm{Pr}(\ulcorner \exists v_0(\overline{F}v_0 = \overline{x}) \urcorner) \tag{6.2}$$

Further we have from lemma 6.5.2 and D2 that:

$$\mathbf{PRA} \vdash \forall v_0(\overline{F}v_0 = \overline{x} \to (L = \overline{x} \vee \overline{x}\overline{R}L)) \tag{6.3}$$

{eq:22}
$$\mathbf{PRA} \vdash (\ulcorner \forall v_0(\overline{F}v_0 = \overline{x} \to (L = \overline{x} \vee \overline{x}\overline{R}L)) \urcorner) \tag{6.4}$$

From 6.2 and 6.4 we have the following:

{eq:23}
$$\mathbf{PRA} \vdash L = \overline{x} \to \mathrm{Pr}(\ulcorner L = \overline{x} \vee \overline{x}\overline{R}L \urcorner) \tag{6.5}$$

The following statement is also clearly true by demonstrable Σ_1 completeness:

$$\mathbf{PRA} \vdash \overline{x} \neq \overline{y} \wedge \neg(\overline{x}\overline{R}\overline{y}) \to \mathrm{Pr}(\ulcorner \overline{x} \neq y \wedge \neg(\overline{x}\overline{R}\overline{y}) \urcorner)$$

This with 6.5 gives us:

$$\mathbf{PRA} \vdash L = \overline{x} \wedge \overline{x} \neq \overline{y} \wedge \neg\overline{x}\overline{R}\overline{y} \to \mathrm{Pr}(\ulcorner L = \overline{x} \vee \overline{x}\overline{R}L \urcorner) \wedge \mathrm{Pr}(\ulcorner \overline{x} \neq \overline{y} \wedge \neg\overline{x}\overline{R}\overline{y} \urcorner)$$

From which we can deduce:

$$\mathbf{PRA} \vdash L\overline{x} \wedge \overline{x} \neq \overline{y} \wedge \neg\overline{x}\overline{R}\overline{y} \rightarrow \Pr(\ulcorner L \neq \overline{y} \urcorner)$$

Which gives us 2)

3) From the least number principle we have that:

$$\mathbf{PRA} \vdash L = \overline{x} \wedge \overline{x} > \overline{0} \rightarrow \exists v(\overline{\varphi}(v + \overline{1}) = \overline{x} \wedge \overline{\varphi}v \neq \overline{x})$$

By the definition of φ we have for such a v the following:

$$\mathbf{PRA} \vdash \overline{\varphi}(v + \overline{1}) = \overline{x} \wedge \overline{\varphi}v \neq \overline{x} \rightarrow \text{Prov}(v + \overline{1}, \ulcorner L \neq \overline{x} \urcorner)$$

And thus we have the following:

$$\mathbf{PRA} \vdash L = \overline{x} \wedge \overline{x} > \overline{0} \rightarrow \Pr(\ulcorner L \neq \overline{x} \urcorner)$$

$\dashv$

Lemma 6.5 and 6.8 gives us a few of the facts that we need about L and φ; at least the facts about them that we can prove in **PRA**. We will also need the following result, which cannot be proven in **PRA**.

{lem:5}

Lemma 6.9 The following two statements are true, but they cannot be proven in **PRA**.

1. $L = \overline{0}$

2. For $0 \leq x \leq n$ we have that $\mathbf{PRA} + L = \overline{x}$ is consistent.

Proof. **1)** By lemma 6.5.3 the limit L exists. If $x > 0$ we have by lemma 6.8 that:

$$\begin{aligned} L = \overline{x} &\Rightarrow \mathbf{PRA} \vdash L \neq \overline{x} \\ &\Rightarrow L \neq \overline{x} \end{aligned}$$

Since **PRA** is sound. But this is a contradiction and we must conclude that $L = 0$.

2) Since we have that $L = \overline{0}$ is true and we have that **PRA** is sound, we have that $\mathbf{PRA} + L = \overline{0}$ is consistent. For $x > 0$ we will apply lemma 6.8.1 and get:

$$\mathbf{PRA} \vdash L = \overline{0} \wedge \overline{0}\overline{R}\overline{x} \rightarrow \text{Con}_{\mathbf{PRA}+L=\overline{x}}$$

We have that the antecedent is true and hence that $\text{Con}_{PRA+L=\overline{x}}$ is true, which proves this part of the lemma. $\dashv$

We have now shown all the important basic properties that φ and L holds. In the next part of the proof we will simulate the Kripke model $\mathcal{K} = \langle W, R, \phi \rangle$, where $1 \notin \phi(\alpha)$. For this end we will let $L = \overline{x}$, for $x > 0$, assume the rule nodes of $W = \{1, \dots n\}$. We will start of by defining the interpretation *. So for any p let:

$$p^* = \bigvee \{L = \overline{x} : 1 \leq x \leq n \text{ and } x \in \phi(p)\}$$

If this disjunction is empty, we will set it to be $\overline{0} = \overline{1}$. Further we are only interested the sentence α; i.e the set:

$$S(\alpha) = \{\beta : \ \beta \text{ is a subformula of } \ \alpha\}$$

We will not look at $p \notin S(\alpha)$

The following lemma is the crucial result about this interpretation, and the theorem will follow easily from this result:

{lem:10}

Lemma 6.10 Let $1 \leq x \leq n$. For any β and * as defined just above we have that:

1. $x \in \phi(\beta) \Rightarrow \mathbf{PRA} \vdash L = \overline{x} \to \beta^*$
2. $x \notin \phi(\beta) \Rightarrow \mathbf{PRA} \vdash L = \overline{x} \to \neg\beta^*$

Proof. We will use induction on complexity of ψ. If $\beta = p$, then since $L = \overline{x}$ is a disjunct of p^* we get:

$$x \in \phi(\varphi) \Rightarrow \mathbf{PRA} \vdash L = \overline{x} \to p^*$$

Which proves 1, for ψ atomic. For 2 observe that if $x \notin \phi(p)$, then $L = \overline{x}$ contradicts all the disjuncts of p^* and thus:

$$x \notin \phi(p) \to \mathbf{PRA} \vdash L = \overline{x} \to \neg p^*$$

The cases where ψ is $\neg\gamma, \gamma \wedge \sigma, \gamma \vee \sigma$ and $\gamma \to \sigma$ are trivial. So we will just look at the case where $\psi = \Box\gamma$. Here we make the following deductions:

$$\begin{aligned}
x \in \phi(\Box\gamma) &\Rightarrow \forall y(xRy \Rightarrow y \in \phi(\gamma)) \\
&\Rightarrow \forall(xR \Rightarrow \mathbf{PRA} \vdash L = \overline{y} \to \gamma^*) \\
&\Rightarrow \bigwedge_{xRy} (\mathbf{PRA} \vdash L = \overline{y} \to \gamma^*) \\
&\Rightarrow \mathbf{PRA} \vdash \bigvee_{xRy} L = \overline{y} \to \gamma^* \\
&\Rightarrow \mathbf{PRA} \vdash \Pr(\ulcorner \textstyle\bigvee_{xRy} L = \overline{y} \urcorner) \to \Pr(\ulcorner \gamma^* \urcorner)
\end{aligned}$$

And by the last line we can get the following by using the axioms of **GL**

{eq:1} $$x \in \phi(\Box\gamma) \Rightarrow \mathbf{PRA} \vdash \mathrm{Pr}(\ulcorner \textstyle\bigvee_{xRy} L = \overline{y} \urcorner) \to \mathrm{Pr}(\ulcorner \gamma^* \urcorner) \tag{6.6}$$

We can now invoke lemma 6.9 2 and 3 and get:

$$\mathbf{PRA} \vdash L = \overline{x} \to \bigwedge_{\neg(xRz)} \mathrm{Pr}(\ulcorner L \neq z \urcorner) \tag{6.7}$$ {eq:2}

and therfore we have that:

$$\mathbf{PRA} \vdash L = \overline{x} \to \mathrm{Pr}(\ulcorner \textstyle\bigvee_{xRy} L = \overline{y} \urcorner) \tag{6.8}$$ {eq:3}

Now by 6.6 and 6.8 we get that:

$$\begin{aligned} \vdash_x \Box\gamma &\Rightarrow \mathbf{PRA} \vdash L = \overline{x} \to \mathrm{Pr}(\ulcorner\ \gamma^* \urcorner) \\ &\Rightarrow \mathbf{PRA} \vdash L = \overline{x} \to (\Box\gamma)^* \end{aligned}$$

I.e we have proven part 1 of the lemma. Similarly we can do the following deduction:

$$\begin{aligned} x \notin \phi(\Box\gamma) &\Rightarrow \exists y(xRy \wedge y \notin \phi(\gamma)) \\ &\Rightarrow \exists y(xRy \wedge \mathbf{PRA} \vdash L = \overline{y} \to \neg\gamma^*) \\ &\Rightarrow \exists y(xRy \wedge \mathbf{PRA} \vdash \gamma^* \to L \neq \overline{y}) \\ &\Rightarrow \exists y(xRy \wedge \mathbf{PRA} \vdash \mathrm{Pr}(\ulcorner \gamma^* \urcorner) \to \mathrm{Pr}(\ulcorner L \neq \overline{y} \urcorner) \end{aligned}$$

But by lemma 6.9 we get that if xRy:

$$\mathbf{PRA} \vdash L = \overline{x} \to \neg\mathrm{Pr}(\ulcorner L \neq \overline{y} \urcorner)$$

all in all this gives us:

$$\mathbf{PRA} \vdash L = \overline{x} \to \neg\mathrm{Pr}(\ulcorner \gamma^* \urcorner)$$

Which is just just the following we where trying to show:

$$\mathbf{PRA} \vdash L = \overline{x} \to \neg(\Box\gamma)^*$$

$\dashv$

We can now finally prove Solovay's first completeness theorem:

Proof of Solovay's first completeness theorem. By lemma 6.10 we have that

$$1 \notin \phi(\alpha) \Rightarrow \mathbf{PRA} \vdash L = \overline{1} \to \neg\alpha^*$$

But by lemma 6.9 we have that $\mathbf{PRA} + L = 1$ is consistent, from which it follows that $\mathbf{PRA} + \neg\alpha^*$ is consistent; so α^* is not a theorem af **PRA** and thus we have: $\mathbf{PRA} \nvdash \alpha^*$ and the theorem follows by contraposition. ⊣

With this proof we can give a interpretation of the set W and relation R in a model of **GL**. The set W consists of recursively axiomitized extensions of **PRA**. And we have that $w_1 R w_2$ if and only if $w_1 \vdash \mathrm{Con}(w_2)$, i.e the theory w_1 has the consistency of theory w_2 as one of its theorems. It is clear that this relation is transitive and conversely well-founded.

Lastly we can give an uniform version of Solovay's first completeness theorem:

Theorem 6.11 There is an arithmetical interpretations * such that for each modal formula α we have that:

$$\mathbf{PRA} \vdash \alpha^* \text{ iff } \vdash_{\mathbf{GL}} \alpha$$

The proof of this will be left out.

6.4 The Second Theorem

{chap:second}

Solovay's Second Completeness Theorem is a strengthening of the first one, since it tells about trueness of a formulae α^* in the standard model $\mathcal{N} = \langle \omega, +, \cdot \rangle$ of arithmetic. The proof will follow that of the first theorem, but we will look at the modal logic **GLS** instead of the modal logic **GL**.

Theorem 6.12 For all modal sentences α, the following is equivalent:

1. $\mathbf{GLS} \vdash \alpha$
2. $\mathbf{GL} \vdash \bigwedge_{\Box\beta \in S(\alpha)} (\Box\beta \to \beta) \to \alpha$
3. α is true in all α-reflexive FT Kripke models
4. $\forall^*(\alpha^* \text{ is true})$

Some parts of this theorem has already been proven. We have (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3) by theorem 4.20. The implication (1) $\Rightarrow$ (4) is true since, if α is a theorem of **GL** it is also a theorem of **PRA**, and thus it is true in $\mathcal{N}$. Further since every theorem of **PRA** is true in $\mathcal{N}$, then for every formula F of arithmetic, if $\mathrm{Pr}(F)$ is true then

F is a theorem and thus is true. This means that for every interpretation * and modal formula α that $(\Box\alpha \to \alpha)^*$ is true. So we just have to prove (4) $\Rightarrow$ (3)

For proving (4) $\Rightarrow$ (3) we will again make use of contraposition. Let $\mathcal{K} = \langle(1,\ldots,n), R, \phi)\rangle$ be given and let 1 be the root. Further let α be such that $1 \notin \phi(\alpha))$. We will assume that $\mathcal{K}$ is α-reflexive. This means that we have: $1 \in \phi(\Box\beta \to \beta)$ for all $\beta \in S(\alpha)$

We will set $0Rw$ for all $w \in W$. We will now create a new model $\mathcal{K}'$ where we have added 0, so in this proof it is part of the pointed Kripke model we will look at. We will create this new model in the following way:

$W' = \{0, 1\ldots,n\}$

R' extends R by assuming that $0R'x$ for all $x \in W$

$\alpha_0 = 0$

ϕ' extends ϕ by putting $0 \in \phi'(p)$ iff $1 \in \phi(p)$ for all $p \in S(\varphi)$

We will abuse notation and let R denote R', ϕ denote ϕ' and $\vDash$ denote $\vDash^{\mathcal{K}'}$. The following lemma is a special case of Lemma 4.24.

Lemma 6.13 For all $\beta \in S(\alpha)$ we have that:

$$\vDash_0 \beta \text{ iff } \vDash_1 \beta$$

This is the same as:

$$0 \in \phi(\beta) \text{ iff } 1 \in \phi(\beta)$$

We can see the modal $\mathcal{K}'$ as a derived model of $\mathcal{K}$, so it makes sense to invoke the lemma here.

We will now define a function φ in the same way as before.

$$\varphi(0) = 0$$
$$\varphi(x+1) = \begin{cases} y & \text{Prov}(\overline{x}+\overline{1}, \ulcorner L \neq \overline{y} \urcorner) \wedge xRy \\ \varphi(x) & \text{else} \end{cases}$$

All the Lemmas about φ and L still holds, since the function φ is only determined by the frame $\langle W, R\rangle$ and not the Kripke model that we are looking at. But the behavior of ϕ has changed, since we must added the node 0 and we can only use sub formulas of α. So we define:

$$p^* = \bigvee\{L = \overline{x} : 0 \leq x \leq n \wedge x \in \phi(p)\}$$

For $p \in S(\alpha)$ and let p^* be random for all p's that is not a subformula of α. We now prove and state the following lemma is analogies to lemma 6.9:

Lemma 6.14 Let $0 \leq x \leq n$. For any $\beta \in S(\alpha)$ and * as defined above we have:

1. $x \in \phi(\beta) \Rightarrow \mathbf{PRA} \vdash L = \overline{x} \rightarrow \beta^*$
2. $x \notin \phi(\beta) \Rightarrow \mathbf{PRA} \vdash L = \overline{x} \rightarrow \neg\beta^*$

Proof. For $0 < x$ the proof is identical to the proof of Lemma 6.10. So we will only prove the case where $x = 0$. The is again an induction on the complexity of β. We will only prove the cases where $\beta = \Box\gamma$.

Let $\beta = \Box\gamma$. We then have:

$$\begin{aligned} 0 \in \phi(\Box\gamma) &\Rightarrow \forall x(1 \leq x \leq n \Rightarrow x \in \phi(\gamma)) \\ &\Rightarrow \forall x(1 \leq x \leq n \Rightarrow \mathbf{PRA} \vdash L = \overline{x} \rightarrow \gamma^*) \end{aligned}$$

Since $x > 1$ and this case of the lemma has been proven, when we proved the lemma for the first completeness theorem. We can also make the following deduction by the induction hypothesis:

$$\begin{aligned} 0 \in \phi(\Box\gamma) &\Rightarrow 1 \in (\gamma) \\ &\Rightarrow 0 \in \gamma) \\ &\Rightarrow \mathbf{PRA} \vdash L = \overline{0} \rightarrow \gamma^* \end{aligned}$$

By combing these two we get:

$$\begin{aligned} 0 \in \phi(\Box\gamma) &\Rightarrow \bigwedge_{x \leq n} (\mathbf{PRA} \vdash L = \overline{x} \rightarrow \gamma^*) \\ &\Rightarrow \mathbf{PRA} \vdash (\bigvee_{x \leq n} L = \overline{x}) \rightarrow \gamma^* \\ &= \mathbf{PRA} \vdash \mathrm{Pr}(\ulcorner \bigvee L = \overline{x} \urcorner) \rightarrow \mathrm{Pr}(\ulcorner \gamma^* \urcorner) \end{aligned}$$

But by Corollary 6.6 we have that $\mathbf{PRA} \vdash \bigvee L = \overline{x}$ and thus $\mathbf{PRA} \vdash \mathrm{Pr}(\ulcorner \bigvee L = \overline{x} \urcorner)$ so all in all we have:

$$\begin{aligned} 0 \in (\Box\gamma) &\Rightarrow \mathbf{PRA} \vdash \mathrm{Pr}(\ulcorner \gamma^* \urcorner) \\ &\Rightarrow \mathbf{PRA} \vdash L = \overline{0} \rightarrow \mathrm{Pr}(\ulcorner \gamma^* \urcorner) \end{aligned}$$

This proves (1). The proof of (2) is a bit easier. We have:

$$\begin{aligned} 0 \notin \phi(\Box\gamma) &\Rightarrow \exists x(1 \leq x \leq n \wedge x \notin \phi(\gamma)) \\ &\Rightarrow \exists x(1 \leq x \leq n \wedge \mathbf{PRA} \vdash L = \overline{x} \rightarrow \neg\gamma^*) \\ &\Rightarrow \exists x(1 \leq x \leq n \wedge \mathbf{PRA} \vdash \gamma^* \rightarrow L \neq \overline{x}) \\ &\Rightarrow \mathbf{PRA} \vdash L = \overline{0} \rightarrow \neg\mathrm{Pr}(\ulcorner \gamma^* \urcorner) \end{aligned}$$

And thus by Lemma 6.8 we have that $\mathbf{PRA} \vdash L = \overline{0} \to \neg\mathrm{Pr}(\ulcorner L \neq \overline{x} \urcorner)$ for $x > 0$ $\dashv$

We thus have that $L = \overline{0}$ is true, and we can now finally prove the second completeness theorem:

Proof of the Second Completeness theorem. Assume that α is false in $\mathcal{K}$ i.e $1 \notin \phi(\alpha)$. Then by the just proven lemma we get $0 \notin \phi(\alpha)$ and the just proven lemma gives:

$$\mathbf{PRA} \vdash L = \overline{0} \to \neg\alpha^*$$

Since we have that $L = \overline{0}$ is true we then get $\neg\alpha^*$ which just means that α^* is false. $\dashv$

Having proved the Second Completeness Theorem, we will in the next section look at a use of it.

6.4.1 Using the Second Completeness Theorem

We can use the second completeness theorem to prove the following theorem named after Rosser:

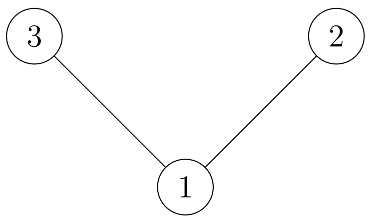
Theorem 6.15 There is a arithmetical sentences F such that:

1. $\mathbf{PRA} \nvdash F$
2. $\mathbf{PRA} \nvdash \neg F$
3. $\mathbf{PRA} \vdash \mathrm{Con} \to \neg\,\mathrm{Pr}(\ulcorner F \urcorner)$
4. $\mathbf{PRA} \vdash \mathrm{Con} \to \neg\mathrm{Pr}(\ulcorner \neg F \urcorner)$

Proof. We define the following pointed Kripke model:

$$\mathcal{K} = \langle \{1, 2, 3\}, \{(1, 2), (1, 3)\}, \{(1, p), (2, p)\}, 1 \rangle$$

it can be visualized by the following graph: Where p is true in world 2. We will



further let α be the following formula:

$$\neg\Box p \wedge \neg\Box\neg p \wedge \Box(\neg\Box\bot \rightarrow \neg\Box p \wedge \neg\Box\neg p)$$

We have that α is true in $\mathcal{K}$. Since we have that:

1. $1 \in \phi(\neg\Box p)$ since we have that $1R3$ and that $3 \notin \phi(p)$
2. $1 \in \phi(\neg\Box\neg p)$ since we have that $1R2$ and that $2 \in \phi(p)$
3. $1 \in \phi(\Box(\neg\Box\bot \rightarrow \neg\Box p \wedge \neg\Box\neg p)$ since we have that $2, 3 \in \phi(\Box\bot)$

It can be shown that this model is α-reflexive; the proof of this can be found in (Smorynski 1985). $\dashv$

This result can be strengthened and it can be shown that the found formula is actually Σ_1. This result can also be found in (Smorynski 1985). This result shows that Solovay's second theorem is a tool we can use to prove some results about incompleteness of **PRA**, in a way where we "just" construct a Kripke model of **GL** with the correct properties.

6.5 Generalisations of the Completeness Theorems

In this section we have shown the Solovay's Completeness Theorems for **PRA**. But these theorems holds for a much wider class of fragments of Peano Arithmetics. It can be shown that the theorem holds for theories **T** that fulfills the following to conditions:

1. **T** extends $I\Delta_0 + \mathrm{EXP}$
2. Let $F(x)$ be Δ_0 formula, then **T** does not prove any false sentences of the form $\exists x F(x)$

This proof does not use the Recursion theorem for creating the function φ, but instead uses the diagonalization lemma. The proof of this will not this will not be given here, but it can be found in (Jongh, Jumelet, and Montagna 1991). This generalization shows that **GL** axiomatize a very big range of different fragments of arithetmics; i.e the proof predicate in all of these fragments behaves in the same way, as we have that the proof predicate of **PRA**do.

It is not known if Solovay's theorems holds for weaker conditions than $I\Delta_0 +$ EXP; i.e we do not know if it holds for example for the theory $I\Delta_0 + \Omega_1$.

Solovay's theorems can also be proven for some fragments without the use of fixed points. The two different proof strategies seen so fair each uses fixed points.

Either by using the recursion theorem or by using the digitalization theorem for a given arithmetic theory. Fedor Pakhomov has proven the theorems without the use of the fixed point lemma or the recursion theorem in (Pakhomov 2017). This newer proof might be able to giver a specific lower bound on the strength of the fragments Solovays theorems holds for.

6.6 Concluding remarks: Implications of Solovay's Theorems

The clearest implication of the generalized versions of Solovay's Completeness Theorems is that the proof predicate of arithmetics can be axiomatized; everything there is to say about the predicate, can be deduced from the derivability conditions and Löb's theorem. This can be seen both as a positive and negative result. Positive since the proof predicate follows some simple rules and these rules does not alter even though you add more induction to the fragment of arithmetics you are working with. The last point can also be seen as a negative one; there is no way to differentiate the different fragments of arithmetics by looking at their proof predicate, since the proof predicates are all axiomatized by the same modal logic.

Further the proportional provability logic is not effected by Quines critique of modal logic as being unintelligible, since it has a very clear and unambiguous arithmetic interpretation. This sets it apart from the more philosophical interpretations of modal logic, since these interpretations do not have a clear meaning in a mathematical system.

Lastly the theorems also show that modal logic can be interesting for mathematicians that are not interested in the philosophical part of logic. The theorems shows that modal logic can be used to get further knowledge about mathematical systems and it can probably be used in other areas of mathematics. Modal logic also have some uses in both topology and set theory (S. Artemov 2007).

7 Further Results in Provability Logic

{chap:Further}

In this chapter we will enrich the language $\mathcal{L}_\Box$ with both more modal operators and quantifiers. For these language a number of different results can be proven. We will also state some results about provability logic where we enrich our language $\mathcal{L}_\Box$ with quantifiers. In the case with more modal operators the results will be positive; i.e there are versions of Solovay's completeness theorems for these kinds of modal logic. But in the case where we enrich our language with quantifiers our results will be negative; i.e we cant prove versions of Solovay's completeness theorems for these kinds of modal logic.

This chapter will skip the most of the proofs of these results, but the proofs can be found in (George S. Boolos 1993). The part about multi-modal logic will also be more explained more in depth than the part about the quantified modal logic.

7.1 Multi-modal provability logic

We can extend our language $\mathcal{L}_\Box$ with more modality operators. We will start of by extending it with the modal operator: $\boxed{1}$ and its dual $\langle 1 \rangle$. In the next subsection it will be explained what we will mean with the $\boxed{1}$. Latter on we will extend the language with even more modal operators.

7.1.1 The system GLB

Definition 7.1 We will say that a arithmetical theory $\mathbf{T}$ is ω-inconsistent iff for some formula $\alpha(x)$, $\mathbf{T} \vdash \exists x \alpha(x)$ and for every $n \in \omega$ we have: $\mathbf{T} \vdash \neg\alpha(x)$. $\mathbf{T}$ is called ω-consistent iff it is not ω-inconsistent. $\dashv$

We have that if $\mathbf{T}$ is ω-consistent then $\mathbf{T} \nvdash \exists x x \neq x$ and thus $\mathbf{T}$ is consistent. So ω-consistency implies consistency; but the converse does not hold.

Definition 7.2 A sentence α is ω-inconsistent in $\mathbf{T}$ if the axioms of $\mathbf{T}$ plus α is ω-inconsistent. α is ω-consistent iff it is not ω-inconsistent.

We further say that a sentence α is ω-provable in $\mathbf{T}$ iff $\neg\alpha$ is ω-inconsistent with $\mathbf{T}$. $\dashv$

It is clear that if α is provable in **T** then it is ω-provable in **T**. We will introduce a new modal system **GLB**, where **B** stands for bimodal, where we add two new modal operators: $\boxed{1}$and $\langle 1 \rangle$to our modal language $\mathcal{L}_\Box$. We will call this new language $\mathcal{L}_{\boxed{1}}$

Definition 7.3 The language $\mathcal{L}_{\boxed{1}}$ is the language $\mathcal{L}_\Box$ extend with the modal operator $\boxed{1}$, where the syntax $\boxed{1}$ is the same as that of $\Box$. The operator $\langle 1 \rangle$ is defined as the dual of $\boxed{1}$ $\dashv$

We now define the system of **GLB**. We will later on discuss the semantics of **GLB**, but this is not of important right now.

Definition 7.4 The axioms of **GLB** are all tautologies and all sentences of the following kind:

AB1 $\Box(\alpha \to \beta) \to (\Box\alpha \to \Box\beta)$

AB2 $\boxed{1}(\alpha \to \beta) \to (\boxed{1}\alpha \to \boxed{1}\beta)$

AB3 $\Box(\Box\alpha \to \alpha)\Box\alpha$

AB4 $\boxed{1}(\boxed{1}\alpha \to \alpha)\ \boxed{1}\alpha$

AB5 $\Box\alpha \to \boxed{1}\alpha$

AB6 $\neg\Box\alpha \to \boxed{1}\neg\Box\alpha$

The deduction rules are the following:

MP Modus ponens

Nec $\Box$ -necessitation; from α infer $\Box\alpha$.

$\dashv$

It is clear that $\boxed{1}$-necessitation is a rule of **GLB**, since we have that if **GLB** $\vdash \alpha$ then **GLB** $\vdash \Box$ and by AB5 we then have **GLB** $\vdash \boxed{1}\alpha$.

The next goal is to prove an arithmetical soundness theorem for **GLB**. For this end we need the following definition:

Definition 7.5 We call the following rule the *ω-rule*: Infer $\forall x\alpha(x)$ for all $\alpha(\overline{n})$, where $n \in \omega$. A sentence is provable under the ω-rule in **T** if it belongs to all classes containing the axioms of **T** and closed under MP, Nec and the ω-rule. We further say that a sentence F is provable in **PRA** by *one application of the ω-rule* if for some formula $G(x)$ we have that **PRA** $\vdash G(\overline{n})$ for all n and **PRA** $\vdash \forall x G(x) \to F$. $\dashv$

It can be shown that a sentence F is ω-provable if and only if it is provable by one application of the ω-rule. With this we can define the notion of an ω-proof.

Definition 7.6 A sentence $\forall x G(x) \to F$ is called an *ω-proof* prof of F if $\mathbf{PRA} \vdash G(\overline{n})$ for all n and $\mathbf{PRA} \vdash \forall x G(x) \to F$. $\dashv$

It is clear that if F has an ω-proof then it ω-provable.

We will state one last definition in the same vein as the others above:

Definition 7.7 $\mathbf{PRA}^+$ is the theory extending $\mathbf{PRA}$ with all sentences $\forall x G(x)$ such that for every $n \in \omega$ we have that $\mathbf{PRA} \vdash G(\overline{n})$. $\dashv$

The following theorem can then be proven about the relationships between the above definitions:

{thm:omega}

Theorem 7.8 The following are equivalent:

1. F is ω-provable.
2. $\mathbf{PRA}^+ \vdash F$.
3. F is provable by one application of the ω-rule.
4. There is an ω-proof of F.

We need a few more definitions before we can state the arithmetical soundness theorem for **GLB**:

Definition 7.9 Let $\omega\mathrm{Prov}(y, x)$ be the formula of **PRA** the formalizes that y is the code of an ω-proof of x, and let $\omega\mathrm{Pr}(x) = \exists y \omega\mathrm{Prov}(y, x)$ $\dashv$

We then have that $\omega\mathrm{Pr}(x)$ by theorem 7.8 is provable coextensive with the formulas stating in **PRA** the following properties: "ω-provable", "provable in $\mathbf{PRA}^+$ and "provable by one application of the ω-rule". This means that for each sentence F in **PRA** that we have:

$$\mathbf{PRA} \vdash \mathrm{Pr}(\ulcorner F \urcorner) \to \omega\mathrm{Pr}(\ulcorner F \urcorner)$$

With these results we can now extend the interpretation of $\mathcal{L}_{\Box}$ in **PRA** to one of $\mathcal{L}_{\boxed{1}}$:

Definition 7.10 An interpretation * of $\mathcal{L}_{\boxed{1}}$ in **PRA** is an extension of an interpretation $\mathcal{L}_{\Box}$ in **PRA** where we add the following:

$$\boxed{1}(\alpha)^* = \omega\mathrm{Pr}(\ulcorner \alpha^* \urcorner)$$

$\dashv$

We can now state the arithmetical soundness theorem for **GLB**:

Theorem 7.11 (The aritmetical soundness theorem for **GLB**) For any modal formula α and interpretation of $\mathcal{L}_{\boxed{1}}$ in **PRA** we have that:

$$\vdash_{\mathbf{GLB}} \alpha \rightarrow \ \mathbf{PRA} \vdash \alpha^*$$

We omit the proof here. We can not prove the arithmetical completeness theorem for **GLB** without the help of another multi modal logic.

This is because there is no good Kripke semantics for the logic **GLB**. We will start of by defining a Kripke modal for the logic **GLB**; this definitions is a extension of a "normal" frame, but with two relations instead of one

Definition 7.12 A frame for a modal logic with two modal operators is a triple $\mathcal{H} = \langle W, R, R_1 \rangle$ where both R and R_1 are relations on W. A model is a quadruple $\mathcal{K} = \langle W, R, R_1, \phi \rangle$ were ϕ is a valuation function on W. The truth of modal formula α in a given node $w \in W$ is defined in the obvious way, and the two main clauses of the definition is:

1. $\vdash_w^{\mathcal{K}} \Box\alpha$ iff for all $v \in W$ such that wRv we have $\vdash_v^{\mathcal{K}} \alpha$
2. $\vdash_w^{\mathcal{K}} \boxed{1}\,\alpha$ iff for all $v \in W$ such that wR_1v we have $\vdash_v^{\mathcal{K}} \alpha$

$\dashv$

The problem here for is that it can be shown, no matter what the relation R_1 will be the empty relation W and therefor $\boxed{1}\,\bot$ will be valid and thus contradict that $\vdash_{\mathbf{GLB}} \boxed{1}\,\bot$ from the arithmetical soundness of **GLB**. Giorgie Dzhaparidze found a way around this by looking at another multi modal logic, which will be introduced in the next section. His result was improved by Konstantin Ignatiev .

7.1.2 The system IDzh and completeness of GLB

Since **GLB** does not have any good Kripke semantic we will at a multi modal logic that has such a semantic; we will call this modal logic for **IDzh** Ignatiev and Dzhaparidze.

Definition 7.13 The language of **IDzh** is the same as **GLB**. Further the axioms of **IDzh** are all tautologies and the following modal formulas:

AI1 $\Box(\alpha \rightarrow \beta) \rightarrow (\Box\alpha \rightarrow \Box\beta)$

AI2 $\boxed{1}\,(\alpha \rightarrow \beta) \rightarrow (\boxed{1}\,\alpha \rightarrow \boxed{1}\,\beta)$

AI3 $\Box(\Box\alpha \rightarrow \alpha) \rightarrow \Box\alpha$

AI4 $\boxed{1}(\boxed{1}\alpha \to \alpha) \to \boxed{1}\alpha$

AI5 $\Box\alpha \to \boxed{1}\Box\alpha$

AI6 $\neg\alpha \to \boxed{1}\neg\Box\alpha$.

The deduction rules are the following:

MP Modus pones

Nec $\Box$-necessitation

Nec_1 $\boxed{1}$-necessitation

Here we add the inference Nec_1 since this rule can not be proven from the other rules and axioms in this modal logic. ⊣

The modal logic **IDzh** can be shown to be weaker than **GLB** and thus **IDzh** $\subseteq$ **GLB**.

The multi modal logic **IDzh** has the following Kripke semantic for which a soundness and completeness theorem can be proven.

Definition 7.14 An **IDzh**-model is a quadruple $\mathcal{K} = \langle W, R, R_1, \phi \rangle$, where W is a finite non-empty set, ϕ is a valuation function W, and R and R_1 are transitive irreflexive relation on W such that for all $w, v_1, v_2 \in W$ we have that:

$$\text{If } wR_1v_1 \text{ then } wRv_2 \text{ if and only if } v_1Rv_2$$

⊣

This means that we can not have that wRv and wR_1v since then vRv; contradicting the irreflexivity R

For such models the following theorem can be proven:

Theorem 7.15 α is valid in all **IDzh**-models if and only if $\vdash_{\mathbf{IDzh}} \alpha$.

This theorem shows that **IDzh** has a natural Kripke semantic to which it is sound and complete.

We will need the following definitions to state the theorem from which the arithmetical completeness theorem for **GLB** follows:

Definition 7.16 For any modal formula α we define $\Delta\alpha$ as the formula:

$$\alpha \wedge \Box\alpha \wedge \boxed{1}\alpha \wedge \Box\boxed{1}\alpha$$

We define the formula $\Psi\alpha$ as:

$$\bigwedge_{\Box\beta\in S(\alpha)} \Delta(\Box\beta \rightarrow \boxed{1}\,\beta)$$

$\dashv$

It can be shown that $\vdash_{\mathbf{GLB}} \Psi\alpha$. To show completeness of **GLB** the following three statements should be proven to be equivalent:

1. $\vdash_{\mathbf{IDzh}} \Psi\alpha \rightarrow \alpha$
2. $\vdash_{\mathbf{GLB}} \alpha$
3. $\mathbf{PRA} \vdash \alpha^*$ for all *

We have that (1) $\Rightarrow$ (2) since $\mathbf{IDzh} \subset \mathbf{GLB}$ and the fact that $\vdash_{\mathbf{GLB}} \Psi\alpha$. That (2) $\Leftrightarrow$ (3) is just the arithmetical soundness theorem for **GLB**. The proof of (3) $\Rightarrow$ (1) will obviously prove the arithmetical completeness theorem for **GLB**. The proof of this can be found in (George S. Boolos 1993) and is beyond the scope of this project.

We can also look at the multi modal logic **GLSB** which is the modal logic that have all the theorems of **GLB**and all formulas: $\boxed{1}\,\alpha \rightarrow \alpha$ as axioms, and which only have modus ponens as its rule of inference. A variant of Solovay's second completeness theorem can be shown for this multi modal logic.

7.1.3 The system GLP

We will end this section by introducing the system **GLP** The language $\mathcal{L}_{[n]}$ of **GLP** is an extension of $\mathcal{L}_{\Box}$, where instead of $\Box$ we write $[0]$ and we furhter add a countable infinite amount of boxes: $[1], [2], \ldots$ representing provability in $\mathbf{PRA}^{+}$, $\mathbf{PRA}^{++}$ and so on, where $\mathbf{PRA}^{++}$ is $\mathbf{PRA}^{+}$ with all formulas of the form $\forall x G(x)$ such that for every $n \in \omega$ such that $\mathbf{PRA}^{+} \vdash G(\overline{n})$ added. We define their duals $\langle 0\rangle, \langle 1\rangle, \langle 2\rangle, \ldots$ in the obvious way and these represent consistency, ω-consistency, ω-ω-consistency and so on. We can now define the system **GLP**:

Definition 7.17 The axioms and inferences rules of **GLP** are the following:

A1 $[n](\alpha \rightarrow \beta) \rightarrow ([n]\alpha \rightarrow [n]\beta)$

A2 $[n]([n]\alpha \rightarrow \alpha) \rightarrow [n]\alpha$

A3 $[n]\alpha \rightarrow [n+1]\alpha$

A4 $\neg[n]\alpha \rightarrow [n+1]\neg[n]\alpha$

MP Modus Ponens

Nec_0 [0]-necessiation

$\dashv$

Following Dzhaparidze the arithmetical completeness theorem can be proven for this system of multi modal logic. The proof follows that of the proof of the arithmetical completeness theorem for **GLB**.

Again we can look at the multi modal logic **GLSP** which is has all theorems and sentences $[n]\alpha \to \alpha$ as its axioms and which only have modus ponens as it inference rule. Again a variant of Solovay's second completeness theorem holds for this logic.

So Solovay's completeness theorems generalizes nicely to multi modal logics; i.e the concept of ω-provability (and beyond) can also be axiomatized.

The proofs of these results are rather involved, but they still follow the same idea as Solovay's original idea. This shows how deep the concept of embedding modal logic into arithmetic is. But this fundamental idea do not generalize to all extensions of **GL**, which will be discussed in the next section.

7.2 Quantifed provability logic

There is another way to extend the logic **GL**; we can add quantifiers to the language. We will call this logic for quantified modal logic (QML). The first goal is to define what a formula is:

Definition 7.18 α is a formula of QML if and only if it can be obtained from a formula of first order logic by replacing occurrences of the negation sign "$\neg$" with occurrences of $\Box$. $\dashv$

There is not a version of Solovay's completeness theorems for this logic; i.e it is not arithmetically complete with respect to any fragment of arithmetics. Furthermore this logic do not have the fixed point property and is not complete with respect to any class of Hintikka frames. These results can actually be shown to hold for an even more conservative extension of **GL**: one where we only always one place predicates are allowed and where we do not permit nestings of the $\Box$-operator. Further information on this topic and proofs of these statements can be found in (George S. Boolos 1993), but this goes way beyond the scope of this project and are left out.

8 Bibliography

Aristoteles (2021). *Metafysik*. Forlaget Klim.

– (1971). *Aristotle's Categories and De interpretatione*. Clarendon Aristotle series. Oxford: Oxford University Press.

Artemov, Sergei (2007). "Handbook of modal logic: 1st ed". In: *Handbook of modal logic*. Ed. by P Blackburn, J van Benthem, and F Wolter. Vol. 3. Studies in logic and practical reasoning. Elsevier. Chap. 16.

Artemov, Sergei N. and Lev D. Beklemishev (2005). "Provability Logic". In: *Handbook of Philosophical Logic, 2nd Edition*. Handbook of Philosophical Logic. Dordrecht: Springer Netherlands, pp. 189–360.

Barry Cooper, S (2004). *Computability Theory*. Studies in logic and the foundations of mathematics. Boca Raton: Chapman & Hall/CRC.

Blackburn, Patrick (2002). *Modal logic*. Ed. by Maarten de. Rijke and Yde Venema. Cambridge tracts in theoretical computer science ; 53. Cambridge: Cambridge University Press.

Blackburn, Patrick, Johan van Benthem, and Frank Wolter, eds. (2007). *Handbook of modal logic: 1st ed*. Vol. 3. Studies in logic and practical reasoning. Amsterdam: Elsevier.

Boolos, George S. (1993). *The logic of provability*. Cambridge: Cambridge University Press.

Boolos, George S., John P. Burgess, and Richard C. Jeffrey (2007). *Comptability and logic*. 5th ed. Cambridge: Cambridge University Press.

Boolos, George S. and Giovanni Sambin (1991). "Provability: The Emergence of a Mathematical Modality". In: *Studia logica* 50.1, pp. 1–23.

Boolos, George. S. (1979). *The unprovability of consistency : an essay in modal logic*. Cambridge: Cambridge University Press.

Buss, Samuel R., ed. (1998a). *Handbook of proof theory*. Studies in logic and the foundations of mathematics. Amsterdam ; Elsevier.

– (1998b). "Handbook of proof theory". In: *Handbook of proof theory*. Ed. by Samuel R. Buus. Studies in logic and the foundations of mathematics. Amsterdam ; Elsevier. Chap. 1, pp. 79–147.

Chang, C. C. and H Jerome Keisler (2012). *Model Theory*. 3. th. Mineola: Dover Publications, inc.

Cohen, Paul (1966). *Set Theory and the Continuum Hypothesis*. W. A. Benjamin, Inc.

Copeland, B. Jack (2020). “The Church-Turing Thesis”. In: *The Stanford Encyclopedia of Philosophy*. Ed. by Edward N. Zalta. Summer 2020. Metaphysics Research Lab, Stanford University.

Cutland, N.J (1980). *Computability : an introduction to recursive function theory*. Cambridge: Cambridge University Press.

Davis, Martin, ed. (1965). *The undecidable : basic papers on undecidable propositions, unsolvable problems and computable functions*. Hewlett, N. Y: Raven Press.

Enderton, Herbert B. (2001). *A Mathematical Introduction to Logic*. Academic Press.

Garson, James W (2006). *Modal Logic for Philosophers*. Cambridge: Cambridge University Press.

Gödel, Kurt (1986a). “Eine Interpretation des intuitionistschen Aussagenkalküls”. In: *Collected works*. Ed. by Solomon Feferman. Oxford University Press, pp. 300–301.

– (1986b). “Über formal unentschiedbare Sätze der Principia Mathematica und verwandter System I”. In: *Collected works*. Ed. by Solomon Feferman. Oxford University Press, pp. 144–195.

Goldblatt, Robert (2003). “Mathematical modal logic: A view of its evolution”. In: *Journal of applied logic* 1.

Hájek, Petr. and P Pudlak (1998). *Metamathematics of First-Order Arithmetic*. Perspectives in Mathematical Logic. Berlin: Springer.

Hendricks, Vincent Fella and Stig Andur Pedersen (2011). *Moderne elementær logik*. Ed. by Vincent Fella Hendricks and Stig Andur Pedersen. 2. revider. Kbh: Automatic Press.

Hilbert, David (1926). “Über das Unendliche”. In: *Mathematische annalen* 95.1, pp. 161–190.

– (1930). *Grundlagen der Geometrie, 7. umgearb. und verm. Aufl.* Wissenschaft und Hypothese ; 7. Leipzig und Berlin.

Hintikka, K. Jaakko J. (1962). *Knowledge and belief*. Ed. by Jaakko. Hintikka. Contemporary philosophy. Ithaca, N. J: Cornell Univ. Press.

– (1969). *Models for modalities : Selected essays*. Ed. by Jaakko. Hintikka. Dordrecht: D. Reidel.

Hughes, G.E and M.J Cresswell (1971). *An introduction to modal logic*. Methuen.

Japaridze, G and Dick de Jongh (1998). “Handbook of proof theory”. In: *Handbook of proof theory*. Ed. by Samuel R. Buus. Studies in logic and the foundations of mathematics. Amsterdam ; Elsevier. Chap. 7, pp. 475–546.

Jongh, Dick de, Marc Jumelet, and Franco Montagna (1991). “On the Proof of Solovay’s Theorem”. In: *Studia logica* 50.1, pp. 51–69.

Jørgensen, Thorvald (2021). "Project outside the course scope: Introduction to Modal Logic". In: URL: `https://github.com/thorvald94/Modal-logic/blob/main/FagProjekt.pdf`.

– (2022). "Project outside the course scope: Gödel's Incompleteness Theorems". In: URL: `https://github.com/thorvald94/GodelIncompleteness/blob/main/project.pdf`.

Kleene, S.C. (1952). *Introduction to metamathematics*. 8. repr. Bibliotheca mathematica ; vol. 1. Groningen: Wolters-Noordhoff.

Kripke, Saul A (1963). "Semantical Analysis of Modal Logic I Normal Modal Propositional Calculi". In: *Mathematical logic quarterly* 9.

Lemmon, E. J. (1977). *An introduction to modal logic : the "Lemmon notes"*. Ed. by Dana. Scot. American philosophical quarterly. Monograph series ; monograph no. 11. Oxford: Basil Blackwell.

Lindström, Per (1996). "Provability logic-a short introduction". In: *Theoria (Lund, Sweden)* 62.1-2, pp. 19–61.

– (1997). *Aspects of Incompleteness*. Berlin/Heidelberg: Springer.

Liu, Yang (2013). *Incompleteness result and provability logic*.

Löb, Martin (1955). "Solution of a Problem of Leon Henkin". In: *Journal of Symbolic Logic* 20, pp. 115–118.

Łukasiewicz, Jan. (1957). *Aristotle's syllogistic from the standpoint of modern formal logic.* 2. ed. enl. Oxford: Clarendon.

Mendelson, Elliott (1964). *Introduction to Mathematical Logic*. Van Norstrand.

Owens, James. C (1973). "Diagonalization and the Recursion Theorem". In: *Notre Dame Journal of Formal Logic* XIV.No 1, pp. 95–99.

Pakhomov, Fedor (2017). "Solovay's completeness without fixed points". In: URL: `http://arxiv.org/licenses/nonexclusive-distrib/1.0`.

Quine, W. V (1966). "Necessary Truth". In: *The Ways of Paradox and other essays.* New York: Random House, pp. 48–56.

Raatikainen, Panu (2022). "Gödel's Incompleteness Theorems". In: *The Stanford Encyclopedia of Philosophy*. Ed. by Edward N. Zalta. Spring 2022. Metaphysics Research Lab, Stanford University.

Reidhaar-Olson, L (1990). "A new proof of the fixed-point theorem of provability logic". In: *Notre Dame journal of formal logic* 31.1, pp. 37–43.

Robinson, R. M. (1950). "An Essentially Undecidable Axiom System". In: *Proceedings of the International Congress of Mathematics*, pp. 729–730.

Rosser, John Barkley (1936). "Extensions of some theorems of Gödel and Church". In: *Journal of Symbolic Logic*.

Segerberg, Krister (1971). *An Essay in Classical Modal Logic*. Filosofska Studier, vol.13. Uppsala Universitet.

Sipser, Michael (2013). *Introduction to the theory of computation.* 3. ed. Boston: Thomson Course Technology.

Skolem, Th. (1923). *Begründung der elementaren Arithmetik durch die rekurrierende Denkweise ohne Anwendung scheinbarer veränderlichen mit unendlichem Ausdehnungsbereich.* Videnskapsselskapets skrifter. Mat.-naturv. klasse ; 1923:6. Kristiania: Jacob Dybwad.

Smiley, T J (1963). "The Logical Basis of Ethics". In: *Acta Philosophica Fennica* 16, pp. 237–.

Smorynski, Craig (1977a). "Beth's theorem and self-referential sentences". In: *Logic Colloguim 77.* Ed. by A Macintyre, L Pacholksi, and J Paris. Studies in logic and the foundations of mathematics. Amsterdam, New York, Oxford: North.Holland Publishing Company, pp. 253–261.

– (1977b). "The Incompleteness Theorems". In: *The Handbook of Mathematical logic.* Ed. by John Barwise. North-Holland Publishing Company.

– (1985). *Self-Rference and modal logic.* Springer-verlag.

Soare, Robert I (1987). *Recursively Enumerable Sets and Degrees : A Study of Computable Functions and Computably : Generated Sets.* Perspectives in Mathematical Logic. Berlin ; Springer-Verlag.

– (2016). *Turing Computability: Theory and Applications.* Theory and Applications of Computability. Berlin, Heidelberg: Springer Berlin / Heidelberg.

Solovay, Robert M (1976). "Provability interpretations of modal logic". In: *Israel journal of mathematics* 25.3-4.

Urbaniak, Rafal and Pawel Pawlowski (2018). "Logics of (Formal and Informal) Provability". In: *Introduction to Formal Philosophy.* Springer Undergraduate Texts in Philosophy. Springer International Publishing, pp. 191–237.

Verbrugge, Rineke (L.C.) (2017). "Provability Logic". In: *The Stanford Encyclopedia of Philosophy.* Ed. by Edward N. Zalta. Fall 2017. Metaphysics Research Lab, Stanford University.

Whitehead, Alfred North. and Bertrand Russell (1973). *Principia mathematica.* 2. ed., reprinted. Cambridge: Cambridge University Press.