Die approbierte Originalversion dieser Diplom-/Masterarbeit ist in der Hauptbibliothek der Technischen Universität Wien aufgestellt und zugänglich.
http://www.ub.tuwien.ac.at

The approved original version of this diploma or master thesis is available at the main library of the Vienna University of Technology.
http://www.ub.tuwien.ac.at/eng

FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Berechnungsinterpretationen des Markov-Prinzip

MASTERARBEIT

zur Erlangung des akademischen Grades

Master of Science

im Rahmen des Studiums

Computational Logic

eingereicht von

Matteo Manighetti
Matrikelnummer 1528764

an der Fakultät für Informatik

der Technischen Universität Wien

Betreuung: Privatdoz. Dipl.-Ing Dr. tech. Stefan Hetzl
Mitwirkung: Dr. Federico Aschieri

Wien, 30. September 2016

Matteo Manighetti	Stefan Hetzl

FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Computational interpretations of Markov's principle

MASTER'S THESIS

submitted in partial fulfillment of the requirements for the degree of

Master of Science

in

Computational Logic

by

Matteo Manighetti
Registration Number 1528764

to the Faculty of Informatics

at the TU Wien

Advisor: Privatdoz. Dipl.-Ing Dr. tech. Stefan Hetzl
Assistance: Dr. Federico Aschieri

Vienna, 30th September, 2016

Matteo Manighetti

Stefan Hetzl

Erklärung zur Verfassung der Arbeit

Matteo Manighetti
Address

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 30. September 2016

Matteo Manighetti

Acknowledgements

"Ah, ah!" contrefis-je, "vous êtes sans doute de ceux, garçon un demi, qui se vantent de ne rien comprendre aux mathématiques".
"Pour ma part" dit Saxel.
"Et vous ne vous en attristez pas?"
"Je devrais?"
"Sans doute. Quelle satisfaction peut-on bien éprouver à ne pas comprendre quelque chose?"

— Raymond Queneau, *Odile*

I would first like to thank Federico Aschieri, who by giving me unvaluable suggestion both for the practice of research and scientific writing did far more than the mere work of co supervising this thesis. Thanks also to Stefan Hetzl who was available and helpful as a supervisor. A special acknowledgement goes to Andrea Condoluci, who helped with some key insights to the development of the thesis.

I am grateful to the Joint Commission of the European Master's Program in Computational Logic and all people involved in organizing it, who gave me the opportunity to have a unique study experience.

I also use the opportunity of this work to thank all those who helped me and supported me during my studies. Thanks to my parents and my sister, who gave me the strength I needed during these two years around the world. Thanks to my friends, and in particular to the EMCL colleagues in Dresden, Bolzano and Vienna. And finally a very special thanks to Nika and Andrea, for countless moments and discussions I am going to miss.

Kurzfassung

In dieser Masterarbeit behandeln wir das Markov-Prinzip, eine Aussage, die ihren Ursprung in der russischen Schule der konstruktiven Mathematik hat und ursprünglich besagt, dass "falls es unmöglich ist, dass ein Algorithmus nicht terminiert, er terminiert". Dieses Prinzip wurde auf viele unterschiedliche Kontexte angepasst, und insbesondere interessiert uns seine am weitesten verbreitete Version in der Arithmetik, die wie folgt formuliert werden kann: "gegeben eine total rekursive Funktion f, falls es unmöglich ist, dass es kein n gibt für das $f(n) = 0$ gilt, dann existiert ein n, so dass $f(n) = 0$ gilt". Dies ist eine im Allgemeinen nicht akzeptierte konstruktivistische Aussage, da es für eine existenzielle Aussage möglich sein muss ein Beispiel anzugeben. Hier gibt es keine Möglichkeit ein solches n zu wählen.

Wir besprechen die konstruktive Mathematik im Detail aus verschiedenen Blickwinkeln, und wir verdeutlichen ihre Beziehung zum Markov-Prinzip. Insbesondere stellen wir mehrere Realisierbarkeitssemantiken vor, welche Interpretationen logischer Systeme durch verschiedene Berechnungskonzepte bereitstellen (vor allem, rekursive Funktionen und Lambda-Kalküle). Dieses Forschungsfeld stellt den Ausgangspunkt für ein bekanntes Paradigma dar, welches oft *Curry-Howard Isomorphismus* genannt wird, oder auch ammiersprachen.

Durch die Untersuchung des Curry-Howard Isomorphismus mit modernen Forschungsmethoden entwickeln wir eine verfeinerte Interpretation des Markov-Prinzips. Wir benutzen diese Resultate im Anschlußum logische Eigenschaften von Systemen mit Bezug zum Markov-Prinzip zu untersuchen.

Abstract

In this thesis we are concerned with Markov's principle, a statement that originated in the Russian school of Constructive Mathematics and stated originally that "if it is impossible that an algorithm does not terminate, then it will terminate". This principle has been adapted to many different contexts, and in particular we are interested in its most common version for arithmetic, which can be stated as "given a total recursive function f, if it is impossible that a there is no n for which $f(n) = 0$, then there exists an n such that $f(n) = 0$". This is in general not accepted in constructivism, where stating an existential statement requires one to be able to show at request a witness for the statement: here there is no clear way to choose such an n.

We introduce more in detail the context of constructive mathematics from different points of view, and we show how they are related to Markov's principle. In particular, several *realizability* semantics are presented, which provide interpretations of logical systems by means of different computational concepts (mainly, recursive functions and lambda calculi). This field of research gave origin to the well known paradigm often called *Curry-Howard isomorphism*, or also *propositions as types*, that states a correspondence between proofs in logic and programs in computer science. Thanks to this the field of proof theory, that is the metamathematical investigations of proofs as mathematical objects, became of interest for computer science and in particular for the study of programming languages.

By using modern research on the Curry-Howard isomorphism, we will obtain a more refined interpretation of Markov's principle. We will then use this results to investigate the logical properties of systems related to the principle.

Contents

CHAPTER 1

Introduction

Defining a proper notion of constructive mathematics and building a constructive foundation of mathematics were two central concerns of mathematical logic in the past century. Starting with Hilbert's program, and continuing through other traditions such as Brouwer's intuitionism, numerous attempts have been made, often ending up in harsh contrasts - the most famous being the one between the two just mentioned schools.

The Russian constructive school pursued the program of Constructive Recursive Mathematics, led by the intuitions of A. A. Markov who was the first in trying to put the notion of *algorithm* at the heart of a foundation of mathematics.

Although ultimately less successful in the field of constructivism, some of the ideas of Markov proved later to be fundamental in understanding proofs in fields of mathematics such as analysis.

In order to present a more modern explanation of Markov's standpoint, we will first need to present a more general overview of the context of constructive mathematics.

1.1 The formalist approach

The birth itself of the modern conception of proof theory is often associated with Hilbert's famous program. As it was stated in the *Grundlagen der Geometrie* the program posed four major problems that should be addressed in order to develop a reliable foundation for a mathematical theory:

- The formalization of the theory, including a choice of its basic objects, relations, and axioms.
- The proof of the consistency of the axioms.

- The question of the mutual independence and completeness of the axioms.
- The decision problem: is there an automatic method for deciding truth of statements in the theory?

In this thesis, we are mainly concerned with the first two points. These underline the two main characteristics of Hilbert's thought: *formalism* and *finitism*. The Hilbertian formalism requires the elements of the theory to be expressed as certain statements in a formal language; the mathematical practice thus could be viewed as a manipulation of these statements, in accordance to some rules. This attracted criticism from other philosophical schools, first and foremost the intuitionist school, in that it seemed like it was removing the concept of *mathematical truth*, in favour of giving rise to a mere mechanical game of symbols. However, the second main aspect of the Hilbertian standpoint further clarifies the approach also in relation to this criticism: the main feature of the axiomatic system that was to be sought was its *consistency*, i.e. the inability of deriving a contradiction from the axioms; in the original plan, this crucial feature had to be proved by *finitistic* means. Hilbert meant with this word that they should rely on inspectable[1] evidence. Such a consistency proof was seen as something that nobody could doubt of.

Hilbert's program is tightly linked to Gödel's famous incompleteness results. We will not enter in the debate of what incompleteness meant for the development of the program; however, it is interesting to mention that Gödel clearly specified his views with respect to the Hilbertian finitism in his Yale lectures [Göd41]. There, he states that he regards a system as finitist if it satisfies the following points:

- All functions and relations that are primitive in the system are respectively computable and decidable.
- The existential quantifier is not primitive in the system. That is, existential quantifications are only an abbreviation for an explicit construction of a witness.
- Universal quantifications can be negated only in the sense that there exists a counterexample in the sense here defined, that is an explicit construction of a counterexample.

In particular, we will draw inspiration from the second point for our notion of constructive system:

Definition 1 (Constructive system)**.** We call a logical system *constructive* if it satisfies the following two properties:

Disjunctive property Whenever $A \vee B$ is provable in the system, then either A is provable or B is provable.

Existential property Whenever $\exists x A(x)$ is provable in the system, then there exists a term t such that $A(t)$ is provable.

[1] In German *anschaulich*

1.2 Intuitionitic logic and realizability semantics

The intuitionistic school of L.E.J. Brouwer was probably the main opponent of the formalist approach. We mentioned before that the intuitionists accused Hilbert of reducing the mathematical practice to a game of symbol manipulation without a real meaning. Indeed, the intuitionists appealed to a much more sophisticated notion of mathematics, conceiving essentially mathematical objects as free creations of the mind of the mathematicians. The mathematical practice is then a matter of human communication. Therefore, an object exists only in the moment a mathematician can mentally construct it: how can one accept an indirect argument as a mental construction? Clearly, if we can prove the impossibility of the non existence of an object, we have no way to obtain a construction we can communicate.

The BHK explanation of intuitionistic truth

The refusal of formalism made by Brouwer also prevented him from really accepting any formalization of an "intuitionistic logic". An explanation of the usual logical connectives from the intuitionistic point of view, and the beginning of the development of an intuitionistic logical system are due to Brouwer's student Arend Heyting; this is usually known as the Brouwer-Heyting-Kolmogorov interpretation, and provides an informal notion of an intuitionistic truth:

- There is no construction of $\bot$.
- A construction of $A \wedge B$ consists of a construction of A and a construction of B
- A construction of $A \vee B$ consists of a construction of A or a construction of B
- A construction of $A \to B$ is a construction which transforms any construction of A into a construction of B
- A construction of $\exists x A(x)$ consists of an element d of the domain and a construction of $A(d)$
- A construction of $\forall x A(x)$ is a method which transforms every element d of the domain into a construction of $A(d)$.

Negation is then interpreted as $\neg A := A \to \bot$. We can already see from this that the principle of excluded middle $A \vee \neg A$ is not justified under this interpretation: it expands to $A \vee (A \to \bot)$, and asks for either a proof of A, or a method to transform proofs of A into the absurdity; but clearly we have no way to do this in general. The underivability of the excluded middle as a rule proved to be the common feature of different systems of constructive logic, and thus intuitionistic logic quickly became interesting per se, regardless of the intuitionistic standpoint in mathematics.

Realizability semantics

The BHK semantics we have defined in the previous paragraph allows us to draw some conclusions and obtain some initial results about systems of intuitionistic logic, such as the simple argument we have used to show that the excluded middle is not justifiable. However, one immediately notices how this semantics is voluntarily informal: the notions of construction and method that are mentioned, are left unspecified. Realizability semantics are a family of semantics that can be thought of as concrete versions of the BHK semantics, whenever we consider a specific intuitionistic theory. Historically, the first such example was the original *number realizability* of Kleene for the intuitionistic system of arithmetic HA [Kle45] that used objects of recursion theory in order to give concrete meaning to the concepts of *construction* and *algorithm* we used previously. More formally, it states when a number e realizes a formula E by induction on the shape of the formula:

- e realizes $(r = t)$, if $(r = t)$ is true.
- e realizes $(A \wedge B)$, if e codes a pair (f, g) such that f realizes A and g realizes B.
- e realizes $A \vee B$, if e codes a pair (f, g) such that if $f = 0$ then g realizes A, and if $f > 0$ then g realizes B.
- e realizes $A \to B$, if, whenever f realizes A, then the e-th partial recursive function is defined at f and its value realizes B.
- e realizes $\neg A$, if no f realizes A.
- e realizes $\forall x A(x)$, if, for every n, the e-th partial recursive function is defined at n and its value realizes $A(n)$.
- e realizes $\exists x A(x)$, if e codes a pair (n, g) and g realizes $A(n)$.

Since the objects of the domain of interpretation are numbers, we can internalize the notion we have just defined by formalizing it inside the same theory of arithmetic we are interpreting. A formalized realizability semantics together with a semantic soundness theorem (which is often called adequacy in this framework) allows a finer analysis of intuitionistic systems. For example, given the adequacy of Kleene semantics for a system of intuitionistic arithmetic we could conclude about constructivity of the system according to our definition 1: whenever $A \vee B$ is provable then by adequacy it is realizable, and therefore we will have a realizer coding either a realizer of A or one of B; similarly whenever $\exists x A(x)$ is provable, then by adequacy it is realizable and the realizer codes some n and a realizer of $A(n)$.

Moreover, realizability is able to tell more about the computational content of intuitionistic systems. Kleene realizers are understood as codes for a Gödel numbering of the recursive functions, and thus can represent something that we can use in order to compute. Going further in this direction, Kreisel's *modified realizability* [Kre59] defines realizers as elements of a system

of typed λ-calculus: these can be in turn very similar to statements of a modern functional programming language. We can think therefore of realizability interpretations as the link between constructive systems and computational systems.

1.3 Constructive Recursive Mathematics and the controversy about Markov's principle

Constructive recursive mathematics was developed by the Russian school of constructivism starting from the 1940s. Its main contributor was A.A. Markov [MN54], and most of the research developments in this field happened until the 1970s.

In a fashion similar to the finitistic approach, the focus in CRM is on the fact that mathematical objects should be finitely representable. In particular, they should be representable by means of suitably defined *algorithms*.

The main points of the approach of CRM are, as found in [TD88]

- The objects of mathematics are algorithms. Algorithms are meant in a mathematically precise sense in the sense that they should be presented as "words" in some finite alphabet of symbols.
- Limitations due to finite memory capacity are disregarded, the length of symbol strings is unbounded (though always finite).
- Logically compound statements not involving $\exists$, $\vee$ are understood in a direct way, but existential statements and disjunctions always have to be made explicit.
- If it is impossible that an algorithmic computation does not terminate, we may assume that it does terminate.

The last of these points is what is commonly referred to as "Markov's principle", and was the main point of controversy between the intuitionists and the Russian school. Indeed, all the points that were listed fit naturally in classical recursion theory; if we think at Markov's principle in this context, it represents unbounded search: it is certain that the algorithm will halt at some point, but there is no guarantee that this will happen before the end of the universe. This was firmly disagreed by intuitionists and indeed we will see that it cannot be proven from intuitionistic logic.

1.4 Natural deduction and the Curry-Howard isomorphism

In section 1.2 we highlighted how realizability sets a correspondence between constructive systems and models of computation. An even deeper link was noted by Haskell Curry: the rules for implication introduction and elimination of natural deduction (fig. 1.1) can be put in correspondence with the rules for abstraction and application of Church's simply typed lambda calculus.

Even though it was known from the 1940s, this correspondence was not further explored until some decades later. A reason for this delay could be found in the similar lack of success of the proof system of Natural Deduction. Introduced by Gentzen together with the immediately more popular Sequent Calculus, Natural Deduction presents inference rules in couples of *introduction* and *elimination* rules for every logical connective. Its other feature is that proofs are dependent on *assumptions* that can be made and then discharged (represented by bracketing), thus rendering the proof independent of the previously made assumption. A system of natural deduction for intuitionstic logic is presented in fig. 1.1.

$$\frac{\begin{array}{cc}\vdots & \vdots \\ A_1 & A_2\end{array}}{A_1 \wedge A_2}\ \wedge\text{-I} \qquad \frac{\begin{array}{c}\vdots \\ A_1 \wedge A_2\end{array}}{A_1}\ \wedge\text{-E}_1 \qquad \frac{\begin{array}{c}\vdots \\ A_1 \wedge A_2\end{array}}{A_2}\ \wedge\text{-E}_2$$

$$\frac{\begin{array}{c}[A] \\ B\end{array}}{A \to B}\ \to\text{-I} \qquad \frac{\begin{array}{cc}\vdots & \vdots \\ A \to B & A\end{array}}{B}\ \to\text{-E}$$

$$\frac{\begin{array}{c}\vdots \\ A\end{array}}{A \vee B}\ \vee\text{-I}_1 \qquad \frac{\begin{array}{c}\vdots \\ B\end{array}}{A \vee B}\ \vee\text{-I}_2 \qquad \frac{\begin{array}{ccc}\vdots & [A] & [B] \\ A \vee B & C & C\end{array}}{C}\ \vee\text{-E}$$

$$\frac{\begin{array}{c}\vdots \\ A\end{array}}{\forall x A}\ \forall\text{-I } (x \text{ not free in the assumptions}) \qquad \frac{\begin{array}{c}\vdots \\ \forall x A\end{array}}{A[t/x]}\ \forall\text{-E}$$

$$\frac{\begin{array}{c}\vdots \\ A[t/x]\end{array}}{\exists x A}\ \exists\text{-I} \qquad \frac{\begin{array}{cc}\vdots & [A] \\ \exists x A & C\end{array}}{C}\ \exists\text{-E } (x \text{ not free in } C \text{ and in the assumptions})$$

$$\frac{\bot}{A}\ \bot\text{-E}$$

Figure 1.1: Natural deduction for intuitionistic logic

Sequent calculus provided a more technically convenient presentation of classical logic; moreover, Gentzen introduced it with the specific aim of proving its consistency, by means of what became to be known as Gentzen's *Hauptsatz*, or cut-elimination theorem. Since we are not interested in sequent calculus, we will not talk about this theorem further. We are however interested in a somehow corresponding notion in the framework of natural deduction, which

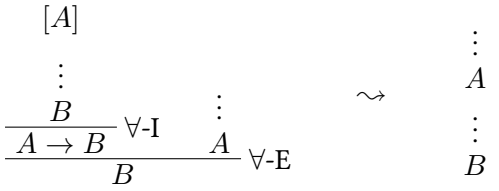

Figure 1.2: Normalization of a non-normal proof

is *proof normalization*. A normal proof is one where no detours appear; formally, a detour is a configuration in which an introduction rule is immediately followed by an elimination of the same connective that was introduced. Given that the two kinds of rules are one the inverse of the other, such an inference can be removed in order to make the proof more direct: an example of such procedure is shown in fig. 1.2.

Normalization then is the process of removing detours from a proof, with the aim of obtaining a normal one. As we mentioned, the unavailability of a normalization theorem [2], stating that every proof could be normalized, meant that sequent calculus became the system of choice for a long period, until Dag Prawitz finally crafted a direct normalization proof for natural deduction in 1965.

In his work (see for example [Pra06]), Prawitz further clarified a key feature of the rules of natural deduction: the introduction rules can be thought of as *definitional* rules that describe when one is allowed to assert a certain connective, and thus its meaning; in the same way, elimination rules can be seen as *operational* rules that describe how one can use a formula depending on its main connective [3].

As natural deduction started gathering more interest, William Howard studied more in depth the relationship between deduction rules of natural deduction and typing rules of typed lambda calculus, and presented what came to be known as the Curry-Howard isomorphism [How69]. Under this isomorphism, formulas are put in correspondence with types, hence the title of Howards's work *The formulae as types notion of construction*; the correspondence stretches even further, and takes different names according to the different traditions that originated from the original work. We borrow the terminology of Wadler [Wad15] and state the full framework as:

- *Propositions* as *types*, the original intuition of Howard

[2] In his thesis Gentzen had actually included a set of detour conversions and a proof of normalization for intuitionistic natural deduction. However this remained unknown until 2005, when a manuscript of the thesis was found. For more details see [PG08]

[3] This idea was already expressed by Gentzen: *The introductions constitute, as it were, the "definitions" of the symbols concerned, and the eliminations are, in the final analysis, only consequences of this, which may be expressed something like this: At the elimination of a symbol, the formula with whose outermost symbol we are dealing may be used only "in respect of what it means according to the introduction of that symbol".* ([Gen35])

- *Proofs* as *programs*: since every proof tree can be made to correspond with a type derivation, we have a lambda term corresponding to the proof.
- *Simplification of proofs* as *evaluation of programs*: the process of detour removal is nothing but a computation, where a complex term gets reduced in order to obtain a result of the computation.

1.5 Contents of the thesis

Modern research in the Curry-Howard tradition draws heavily from all the standpoints we briefly discussed. It stems from constructivism, and intuitionistic systems are the base for most Curry-Howard systems; it is formalist in the sense that proofs are the main object of the investigation; it is finitist in the sense that, in addition to the requirement that objects of computation should be finite, it tries to make sense of classical reasoning by these means.

We will sit in this tradition, and therefore although the main object of the discussion will be a mathematical principle, we will be interested in its computational and metalogical properties. As it was already mentioned, Markov's principle was already controversial in the debate about constructivism and foundations in the first half of the XX century: chapter 2 will be devoted to a more in-depth accounting of the birth of realizability semantics and of the status of Markov's principle in each of them.

After that we will introduce some results in the more modern line of research of realizability and Curry Howard systems for classical logic. In chapter 3, we shall introduce a Curry Howard system able to provide a realizability semantics for the semi-classical system of arithmetic with limited excluded middle ($\mathsf{HA} + \mathsf{EM}_1$). In chapter 4 we will prove some additional results on the computational and constructive properties of $\mathsf{HA} + \mathsf{EM}_1$, and we will use them to give a new computational interpretation of Markov's principle.

Based on the intuitions of chapter 4, chapter 5 will introduce a Curry Howard system for a system of full classical arithmetic and a corresponding restricted version that will be shown constructive thanks to Markov's principle.

CHAPTER 2

Intuitionistic realizability and Markov's principle

Intuitionistic logic proved to be the underlying logic for many kinds of constructive mathematics. Therefore it is often referred to as *the* constructive logic. The idea of realizability semantics originated in the context of intuitionistic systems, and so where the first Curry-Howard systems: indeed it was long believed that these were the only systems that allowed a computational interpretation.

After introducing the basic ideas of intuitionistic arithmetic needed to develop the theory of realizability, this chapter will present some classical realizability results and their relation to Markov's principle.

2.1 Heyting Arithmetic and Markov's principle

Throughout the introduction we made continuous references to *Arithmetic*. By this name we mean, in its broadest sense, the theory of natural numbers with the usual operations of sum and product. From the point of view of logic, although a complete axiomatization cannot exist because of Gödel's theorems, the most common axiom system for this theory is known as Peano Arithmetic, PA. It takes the name from Giuseppe Peano, and in its modern presentation it consists of a classical theory over the language with constant terms $0, \mathbf{s}, +$ and the predicate $=$, with the axioms

- $\forall x(x = x)$
- $\forall x \forall y(x = y \to y = x)$
- $\forall x \forall y \forall z(x = y \to y = z \to x = z)$

- $\forall x \forall y (x = y \to \mathbf{s}x = \mathbf{s}y)$
- $\forall x \forall y (\mathbf{s}x = \mathbf{s}y \to x = y)$
- $\forall x (\mathbf{s}x = 0 \to \bot)$
- $\forall x (x + 0 = x)$
- $\forall x \forall y (x + \mathbf{s}y = \mathbf{s}(a + b))$
- $\forall x (x \cdot 0 = 0)$
- $\forall x \forall y (x \cdot \mathbf{s}y = (x \cdot y) + x)$
- $\forall x (\varphi(x) \to \varphi(\mathbf{s}x)) \to \varphi(0) \to \forall x \varphi(x)$, for all formulas φ

The first four axioms define our notion of equality as an equivalence relation preserved by the successor operation. Then the following two state that the successor is a bijection between the naturals and naturals greater than zero. After them we have the definitions for addition and multiplication, and finally the induction axiom scheme.

By Heyting Arithmetic, HA, we mean the intuitionistic theory of the same axioms. In this context, we formulate Markov's principle as the statement

$$\neg\neg \exists x A(x) \to \exists x A(x)$$

where A is a quantifier-free formula. Alternatively, we can also use the following form, which is equivalent under the axioms of HA:

$$\neg \forall x A(x) \to \exists x \neg A(x)$$

It was mentioned in the introduction that the intuitionists did not accept Markov's principle. In line with this, neither of the formulas we just presented can be proved in the system of Heyting's intuitionistic arithmetic; however as we are going to see realizability interpretation provide mixed answer on this.

2.2 Gödel's *Dialectica* interpretation

Although not usually included under the category of realizability interpretations, the functional interpretation of intuitionistic arithmetic introduced by Gödel, commonly referred to as the *Dialectica* interpretation [Göd58], is probably the first step into this line of research. As is made explicit in the title of the series of lectures where he first introduced his ideas, *In what sense is intuitionistic logic constructive* [Göd41], Gödel aimed at making clearer the constructive meaning of the intuitionistic logical constants. In order to do this, he proposed a system of typed recursive functionals where to interpret intuitionistic theories; this approach was in his opinion finitist, as we noted in the introduction, and therefore more suitable to develop an analysis of constructivity and consistency.

Formally, the *Dialectica* interpretation assigns to every formula F of HA a formula F_D in a system of typed functionals that we will call **T**; F_D is of the form $\exists y \forall z A(y, z, x)$, where x, y, z are list of variables of arbitrary type and A is quantifier free. The definition is by induction on the structure of the formula: for A atomic, $A_D = A$ (identifying the symbols of the languages HA and **T**); if $F_D = \exists x \forall y A(x, y)$ and $G_D = \exists u \forall v B(u, v)$, then

- $(F \wedge G)_D = \exists x, u \forall y, v(A(x, y) \wedge B(u, v))$
- $(F \vee G)_D = \exists t, x, u \forall y, v(t = 0 \to A(x, y) \wedge t = 1 \to B(u, v))$
- $(\forall z F)_D = \exists X \forall z, y A(X(z), y, z)$
- $(\exists z F)_D = \exists z, x \forall y A(x, y, z)$
- $(F \to G)_D = \exists U, Y \forall x, v A(x, Y(x, v)) \to B(U(x), v)$
- $(\neg F)_D = \exists Y \forall x \neg A(x, Y(x))$

Note that 6 follows from 5 when defining $\neg A = A \to \bot$. If we compare this with the usual BHK semantics, which also forms the basis of other realizability semantics, we can see that it is substantially different in particular in the definition of the implication: here we find no mention of a method to transform "any proof" as we had in BHK.[1]

If one thinks of the Dialectica as a Game Semantics, its peculiarity becomes clearer: consider a game between two players, where we win if we find a term u such that there is no t for which $A_D(u, t)$ holds; then we have a winning strategy if we can state $\exists x \forall y\ A_D(x, y)$. The cases for the connectives different from $\to$ is quite intuitive in this framework:

- In the case of $A \wedge B$, we need to find winning strategies x for A and u for B
- In the case of $A \vee B$, we declare (depending on t) whether we are going to give a winning strategy x for A or u for B
- In the case of $\forall x\ A$, we need to give a winning strategy $X(z)$ for $A(z)$ for every numeral z the opponent might give
- In the case of $\exists x\ A$, we need to give a numeral z, together with a winning straregy for $A(z)$.

[1] With regard to this, Gödel noted: "[the fact that one does not need to quantify over all proofs] shows that the interpretation of intuitionistic logic, in terms of computable functions, in no way presupposes Heyting's and that, moreover, it is constructive and evident in a higher degree than Heyting's. For it is exactly the elimination of such vast generalities as "any proof" which makes for greater evidence and constructivity." [Göd72]

The case of implication requires more explanation. Here, the opponent gives us a strategy x for A: note that it need not be a winning one. In order to win, we need either to provide a winning strategy for B, or to show that the strategy he gave us was actually not winning. From this comes the shape of the interpretation of the implication: we need to give a method U to obtain a strategy for B such that, whenever v is a strategy that wins against $U(x)$, we can build a strategy $Y(x, v)$ that wins against x.

Markov's principle and the *Dialectica*

The difference between the BHK semantics and the *Dialectica* interpretation goes in fact much farther than this, and although one can easily check that all formulas that are provable in HA are provable in **T**, the converse is not the case. It turns out that Markov's principle is precisely one of the formulas that obtain a justification in **T** but are not provable in HA. If we consider the second form of Markov's principle introduced in the previous section, we have that

$(\forall x A)_D = \forall x A(x)$
$(\neg\forall x A)_D = \exists x\, \neg A(x)$

$(\neg A)_D = \neg A$
$(\exists x \neg A)_D = \exists x\, \neg A(x)$

$(\neg\forall x A \to \exists x \neg A)_D = \exists U \forall x (\neg A(x) \to \neg A(U(x)))$

Since $\exists x \neg A(x)$ is already in the required form, it is not touched by the Dialectica. In the case of $\neg\forall x\ A$, the Dialectica interpretation of the negation states that there should be a counterexample, and asks for a functional that maps witnesses of $\forall x\ A$ (which are void in the interpretation) to counterexamples of A; this means that the interpretation is once again $\exists x \neg A(x)$. Therefore, since both formulas get the same interpretation, Markov's principle can be trivially interpreted.

It is interesting to note that Gödel was aware of this result and viewed it as yet another example of the fact that intuitionistic logic was not well suited as a basic constructive logic, and the system **T** was on the other side behaving much better[2]

One might now wonder how such an interpretation can be used in practice. Consider the case where we have an interpretation of the premise $\neg\forall x A$, and we want to use modus ponens together with Markov's principle to get the conclusion. We can easily see that the Dialectica interpretation validates modus ponens, as shown for example in [Koh08]: assume we have the two formulas in **T**

[2] "The higher degree of constructivity also appears in other facts, e.g., that Markov's principle $\neg\forall x A(x) \to \exists x \neg A(x)$ (see [Kle60], page 157, footnote) is trivially provable for any primitive recursive A and, in a more general setting, for any decidable property o of any objects x. This, incidentally, gives an interest to this interpretation of intuitionistic logic (no matter whether in terms of computable functions of higher types or of Turing functions) even if Heyting's logic is presupposed." [Göd72]

$\forall y\ A_D(t_1, y)$
$\forall x, v\ (A_D(x, t_2(x, v)) \to B_D(t_3(x), v))$

Then we can take t_1 for x in the second formula, and $t_2(t_1, v)$ for y in the first. This results in

$A_D(t_1, t_2(t_1, v))$
$A_D(t_1, t_2(t_1, v)) \to B_D(t_3(t_1), v)$

Therefore we have $B_D(t_3(t_1), v)$ for all v, and thus the functional assigned to B is $t_3(t_1)$. Thus, we can view modus ponens as functional application. In our case we have

$\neg A(t_1)$
$\forall y(\neg A(y) \to \neg A(U(y)))$

And therefore applying modus ponens results in the application $U(t_1) = t_1$, since $U = \lambda x.x$.

2.3 Kleene's realizability

Kleene was the first to investigate the notion of realizability, and indeed he was the one to introduce the word itself[3]. Upon developing the system of recursive functions, he aimed at making the system of intuitionistic arithmetic "more precise", and he planned to do so by employing the system of recursive functions he contributed to formalize. More precisely, the objects of the domain of the interpretation (i.e. the realizers) are the Gödel numbers of the recursive functions: thus Kleene's realizability is often referred to as *number realizability*.

Consider the standard model of arithmetic $\mathbb{N}$ and a standard pairing function $\langle -, - \rangle : \mathbb{N}^2 \to \mathbb{N}$, together with its corresponding projection functions π_1, π_2 such that $\pi_i(\langle n_1, n_2 \rangle) = n_i$. By $\{n\}m$ we represent the result of the computation of the n-th partial recursive function on m, in a suitable model of the partial recursive functions; by $\overline{n}$ we mean the numeral (in HA) representing n. In the classic definition of Kleene, any number n is a realizer of a formula F under the following cirmunstances:

$n\,\mathbf{r}\,s = t$ if $s = t$

$n\,\mathbf{r}\,A \wedge B$ if $\pi_1(n)\,\mathbf{r}\,A$ and $\pi_2(n)\,\mathbf{r}\,B$

$n\,\mathbf{r}\,A \to B$ if for all m such that $m\,\mathbf{r}\,A$, $\{n\}m$ is a terminating computation and $\{n\}m\,\mathbf{r}\,B$

$n\,\mathbf{r}\,A \vee B$ if $\pi_1(n) = 0$ and $\pi_2(n)\,\mathbf{r}\,A$, or if $\pi_1(n) = 1$ and $\pi_2(n)\,\mathbf{r}\,B$

$n\,\mathbf{r}\,\forall x A(x)$ if for all m, $\{n\}m$ is a terminating computation and $\{n\}m\,\mathbf{r}\,A(\overline{m})$

$n\,\mathbf{r}\,\exists x A(x)$ if $\pi_1(n)\,\mathbf{r}\,A(\ \overline{\pi_2(n)}\ )$

[3] As mentioned in [Kle45], the initial development of the system is actually due to Kleene's first student David Nelson.

We can build a realizer for Markov's principle according to this definition. Consider the number n such that $\{n\}m = \langle 0, \mu i.A(i)\rangle$; here, μ denotes the usual minimization operation from the theory of partial recursive functions. This is a realizer of $\neg\neg\exists x A(x) \to \exists x A(x)$ only if whenever m is a realizer of $\neg\neg\exists x A(x)$, $\{n\}m$ is a realizer of $\exists x A(x)$. Unraveling the definitions, we need $\langle 0, \mu i.A(i)\rangle$ to be a realizer of $\exists x A(x)$, i.e. $0\,\mathbf{r}\,A(\ \overline{\mu i.A(i)}\ )$. If one assumes that $\mu i.A(i)$ does not correspond to a terminating computation, then this would mean that $\exists x A(x)$ is not realizabile; in turn, if there is no realizer of $\exists x A(x)$ then any number is a realizer of $\exists x A(x) \to \bot \equiv \neg\exists x A(x)$; finally, since we have a realizer for $\neg\exists x A(x) \to \bot$, this would give us a realizer of $\bot$, and thus a contradiction. This ensures the termination of the computation, and therefore we have $A(\ \overline{\mu i.A(i)}\ ) \equiv \top$, and any number is a realizer of $\top$.

We can easily see the catch here: the termination of the computation is ensured by classical reasoning, and what we have done is a simple shift of the classical reasoning contained in Markov's principle to the metalevel, in this case the theory of partial recursive functions. This is of course not satisfying at all from a strictly constructive point of view.

2.4 Kreisel's modified realzability

A big step forward in the field of realizability in the direction of computer science was done by Georg Kreisel with his system of *modified realizability* [Kre59]. Kreisel's realizability differentiates itself from Kleene's by using a typed lambda calculus as the domain of interpretation. Types here are put in correspondence with formulas of HA, somehow predating Howard's idea of completely identifying them by some years; moreover, the use of lambda calculus and the subsequent success of lambda calculus as the foundation for functional programming languages laid the foundation for the link between computer science and proof theory.

We begin the presentation of modified realizability by presenting the system of lambda calculus. First we need to introduce the types we are going to use:

- N is a type (intuitively, the type of naturals)
- If σ, τ are types, then $\sigma \to \tau$, $\sigma \times \tau$, $\sigma + \tau$ are types

Then, we introduce the typed terms of the system:

- For every type σ, a countable set of variables $x^\sigma, y^\sigma, \ldots$
- $0 : \mathsf{N}$, $\mathbf{s} : \mathsf{N} \to \mathsf{N}$
- For all types σ, $\mathsf{R}^\sigma : \sigma \to (\mathsf{N} \to \sigma \to \sigma) \to \mathsf{N} \to \sigma$
- For all types σ, τ, projections $\pi_1^{\sigma,\tau} : \sigma \times \tau \to \sigma$, $\pi_2^{\sigma,\tau} : \sigma \times \tau \to \tau$ and pairing $\langle -, - \rangle : \sigma \to \tau \to \sigma \times \tau$
- If $t : \tau$, then $\lambda x^\sigma . f : \sigma \to \tau$

- If $s : \sigma \to \tau$, $t : \sigma$, then $st : \tau$

And third, the set of reduction rules:

- $(\lambda x.t)s \mapsto t[s/x]$
- $\pi_1(\langle s, t\rangle) \mapsto s$, $\pi_2(\langle s, t\rangle) \mapsto t$
- $\mathsf{R}xy0 \mapsto x$, $\mathsf{R}xy(\mathbf{s}z) \mapsto yz\mathsf{R}xyz$

We are now ready to define the realizability interpretation. We will not treat directly the case of $\vee$, but we will assume that $A \vee B$ is a shorthand for $\exists x((x = 0 \to A) \wedge (\neg(x = 0) \to B))$ We do so by first assigning a type $tp(A)$ to every formula A:

$$tp(\bot) = tp(s = t) = \mathsf{N} \quad tp(A \wedge B) = tp(A) \times tp(B) \quad tp(A \to B) = tp(A) \to tp(B)$$
$$tp(\forall x A) = \mathsf{N} \to tp(A) \qquad tp(\exists x A) = \mathsf{N} \times tp(A)$$

Finally, we can state

$t \,\mathbf{mr}\, s = t$ if $s = t$

$t \,\mathbf{mr}\, A \wedge B$ if $\pi_1(t) \,\mathbf{mr}\, A$ and $\pi_2(t) \,\mathbf{mr}\, B$

$t \,\mathbf{mr}\, A \to B$ if for all $s : tp(A)$, $ts \,\mathbf{mr}\, B$

$t \,\mathbf{mr}\, \forall x A(x)$ if for all $m : \mathsf{N}$, $tm \,\mathbf{mr}\, A(\overline{m})$

$t \,\mathbf{mr}\, \exists x A(x)$ if $\pi_1(t) \,\mathbf{mr}\, A(\ \overline{\pi_2(t)}\ )$

The term calculus comes with some important properties, the main one being strong normalization. This means that every term will reduce to a normal form after a finite number of reduction steps.

If we analyze modified realizability from a game semantical point of view as we did with the Dialectica, we will notice that it only differs in the definition of the implication. Indeed, here we go back to a definition in the style of the BHK. Game semantically, here we are only talking about winning strategies: this means that when playing on the formula $A \to B$, the opponent will always give us a winning strategy for A, to which we should answer with a winning strategy for B. However, winning strategies cannot be effectively recognized, so the correctness of moves cannot be checked: this is why, when it comes to game semantics, the Dialectica represents a clearer interpretation.

The fact that Markov's principle cannot be interpreted by means of the modified realizability was already shown by Kreisel [Kre62], and was indeed presented as one of the main points

of his system. One can argue like this: assume that Markov's principle is realizable. Then in particular, for every value of n one could realize $\neg\forall x\ \mathbf{T}^{\perp}(n,n,x) \to \exists x\ \mathbf{T}(n,n,x)$, where $\mathbf{T}$ is Kleene's predicate and is interpreted as saying "the Turing machine ϕ_n terminates the computation after x steps on input n" (this is known to be primitive recursive and thus representable in HA). Let then n be fixed, and since we have that $tp(\neg\forall x\mathbf{T}^{\perp}(n,n,x)) = (\mathsf{N} \to \mathsf{N}) \to \mathsf{N}$, consider the dummy term $d := \lambda x^{\mathsf{N}} y^{\mathsf{N}}.0 : (\mathsf{N} \to \mathsf{N}) \to \mathsf{N}$. By applying the realizer of Markov's principle to this dummy term, we will get a term of type $tp(\exists x\mathbf{T}) = \mathsf{N} \times \mathsf{N}$; this last term will then normalize to a term of the form $\langle m, t\rangle$, such that m is a numeral. Distinguish two cases:

1. If $\mathbf{T}(n,n,m)$ holds, then we have found that the nth Turing machine will halt on input n after m steps
2. If $\mathbf{T}(n,n,m)$ does not hold, we claim that the nth Turing machine does not halt on input n. Suppose that it halts, then we would have that $\forall x\ \mathbf{T}^{\perp}(n,n,x)$ is false and thus not realizable; this in turn means that $\neg\forall x\ \mathbf{T}^{\perp}(n,n,x)$ is trivially realizable by any term, and in particular by the dummy term d; by the definition of realizability, the realizer for Markov's principle applied to d gives a realizer for $\exists x\mathbf{T}(n,n,x)$. We have already denoted the normal form of this term as $\langle m, t\rangle$, and since it is a realizer of $\exists x\mathbf{T}(n,n,x)$ it must be the case that t is a realizer of $\mathbf{T}(n,n,m)$. This means that $\mathbf{T}(n,n,m)$ holds, which is a contradiction.

Since the term calculus is strongly normalizing, we would have described a procedure that, given any m, decides in finite time whether the nth Turing machine will halt on input n, which is well known to be an undecidable problem.

CHAPTER 3

Realizability and classical systems

The previous chapter showed how realizability can be employed as a tool to analyze the constructivity of deductive systems, and to extract computational content from proofs in these systems. Given the constructive nature of realizability semantics and the inherent non constructivity of classical logic, it would seem impossible to obtain such a semantics for systems based on classical logic. This was widely believed until the nineties, when a correspondence between control operators in programming languages and classical reasoning in proofs was discovered. In this chapter, after a brief history of this idea, we will present a related idea for realizability interpretations called *Interactive realizability*. Finally, we will introduce the Curry-Howard system $\mathsf{HA} + \mathsf{EM}_1$ for intuitionistic arithmetic with classical reasoning limited to formulas of the form $\exists x \mathsf{P}$ with P atomic, together with its realizability interpretation.

3.1 Exceptions and classical logic

Though successful in establishing links between intuitionistic theories and computational mechanisms, the Curry-Howard correspondence was for a long time regarded as incompatible with classical theories. Indeed, if we try to extend to classical logic the system of natural deduction we have introduced in chapter 1, we need to add a rule either for the excluded middle or for the double negation elimination (i.e. *reductio ad absurdum*). In the first case, we need to do a disjunction elimination without having any possibility of knowing which of the two disjuncts actually holds; in the second, we assert a formula and all we know is that its negation leads to an absurdum. It looks like we have no possibilities of recovering any computational construct.

However, we have also mentioned that classical systems of natural deduction too are equipped with a normalization theorem. It was exactly in this observation that the solution to the riddle laid undiscovered for many years[1]. Let's take a look at the rules that Prawitz gave for the

[1]The link between Prawitz's reductions and typing of the $\mathcal{C}$ operator was established only *a posteriori*, for example in [Gro01]

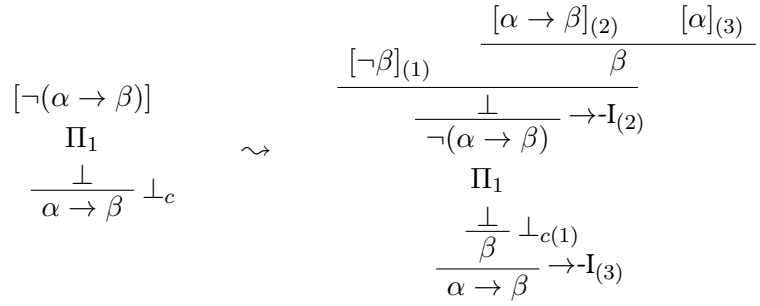

Figure 3.1: Prawitz's normalization step for *reductio ad absurdum* on an implication

normalization of the double negation elimination in fig. 3.1: the aim is to apply the rule $\bot_c$ to a formula of lower complexity, and so one assumes the negation of the conclusion together with the entire implication and the antecedent; classical reasoning is then only applied to the negated assumption. Similar rules were given for the other logical connectives. This reduction looks very similar to the one that Felleisen gave for his $\mathcal{C}$ operator:

$$\mathcal{C}(\lambda k.M) \to \lambda n.\mathcal{C}(\lambda k.M[k := \lambda f.k(fn)])$$

Presented in [Fel88], this operator introduced the notion of *continuation*, and was the basis for the introduction of such constructs in programming languages (an example being the construct `call/cc` available in Scheme). It was Griffin then, who in [Gri89] proposed to type Felleisen's operator as $\neg\neg A \to A$. The idea that sequential control operators could provide a computational correspondent to classical reasoning (as opposed to pure functional flow of computation and intuitionistic reasoning) proved to be very successful, and breathed new life into the *propositions as types* paradigm. Starting from ideas similar to Griffin's several other systems were developed, such as the ones from Parigot [Par92] and Krivine [Kri09]. Generalizing to other control operators, de Groote [Gro95] showed that mechanisms of exceptions can be put in correspondence with uses of the excluded middle.

The approach of enriching systems of lambda calculus with imperative constructs provided also a new way to approach semi-classical principle, by extending Kreisel's modified realizability with delimited control operators. Using this method, Hugo Herbelin introduced in [Her10] a system of intuitionistic logic with the addition of two logical rules crafted in order to correspond to `catch` and `throw` instructions for a system of delimited exceptions.

3.2 Interactive realizability

The possibilities opened by new Curry-Howard correspondences for classical logic did not, on the other side, provoke a similar number of new systems in the field of realizability semantics. The first and major example remains the work of Krivine [Kri10], who recently applied ideas of classical realizability to set theory in order to obtain a technique alternative to forcing.

Interactive realizability is a new realizability semantics for classical systems introduced by Aschieri and Berardi [AB12; ABB13] based on the concept of *learning*: the main idea is that realizers are programs that *make hypotheses*, *test* them and *learn* by refuting the incorrect ones. This is obtained by means of systems of lambda calculus with exceptions mechanisms: a program will continue to execute under some assumptions, and whenever it uses an instance of an assumption, the instance gets tested; if the assumption is discovered to be false an exception is raised, and the program can continue to run using the new knowledge gained from the counterexample. Different systems of interactive realizability have been put forward for various systems such as Heyting Arithmetic with limited classical principles, or more recently full first order logic and non-classical logics.

3.3 The system $\mathsf{HA} + \mathsf{EM}_1$

Following the terminology of [Aka+04], we will now consider the semi-classical principle EM_1, that is excluded middle restricted to formulas of the form $\exists\alpha\mathsf{P}$ with P an atomic predicate[2]. System $\mathsf{HA} + \mathsf{EM}_1$, introduced in [ABB13], applies the idea of interactive realizability to an intuitionistic logic extended with this principle. We could view this as adding the axiom $\forall\alpha^{\mathsf{N}}\mathsf{P} \vee \exists\alpha^{\mathsf{N}}\neg\mathsf{P}$ for every atomic P; this however carries no useful computational meaning. The new principle is therefore treated as a disjunction elimination, where the main premise is the classical axiom and gets cut.

If we try to fit this in a Curry-Howard system, we have now two proof terms representing a construction of the same conclusion, corresponding to the two proof branches where the first and then the second disjunct are assumed. By looking at the shape of the two assumptions, we can see that in the first case we need a condition to hold for all values, while in the second we are looking for a counterexample. The idea is that we should create a new proof term where we include both possible computations, and during the computation itself we might switch from the first to the second. Hence the $\textsc{em}_1$ rule that we add to the system has the following form:

$$\frac{\Gamma, a : \forall\alpha^{\mathsf{N}}\mathsf{P} \vdash u : C \quad \Gamma, a : \exists\alpha^{\mathsf{N}}\neg\mathsf{P} \vdash v : C}{\Gamma \vdash u \parallel_a v : C}$$

Here a represents a communication channel between the two possible computations. The hypothesis $\forall\alpha^{\mathsf{N}}\mathsf{P}$ is computationally void: it only serves as a certificate for the correctness of u; conversely, the branch where we assume $\exists\alpha^{\mathsf{N}}\neg\mathsf{P}$ might ask for an actual witness in order to proceed. Informally, what we want to accomplish with the reduction rules is that we should reduce inside u and check for all the used instances of the universal hypothesis whether $\mathsf{P}[n/\alpha]$ is actually true. Whenever one such instance is refuted, we have found a witness for $\neg\mathsf{P}$, and we can employ it for the execution of v. This is obtained by new terms that we should use when we introduce assumptions that are to be eliminated via classical reasoning: we introduce the two typing rules

$$\Gamma, a : \forall\alpha^{\mathsf{N}}\mathsf{P} \vdash \mathtt{H}_a^{\forall\alpha\mathsf{P}} : \forall\alpha^{\mathsf{N}}\mathsf{P}$$

[2]This class of formulas corresponds with the class of Σ_1^0 formulas of the arithmetical hierarchy

$$\Gamma, a : \exists\alpha^{\mathsf{N}}\neg\mathsf{P} \vdash \mathtt{W}_a^{\exists\alpha\neg\mathsf{P}} : \exists\alpha^{\mathsf{N}}\neg\mathsf{P}$$

In the first case, we introduce a term that makes the *hypothesis* that P holds for all values of α; in the second, the proof term waits for a *witness* for which P does not hold. From an operational point of view, terms of the form $\mathtt{H}^{\forall\alpha\mathsf{P}}$ are the ones who can raise an exception, and terms of the form $\mathtt{W}_a^{\exists\alpha\neg\mathsf{P}}$ are those who will catch it.

In fig. 3.2, we define a system of natural deduction for $\mathsf{HA} + \mathsf{EM}_1$ together with a term assignment in the spirit of Curry-Howard correspondence for classical logic; for a general treatment of this kind of systems, one could refer to textbooks such as [SU06]. Let $\mathcal{L}$ be the language of HA, three distinct classes of variables appear in the proof terms: one for proof terms, denoted usually as $x, y, \ldots$; one for quantified variables of $\mathcal{L}$, denoted usually as $\alpha, \beta, \ldots$; one for hypotheses bound by EM_1, denoted usually as $a, b, \ldots$. Atomic predicates are denoted by $\mathsf{P}, \mathsf{P}_0, \mathsf{P}_1, \ldots$; moreover, by $\mathsf{P}^\perp$ we denote the complement predicate of P, and since atomic predicates are decidable in HA we have that $\mathsf{P}^\perp \equiv \neg\mathsf{P}$. In the term $u \parallel_a v$ all the occurrences of a in u and v are bound. We assume the usual capture-avoiding substitution for the lambda calculus, and in addition to this we add a new kind of substitution:

Definition 2 (Witness substitution)**.** Let v be any term and n a closed term of $\mathcal{L}$. Then

$$v[a := n]$$

is the term obtained replacing every occurrence of $\mathtt{W}_a^{\exists\alpha\mathsf{P}^\perp}$ in v by $(n, \mathtt{True})$ if $\mathsf{P}[n/\alpha] \equiv \mathtt{False}$, and by $(n, \mathtt{H}_a^{\forall\alpha\alpha=0}\mathsf{S}0)$ otherwise

Note that the reduction rules for the system in fig. 3.3 make it clear that the second case will never actually happen; however it is needed in order to prove the normalization of the system.

3.4 Realizability interpretation of $\mathsf{HA} + \mathsf{EM}_1$

As we anticipated, this system can be equipped with a realizability interpretation based on the ideas of interactive realizability. In order to do this, we first need to define some classes of terms:

Definition 3 (Terms in normal form)**.**

- SN is the set of strongly normalizing untyped proof terms
- NF is the set of normal untyped proof terms
- PNF is the set of the Post normal forms (intuitively, normal terms representing closed proof trees made only of Post rules whose leaves are universal hypothesis followed by an elimination rule), that is: $\mathtt{True} \in \mathsf{PNF}$; for every closed term n of $\mathcal{L}$, if $\mathtt{H}_a^{\forall\alpha\mathsf{P}} n \in \mathsf{NF}$, then $\mathtt{H}_a^{\forall\alpha\mathsf{P}} n \in \mathsf{PNF}$; if $t_1, \ldots, t_n \in \mathsf{PNF}$, then $\mathsf{r}t_1 \ldots t_n \in \mathsf{PNF}$.

Definition 4 (Quasi-Closed terms)**.** If t is an untyped proof term which contains as free variables only EM_1-hypothesis variables $a_1, \ldots, a_n$, such that each occurrence of them is of the form $\mathtt{H}_{a_i}^{\forall\alpha\mathsf{P}_i}$ for some P_i, then t is said to be *quasi-closed*.

We can now give the definition of realizers for $\mathsf{HA} + \mathsf{EM}_1$. Realizers will be quasi closed terms, and the definition will be by induction on the formula to be realized; the cases for $\wedge$, $\to$ and $\forall$ are the same as the ones for intuitionistic realizability we are already familiar with. The case for atomic formulas will need to be extended to take into account the case were we have open universal assumptions (since realizers are quasi-closed). Finally, the realizers for $\vee$ and $\exists$ will need a different kind of definition, with induction done also on the shape of the term.

Definition 5 (Realizability for $\mathsf{HA} + \mathsf{EM}_1$)**.** Assume t is a *quasi-closed* term in the grammar of untyped proof terms of $\mathsf{HA} + \mathsf{EM}_1$ and C is a *closed* formula. We define the relation $t \Vdash C$ by induction on C.

1. $t \Vdash \mathsf{P}$ if and only if one of the following holds:
   i) $t \in \mathsf{PNF}$ and $\mathsf{P} \equiv \mathtt{False}$ implies t contains a subterm $\mathtt{H}_a^{\forall\alpha\mathsf{Q}} n$ with $\mathsf{Q}[n/\alpha] \equiv \mathtt{False}$;
   ii) $t \notin \mathsf{NF}$ and for all t', $t \mapsto t'$ implies $t' \Vdash \mathsf{P}$
2. $t \Vdash A \wedge B$ if and only if $\pi_0 t \Vdash A$ and $\pi_1 t \Vdash B$
3. $t \Vdash A \to B$ if and only if for all u, if $u \Vdash A$, then $tu \Vdash B$
4. $t \Vdash A \vee B$ if and only if one of the following holds:
   i) $t = \iota_0(u)$ and $u \Vdash A$ or $t = \iota_1(u)$ and $u \Vdash B$;
   ii) $t = u \parallel_a v$ and $u \Vdash A \vee B$ and $v[a := m] \Vdash A \vee B$ for every numeral m;
   iii) $t \notin \mathsf{NF}$ is neutral and for all t', $t \mapsto t'$ implies $t' \Vdash A \vee B$.
5. $t \Vdash \forall\alpha^{\mathsf{N}} A$ if and only if for every closed term n of $\mathcal{L}$, $tn \Vdash A[n/\alpha]$
6. $t \Vdash \exists\alpha^{\mathsf{N}} A$ if and only if one of the following holds:
   i) $t = (n, u)$ for some numeral n and $u \Vdash A[n/\alpha]$;

ii) $t = u \parallel_a v$ and $u \Vdash \exists\alpha^{\mathsf{N}} A$ and $v[a := m] \Vdash \exists\alpha^{\mathsf{N}} A$ for every numeral m;

iii) $t \notin \mathsf{NF}$ is neutral and for all t', $t \mapsto t'$ implies $t' \Vdash \exists\alpha^{\mathsf{N}} A$.

As we said, realizers are quasi closed terms: this means that in general realizers could contain open universal assumptions, and thus their correctness depends on them. The base cases of the definition of the realizers for the disjunction and existential quantifiers are again the same as the ones for modified realizability; however, we add a second clause that takes into account the situation where the realizer has used some assumptions; in these cases, we ask that both parts of a term of the shape $u \parallel_a v$ are realizers of the formula in their turn. In a realizer with such a shape, u will then be a realizer with a new open assumption in the form of a term $\mathsf{H}_a^{\forall\alpha\mathsf{P}}$, as the ones just described; v, on the opposite, needs a witness in order to compute and therefore we need to substitute a witness in it in order to obtain a realizer. What this means is that these realizers will still contain a realizer in the usual shape of the clauses (i), but in the form of a *prediction*, as we will see in proposition 2.

We conclude the section by giving some properties of the system, as they are found in the original paper [ABB13], that will be employed in the rest of the thesis. First of all, we define a version of the properties of reducibility candidates in the style of Girard [GTL89]

Definition 6. Let t be a realizer of a formula A, define the following properties for t, plus an inhabitation property **(CR5)** for A:

(CR1) If $t \Vdash A$, then $t \in \mathsf{SN}$.

(CR2) If $t \Vdash A$ and $t \mapsto^* t'$, then $t' \Vdash A$.

(CR3) If $t \notin \mathsf{NF}$ is neutral and for every t', $t \mapsto t'$ implies $t' \Vdash A$, then $t \Vdash A$.

(CR4) If $t = u \parallel_a v$, $u \Vdash A$ and $v[a := m] \Vdash A$ for every numeral m, then $t \Vdash A$.

(CR5) There is a u such that $u \Vdash A$.

Proposition 1. *Every term t has the properties **(CR1)**, **(CR2)**, **(CR3)**, **(CR4)** and the inhabitation property **(CR5)** holds.*

Proof. By induction on C.

- $C = \mathsf{P}$ is atomic.

  (CR1). By induction on the definition of $t \Vdash \mathsf{P}$. If $t \in \mathsf{PNF}$, then $t \in \mathsf{SN}$. If $t \notin \mathsf{NF}$ is neutral, then $t \mapsto t'$ implies $t \Vdash \mathsf{P}$ and thus by induction hypothesis $t' \in \mathsf{SN}$; so $t \in \mathsf{SN}$.

Suppose then $t = u \parallel_a v$. Since $u \Vdash \mathsf{P}$ and for all numerals n, $v[a := n] \Vdash \mathsf{P}$, we have by induction hypothesis $u \in \mathsf{SN}$ and for all numerals n, $v[a := n] \in \mathsf{SN}$; but these last two conditions are easily seen to imply $u \parallel_a v \in \mathsf{SN}$.

(CR2). Suppose $t \Vdash \mathsf{P}$. It suffices to assume that $t \mapsto t'$ and show that $t' \Vdash \mathsf{P}$. We proceed by induction on the number of the occurrences of the symbol $\parallel$ in t. If t is neutral, since it is not the case that $t \in \mathsf{PNF}$, by definition of $t \Vdash \mathsf{P}$ we obtain $t' \Vdash \mathsf{P}$. Therefore, assume t is not neutral and thus $t = u \parallel_a v$, with $u \Vdash \mathsf{P}$ and for all numerals n, $v[a := n] \Vdash \mathsf{P}$. If $t' = u$ or $t' = v[a := m]$ for some numeral m, we obtain the thesis. If $t' = u' \parallel_a v$, with $u \mapsto u'$, then by induction hypothesis, $u' \Vdash \mathsf{P}$. So $u' \parallel_a v \Vdash \mathsf{P}$ by definition. If $t' = u \parallel_a v'$, with $v \mapsto v'$, then for every numeral n, $v[a := n] \mapsto v'[a := n]$, and thus by induction hypothesis $v'[a := n] \Vdash \mathsf{P}$. So $u \parallel_a v' \Vdash \mathsf{P}$ by definition.

(CR3) and **(CR4)** are trivially true by definition of $t \Vdash \mathsf{P}$.

(CR5). We have that $\mathtt{H}_a^{\forall\alpha\,\alpha=0}\mathsf{S}0 \Vdash \mathsf{P}$.

- $C = A \to B$.

(CR1). Suppose $t \Vdash A \to B$. By induction hypothesis **(CR5)**, there is an u such that $u \Vdash A$; therefore, $tu \Vdash B$. By induction hypothesis **(CR1)**, $tu \in \mathsf{SN}$ and thus $t \in \mathsf{SN}$.

(CR2) and **(CR3)** are proved as in [GTL89].

(CR4). ($\Rightarrow$) Suppose $u \parallel_a v \Vdash A \to B$ and let $t \Vdash A$. Then $(u \parallel_a v)t \Vdash B$ and by **(CR2)**, $ut \parallel_a vt \Vdash B$. By **(CR4)**, $ut \Vdash B$ and for all numerals n, $v[a := n]t = vt[a := n] \Vdash B$. We conclude that $u \Vdash A \to B$ and $v[a := n] \Vdash A \to B$.
($\Leftarrow$). Suppose $u \Vdash A \to B$ and $v[a := n] \Vdash A \to B$ for every numeral n. Let $t \Vdash A$. We show by induction on the sum of the height of the reduction trees of u, v, t (they are all in SN by **(CR1)**) that $(u \parallel_a v)t \Vdash B$. By induction hypothesis **(CR3)**, it is enough to assume $(u \parallel_a v)t \mapsto z$ and show $z \Vdash B$. If $z = ut$ or $v[a := n]t$, we are done. If $z = (u' \parallel_a v)t$ or $z = (u \parallel_a v')t$ or $(u \parallel_a v)t'$, with $u \mapsto u'$, $v \mapsto v'$ and $t \mapsto t'$, we obtain $z \Vdash B$ by **(CR2)** and induction hypothesis. If $z = (ut \parallel_a vt)$, by induction hypothesis **(CR4)**, $z \Vdash B$.

(CR5). By induction hypothesis **(CR5)**, there is a term u such that $u \Vdash B$. We want to show that $\lambda\_.u \Vdash A \to B$. Suppose $t \Vdash A$: we have to show that $(\lambda\_.u)t \Vdash B$. We proceed by induction on the sum of the height of the reduction trees of u and t (by **(CR1)**, $u, t \in \mathsf{SN}$). By induction hypothesis **(CR3)**, it is enough to assume $(\lambda\_.u)t \mapsto z$ and show $z \Vdash B$. If $z = u$, we are done. If $z = (\lambda\_.u')t$ or $z = (\lambda\_.u)t'$, with

$u \mapsto u' \Vdash B$ (by **(CR3)**) and $t \mapsto t' \Vdash B$ (by **(CR3)**), we obtain $z \Vdash B$ by induction hypothesis.

- $C = \forall \alpha^{\mathsf{N}} A$ or $C = A \wedge B$. Similar to the case $C = A \to B$.

- $C = A_0 \vee A_1$.

  (CR1) By induction on the definition of $t \Vdash A_0 \vee A_1$. If $t = \iota_i(u)$, then $u \Vdash A_i$, and by induction hypothesis **(CR1)**, $u \in \mathsf{SN}$; therefore, $t \in \mathsf{SN}$. If $t \notin \mathsf{NF}$ is neutral, then $t \mapsto t'$ implies $t' \Vdash A_0 \vee A_1$ and thus $t' \in \mathsf{SN}$ by induction hypothesis; therefore, $t \in \mathsf{SN}$. Suppose then $t = u \parallel_a v$. Since $u \Vdash A_0 \vee A_1$ and for all numerals n, $v[a := n] \Vdash A_0 \vee A_1$, we have by induction hypothesis $u \in \mathsf{SN}$ and for all numerals n, $v[a := n] \in \mathsf{SN}$. We conclude as in the case $C = \mathsf{P}$ that $t \in \mathsf{SN}$.

  (CR2). Suppose $t \Vdash A_0 \vee A_1$. It suffices to assume that $t \mapsto t'$ and show that $t' \Vdash A_0 \vee A_1$. We proceed by induction on the definition of $t \Vdash A_0 \vee A_1$. If $t = \iota_i(u)$, then $t' = \iota_i(u')$, with $u \mapsto u'$. By definition of $t \Vdash A_0 \vee A_1$, we have $u \Vdash A_i$. By induction hypothesis **(CR2)**, $u' \Vdash A_i$ and thus $t' \Vdash A_0 \vee A_1$. If $t \notin \mathsf{NF}$ is neutral, by definition of $t \Vdash A_0 \vee A_1$, we obtain that $t' \Vdash A_0 \vee A_1$. If $t = u \parallel_a v$, with $u \Vdash A_0 \vee A_1$ and for all numerals n, $v[a := n] \Vdash A_0 \vee A_1$. If $t' = u$ or $t' = v[a := m]$, we are done. If $t' = u' \parallel_a v$, with $u \mapsto u'$, then by induction hypothesis, $u' \Vdash A_0 \vee A_1$. So $u' \parallel_a v \Vdash A_0 \vee A_1$ by definition. If $t' = u \parallel_a v'$, with $v \mapsto v'$, then for every numeral n, $v[a := n] \mapsto v'[a := n]$ and thus by induction hypothesis $v'[a := n] \Vdash A_0 \vee A_1$. So $u \parallel_a v' \Vdash A_0 \vee A_1$ by definition.

  (CR3) and **(CR4)** are trivial.

  (CR5). By induction hypothesis **(CR5)**, there is a term u such that $u \Vdash A_0$. Thus $\iota_0(u) \Vdash A_0 \vee A_1$.

- $C = \exists \alpha^{\mathsf{N}} A$. Similar to the case $t = A_0 \vee A_1$.

□

This first property can be used in order to state a first result on the meaning of realizers: if we denote by $\mathcal{EM}[u]$ a term of the form $((u \parallel v_1) \parallel v_2) \ldots) \parallel v_n$ for any $n \geq 0$, then

Proposition 2 (Weak Disjunction and Numerical Existence Properties)**.**

1. *Suppose* $t \Vdash A \vee B$. *Then either* $t \mapsto^* \mathcal{EM}[\iota_0(u)]$ *and* $u \Vdash A$ *or* $t \mapsto^* \mathcal{EM}[\iota_1(u)]$ *and* $u \Vdash B$.

2. *Suppose* $t \Vdash \exists \alpha^{\mathsf{N}} A$. *Then* $t \mapsto^* \mathcal{EM}[(n, u)]$ *for some numeral* n *such that* $u \Vdash A[n/\alpha]$.

Proof.

1. Since $t \in \mathsf{SN}$ by **(CR1)**, let t' be such that $t \mapsto^* t' \in \mathsf{NF}$. By **(CR2)**, $t' \Vdash A \vee B$. If $t' = \iota_0(u)$, we are done. The only possibility left is that $t' = v \parallel v_1 \parallel v_2 \ldots \parallel v_n$, with v not of the form $w_0 \parallel w_1$. By definition 5.4.(ii) we have $v \Vdash A \vee B$, and since v is normal and not of the form $w_0 \parallel w_1$, by definition 5.4.(i) we have either $v = \iota_0(u)$, with $u \Vdash A$, or $v = \iota_1(u)$, with $u \Vdash B$.

2. Similar to 1.

□

Informally, this means that a realizer of a disjunction "contains" a realizer of one of the disjuncts, and a realizer of an existential statement similarly contains a witness. However, these realizers might rely on universal assumptions. We can specialize this theorem in the case of simpler existential formulas:

Theorem 1 (Existential Witness Extraction)**.** *Suppose* t *is closed,* $t \Vdash \exists \alpha^{\mathsf{N}} \mathsf{P}$ *and* $t \mapsto^* t' \in \mathsf{NF}$. *Then* $t' = (n, u)$ *for some numeral* n *such that* $\mathsf{P}[n/\alpha] \equiv \mathtt{True}$.

Proof. By proposition 2, there is some numeral n such that $t' = \mathcal{EM}[(n, u)]$ and $u \Vdash \mathsf{P}[n/\alpha]$. So

$$t' = (n, u) \parallel_{a_1} v_1 \parallel_{a_2} v_2 \ldots \parallel_{a_m} v_m$$

Since t' is closed, u is quasi-closed and all its free variables are among $a_1, a_2, \ldots, a_m$. We observe that u must be closed. Otherwise, by definition 5.1.(i) and $u \Vdash \mathsf{P}[n/\alpha]$ we deduce that $u \in \mathsf{PNF}$, and thus u should contain a subterm $\mathtt{H}_{a_i}^{\forall \alpha \mathsf{Q}} n$; moreover, $\mathsf{Q}[n/\alpha] \equiv \mathtt{False}$ otherwise u would not be normal; but then we would have either $m \neq 0$ and $t' \notin \mathsf{NF}$ because $t' \mapsto v_1[a_1 := n] \parallel_{a_2} v_2 \ldots \parallel_{a_m} v_m$, or $m = 0$ and t' non-closed. Since u is closed, we obtain $t' = (n, u)$, for otherwise $t' \mapsto (n, u) \parallel_{a_2} v_2 \ldots \parallel_{a_m} v_m$ and $t' \notin \mathsf{NF}$. Since $u \Vdash \mathsf{P}[n/\alpha]$, by definition 5.1.(i) it must be $\mathsf{P}[n/\alpha] \equiv \mathtt{True}$. □

We now come to the main theorem, the soundness of the realizability semantics:

Theorem 2 (Adequacy Theorem)**.** *Suppose that* $\Gamma \vdash w : A$ *in the system* $\mathsf{HA} + \mathsf{EM}_1$*, with*

$$\Gamma = x_1 : A_1, \ldots, x_n : A_n, a_1 : \exists \alpha_1^{\mathsf{N}} \mathsf{P}_1^{\perp}, \ldots, a_m : \exists \alpha_m^{\mathsf{N}} \mathsf{P}_m^{\perp}, b_1 : \forall \alpha_1^{\mathsf{N}} \mathsf{Q}_1, \ldots, b_l : \forall \alpha_l^{\mathsf{N}} \mathsf{Q}_l$$

and that the free variables of the formulas occurring in Γ *and* A *are among* $\alpha_1, \ldots, \alpha_k$. *For all closed terms* $r_1, \ldots, r_k$ *of* $\mathcal{L}$*, if there are terms* $t_1, \ldots, t_n$ *such that*

$$\textit{for } i = 1, \ldots, n,\ t_i \Vdash A_i[r_1/\alpha_1 \cdots r_k/\alpha_k]$$

then

$$w[t_1/x_1 \cdots t_n/x_n\, r_1/\alpha_1 \cdots r_k/\alpha_k\, a_1 := i_1 \cdots a_m := i_m] \Vdash A[r_1/\alpha_1 \cdots r_k/\alpha_k]$$

for every numerals $i_1, \ldots, i_m$.

Before proving this theorem, we need an auxiliary lemma

Lemma 1.

1. If for every $t \Vdash A$, $u[t/x] \Vdash B$, then $\lambda x\, u \Vdash A \to B$.
2. If for every closed term m of $\mathcal{L}$, $u[m/\alpha] \Vdash B[m/\alpha]$, then $\lambda\alpha\, u \Vdash \forall\alpha^{\mathsf{N}} B$.
3. If $u \Vdash A_0$ and $v \Vdash A_1$, then $\pi_i\langle u, v\rangle \Vdash A_i$.
4. If $w_0[x_0.u_0, x_1.u_1] \Vdash C$ and for all numerals n, $w_1[x_0.u_0, x_1.u_1][a := n] \Vdash C$, then $(w_0 \parallel_a w_1)[x_0.u_0, x_1.u_1] \Vdash C$.
5. If $t \Vdash A_0 \vee A_1$ and for every $t_i \Vdash A_i$ it holds $u_i[t_i/x_i] \Vdash C$, then $t[x_0.u_0, x_1.u_1] \Vdash C$.
6. If $t \Vdash \exists\alpha^{\mathsf{N}} A$ and for every term n of $\mathcal{L}$ and $v \Vdash A[n/\alpha]$ it holds $u[n/\alpha][v/x] \Vdash C$, then $t[(\alpha, x).u] \Vdash C$.

Proof of lemma 1.

1. As in [GTL89].
2. As in [GTL89].
3. As in [GTL89].
4. We may assume a does not occur in u_0, u_1. By hypothesis, $w_0[x_0.u_0, x_1.u_1] \Vdash C$ and for every numeral n, $w_1[x_0.u_0, x_1.u_1][a := n] \Vdash C$. By **(CR1)**, in order to show $w_0 \parallel_a w_1[x_0.u_0, x_1.u_1] \Vdash C$, we may proceed by induction on the sum of the sizes of the reduction trees of w_0, w_1, u_0, u_1. By **(CR3)**, it then suffices to assume that $w_0 \parallel_a w_1[x_0.u_0, x_1.u_1] \mapsto z$ and show $z \Vdash C$. If $z = w_0[x_0.u_0, x_1.u_1]$ or $w_1[a := n][x_0.u_0, x_1.u_1]$ for some numeral n, we are done. If $z = w_0' \parallel_a w_1[x_0.u_0, x_1.u_1]$ or $z = w_0 \parallel_a w_1'[x_0.u_0, x_1.u_1]$ or $z = w_0 \parallel_a w_1[x_0.u_0', x_1.u_1]$ or $z = w_0 \parallel_a w_1[x_0.u_0, x_1.u_1']$, with $w_i \mapsto w_i'$ and $u_i \mapsto u_i'$, then by **(CR2)** we can apply the induction hypothesis and obtain $z \Vdash C$. If

   $$z = (w_0[x_0.u_0, x_1.u_1]) \parallel_a (w_1[x_0.u_0, x_1.u_1])$$

   then $z \Vdash C$ by **(CR4)**.

5. Suppose $t \Vdash A_0 \vee A_1$ and for every $t_i \Vdash A_i$ it holds $u_i[t_i/x_i] \Vdash C$. In order to show $t[x_0.u_0, x_1.u_1] \Vdash C$, we reason by induction of the definition of $t \Vdash A_0 \vee A_1$. Since by **(CR5)** there are v_0, v_1 such that $v_i \Vdash A_i$, we have $u_i[v_i/x_i] \Vdash A_i$, and thus by **(CR1)**, $u_i[v_i/x_i] \in \mathsf{SN}$ and $t \in \mathsf{SN}$. We have three cases:

   - $t = \iota_i(u)$. Then $u \Vdash A_i$. We want to show that for every $u' \Vdash A_i$, $\iota_0(u')[x_0.u_0, x_1.u_1] \Vdash C$. By **(CR3)**, it suffices to assume that $\iota_0(u)[x_0.u_0, x_1.u_1] \mapsto z$ and show $z \Vdash C$. We reason by induction on the sum of the sizes of the reduction trees of u, u_0, u_1. If $z = \iota_i(u')[x_0.u_0, x_1.u_1]$ or $z = t[x_0.u_0', x_1.u_1]$ or $z = t[x_0.u_0, x_1.u_1']$, with $u \mapsto u'$ and $u_i \mapsto u_i'$, then by **(CR2)** we can apply the induction hypothesis and obtain $z \Vdash C$. If $z = u_i[u/x_i]$, since $u \Vdash A_i$, we obtain $z \Vdash C$.

   - $t = w_0 \parallel_a w_1$. By induction hypothesis $w_0[x_0.u_0, x_1.u_1] \Vdash C$ and for all numerals n, $w_1[a := n][x_0.u_0, x_1.u_1] \Vdash C$. By 4., $w_0 \parallel_a w_1[x_0.u_0, x_1.u_1] \Vdash C$.

   - $t \notin \mathsf{NF}$ is neutral. We reason by induction on the sum of the sizes of the reduction trees of u_0, u_1. By **(CR3)**, it suffices to assume that $t[x_0.u_0, x_1.u_1] \mapsto z$ and show $z \Vdash C$. If $z = t'[x_0.u_0, x_1.u_1]$, we apply the (main) induction hypothesis and obtain $z \Vdash C$. If $z = t[x_0.u_0', x_1.u_1]$ or $z = t[x_0.u_0, x_1.u_1']$, with $u \mapsto u'$ and $u_i \mapsto u_i'$, then by **(CR2)** we can apply the induction hypothesis and obtain $z \Vdash C$.

6. Analogous to 5.

□

Proof. Proof of the Adequacy Theorem

Notation: for any term v and formula B, we denote

$$v[t_1/x_1 \cdots t_n/x_n \; r_1/\alpha_1 \cdots r_k/\alpha_k \; a_1 := i_1 \cdots a_m := i_m]$$

with $\overline{v}$ and

$$B[r_1/\alpha_1 \cdots r_k/\alpha_k]$$

with $\overline{B}$. We proceed by induction on w . Consider the last rule in the derivation of $\Gamma \vdash w : A$:

1. If it is the rule $\Gamma \vdash \mathtt{H}_{b_j}^{\forall\alpha_j\mathsf{P}_j} : \forall\alpha_j^{\mathsf{N}}\mathsf{P}_j$, then $w = \mathtt{H}_{b_j}^{\forall\alpha_j\mathsf{P}_j}$ and $A = \forall\alpha_j^{\mathsf{N}}\mathsf{P}_j$. So $\overline{w} = \mathtt{H}_{b_j}^{\forall\alpha_j\overline{\mathsf{P}_j}}$. Let n be any closed term of $\mathcal{L}$. We must show that $\overline{w}n \Vdash \overline{\mathsf{P}_j}[n/\alpha_j]$. We have $\mathtt{H}_{b_j}^{\forall\alpha_j\overline{\mathsf{P}_j}}n \in \mathsf{SN}$; moreover, if $\mathtt{H}_{b_j}^{\forall\alpha_j\overline{\mathsf{P}_j}}n \mapsto z$, then z is $\mathtt{True}$ and $\overline{\mathsf{P}_j}[n/\alpha_j] \equiv \mathtt{True}$, and thus $z \Vdash \overline{\mathsf{P}_j}[n/\alpha_j]$; if $\mathtt{H}^{\forall\alpha_j\overline{\mathsf{P}_j}}n \in \mathsf{NF}$, then $\overline{\mathsf{P}_j}[n/\alpha_j] \equiv \mathtt{False}$. We conclude $\mathtt{H}_{b_j}^{\forall\alpha_j\overline{\mathsf{P}_j}} \Vdash \forall\alpha_j^{\mathsf{N}}\overline{\mathsf{P}_j} = \overline{A}$.

2. If it is the rule $\Gamma \vdash \mathtt{W}_{a_j}^{\exists\alpha_j \mathsf{P}_j{}^{\perp}} : \exists\alpha_j^{\mathsf{N}}\mathsf{P}_j^{\perp}$, then $w = \mathtt{W}_{a_j}^{\exists\alpha_j \mathsf{P}_j{}^{\perp}}$ and $A = \exists\alpha_j^{\mathsf{N}}\mathsf{P}_j^{\perp}$. We have two possibilities. i) $\overline{w} = (i_j, \mathtt{True})$ and $\overline{\mathsf{P}_j}[i_j/\alpha_j] \equiv \mathtt{False}$. But this means that $\overline{w} \Vdash \exists\alpha_j^{\mathsf{N}}\overline{\mathsf{P}_j}^{\perp}$. ii) $\overline{w} = (i_j, \mathtt{H}_{a_j}^{\forall\alpha\, \alpha=0}\mathsf{S}0)$. Again, $\overline{w} \Vdash \exists\alpha_j^{\mathsf{N}}\overline{\mathsf{P}_j}^{\perp}$.

3. If it is a $\vee$-I rule, say left (the other case is symmetric), then $w = \iota_0(u)$, $A = B \vee C$ and $\Gamma \vdash u : B$. So, $\overline{w} = \iota_0(\overline{u})$. By induction hypothesis $\overline{u} \Vdash \overline{B}$ and thus $\overline{u} \in \mathsf{SN}$. We conclude $\iota_0(\overline{u}) \Vdash \overline{B} \vee \overline{C} = \overline{A}$.

4. If it is a $\vee$-E rule, then
$$w = u[x.w_1, y.w_2]$$
and $\Gamma \vdash u : B \vee C, \Gamma, x : B \vdash w_1 : D, \Gamma, y : C \vdash w_2 : D$, $A = D$. By induction hypothesis, we have $\overline{u} \Vdash \overline{B} \vee \overline{C}$; moreover, for every $t \Vdash \overline{B}$, we have $\overline{w}_1[t/x] \Vdash \overline{B}$ and for every $t \Vdash \overline{C}$, we have $\overline{w}_2[t/y] \Vdash \overline{C}$. By lemma 1, we obtain $\overline{w} = \overline{u}[x.\overline{w}_1, y.\overline{w}_2] \Vdash \overline{D}$.

5. The cases $\exists$-I and $\exists$-E are similar respectively to $\vee$-I and $\vee$-E.

6. If it is the $\forall$-E rule, then $w = ut$, $A = B[t/\alpha]$ and $\Gamma \vdash u : \forall\alpha^{\mathsf{N}}B$. So, $\overline{w} = \overline{u}\overline{t}$. By inductive hypothesis $\overline{u} \Vdash \forall\alpha^{\mathsf{N}}\overline{B}$ and so $\overline{u}\overline{t} \Vdash \overline{B}[\overline{t}/\alpha]$.

7. If it is the $\forall$-I rule, then $w = \lambda\alpha u$, $A = \forall\alpha^{\mathsf{N}}B$ and $\Gamma \vdash u : B$ (with α not occurring free in the formulas of Γ). So, $\overline{w} = \lambda\alpha\overline{u}$, since we may assume $\alpha \neq \alpha_1, \ldots, \alpha_k$. Let t be any closed term of $\mathcal{L}$; by lemma 1), it is enough to prove that $\overline{u}[t/\alpha] \Vdash \overline{B}[t/\alpha]$, which amounts to show that the induction hypothesis can be applied to u. For this purpose, we observe that, since $\alpha \neq \alpha_1, \ldots, \alpha_k$, for $i = 1, \ldots, n$ we have
$$t_i \Vdash \overline{A}_i = \overline{A}_i[t/\alpha]$$

8. If it is the induction rule, then $w = \mathsf{R}uvt$, $A = B(t)$, $\Gamma \vdash u : B(0)$ and $\Gamma \vdash v : \forall\alpha^{\mathsf{N}}.B(\alpha) \to B(\mathsf{S}(\alpha))$. So, $\overline{w} = \mathsf{R}\overline{u}\overline{v}l$, for some numeral $l = \overline{t}$.

   We prove that for all numerals n, $\mathsf{R}\overline{u}\overline{v}n \Vdash \overline{B}(n)$. By **(CR3)**, it is enough to suppose that $\mathsf{R}\overline{u}\overline{v}n \mapsto w$ and show that $w \Vdash \overline{B}(n)$. By induction hypothesis $\overline{u} \Vdash \overline{B}(0)$ and $\overline{v}m \Vdash \overline{B}(m) \to \overline{B}(\mathsf{S}(m))$ for all closed terms m of $\mathcal{L}$. So by **(CR1)**, we can reason by induction on the sum of the sizes of reduction trees of $\overline{u}$ and $\overline{v}$ and the size of m. If $n = 0$ and $w = \overline{u}$, then we are done. If $n = \mathsf{S}(m)$ and $w = \overline{v}m(\mathsf{R}\overline{u}\overline{v}m)$, by induction hypothesis $\mathsf{R}\overline{u}\overline{v}m \Vdash \overline{B}(m)$; therefore, $w \Vdash \overline{B}(\mathsf{S}m)$. If $w = \mathsf{R}u'\overline{v}m$, with $\overline{u} \mapsto u'$, by induction hypothesis $w \Vdash \overline{B}(m)$. We conclude the same if $w = \mathsf{R}\overline{u}v'm$, with $\overline{v} \mapsto v'$.

   We thus obtain that $\overline{w} \Vdash \overline{B}(l) = \overline{B(t)}$.

9. If it is the EM_1 rule, then $w = u \parallel_a v$, $\Gamma, a : \forall\alpha^{\mathsf{N}}\mathsf{P} \vdash u : C$ and $\Gamma, a : \exists\alpha^{\mathsf{N}}\mathsf{P}^{\perp} \vdash v : C$ and $A = C$. By induction hypothesis, $\overline{u} \Vdash \overline{C}$ and for all numerals m, $\overline{v}[a := m] \Vdash \overline{C}$. By **(CR4)**, we conclude $\overline{w} = \overline{u} \parallel_a \overline{v} \Vdash \overline{C}$.

10. If it is a Post rule, the case w is $\mathtt{True}$ is trivial, so we may assume $w = \mathsf{r}t_1 \dots t_n$, $A = \mathsf{P}$ and $\Gamma \vdash t_1 : \mathsf{P}_1, \dots, \Gamma \vdash t_n : \mathsf{P}_n$. By induction hypothesis, for $i = 1, \dots, n$, we have $\bar{t}_i \Vdash \overline{\mathsf{P}_i}$. By **(CR1)**, we can argue by induction on the size of the reduction tree of $\overline{w}$. We have two cases. i) $\overline{w} \in \mathsf{NF}$. For $i = 1, \dots, n$, by theorem 1, we obtain $\bar{t}_i \in \mathsf{PNF}$. Therefore, also $\overline{w} \in \mathsf{PNF}$. Assume now $\overline{\mathsf{P}} \equiv \mathtt{False}$. Then, for some i, $\overline{\mathsf{P}_i} \equiv \mathtt{False}$. Therefore, $\bar{t}_i$ contains a subterm $[a]\mathtt{H}^{\forall\alpha\mathsf{Q}}n$ with $\mathsf{Q}[n/\alpha] \equiv \mathtt{False}$ and thus also $\overline{w}$. We conclude $\overline{w} \Vdash \overline{\mathsf{P}}$. ii) $\overline{w} \notin \mathsf{NF}$. By **(CR3)**, it is enough to suppose $\overline{w} \mapsto z$ and show $z \Vdash \overline{\mathsf{P}}$. We have $z = \mathsf{r}\bar{t}_1 \dots \bar{t}'_i \dots \bar{t}_n$, with $\bar{t}_i \mapsto \bar{t}'_i$, and by **(CR2)**, $\bar{t}'_i \Vdash \overline{\mathsf{P}_i}$. By induction hypothesis, $z \Vdash \overline{\mathsf{P}}$.

□

As an easy corollary, we get strong normalization of the system

Corollary (Strong Normalization of $\mathsf{HA} + \mathsf{EM}_1$)**.** *All terms of* $\mathsf{HA} + \mathsf{EM}_1$ *are strongly normalizing.*

Grammar of Untyped Terms

$$t, u, v ::= c \mid x \mid tu \mid tm \mid \lambda x u \mid \lambda \alpha u \mid \langle t, u\rangle \mid \pi_0 u \mid \pi_1 u \mid \iota_0(u) \mid \iota_1(u) \mid (m, t) \mid t[x.u, y.v] \mid t[(\alpha, x).u]$$

$$\mid u \parallel_a v \mid \mathtt{H}_a^{\forall \alpha \mathsf{P}} \mid \mathtt{W}_a^{\exists \alpha \mathsf{P}^\perp} \mid \mathsf{True} \mid \mathsf{R}uvm \mid \mathsf{r}t_1 \dots t_n$$

where m ranges over terms of $\mathcal{L}$, x over variables of the lambda calculus and a over EM_1 hypothesis variables. Moreover, in terms of the form $u \parallel_a v$ there is a P such that all the free occurrences of a in u are of the form $\mathtt{H}_a^{\forall \alpha \mathsf{P}}$ and those in v are of the form $\mathtt{W}_a^{\exists \alpha \mathsf{P}^\perp}$.

Contexts With Γ we denote contexts of the form $e_1 : A_1, \dots, e_n : A_n$, where e_i is either a proof-term variable $x, y, z \dots$ or a EM_1 hypothesis variable $a, b, \dots$

Axioms $\Gamma, x : A \vdash x : A \quad \Gamma, a : \forall \alpha^{\mathsf{N}} \mathsf{P} \vdash \mathtt{H}_a^{\forall \alpha \mathsf{P}} : \forall \alpha^{\mathsf{N}} \mathsf{P} \quad \Gamma, a : \exists \alpha^{\mathsf{N}} \mathsf{P}^\perp \vdash \mathtt{W}_a^{\exists \alpha \mathsf{P}^\perp} : \exists \alpha^{\mathsf{N}} \mathsf{P}^\perp$

Conjunction $\dfrac{\Gamma \vdash u : A \quad \Gamma \vdash t : B}{\Gamma \vdash \langle u, t\rangle : A \wedge B} \qquad \dfrac{\Gamma \vdash u : A \wedge B}{\Gamma \vdash \pi_0 u : A} \qquad \dfrac{\Gamma \vdash u : A \wedge B}{\Gamma \vdash \pi_1 u : B}$

Implication $\dfrac{\Gamma \vdash t : A \to B \quad \Gamma \vdash u : A}{\Gamma \vdash tu : B} \qquad \dfrac{\Gamma, x : A \vdash u : B}{\Gamma \vdash \lambda x u : A \to B}$

Disjunction Intro. $\dfrac{\Gamma \vdash u : A}{\Gamma \vdash \iota_0(u) : A \vee B} \qquad \dfrac{\Gamma \vdash u : B}{\Gamma \vdash \iota_1(u) : A \vee B}$

Disjunction Elim. $\dfrac{\Gamma \vdash u : A \vee B \quad \Gamma, x : A \vdash w_1 : C \quad \Gamma, x : B \vdash w_2 : C}{\Gamma \vdash u[x.w_1, x.w_2] : C}$

Universal Quantification $\dfrac{\Gamma \vdash u : \forall \alpha^{\mathsf{N}} A}{\Gamma \vdash ut : A[t/\alpha]} \quad \dfrac{\Gamma \vdash u : A}{\Gamma \vdash \lambda \alpha u : \forall \alpha^{\mathsf{N}} A}$

where t is a term of the language $\mathcal{L}$ and α does not occur free in any formula B occurring in Γ.

Existential Quantification $\dfrac{\Gamma \vdash u : A[t/\alpha]}{\Gamma \vdash (t, u) : \exists \alpha^{\mathsf{N}}.A} \qquad \dfrac{\Gamma \vdash u : \exists \alpha^{\mathsf{N}} A \quad \Gamma, x : A \vdash t : C}{\Gamma \vdash u[(\alpha, x).t] : C}$

where α is not free in C nor in any formula B occurring in Γ.

Induction $\dfrac{\Gamma \vdash u : A(0) \quad \Gamma \vdash v : \forall \alpha^{\mathsf{N}}.A(\alpha) \to A(\mathsf{S}(\alpha))}{\Gamma \vdash \lambda \alpha^{\mathsf{N}} \mathsf{R} uv\alpha : \forall \alpha^{\mathsf{N}} A}$

Post Rules $\dfrac{\Gamma \vdash u_1 : A_1 \; \Gamma \vdash u_2 : A_2 \; \cdots \; \Gamma \vdash u_n : A_n}{\Gamma \vdash u : A}$

where $A_1, A_2, \dots, A_n, A$ are atomic formulas of HA and the rule is a Post rule for equality, for a Peano axiom or for a classical propositional tautology or for booleans and if $n > 0$, $u = \mathsf{r}u_1 \dots u_n$, otherwise $u = \mathsf{True}$.

EM1 $\dfrac{\Gamma, a : \forall \alpha^{\mathsf{N}} \mathsf{P} \vdash w_1 : C \quad \Gamma, a : \exists \alpha^{\mathsf{N}} \mathsf{P}^\perp \vdash w_2 : C}{\Gamma \vdash w_1 \parallel_a w_2 : C}$

Figure 3.2: Term Assignment Rules for $\mathsf{HA} + \mathsf{EM}_1$

Reduction Rules for HA

$$(\lambda x.u)t \mapsto u[t/x] \qquad (\lambda \alpha.u)t \mapsto u[t/\alpha]$$

$$\pi_i\langle u_0, u_1\rangle \mapsto u_i, \text{ for i=0,1}$$

$$\iota_i(u)[x_1.t_1, x_2.t_2] \mapsto t_i[u/x_i], \text{ for i=0,1}$$

$$(n, u)[(\alpha, x).v] \mapsto v[n/\alpha][u/x], \text{ for each numeral } n$$

$$\mathsf{R}uv0 \mapsto u$$

$$\mathsf{R}uv(\mathsf{S}n) \mapsto vn(\mathsf{R}uvn), \text{ for each numeral } n$$

Permutation Rules for $\mathbf{EM}_1$

$$(u \parallel_a v)w \mapsto uw \parallel_a vw$$

$$\pi_i(u \parallel_a v) \mapsto \pi_i u \parallel_a \pi_i v$$

$$(u \parallel_a v)[x.w_1, y.w_2] \mapsto u[x.w_1, y.w_2] \parallel_a v[x.w_1, y.w_2]$$

$$(u \parallel_a v)[(\alpha, x).w] \mapsto u[(\alpha, x).w] \parallel_a v[(\alpha, x).w]$$

Reduction Rules for $\mathbf{EM}_1$

$$u \parallel_a v \mapsto u, \text{ if } a \text{ does not occur free in } u$$

$$u \parallel_a v \mapsto v[a := n], \text{ if } \mathtt{H}_a^{\forall \alpha \mathsf{P}} n \text{ occurs in } u \text{ and } \mathsf{P}[n/\alpha] \text{ is closed and } \mathsf{P}[n/\alpha] = \mathtt{False}$$

$$(\mathtt{H}_a^{\forall \alpha \mathsf{P}})n \mapsto \mathtt{True} \text{ if } \mathsf{P}[n/\alpha] \text{ is } \textit{closed} \text{ and } \mathsf{P}[n/\alpha] \equiv \mathtt{True}$$

Figure 3.3: Reduction Rules for HA + EM_1

CHAPTER 4

Markov's principle in $\mathsf{HA} + \mathsf{EM}_1$

In the previous chapters we have developed the basic tools for understanding Curry-Howard systems and realizability semantics. In this chapter, we will perform a deeper analysis of the system $\mathsf{HA}+\mathsf{EM}_1$, and propose a restricted version (that we will call $\mathsf{HA}+\mathsf{EM}_1^-$) that gains more properties. In particular, we will prove a subject reduction theorem and then use it in order to show that the restricted system satisfies the requirements of constructive logic: whenever we prove a disjunction we are able to prove one of the disjuncts, and whenever we prove a simply existential statement, we are able to exhibit a witness. Finally, we will show that Markov's principle is provable in this restricted system and that it has a realizer that exhibits its computational content; moreover, we will show that Markov's principle is equivalent to the restricted form of excluded middle we have introduced.

Consider the system $\mathsf{HA} + \mathsf{EM}_1$ of [ABB13] presented in section 3.3. We modify the rule $\textsc{em}_1$ by restricting it to the case where the conclusion is of the form $\exists x C$ with C an atomic formula:

$$\frac{\Gamma, \forall x \mathsf{P} \vdash \exists x C \qquad \Gamma, \exists x \mathsf{P}^{\perp} \vdash \exists x C}{\Gamma \vdash \exists x C}\ \textsc{em}_1^-$$

We call this new rule $\textsc{em}_1^-$.

4.1 Subject reduction for $\mathsf{HA} + \mathsf{EM}_1^-$

The subject reduction property asserts that whenever a proof term has a certain type, and it gets reduced a certain number of times, the reduced term will have the same type. When types are taken to correspond to formulas, subject reduction gives us two very important facts:

- From the paradigmatic point of view, it connects the concepts of *proof normalization* and *computation*. Reduction rules for the proof terms are usually direct simulations of proof normalization steps. If the system does enjoy the subject reduction property, we can effectively identify these two notions.
- From a proof-theoretic point of view, when it is added to an adequate realizability interpretation it enables one to draw conclusions on the logical system based on the behaviour of the proof terms. A crucial example of this is given in section 4.2.

More formally, we can write

Definition 7 (Subject reduction)**.** A system enjoys subject reduction if whenever $\Gamma \vdash M : \tau$ and $M \mapsto^* N$, then also $\Gamma \vdash N : \tau$

In [ABB13] it is mentioned that system $\mathsf{HA} + \mathsf{EM}_1$ has the subject reduction property, however the result is not proved. Moreover, classic textbooks such as [SU06] only offer a full proof for simply typed systems (i.e. where the only set of rules is $\to$-I and $\to$-E). We shall now give a detailed proof for the system $\mathsf{HA} + \mathsf{EM}_1^-$.

We first need two preliminary lemmas, similar to the ones presented in [SU06] but extended for our new rules. The main one is the *Generation Lemma*, that given a typed term will allow us to talk about the terms and types used in its type derivation. Then we will need to make sure that substitutions (both ordinary and the witness substitution we have previously defined) do not affect typing of a term.

Lemma 2 (Generation Lemma)**.** Suppose $\Gamma \vdash t : \tau$.

(i) If t is of the form $\lambda x.u$ and $x \notin dom(\Gamma)$, then $\tau = \tau_1 \to \tau_2$ and $\Gamma, x : \tau_1 \vdash u : \tau_2$

(ii) If t is of the form uv, then $\Gamma \vdash u : \sigma \to \tau$ and $\Gamma \vdash v : \sigma$ for some σ

(iii) If t is of the form $\lambda\alpha.u$ and α is not free in Γ then $\tau = \forall\alpha^{\mathsf{N}}\sigma$ and $\Gamma \vdash u : \sigma$

(iv) If t is of the form um, where m is a term in $\mathcal{L}$, then $\tau = \sigma[m/\alpha]$, and $\Gamma \vdash u : \forall\alpha^{\mathsf{N}}\sigma$.

(v) If t is of the form $u[x.w_1, x.w_2]$, then there are τ_1,τ_2 such that $\Gamma \vdash u : \tau_1 \vee \tau_2$, $\Gamma, x : \tau_1 \vdash w_1 : \tau$, $\Gamma, x : \tau_2 \vdash w_2 : \tau$

(vi) If t is of the form $\iota_i(u)$, then $\tau = \tau_1 \vee \tau_2$ and $\Gamma \vdash u : \tau_i$

(vii) If t is of the form $\langle u, v\rangle$, then $\tau = \tau_1 \wedge \tau_2$ and $\Gamma \vdash u : \tau_1$, $\Gamma \vdash v : \tau_2$

(viii) If t is of the form $\pi_i(u)$, then $\Gamma \vdash u : \tau \wedge \sigma$ or $\Gamma \vdash u : \sigma \wedge \tau$ (resp. if $i = 1$ or 2)

(ix) If t is of the form $u[(\alpha, x).v]$, where α is not free in τ and Γ, then there is σ such that $\Gamma, x : \sigma \vdash v : \tau$ and $\Gamma \vdash u : \exists\alpha^{\mathsf{N}}.\sigma$

(x) If t is of the form (m, u), then $\tau = \exists\alpha^{\mathsf{N}}.\tau_1$ and $\Gamma \vdash u : \tau_1[m/\alpha]$

(xi) If t is of the form $\mathsf{R}uvm$, then $\tau = \sigma(m)$, $\Gamma \vdash u : \sigma(0)$, $\Gamma \vdash v : \forall\alpha^{\mathsf{N}}.\sigma(\alpha) \to \sigma(\mathsf{S}\alpha)$

(xii) If t is of the form $[a]_{\mathtt{H}}^{\forall\alpha\mathsf{P}}$, then $\Gamma \vdash [a]_{\mathtt{H}}^{\forall\alpha\mathsf{P}} : \forall\alpha^{\mathsf{N}}\mathsf{P}$ and $\Gamma \vdash a : \forall\alpha^{\mathsf{N}}\mathsf{P}$

(xiii) If t is of the form $u \parallel_a v$, then $\Gamma, a : \forall\alpha^{\mathsf{N}}\mathsf{P} \vdash u : \tau$ and $\Gamma, a : \exists\alpha^{\mathsf{N}}\mathsf{P}^{\perp} \vdash v : \tau$. Moreover, $\tau = \exists\alpha\mathsf{P}$.

Proof. Consider for example the case of $t = \lambda x.u$. Then since the term has a type, the type derivation must end with the $\to$-introduction rule. Then it follows that $\tau = \tau_1 \to \tau_2$ and $\Gamma, x : \tau_1 \vdash u : \tau_2$. The other cases are similar. □

Lemma 3 (Substitution preserves types)**.**

(i) If $\Gamma \vdash u : \tau$ and $\Gamma(x) = \Gamma'(x)$ for all x free in u, then $\Gamma' \vdash u : \tau$

(ii) If $\Gamma, x : \sigma \vdash u : \tau$ and $\Gamma \vdash t : \sigma$, then $\Gamma \vdash u[t/x] : \tau$

(iii) If $\Gamma \vdash u : \tau$, $m \in \mathcal{L}$, then $\Gamma[m/\alpha] \vdash u[m/\alpha] : \tau[m/\alpha]$

Proof.

(i) By induction on the structure of u. The base case is straightforward.

Consider u of the form λyv. We can rename variable y in a way such that it is not free in $\Gamma \cup \Gamma'$. Then, $\tau = \tau_1 \to \tau_2$ by lemma 2 and $\Gamma, y : \tau_1 \vdash v : \tau_2$. From the induction hypothesis, $\Gamma', y : \tau_1 \vdash v : \tau_2$ and using an implication introduction $\Gamma' \vdash v : \tau$. Other cases are analogous.

(ii) By induction on the structure of u.

- Base case: assume $u = y$ is a variable. Then if $y = x$, $\tau = \sigma$ and $u[t/x] = t$; if $y \neq x$, then the thesis follows from the first point.
  If u is a $\textsc{em}_1^-$ hypothesis, the thesis follows from the first point.
- If $u = \lambda yv$, then we can assume, by (i), that $y \neq x$ and y does not occur in Γ. By the generation lemma we have $\tau = \tau_1 \to \tau_2$ and $\Gamma, x : \sigma, y : \tau_1 \vdash v : \tau_2$. By the induction hypothesis $\Gamma, y : \tau_1 \vdash v[t/x] : \tau_2$ and applying implication introduction $\Gamma \vdash \lambda yv[t/x] : \tau_1 \to \tau_2 = \tau$
- If $u = vw$, then by the generation lemma $\Gamma \vdash v : \sigma \to \tau$ and $\Gamma \vdash w : \sigma$ for some σ. Then by the induction hypothesis $\Gamma \vdash v[t/x] : \sigma \to \tau$ and $\Gamma \vdash w[t/x] : \sigma$ and applying the implication elimination rule $\Gamma \vdash v[t/x]w[t/x] : \tau$. By the definition of substitution this also means $\Gamma \vdash vw[t/x] : \tau$.
- If $u = \iota_i(v)$, then by lemma 2 $\tau = \tau_1 \vee \tau_2$ and $\Gamma \vdash v : \tau_i$. By the induction hypothesis, $\Gamma \vdash v[t/x] : \tau_i$ and using the disjunction introduction rule $\Gamma \vdash \iota_i(v[t/x]) : \tau_i$. By definition of substitution this also means $\Gamma \vdash \iota_i(v)[t/x] : \tau_i$

- If $u = v[y.w_1, y.w_2]$, then by lemma 2 there are τ_1,τ_2 such that $\Gamma, x : \sigma \vdash v : \tau_1 \vee \tau_2$, $\Gamma, x : \sigma, y : \tau_1 \vdash w_1 : \tau$, $\Gamma, x : \sigma, y : \tau_2 \vdash w_2 : \tau$. We can apply the induction hypothesis on all these terms and get $\Gamma \vdash v[t/x] : \tau_1 \vee \tau_2$, $\Gamma, y : \tau_1 \vdash w_1[t/x] : \tau$, $\Gamma, y : \tau_2 \vdash w_2[t/x] : \tau$. Then, using the disjunction elimination rule we obtain $\Gamma \vdash v[t/x][y.w_1[t/x], y.w_2[t/x]] : \tau_1 \vee \tau_2$, which by definition of substitution is the same as $\Gamma \vdash (v[y.w_1, y.w_2])[t/x] : \tau_1 \vee \tau_2$

The other cases are similar.

(iii) Again by induction on the structure of u.

- Base case: if $u = x$ is a variable, if judgement $x : \tau$ is in Γ we have the judgement $x : \tau[m/\alpha]$ in $\Gamma[m/\alpha]$. Similarly for the cases of $\mathtt{H}_a^{\forall\alpha\mathsf{P}}$ and $\mathtt{W}_a^{\exists\alpha\mathsf{P}^\perp}$
- If $u = vn$, then by lemma 2 $\tau = \sigma[n/\beta]$ and $\Gamma \vdash v : \forall\beta^{\mathsf{N}}\sigma$. By induction hypothesis $\Gamma[m/\alpha] \vdash v[m/\alpha] : \forall\beta^{\mathsf{N}}\sigma[m/\alpha]$. If $\alpha = \beta$, then $\forall\beta^{\mathsf{N}}\sigma[m/\alpha] = \forall\alpha^{\mathsf{N}}\sigma$; by using universal elimination we have $\Gamma[m/\alpha] \vdash v[m/\alpha](n[m/\alpha]) : \sigma[n[m/\alpha]/\alpha] = \sigma[n/\alpha][m/\alpha]$
  If $\alpha \neq \beta$, then note that $\forall\beta^{\mathsf{N}}\sigma[m/\alpha] = \forall\beta^{\mathsf{N}}(\sigma[m/\alpha])$, and again using universal elimination $\Gamma[m/\alpha] \vdash v[m/\alpha](n[m/\alpha]) : \sigma[n[m/\alpha]/\beta] = \sigma[n/\beta][m/\alpha]$.
- If $u = \lambda\beta v$ then by lemma 2 β is not free in Γ, $\tau = \forall\beta^{\mathsf{N}}\sigma$ and $\Gamma \vdash v : \sigma$.
  Consider first $\alpha \neq \beta$. By induction hypothesis, $\Gamma[m/\alpha] \vdash v[m/\alpha] : \sigma[m/\alpha]$. Using universal introduction (since by renaming of bound variable β is never free in $\Gamma[m/\alpha]$) then $\Gamma[m/\alpha] \vdash \lambda\beta v[m/\alpha] : \sigma[m/\alpha][n/\beta]$, and $\sigma[m/\alpha][n/\beta] = \sigma[n/\beta][m/\alpha]$ since $\alpha \neq \beta$.
  Otherwise, if $\alpha = \beta$, since β is not free in Γ, v and σ the result holds vacuosly.

The other cases are similar. □

Lemma 4 (Witness substitution preserves type)**.** If $\Gamma \vdash u : \tau$, then $\Gamma \vdash u[a := n] : \tau$

Proof. Direct consequence of lemma 3 (ii) □

We are now ready to state the main result for this section:

Theorem 3. $\mathsf{HA} + \mathsf{EM}_1^-$ *has the subject reduction property*

Proof. Assume $\Gamma \vdash t : \tau$ and $t \mapsto_\beta t'$. Proceed by structural induction on the beta reduction.

Reduction rules for HA:

- $t = (\lambda x.u)v : \tau$ and $t \mapsto u[v/x]$. By the generation lemma, $\Gamma \vdash (\lambda x.u) : \sigma \to \tau$ and $\Gamma \vdash v : \sigma$ for some σ. Again by generation lemma, $\Gamma, x : \sigma \vdash u : \tau$. Therefore by lemma 3, $\Gamma \vdash u[v/x] : \tau$.

- $t = (\lambda\alpha.u)v$ and $t \mapsto u[v/\alpha]$. By the generation lemma, $\tau = \tau_1[v/\alpha]$, and $\Gamma \vdash u : \forall\alpha^{\mathsf{N}}\tau_1$. Again by Generation, $\Gamma \vdash u : \tau_1$, and by lemma 3, $\Gamma \vdash u[v/\alpha] : \tau_1[v/\alpha]$
- $t = \pi_i\langle u_0, u_1\rangle$ and $t \mapsto u_i$. Then by lemma 2 $\Gamma \vdash \langle u_0, u_1\rangle : \tau_i \wedge \tau_{1-i}$ (with $\tau_0 = \tau$), and again by lemma 2 $\Gamma \vdash u_0 : \tau_i$ and $\Gamma \vdash u_1 : \tau_{1-i}$. Then for $i = 0, 1$ we have $\Gamma \vdash u_i : \tau_0 = \tau$
- $t = \iota_i(u)[x_1.t_1, x_2.t_2]$ and $t \mapsto t_i[u/x_i]$. By lemma 2 there are τ_1 and τ_2 such that $\Gamma \vdash \iota_i(u) : \tau_1 \vee \tau_2, \Gamma, x : \tau_1 \vdash t_1 : \tau$ and $\Gamma, x : \tau_2 \vdash t_2 : \tau$. Again by lemma 2, $\Gamma \vdash u : \tau_i$, and by lemma 3 $\Gamma \vdash t_i[u/x_i] : \tau$
- $t = (n, u)[(\alpha, x).v]$ and $t \mapsto v[n/\alpha][u/x]$, where α is not free in $\Gamma \cup \{t : \tau\}$. By lemma 2, there is a σ such that $\Gamma, x : \sigma \vdash v : \tau$ and $\Gamma \vdash (n, u) : \exists\alpha^{\mathsf{N}}.\sigma$. Again by lemma 2, $\Gamma \vdash u : \sigma[n/\alpha]$. Using lemma 3 and the fact that α is not free in Γ and τ, we can write $\Gamma, x : \sigma[n/\alpha] \vdash v[n/\alpha] : \tau$; finally, again by lemma 3, $\Gamma \vdash v[n/\alpha][u/x] : \tau$

Rules for induction

- $t = \mathsf{R}uv0$ and $t \mapsto u$. By lemma 2, $\tau = \sigma(0)$ and $\Gamma \vdash u : \sigma(0)$.
- $t = \mathsf{R}uv(\mathsf{S}n)$ and $t \mapsto vn(\mathsf{R}uvn)$. By lemma 2, $\tau = \sigma(\mathsf{S}n)$, $\Gamma \vdash u : \sigma(0)$ and $\Gamma \vdash v : \forall\alpha^{\mathsf{N}}.\sigma(\alpha) \to \sigma(\mathsf{S}\alpha)$. In addition, by generation lemma on the term $\mathsf{R}uvn$ we have $\Gamma \vdash \mathsf{R}uvn : \sigma_1(n)$ and $\Gamma \vdash u : \sigma_1(0)$. Therefore $\sigma_1 = \sigma$. Using the universal quantification rule on v we get $\Gamma \vdash vn : \sigma(n) \to \sigma(\mathsf{S}n)$. Using the implication elimination rule on this and $\mathsf{R}uvn$, we get $\Gamma \vdash vn(\mathsf{R}uvn) : \sigma(\mathsf{S}n)$

Reduction rules for EM_1^- (there is no difference with the case of EM_1):

- $\Gamma \vdash ([a]\mathtt{H}^{\forall\alpha\mathsf{P}})n : \tau$ and $([a]\mathtt{H}^{\forall\alpha\mathsf{P}})n \mapsto \mathtt{True}$. By the generation lemma, $\Gamma \vdash [a]\mathtt{H}^{\forall\alpha\mathsf{P}} : \forall\alpha^{\mathsf{N}}\mathsf{P}$ and also $\Gamma \vdash [a]\mathtt{H}^{\forall\alpha\mathsf{P}} : \forall\alpha^{\mathsf{N}}\tau_1$ and $\tau = \tau_1[m/\alpha]$. Therefore $\mathsf{P} = \tau_1$, and by the condition of the rewrite rule $\tau = \mathsf{P}[m/\alpha] = \mathtt{True}$.
- $\Gamma \vdash u \parallel_a v : \tau$ and $u \parallel_a v \mapsto u$. Then by the generation lemma we have $\Gamma, a : \forall\alpha^{\mathsf{N}}P \vdash u : \tau$. But a is not free in u by definition of the reduction rule, and so $\Gamma \vdash u : \tau$
- $\Gamma \vdash u \parallel_a v : \tau$ and $u \parallel_a v \mapsto v[a := n]$. From lemma 2 $\Gamma, a : \exists\alpha^{\mathsf{N}}\neg P \vdash v : \tau$. From lemma 4, $\Gamma, a : \exists\alpha^{\mathsf{N}}\neg P \vdash v[a := n] : \tau$. Since there are no free occurences of a in $v[a := n]$, $\Gamma \vdash v[a := n] : \tau$.

Permutation rules for EM_1^- :

- $t = (u \parallel_a v)w$ and $t \mapsto uw \parallel_a vw$, where a does not occur free in w. From the generation lemma, $\Gamma \vdash u \parallel_a v : \sigma \to \tau$ and $\Gamma \vdash w : \sigma$ for some σ. Again by generation, $\Gamma, a : \forall\alpha^{\mathsf{N}}\mathsf{P} \vdash u : \sigma \to \tau$ and $\Gamma, a : \exists\alpha^{\mathsf{N}}\mathsf{P}^{\perp} \vdash v : \sigma \to \tau$. Applying implication elimination rule to both terms, and then EM_1^- , we get $\Gamma \vdash uw \parallel_a vw : \tau$

- $t = (u \parallel_a v)[x.w_1, y.w_2]$ and $t \mapsto u[x.w_1, y.w_2] \parallel_a v[x.w_1, y.w_2]$. From lemma 2 there are τ_1, τ_2 s.t $\Gamma \vdash u \parallel_a v : \tau_1 \vee \tau_2$ and $\Gamma, x : \tau_1 \vdash w_1 : \tau, \Gamma, x : \tau_2 \vdash w_2 : \tau$. From lemma 2 again, $\Gamma, a : \forall \alpha^{\mathsf{N}} \mathsf{P} \vdash u : \tau_1 \vee \tau_2$ and $\Gamma, a : \exists \alpha^{\mathsf{N}} \mathsf{P}^{\perp} \vdash v : \tau_1 \vee \tau_2$. Using disjunction elimination on both terms, followed by $\textsc{em}_1^-$, we get $\Gamma \vdash u[x.w_1, y.w_2] \parallel_a v[x.w_1, y.w_2] : \tau$.
- Cases $\pi_i(u \parallel_a v) \mapsto \pi_i u \parallel_a \pi_i v$ and $(u \parallel_a v)[(\alpha, x).w] \mapsto u[(\alpha, x).w] \parallel_a v[(\alpha, x).w]$ are similar to the previous points.

□

4.2 Disjunction and existential properties

The subject reduction theorem we have just proved ensures that, whenever we reduce a proof term with one of the reduction rules, we will obtain another proof term of the same type. This, combined with theorem 2 (the adequacy theorem), allows us to draw conclusions on the behaviour of the logical system based on the behaviour of the proof terms. Such tools will be employed now to prove two important constructive properties of the system $\mathsf{HA} + \mathsf{EM}_1^-$.

Let's first recall the two main theorems we have seen in section 3.4 (the proofs can easily adapted to the new system $\mathsf{HA} + \mathsf{EM}_1^-$.)

Theorem 1 (Existential Witness Extraction)**.** *Suppose t is closed, $t \Vdash \exists \alpha^{\mathsf{N}} \mathsf{P}$ and $t \mapsto^* t' \in \mathsf{NF}$. Then $t' = (n, u)$ for some numeral n such that $\mathsf{P}[n/\alpha] \equiv \mathsf{True}$.*

Although this theorem only talks about Σ_1^0 formulas, this is enough for the purpose of proving the constructivity of $\mathsf{HA} + \mathsf{EM}_1^-$. Indeed, this is the only kind of existential statement that we are allowed to prove with our rule. In order to use the properties of the realizers to talk about the logic system, we will need the adequacy theorem:

Theorem 2 (Adequacy Theorem)**.** *Suppose that $\Gamma \vdash w : A$ in the system $\mathsf{HA} + \mathsf{EM}_1$, with*

$$\Gamma = x_1 : A_1, \dots, x_n : A_n, a_1 : \exists \alpha_1^{\mathsf{N}} \mathsf{P}_1^{\perp}, \dots, a_m : \exists \alpha_m^{\mathsf{N}} \mathsf{P}_m^{\perp}, b_1 : \forall \alpha_1^{\mathsf{N}} \mathsf{Q}_1, \dots, b_l : \forall \alpha_l^{\mathsf{N}} \mathsf{Q}_l$$

and that the free variables of the formulas occurring in Γ and A are among $\alpha_1, \dots, \alpha_k$. For all closed terms $r_1, \dots, r_k$ of $\mathcal{L}$, if there are terms $t_1, \dots, t_n$ such that

$$\text{for } i = 1, \dots, n,\ t_i \Vdash A_i[r_1/\alpha_1 \cdots r_k/\alpha_k]$$

then

$$w[t_1/x_1 \cdots t_n/x_n\ r_1/\alpha_1 \cdots r_k/\alpha_k\ a_1 := i_1 \cdots a_m := i_m] \Vdash A[r_1/\alpha_1 \cdots r_k/\alpha_k]$$

for every numerals $i_1, \dots, i_m$.

Combining these theorems with the new subject reduction theorem, we can now state

Theorem 4 (Disjunction property). *Suppose* $\vdash t : A \vee B$ *in the system* $\mathsf{HA} + \mathsf{EM}_1^-$ *where* t *and* $A \vee B$ *are closed. Then there exists a term* u *s.t.* $\vdash u : A$ *or a term* v *s.t.* $\vdash v : A$

Proof. If t is not in normal form take t' such that $t \mapsto^* t'$, and t' is in normal form. By theorem 3, $\vdash t' : A \vee B$, and then by the adequacy theorem $t' \Vdash A \vee B$. Consider now the possible cases by the definition of realizer:

- If $t' = \iota_i(u)$, from lemma 2 we have that $\vdash u : A$ or $\vdash u : B$ resp. when $i = 0, 1$.
- If $t' = u \parallel_a v$, then by lemma 2 we would have $\vdash t' : \exists\alpha\mathsf{P}$ for some atomic P, but this contradicts the fact that $\vdash t' : A \vee B$; so this case cannot be possible.
- Since t' is already in normal form, the third case cannot be possible.

□

With a very similar argument, we have also

Theorem 5 (Existential property). *Suppose* $\vdash t : \exists\alpha A$ *in the system* $\mathsf{HA} + \mathsf{EM}_1^-$ *where* t *and* $\exists\alpha A$ *are closed. Then there exists a numeral* n *and a term* u *s.t.* $\vdash u : A[n/\alpha]$

Proof. By the adequacy theorem, $t \Vdash \exists\alpha A$. Distinguish cases on the definition of the realizability relation:

- If $t = (n, u)$, then by the generation lemma $\vdash u : A[n/\alpha]$
- If $t = u \parallel_a v$, then by lemma 2 A is atomic. Let t' be such that $t \mapsto^* t' \in \mathsf{NF}$; then, by theorem 1, $t = (n, t')$. By theorem 3 $\vdash (n, t') : \exists\alpha A$, and by lemma 2 we have $\vdash t' : A[n/\alpha]$.

□

4.3 Rule EM_1^- is equivalent to Markov's principle

The fundamental reason behind the constructive analysis of the system $\mathsf{HA} + \mathsf{EM}_1^-$ was its resemblance with Markov's principle. The discussion we have done so far does not depend directly on this; however, the fact that our system is indeed constructive (in the broader sense we have used so far) provides even stronger evidence that the EM_1^- rule should be equivalent to Markov's principle.

Consider the usual system $\mathsf{HA} + \mathsf{EM}_1^-$, and state Markov's principle as the axiom MRK: $\neg\forall\alpha\mathsf{P} \to \exists\alpha\mathsf{P}^\perp$. This gives a proof of the axiom:

$$\dfrac{\dfrac{[\neg\forall\alpha\mathsf{P}]_{(1)} \qquad [\forall\alpha\mathsf{P}]_{\mathrm{EM}_1^-}}{\dfrac{\bot}{\exists\alpha\mathsf{P}^\bot}} \qquad [\exists\alpha\mathsf{P}^\bot]_{\mathrm{EM}_1^-}}{\dfrac{\exists\alpha\mathsf{P}^\bot}{\neg\forall\alpha\mathsf{P}\to\exists\alpha\mathsf{P}^\bot}\,(1)}\,\mathrm{EM}_1^-$$

Conversely, consider the system HA plus the axiom MRK. We can obtain rule EM_1^- as follows: assuming we have proofs $\begin{array}{c}\forall\alpha\mathsf{P}\\ \vdots\\ \exists\alpha C\end{array}$ and $\begin{array}{c}\exists\alpha\mathsf{P}^\bot\\ \vdots\\ \exists\alpha C\end{array}$ build this proof of $\exists\alpha C$:

$$\dfrac{\dfrac{\dfrac{\dfrac{[\forall\alpha C^\bot]_{(1)} \qquad \begin{array}{c}[\forall\alpha\mathsf{P}]_{(2)}\\ \vdots\\ \exists\alpha C\end{array}}{\dfrac{\mathcal{D}_1}{\dfrac{\bot}{\neg\forall\alpha\mathsf{P}}\,(2)}}}{\dfrac{\bot}{\neg\forall\alpha C^\bot}\,(1)} \qquad \dfrac{\dfrac{\dfrac{[\exists\alpha\mathsf{P}^\bot]_{(3)}}{\vdots}}{\dfrac{[\forall\alpha C^\bot]_{(1)} \qquad \exists\alpha C}{\dfrac{\mathcal{D}_1}{\dfrac{\bot}{\neg\exists\alpha\mathsf{P}^\bot}\,(3)}}}}{\dfrac{\mathcal{D}_2}{\forall\alpha\mathsf{P}}}}{\exists\alpha C} \qquad \mathrm{MRK}\ \neg\forall\alpha C^\bot\to\exists\alpha C$$

Where $\mathcal{D}_1$ is given by

$$\dfrac{\dfrac{\forall\alpha C^\bot}{C^\bot(\alpha)} \qquad [C(\alpha)]_\exists}{\dfrac{\bot}{\bot} \qquad \exists\alpha C(\alpha)}\,\exists$$

And $\mathcal{D}_2$ is given by

$$\dfrac{\mathsf{P}(\alpha) \vee \mathsf{P}^{\perp}(\alpha) \qquad [\mathsf{P}(\alpha)]_{\vee\text{-E}} \qquad \dfrac{\dfrac{\neg\exists\alpha\mathsf{P}^{\perp}(\alpha) \qquad \dfrac{[\mathsf{P}^{\perp}(\alpha)]_{(1)}}{\exists\alpha\mathsf{P}^{\perp}(\alpha)}}{\dfrac{\perp}{\neg\mathsf{P}^{\perp}(\alpha)}\,(1)} \qquad [\mathsf{P}^{\perp}(\alpha)]_{\vee\text{-E}}}{\dfrac{\perp}{\mathsf{P}(\alpha)}}}{\dfrac{\mathsf{P}(\alpha)}{\forall\alpha\mathsf{P}(\alpha)}}\,\vee\text{-E}$$

Note that in the last proof we used the axiom $\mathsf{P}(\alpha)\vee\mathsf{P}^{\perp}(\alpha)$ since P is atomic and thus decidable in HA.

4.4 A realizer for Markov's principle

Now that we have a proof tree for Markov's principle in $\mathsf{HA} + \mathsf{EM}_1^-$, we can decorate it in order to get a realizer of the principle:

$$\dfrac{\dfrac{[x : \neg\forall\alpha B]_{(2)} \qquad [\mathtt{H}_a^{\forall\alpha\mathsf{B}} : \forall\alpha B]_{\mathsf{EM}_1^-}}{\dfrac{\dfrac{x\mathtt{H}_a^{\forall\alpha\mathsf{B}} : \perp}{\mathsf{r}x\mathtt{H}_a^{\forall\alpha\mathsf{B}} : B^{\perp}[0/\alpha]}}{(0, \mathsf{r}x\mathtt{H}_a^{\forall\alpha\mathsf{B}}) : \exists\alpha B^{\perp}} \qquad [\mathtt{W}_a^{\exists\alpha\mathsf{B}^{\perp}} : \exists\alpha B^{\perp}]_{\mathsf{EM}_1^-}}{(0, \mathsf{r}x\mathtt{H}_a^{\forall\alpha\mathsf{B}}) \parallel_a \mathtt{W}_a^{\exists\alpha\mathsf{B}^{\perp}} : \exists\alpha B^{\perp}}\,\mathbf{EM}_1^-}{\lambda x.((0, \mathsf{r}x\mathtt{H}_a^{\forall\alpha\mathsf{B}}) \parallel_a \mathtt{W}_a^{\exists\alpha\mathsf{B}^{\perp}}) : \neg\forall\alpha B \to \exists\alpha B^{\perp}}\,(1)$$

The extracted term fully exploits the properties of the system in order to get a more precise computational meaning for Markov's principle. When a realizer for $\neg\forall\alpha B$ is given, it is applied to the hypotetical term. Thus, the computation can proceed by using this assumption and reducing inside the left hand side of the proof term. At some point however, we are guaranteed that the program will use the hypotesis on a term m for which $B[m/\alpha]$ does not hold. At this point, an exception is raised and we gets the witness we were waiting for.

CHAPTER 5

Further generalizations

In the previous section it was shown that Markov's principle is equivalent to the excluded middle restricted to Σ^0_1 formulas and Σ^0_1 conclusions. However when taking a closer look at the formal proof we gave, it can be noticed that the crucial use of Markov's principle in proving this form of the excluded middle is only done on the conclusion. The assumptions are only used in order to obtain a contradiction and then do an *ex falso* reasoning. On the other side, we need Σ^0_1 assumptions in order to be able to prove Markov's principle.

Starting from this observation, we will prove that Markov's principle is equivalent to a rule allowing arbitrary excluded middle with Σ^0_1 conclusions. After introducing this new rule, we will try to use it in order to get a direct translation from proofs of classical arithmetic. We will first introduce the well established tool of negative translations and show how they succeed in embedding classical reasoning inside intuitionistic systems. Then we will introduce a new translation that, although missing the usual properties of negative translations, will be useful for our scope when coupled with a set of proof transformation rules. Thanks to these two tools, we will provide a way to transform classical proofs of simply existential formulas into proofs in $\mathsf{HA} + \mathsf{EM}_1^-$.

We will consider again the system HA of natural deduction for intuitionistic arithmetic, and the $\mathsf{HA} + \mathsf{EM}_1^-$ extension we have already studied. When referring to *classical* proofs, or proofs in Peano Arithmetic PA, we mean proofs in $\mathsf{HA} + \mathsf{EM}$ where we add to HA the rule of full excluded middle:

$$\frac{\Gamma, A \vdash C \qquad \Gamma, \neg A \vdash C}{\Gamma \vdash C}\ \textsc{em}$$

5.1 Full excluded middle with restricted conclusions

Consider a system of natural deduction for intuitionistic arithmetic, to which we add restricted classical reasoning in the form of rule $\textsc{em}^-$:

$$\frac{\Gamma, A \vdash \exists x \mathsf{P} \qquad \Gamma, \neg A \vdash \exists x \mathsf{P}}{\Gamma \vdash \exists x \mathsf{P}}\ \textsc{em}^-$$

That is, we allow to eliminate instances of the excluded middle for arbitrary formulas A, but only if the conclusion is a Σ^0_1 formula.

This deduction, similar to the one of the previous chapter, gives a proof of Markov's principle by using the excluded middle rule on the formula $\exists \alpha \mathsf{P}^\perp$

$$\dfrac{\dfrac{[\exists \alpha \mathsf{P}^\perp]_{\textsc{em}^-} \qquad \dfrac{\dfrac{[\neg \forall \alpha \mathsf{P}]_{(1)} \qquad \dfrac{[\neg \exists \alpha \mathsf{P}^\perp]_{\textsc{em}^-}}{\mathcal{D}}}{\forall \alpha \mathsf{P}}}{\bot}}{\exists \alpha \mathsf{P}^\perp}\ \textsc{em}^-}{\neg \forall \alpha \mathsf{P} \to \exists \alpha \mathsf{P}^\perp}\ (1)$$

Where $\mathcal{D}$ is, as in the previous section,

$$\dfrac{\mathsf{P}(\alpha) \vee \mathsf{P}^\perp(\alpha) \qquad \dfrac{\dfrac{\dfrac{\dfrac{[\mathsf{P}^\perp(\alpha)]_{(1)}}{\exists \alpha \mathsf{P}^\perp(\alpha)} \qquad \neg \exists \alpha \mathsf{P}^\perp(\alpha)}{\bot}}{\neg \mathsf{P}^\perp(\alpha)}\ (1) \qquad [\mathsf{P}^\perp(\alpha)]_{\vee\text{-E}}}{\bot}}{\mathsf{P}(\alpha)}}{\dfrac{\mathsf{P}(\alpha)}{\forall \alpha \mathsf{P}(\alpha)}}\ \vee\text{-E}$$

Conversely, given a system of intuitionistic arithmetic HA with Markov's principle as axiom MRK: $\neg \forall \alpha \mathsf{P} \to \exists \alpha \mathsf{P}^\perp$ we can obtain rule $\textsc{em}^-$ as follows: assuming we have proofs $\begin{array}{c} A \\ \vdots \\ \exists \alpha \mathsf{P} \end{array}$ and $\begin{array}{c} \neg A \\ \vdots \\ \exists \alpha \mathsf{P} \end{array}$ build this proof of $\exists \alpha \mathsf{P}$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\neg A}(2)}{\dfrac{\bot}{\neg\forall\alpha\mathsf{P}^{\bot}}(1)}\quad\exists\alpha\mathsf{P}}{\exists\alpha\mathsf{P}}\quad\dfrac{\dfrac{\dfrac{}{\neg A}(3)}{\dfrac{\bot}{\neg\forall\alpha\mathsf{P}^{\bot}}(1)}\quad\exists\alpha\mathsf{P}}{\exists\alpha\mathsf{P}}}{\exists\alpha\mathsf{P}}\quad\neg\forall\alpha\mathsf{P}^{\bot}\to\exists\alpha\mathsf{P}}\ \text{MRK}$$

Where $\mathcal{D}$ is given by

$$\dfrac{\exists\alpha\mathsf{P}(\alpha)\qquad\dfrac{\dfrac{\forall\alpha\mathsf{P}^{\bot}}{\mathsf{P}^{\bot}(\alpha)}\qquad[\mathsf{P}(\alpha)]_{\exists}}{\bot}}{\bot}\exists$$

We have now a more general result than the one we had in the previous chapter: Markov's principle is equivalent to allowing instances of the excluded middle to be used as axioms if and only if the conclusion of the $\vee$-elimination rule is a Σ^0_1 formula. In one sense this tells us that when conclusions are restricted to be Σ^0_1, allowing premises of arbitrary complexity does not allow us to prove more than what we could prove already with simply existential premises.

5.2 A new negative translation

Negative translations

Negative translations have been known for long time as a tool to embed classical reasoning into intuitionistic logic. Essentially, they consist in a method to transform every formula provable in a classical theory in another formula that is equivalent in classical logic and that, although it is not intuitionistically equivalent, is provable from the translated theory. The most prominent example is probably the so called *Gödel-Gentzen* translation [Göd33], or also *double negation* translation. It assigns to every formula F a formula F^N defined by induction on its structure:

- If F is atomic, $F^N = \neg\neg\, F$
- $(F_1 \wedge F_2)^N$ is $F_1^N \wedge F_2^N$
- $(F_1 \vee F_2)^N$ is $\neg(\neg F_1^N \wedge \neg F_2^N)$
- $(F_1 \to F_2)^N$ is $F_1^N \to F_2^N$

- $(\neg F)^N$ is $\neg F^N$
- $(\forall x\ F)^N$ is $\forall x\ \ F^N$
- $(\exists x\ F)^N$ is $\neg\forall x\ \neg\ F^N$

The following theorem states the result we anticipated informally:

Theorem 6 (Gödel-Gentzen translation)**.** *Let* $\Gamma = A_0, \dots A_n$ *be a set of formulas. Then* $A_1, \dots A_n \vdash A_0$ *is classically derivable if and only if* $A_1^N, \dots A_n^N \vdash A_0^N$ *is intuitionistically derivable.*

For a complete discussion and a proof of this result, one may refer to [Tro73]. The translation proves especially useful in the case of arithmetic, thanks to the following theorem

Theorem 7. *For any formula* A *in the language of arithmetic, if* $\mathsf{PA} \vdash A$ *then* $\mathsf{HA} \vdash A^N$

Proof. Thanks to theorem 6, we already know that $\mathsf{PA} \vdash A$ if and only if $\mathsf{HA}^N \vdash A^N$. What we need to show is that if $\mathsf{HA}^N \vdash A^N$, then $\mathsf{HA} \vdash A^N$. In order to do so, we need to prove the translated axioms in HA. We know that $\mathsf{HA} \vdash ((s = t) \to \neg\neg(s = t)) \wedge (\neg\neg(s = t) \to (s = t))$, and therefore since the axioms for equality only use $\forall$ and $\to$, their translation is easily equivalent to the original axiom.

Consider the translation of an instance of the induction axiom:

$$(\forall x(F(x) \to F(\mathbf{s}x)) \to F(0) \to \forall x F(x))^N = \forall x(F^N(x) \to F^N(\mathbf{s}x)) \to F^N(0) \to \forall x F^N(x)$$

Since the second formula is just the instance of the axiom of induction for the formula F^N, it is provable in HA. Therefore, we can conclude that $\mathsf{HA} \vdash \mathsf{HA}^N$, and thus $\mathsf{HA} \vdash A^N$ □

The negative translation allows to embed all of classical arithmetic inside intuitionistic arithmetic. However, the resulting statements often do not provide a clear computational interpretation: consider for example the translation of an existential statement: we obtain something of the form $\neg\forall x\ \neg F$, and it is not clear how one could exctract a witness. For addressing this issues, one needs another translation such as the A-translation of Friedman [Fri78]. Essentially, it consists in replacing every atomic predicate P with $\mathsf{P} \vee A$ for an arbitrary formula A. When we combine it with the Gödel translation, we obtain the following definition: given formulas F_1, F_2, A, where no free variable of A is quantified in F_1 or F_2

- $\neg_A F_1 = F_1 \to A$, $\bot^A = A$
- $F_1^A = \neg_A\neg_A F_1$ if F_1 is atomic
- $(F_1 \wedge F_2)^A = F_1^A \wedge F_2^A$
- $(F_1 \vee F_2)^A = \neg_A(\neg_A F_1^A \wedge \neg_A F_2^A)$

- $(F_1 \to F_2)^A = F_1^A \to F_2^A$
- $(\forall x\ F_1)^A = \forall x\ F_1^A$
- $(\exists x\ F_1)^A = \neg_A \forall x\ \neg_A F_1^A$

We can see that it behaves very similarly to the usual Gödel-Gentzen translation, but with the addition that negation is parametrized by the formula A. With thechniques very similar to those of theorem 6 and 7 we have that if $\Gamma \vdash F$ in PA, then $\Gamma^A \vdash F^A$ in HA. However, the new translation also allows for a major result for the constructive interpretation of some statements of classical arithmetic:

Theorem 8 (Friedman)**.** *Let* P *be an atomic predicate. Then* $\mathsf{PA} \vdash \exists x\ \mathsf{P}(x)$ *if and only if* $\mathsf{HA} \vdash \exists x\ \mathsf{P}(x)$

Proof. Suppose $\mathsf{PA} \vdash \exists x\ \mathsf{P}(x)$; then $\mathsf{HA} \vdash (\exists x\ \mathsf{P}(x))^A$, i.e. $\mathsf{HA} \vdash (\forall x\ \neg_A \neg_A \neg_A \mathsf{P}(x)) \to A$. Since it can be seen that $\neg_A \neg_A \neg_A F \dashv\vdash \neg_A F$ in HA for all F, $\mathsf{HA} \vdash (\forall x\ \neg_A \mathsf{P}(x)) \to A$. Now, since we can use any formula for A, we use $\exists x\ \mathsf{P}(x)$: in this way we get $\mathsf{HA} \vdash \forall x\ (\mathsf{P}(x) \to \exists x\ \mathsf{P}(x)) \to \exists x\ \mathsf{P}(x)$. Since the antecedent of the formula is provable, we get $\mathsf{HA} \vdash \exists x\ \mathsf{P}(x)$. □

The $\exists$-translation

We will now introduce a new translation and consider it for statements of arithmetic. Like the usual negative translations, it will have the property that translated formulas are classically equivalent to the original ones, and that the translated axioms of arithmetic are intuitionistically provable in HA. However, we will not immediately present a result linking classical provability and intuitionistic provability as we did before; indeed, the synctactic translation method presented here will be used in the next section together with a more proof-theoretic technique in order to provide a new interpretation of the simply existential statements of classical arithmetic.

Our translation is particularly simple when compared with the usual ones. It leaves all logical connectives untouched, except for the case of $\forall$, which is substituted by $\neg\exists\neg$. Formally, we define the translation $\cdot^{\exists}$ by induction on the structure of the formula:

- If F is atomic, $F^{\exists} = F$
- $(F_1 \wedge F_2)^{\exists}$ is $F_1^{\exists} \wedge F_2^{\exists}$
- $(F_1 \vee F_2)^{\exists}$ is $F_1^{\exists} \vee F_2^{\exists}$
- $(F_1 \to F_2)^{\exists}$ is $F_1^{\exists} \to F_2^{\exists}$
- $(\forall x\ F)^{\exists}$ is $\neg\exists x\ \neg F^{\exists}$

- $(\exists x\ F)^\exists$ is $\exists x\ F^\exists$

We know that $\forall x\ A(x)$ is classically equivalent to $\neg\exists x\ \neg A(x)$ regardless of A, and thus we can easily state that $\mathsf{PA} \vdash \mathsf{PA}^\exists$ and $\mathsf{PA}^\exists \vdash \mathsf{PA}$. So it is also easy to see

Proposition 3. $\mathsf{PA} \vdash F$ *if and only if* $\mathsf{PA}^\exists \vdash F^\exists$

Proof. By a straightforward induction on the derivation. □

The question is a bit more complicated for intuitionistic arithmetic: in general, the translated formula is not intuitionistically equivalent to the original one. Nevertheless, we have the following result:

Theorem 9. $\mathsf{HA} \vdash \mathsf{HA}^\exists$. *So, every formula provable in* $\mathsf{HA}^\exists$ *is provable in* HA

Proof. The axioms for equality and the definition of the successor are left untouched by the translation. Consider now the translation of the axiom for induction for an arbitrary formula P:

$$(Ind)^\exists = (P(0) \wedge (\forall\alpha\ (P(\alpha) \to P(\alpha+1))) \to \forall\alpha\ P(\alpha))^\exists =$$
$$P(0) \wedge (\neg\exists\alpha.\ \neg(P(\alpha) \to P(\alpha+1))) \to \neg\exists\alpha\neg P(\alpha)$$

The formal derivation in section 5.2 gives a proof of this formula in HA. Therefore, we have that $\mathsf{HA} \vdash \mathsf{HA}^\exists$, and so also whenever $\mathsf{HA}^\exists \vdash F$ $\mathsf{HA} \vdash F$ □

5.3 Embedding classical proofs in $\mathsf{HA} + \mathsf{EM}^-$

We go back now to the system $\mathsf{HA} + \mathsf{EM}^-$ defined in section 5.1. Since in this new system instances of the excluded middle are allowed on arbitrary formulas, we might be tempted to investigate more on how much of a classical proof we can reconstruct in it. A first approach can be the following: in the case the statement to be proved is itself simply existential, we could allow occurrences of the excluded middle rule whenever we are sure they are the lowermost infecences. More formally, we introduce the notation

$$\dfrac{\begin{array}{cccc}\mathcal{D}_1 & \mathcal{D}_2 & & \mathcal{D}_n \\ \exists\alpha\mathsf{P} & \exists\alpha\mathsf{P} & \dots & \exists\alpha\mathsf{P}\end{array}}{\exists\alpha\mathsf{P}}\ \textsc{em}^-$$

to indicate that $\mathcal{D}_1$, $\mathcal{D}_2$ $\dots\mathcal{D}_n$ are proofs of $\exists\alpha\mathsf{P}$ not using $\textsc{em}^-$, possibly with open assumptions, and the conclusion is obtained by repeated usage of the $\textsc{em}^-$ rule on them (note that $\textsc{em}^-$ is indeed used only on a Σ^0_1 formula). Similarly define the same notation for $\textsc{em}$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{[p]_{(1)} : P(0) \wedge (\neg\exists\alpha.\ \neg(P(\alpha) \to P(\alpha+1)))}}{\pi_1(p) : \neg\exists\alpha.\ \neg(P(\alpha) \to P(\alpha+1))} \quad \dfrac{\dfrac{\dfrac{\dfrac{}{[v]_{(5)} \neg\neg P(\alpha)} \quad \dfrac{\dfrac{\dfrac{}{[y]_{(7)} : P(\alpha) \to P(\alpha+1)} \quad \dfrac{}{[z]_{8} : P(\alpha)}}{yz : P(\alpha+1)}}{u(yz) : \bot}}{\lambda z.u(yz) : \neg P(\alpha)}\,(8)}{v(\lambda z.u(yz)) : \bot}}{\lambda y\, v(\lambda z.u(yz)) : \neg(P(\alpha) \to P(\alpha+1))}\,(7)}{\langle \alpha, \lambda y\, v(\lambda z.u(yz))\rangle : \exists\alpha.\ \neg(P(\alpha) \to P(\alpha+1))}}{\pi_1(p)(\langle \alpha, \lambda y\, v(\lambda z.u(yz))\rangle) : \bot}}{\lambda u.\pi_1(p)(\langle \alpha, \lambda y\, v(\lambda z.u(yz))\rangle) : \neg\neg P(\alpha+1)}\,(6)}{\lambda v\lambda u.\pi_1(p)(\langle \alpha, \lambda y\, v(\lambda z.u(yz))\rangle) : \neg\neg P(\alpha) \to \neg\neg P(\alpha+1)}\,(5)}{\lambda\alpha\lambda v\lambda u.\pi_1(p)(\langle \alpha, \lambda y\, v(\lambda z.u(yz))\rangle) : \forall\alpha(\neg\neg P(\alpha) \to \neg\neg P(\alpha+1))}$$

Figure 5.1: Proof of the inductive step ($\mathcal{D}_1$)

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{[x]_{(4)} : \neg P(0)} \quad \dfrac{}{[p]_{(1)} : P(0) \wedge (\neg\exists\alpha.\ \neg(P(\alpha) \to P(\alpha+1)))}}{\pi_0(p) : P(0)}}{x\pi_0(p) : \bot}}{\lambda x.x\pi_0(p) : \neg\neg P(0)}\,(4) \quad \mathcal{D}_1}{\lambda\alpha\lambda v\lambda u.\pi_1(p)(\langle \alpha, \lambda y\, v(\lambda z.u(yz))\rangle) : \forall\alpha(\neg\neg P(\alpha) \to \neg\neg P(\alpha+1))}\,\text{Ind}}{\lambda\alpha\mathbf{R}(\alpha\ \lambda x.x\pi_0(p)\ \lambda\alpha\lambda v\lambda u.\pi_1(p)(\langle \alpha, \lambda y\, v(\lambda z.u(yz))\rangle)) : \forall\alpha\neg\neg P(\alpha)}}{\lambda\alpha\mathbf{R}(\alpha\ \lambda x.x\pi_0(p)\ \lambda\alpha\lambda v\lambda u.\pi_1(p)(\langle \alpha, \lambda y\, v(\lambda z.u(yz))\rangle))\beta : \neg\neg P(\beta) \quad [t]_{(3)(\exists)} : \neg P(\beta)}}{(\lambda\alpha\ (\mathbf{R}(\alpha\ \lambda x.x\pi_0(p)\ \lambda\alpha\lambda v\lambda u.\pi_1(p)(\langle \alpha, \lambda y\, v(\lambda z.u(yz))\rangle)))\beta)t : \bot}}{q[(\beta,t).((\lambda\alpha\ (\mathbf{R}(\alpha\ \lambda x.x\pi_0(p)\ \lambda\alpha\lambda v\lambda u.\pi_1(p)(\langle \alpha, \lambda y\, v(\lambda z.u(yz))\rangle)))\beta)t)] : \bot}\,(3)\ (\exists\text{-E})}{\lambda q\, q[(\beta,t).((\lambda\alpha\ (\mathbf{R}(\alpha\ \lambda x.x\pi_0(p)\ \lambda\alpha\lambda v\lambda u.\pi_1(p)(\langle \alpha, \lambda y\, v(\lambda z.u(yz))\rangle)))\beta)t)] : \neg\exists\alpha\neg P(\alpha)}\,(2)}{\lambda p\lambda q\, q[(\beta,t).((\lambda\alpha\ (\mathbf{R}(\alpha\ \lambda x.x\pi_0(p)\ \lambda\alpha\lambda v\lambda u.\pi_1(p)(\langle \alpha, \lambda y\, v(\lambda z.u(yz))\rangle)))\beta)t)] : P(0) \wedge (\neg\exists\alpha.\ \neg(P(\alpha) \to P(\alpha+1))) \to \neg\exists\alpha\neg P(\alpha)}\,(1)$$

Figure 5.2: Proof of $(Ind)^{\exists}$ in HA

Then clearly the new construct for EM^- can be directly replaced by instances of Markov's principle using the proof tree from section 5.1. Our task for this section is thus to show that any proof (in PA, i.e. $\mathsf{HA} + \mathsf{EM}$) of a simply existential statement can be rewritten into a proof in $\mathsf{HA} + \mathsf{EM}^-$ of the above form.

In order to do so, we employ new permutation rules extending the ones defined in [AZ16] to move the use of classical reasoning below purely intuitionistic proofs. In general, we could have an unrestricted use of the excluded middle, in the form of the rule EM. For every intuitionistic rule, one needs to move the classical rule below it:

$\to$-introduction:

$$\dfrac{\dfrac{\dfrac{}{C}[A] \quad \dfrac{}{B}[B]_{(1)}}{\vdots}}{\dfrac{C}{B \to C}\,(1)} \quad \dfrac{\dfrac{}{C}[\neg A] \quad \dfrac{}{B}[B]_{(1)}}{\vdots}}{C}\,\text{EM} \quad \rightsquigarrow \quad \dfrac{\dfrac{\dfrac{}{C}[A] \quad \dfrac{}{B}[B]_{(1)}}{\vdots}}{\dfrac{C}{B \to C}\,(1)} \quad \dfrac{\dfrac{}{C}[\neg A] \quad \dfrac{}{B}[B]_{(2)}}{\vdots}}{\dfrac{C}{B \to C}\,(2)}}{B \to C}\,\text{EM}$$

$\to$-elimination/1:

$$\dfrac{\dfrac{\dfrac{}{B \to C}[A] \quad \dfrac{}{B \to C}[\neg A]}{\vdots}}{B \to C}\,\text{EM} \quad \dfrac{}{B}}{C} \quad \rightsquigarrow \quad \dfrac{\dfrac{\dfrac{}{B \to C}[A] \quad \dfrac{}{B}}{\vdots} \quad \dfrac{\dfrac{}{B \to C}[\neg A] \quad \dfrac{}{B}}{\vdots}}{C}\,\text{EM}}{C}$$

$\to$-elimination/2:

$$\dfrac{\dfrac{}{B \to C} \quad \dfrac{\dfrac{}{B}[A] \quad \dfrac{}{B}[\neg A]}{\vdots}}{B}\,\text{EM}}{C} \quad \rightsquigarrow \quad \dfrac{\dfrac{\dfrac{}{B \to C}[A] \quad \dfrac{}{B}}{\vdots} \quad \dfrac{\dfrac{}{B \to C}[\neg A] \quad \dfrac{}{B}}{\vdots}}{C}\,\text{EM}}{C}$$

$\wedge$-introduction/1:

$$\dfrac{\dfrac{\dfrac{}{B}[A] \quad \dfrac{}{B}[\neg A]}{\vdots}}{B}\,\text{EM} \quad \dfrac{}{C}}{B \wedge C} \quad \rightsquigarrow \quad \dfrac{\dfrac{\dfrac{}{B}[A] \quad \dfrac{}{C}}{\vdots} \quad \dfrac{\dfrac{}{B}[\neg A] \quad \dfrac{}{C}}{\vdots}}{B \wedge C}\,\text{EM}}{B \wedge C}$$

$\wedge$-introduction/2:

$$\dfrac{\dfrac{}{B} \quad \dfrac{\dfrac{}{C}[A] \quad \dfrac{}{C}[\neg A]}{\vdots}}{C}\,\text{EM}}{B \wedge C} \quad \rightsquigarrow \quad \dfrac{\dfrac{\dfrac{}{B}[A] \quad \dfrac{}{C}}{\vdots} \quad \dfrac{\dfrac{}{B}[\neg A] \quad \dfrac{}{C}}{\vdots}}{B \wedge C}\,\text{EM}}{B \wedge C}$$

$\wedge$-elimination/1, $\wedge$-elimination/2:

$$\dfrac{\dfrac{\begin{array}{cc}[A] & [\neg A] \\ \vdots & \vdots \\ A_1 \wedge A_2 & A_1 \wedge A_2\end{array}}{A_1 \wedge A_2}\,\textsc{em}}{A_i} \quad \rightsquigarrow \quad \dfrac{\dfrac{\begin{array}{cc}[A] & [\neg A] \\ \vdots & \vdots \\ A_1 \wedge A_2 & A_1 \wedge A_2\end{array}}{A_i} \quad \dfrac{\begin{array}{cc}[A] & [\neg A] \\ \vdots & \vdots \\ A_1 \wedge A_2 & A_1 \wedge A_2\end{array}}{A_i}\,\textsc{em}}{A_i}$$

And similarly for $\vee$-introduction, $\vee$-elimination.

$\exists$-introduction:

$$\dfrac{\dfrac{\begin{array}{cc}[A] & [\neg A] \\ \vdots & \vdots \\ B[m/\alpha] & B[m/\alpha]\end{array}}{B[m/\alpha]}\,\textsc{em}}{\exists \alpha B} \quad \rightsquigarrow \quad \dfrac{\dfrac{\begin{array}{cc}[A] & [\neg A] \\ \vdots & \vdots \\ B[m/\alpha] & B[m/\alpha]\end{array}}{\exists \alpha B} \quad \dfrac{\begin{array}{cc}[A] & [\neg A] \\ \vdots & \vdots \\ B[m/\alpha] & B[m/\alpha]\end{array}}{\exists \alpha B}\,\textsc{em}}{\exists \alpha B}$$

$\exists$-elimination/1:

$$\dfrac{\dfrac{\begin{array}{cc}[A] & [\neg A] \\ \vdots & \vdots \\ \exists \alpha B & \exists \alpha B\end{array}}{\exists \alpha B}\,\textsc{em} \quad \begin{array}{c}[B] \\ \vdots \\ C\end{array}}{C} \quad \rightsquigarrow \quad \dfrac{\dfrac{\begin{array}{cc}[A] & [B] \\ \vdots & \vdots \\ \exists \alpha B & C\end{array}}{C} \quad \dfrac{\begin{array}{cc}[\neg A] & [B] \\ \vdots & \vdots \\ \exists \alpha B & C\end{array}}{C}\,\textsc{em}}{C}$$

$\exists$-elimination/2:

$$\dfrac{\begin{array}{c}\vdots \\ \exists \alpha B\end{array} \quad \dfrac{\begin{array}{cc}[A] & [B] \\ \vdots & \vdots \\ C & C\end{array}}{C}\,\textsc{em}}{C} \quad \rightsquigarrow \quad \dfrac{\dfrac{\begin{array}{cc}\vdots & [A] \\ \exists \alpha B & \vdots \\ & C\end{array}}{C} \quad \dfrac{\begin{array}{cc}[B] & [\neg A] \\ \vdots & \vdots \\ \exists \alpha B & C\end{array}}{C}\,\textsc{em}}{C} \qquad \begin{array}{cc}[B] \\ \vdots \\ C\end{array}$$

Now, we would like to define a permutation for the case of the universal quantifier. However, it turns out that this is not possible: for the case of $\forall$-I we have no general way of defining one. Consider for example the proof

$$\dfrac{\dfrac{\dfrac{[P(x)]_{\textsc{em}}}{(P(x) \vee \neg P(x))} \quad \dfrac{[\neg P(x)]_{\textsc{em}}}{(P(x) \vee \neg P(x))}\,\textsc{em}}{(P(x) \vee \neg P(x))}}{\forall x\ (P(x) \vee \neg P(x))}\,\forall\text{-I}$$

Here clearly we have no way of moving the the excluded middle below universal introduction, since the variable x is free before EM lets us discharge the assumptions. This is where the translation from section 5.2 comes to the rescue: clearly, proofs in $\mathsf{PA}^\exists$ will not contain applications of rules for the universal quantifier, and are thus suitable for our transformations. Therefore, the last rule for which we should give a permutation is the translated rule of induction $(Ind)^\exists$ for $\mathsf{PA}^\exists$:

$$\frac{\Gamma \vdash A(0) \qquad \Gamma \vdash \neg\exists\alpha\neg\left(A(\alpha) \to A(\mathsf{S}(\alpha))\right)}{\Gamma \vdash \neg\exists\alpha\, \neg A(\alpha)}\, Ind^\exists$$

The permutations for $Ind^\exists$ will be:

$$\dfrac{\begin{array}{c}\vdots\\ B(0)\end{array} \qquad \dfrac{\begin{array}{c}[A]\\ \vdots\\ \neg\exists\alpha\,\neg B((\alpha) \to B(\mathsf{S}(\alpha)))\end{array} \qquad \dfrac{\begin{array}{c}[\neg A]\\ \vdots\\ \neg\exists\alpha\,\neg(B(\alpha) \to B(\mathsf{S}(\alpha)))\end{array}}{\neg\exists\alpha\,\neg(B(\alpha) \to B(\mathsf{S}(\alpha)))}\,\text{EM}}{\neg\exists\alpha\,\neg B}$$

converts to:

$$\dfrac{\begin{array}{c}\vdots\\ B(0)\end{array} \qquad \dfrac{\begin{array}{c}[A]\\ \vdots\\ \neg\exists\alpha\,\neg(B(\alpha) \to B(\mathsf{S}(\alpha)))\end{array} \qquad \dfrac{\begin{array}{c}\vdots\\ B(0)\end{array} \qquad \dfrac{\begin{array}{c}[\neg A]\\ \vdots\\ \neg\exists\alpha\,\neg(B(\alpha) \to B(\mathsf{S}(\alpha)))\end{array}}{\neg\exists\alpha\,\neg B}\,\text{EM}}{\neg\exists\alpha\,\neg B}}{\neg\exists\alpha\,\neg B}$$

and

$$\dfrac{\dfrac{\begin{array}{c}[A]\\ \vdots\\ B(0)\end{array} \qquad \dfrac{\begin{array}{c}[\neg A]\\ \vdots\\ B(0)\end{array}}{B(0)}\,\text{EM} \qquad \dfrac{\begin{array}{c}\vdots\\ \neg\exists\alpha\,\neg(B(\alpha) \to B(\mathsf{S}(\alpha)))\end{array}}{\neg\exists\alpha\,\neg B}}{\neg\exists\alpha\,\neg B}$$

converts to:

$$\dfrac{\dfrac{\begin{array}{c}[A]\\ \vdots\\ B(0)\end{array} \qquad \dfrac{\begin{array}{c}\vdots\\ \neg\exists\alpha\,\neg(B(\alpha) \to B(\mathsf{S}(\alpha)))\end{array}}{\neg\exists\alpha\,\neg B} \qquad \dfrac{\dfrac{\begin{array}{c}[\neg A]\\ \vdots\\ B(0)\end{array} \qquad \dfrac{\begin{array}{c}\vdots\\ \neg\exists\alpha\,\neg(B(\alpha) \to B(\mathsf{S}(\alpha)))\end{array}}{\neg\exists\alpha\,\neg B}}{\neg\exists\alpha\,\neg B}\,\text{EM}}{\neg\exists\alpha\,\neg B}$$

By employing the just defined permutation rules, we can state

Proposition 4. *Every proof of a formula F in $\mathsf{PA}^{\exists}$ can be transformed into a proof*

$$\dfrac{\begin{array}{cccc}\mathcal{D}_1 & \mathcal{D}_2 & & \mathcal{D}_n \\ F & F & \dots & F\end{array}}{F}\ EM$$

Where $\mathcal{D}_1, \mathcal{D}_2 \dots \mathcal{D}_n$ are purely intuitionistic proofs.

Proof. Proceed by induction on the structure of the proof. The base case where the proof only containts axioms and a single rule is vacuous. Otherwise, assume there is at least one use of EM (if not the thesis holds vacuosly) and consider the lowermost rule application:

- If it is EM , then the induction hypothesis can be applied to the subtrees corresponding to the two premises of the rule, yelding the thesis.
- As an example to the case of unary rules, consider $\exists$-introduction; then the proof has the shape $\dfrac{\begin{array}{c}\vdots \\ F'[m/\alpha]\end{array}}{\exists \alpha F'}\ \exists\text{-I}$

  Applying the induction hypothesis to the subproof corresponding to the premise, by our assumption we get a proof of the form

$$\dfrac{\begin{array}{cccc}\mathcal{D}_1 & \mathcal{D}_2 & & \mathcal{D}_n \\ F'[m/\alpha] & F'[m/\alpha] & \dots & F'[m/\alpha]\end{array}}{F'[m/\alpha]}\ \text{EM}$$

  Substitute this in the original proof: by applying the permutation rule for $\exists$-introduction $n-1$ times, we move the exist introduction right below the intuitionistic part; the proof then becomes

$$\dfrac{\begin{array}{cccc}\mathcal{D}_1 & \mathcal{D}_2 & & \mathcal{D}_n \\ \dfrac{F'[m/\alpha]}{\exists \alpha F'} & \dfrac{F'[m/\alpha]}{\exists \alpha F'} & \dots & \dfrac{F'[m/\alpha]}{\exists \alpha F'}\end{array}}{\exists \alpha F'}\ \text{EM}$$

  Which satisfies the thesis.

  The cases of the other unary rules are analogous.

- As an example for the case of binary rules, consider $\to$-elimination; then the proof has the shape $\dfrac{\begin{array}{cc}\vdots & \vdots \\ G \to F & G\end{array}}{F}\ \to\text{-E}$

  Applying the induction hypothesis to the subproofs corresponding to the premises, by our assumption we get two proofs where in at least one of the two the last used rule is EM : we select one where this is the case.

  Say we chose the proof of the first premise (the other case is symmetric), then from the induction hypothesis we have obtained a proof of the shape

$$\dfrac{\begin{array}{cccc}\mathcal{D}_1 & \mathcal{D}_2 & & \mathcal{D}_n \\ G \to F & G \to F & \dots & G \to F\end{array}}{G \to F}\ \text{EM}$$

  After substitutig this in the original proof, we can employ the permutation for $\to$-elimination $n-1$ times and obtain the proof

$$\dfrac{\begin{array}{cccccc}\mathcal{D}_1 & \vdots & \mathcal{D}_2 & \vdots & & \mathcal{D}_n \quad \vdots \\ G \to F & G & G \to F & G & & G \to F \quad G\end{array}}{\begin{array}{cccc}F & F & \dots & F\end{array}}\ \text{EM}$$

  If the proof of G is intuitionistic we have the thesis, so assume it is not. Just as before, we can use the induction hypothesis on it, and obtain:

$$\dfrac{\begin{array}{cccccc}\mathcal{D}_1 & \begin{array}{c}\mathcal{E}_1 \\ G\end{array} & \begin{array}{c}\dots \\ \dots\end{array} & \begin{array}{c}\mathcal{E}_m \\ G\end{array} & & \mathcal{D}_n \quad \begin{array}{c}\mathcal{E}_1 \\ G\end{array} \quad \begin{array}{c}\dots \\ \dots\end{array} \quad \begin{array}{c}\mathcal{E}_m \\ G\end{array} \\ G \to F & \multicolumn{3}{c}{\dfrac{}{G}\ \text{EM}} & & G \to F \quad \multicolumn{3}{c}{\dfrac{}{G}\ \text{EM}}\end{array}}{\begin{array}{cccc}F & F & \dots & F\end{array}}\ \text{EM}$$

  After applying $m-1$ times the second permutation for $\to$-elimination, we obtain

$$\dfrac{\dfrac{\begin{array}{cccccc}\mathcal{D}_1 & \mathcal{E}_1 & & \mathcal{D}_1 & \mathcal{E}_m & \\ G \to F & G & & G \to F & G & \end{array}}{\begin{array}{cccc}F & \dots & F\end{array}}\ \text{EM} \quad \dots \quad \dfrac{\begin{array}{cccccc} & \mathcal{D}_n & \mathcal{E}_1 & & \mathcal{D}_n & \mathcal{E}_m \\ & G \to F & G & & G \to F & G\end{array}}{\begin{array}{cccc}F & \dots & F\end{array}}\ \text{EM}}{\begin{array}{cccc}F & \dots & F\end{array}}\ \text{EM}$$

  Which satisfies the thesis. The cases of the other binary rules are analogous.

□

After these transformations we are using the excluded middle only with the statement to prove as a conclusion. A similar result was obtained by Seldin [Sel89], but with a rule for reduction ad absurdum in place of the excluded middle and without induction.

This means that if the statement we are proving is of a certain complexity, we do not need classical reasoning on formulas of higher complexity.

Proposition 5. *Every proof in* $\mathsf{PA}^\exists$ *of a* Σ^0_1 *statement can be transformed into a proof in* $\mathsf{HA}^\exists + \mathsf{EM}^-_1$

Proof. By the proposition 4 we know we can transform any proof in $\mathsf{PA}^\exists$ of a statement $\exists\alpha\mathsf{P}$ into a proof of the form

$$\dfrac{\begin{array}{cccc}\mathcal{D}_1 & \mathcal{D}_2 & & \mathcal{D}_n \\ \exists\alpha\mathsf{P} & \exists\alpha\mathsf{P} & \dots & \exists\alpha\mathsf{P}\end{array}}{\exists\alpha\mathsf{P}}\ \textsc{em}$$

Since every application of EM happens on a simply existential statement, we can directly replace them with $\textsc{em}^-$. Moreover, from section 5.1 we know that $\textsc{em}^-$ is equivalent to $\textsc{em}^-_1$, and thus we obtain a proof in $\mathsf{HA}^\exists + \mathsf{EM}^-_1$ as desired. □

Finally, we can conclude the section with the main theorem

Theorem 10. *If* $\mathsf{PA} \vdash \exists x\ \mathsf{P}$ *with* P *atomic, then* $\mathsf{HA} + \mathsf{EM}^-_1 \vdash \exists x\ \mathsf{P}$

Proof. Given a proof of $\exists x\ \mathsf{P}$ in PA, by proposition 3 we can apply the $\exists$-translation and obtain a proof of $(\exists x\ \mathsf{P})^\exists = \exists x\ \mathsf{P}$ in $\mathsf{PA}^\exists$. Then, by proposition 5, we can transform this in a proof in $\mathsf{HA}^\exists + \mathsf{EM}^-_1$. Finally, thanks to theorem 9, we know that $\mathsf{HA} + \mathsf{EM}^-_1 \vdash \exists x\ \mathsf{P}$. □

CHAPTER 6

Conclusions

We have seen how the interpretation of Markov's principle in constructive settings has been an historically controversial matter. Kreisel showed by means of the modified realizability that it could not be validated by intuitionistic logic, while Kleene's realizability semantics, although successful in interpreting it, reduced it to a mere unbounded search and thus brought it back to non-constructivity. However, we noted how a much more refined interpretation of Markov's principle was already present in Gödel's work; W.W. Tait, in a more recent analysis of Gödel's position on intuitionism, notices how in more modern terms we could state that "if one is looking for methods of proof which automatically yield algorithms for computing a witness for existential theorems, intuitionistic logic is too narrow" [Tai06].

Following more recent lines of research, we introduced the logic $\mathsf{HA} + \mathsf{EM}_1$, a related term calculus following the propositions as types paradigm, and a realizability interpretation of the former into the latter. We saw how the term system of $\mathsf{HA} + \mathsf{EM}_1$ provides a tool to investigate the computational content of Markov's principle, and we interpreted the principle as learning program that gets a witness for the conclusion supposing the assumption does not hold and repeatedly testing it. Moreover, we introduced a restricted version of $\mathsf{HA}+\mathsf{EM}_1$ called $\mathsf{HA} + \mathsf{EM}_1^-$, where we showed that the new logical principle added to the logic is equivalent to Markov's principle. This new system inherits the Curry-Howard correspondence and the realizability interpretation from the one it derives from.

By means of $\mathsf{HA} + \mathsf{EM}_1^-$, we have obtained a new proof of constructivity of intuitionistic arithmetic extended with Markov's principle. Finally, we have generalized the obtained result and shown that Markov's principle is also equivalent to adding to intuitionistic arithmetic the principle EM^-, that is a restricted form of the rule of excluded middle where we are only allowed to use it in disjunction eliminations if the conclusion is simply existential.

This final observation led us to the introduction of a new negative translation in the style of the classic ones by Gödel and Friedman. Our new translation has the advantage of not changing $\exists$ and $\vee$ when compared to the usual ones, but needs a series of permutation rules

to be applied on proofs in order to be useful. Combining these results, we obtained a way to transform classical proofs of Σ^0_1 statements into proofs in $\mathsf{HA} + \mathsf{EM}_1^-$, thus allowing us to extract programs from any of these proofs.

Our system $\mathsf{HA} + \mathsf{EM}_1^-$ is reminescent of the one of Herbelin [Her10]. Here, a deductive system for intuitionistic logic is extended with the two rules THROW and CATCH and is equipped with a Curry-Howard correspondence:

$$\frac{\Gamma \vdash_{\alpha:T,\Delta} p : T}{\Gamma \vdash_{\Delta} \mathtt{catch}_\alpha p : T}\ \textsc{catch} \qquad \frac{\Gamma \vdash_{\Delta} p : T \quad (\alpha : T) \in \Delta}{\Gamma \vdash_{\Delta} \mathtt{throw}_\alpha p : C}\ \textsc{throw}$$

The reduction rules for the lambda terms `catch` and `throw` define a mechanism of delimited exceptions. Herbelin addresses pure first order logic, and obtains for Markov's principle the term

$$\lambda a.\mathtt{catch}_\alpha \mathtt{efq}\ a(\lambda b.\mathtt{throw}_\alpha b) : \neg\neg T \to T$$

where T is a $\forall$, $\to$-free formula. The behaviour of the term is similar to the one presented in section 4.4. Thanks to this, Herbelin proves the constructivity of the logic by showing the disjunctive and existential properties.

However, in this work we have related Markov's principle to the other semi-classical principle EM_1^-, and thus the logical part of the system results much clearer. In addition, we extended a system of arithmetic whereas Herbelin's work addressed pure intuitionistic logic; by presenting also a realizability interpretation, the extracted programs can be interpreted as a way to actually compute the witnesses for existential statements.

Another related work is [AZ14]. Here the authors extend modified realizability, and thus the work has the advantage of using a purely functional language. However, just like modified realizability, the realizability interpretation that is provided does not satisfy subject reduction and is therefore not suitable for the investigation of the logical properties of the system. Moreover, the realizer for Markov's principle is

$$\lambda z^{(\mathsf{N}\to U)\to U}\langle \mathtt{quote}(z\mathtt{mtest}_{\lambda x.P}), \mathtt{if}\ P^{\perp}[\mathtt{quote}(z\mathtt{mtest}_{\lambda x.P})/x]\ \mathtt{then}\ \mathtt{tt0}\ \mathtt{else}\ z\ \mathtt{mtest}_{\lambda x.P}\rangle$$

where $\mathtt{mtest}_{\lambda x.P} := \lambda x^{\mathsf{N}}.\mathtt{if}\ P\ \mathtt{then}\ \mathtt{tt}x\ \mathtt{else}\ \mathtt{tt}x$. This is much less clear than what we have seen so far, and relies on an internal comunication system based on the primitive type U, terms $\top_0 : U, \top_1 : U, \dots$ and $\bot_0 : U, \bot_1 : U, \dots$ and the reduction rules

$$\mathtt{tt}n \mapsto \top_n \qquad \mathtt{ff}n \mapsto \bot_n$$
$$\mathtt{quote}\top_m \mapsto m \qquad \mathtt{quote}\bot_m \mapsto m$$

As mentioned, this thesis has the advantages of a clearer explanation of Markov's principle and of presenting a system that enjoys subject reduction.

Future Work

As known for example from the field of proof mining [Koh08] Markov's principle is fundamental for the aim of extracting constructive information from non purely constructive proofs. A similarly important principle is the *double negation shift*, stated as

$$\forall x \neg\neg A(x) \to \neg\neg \forall x A(x)$$

for A atomic. In [Ili12], Danko Ilik showed that an intuitionistic logic extended with this principle retains the disjunctive and existential properties, using techniques similar to those of Herbelin. In the same work, he mentions that Herbelin had also extended his calculus of delimited control operators to a system proving this principle. Given the relation between Herbelin's work on Markov's principle and our current work, it is interesting to see if one could develop a modified version of $\mathsf{HA} + \mathsf{EM}^{-}$ that is able to interpret the double negation shift. A candidate could be the system $\mathsf{IL} + \mathsf{EM}$ presented in [AZ16]: we conjecture that a version of this system for arithmetic with restrictions similar to those presented in this thesis would be constructive; its relationship with other principles remains to be studied.

Bibliography

[AB12] Federico Aschieri and Stefano Berardi. “A New Use of Friedman’s Translation: Interactive Realizability”. In: *Ontos-Verlag Series in Mathematical Logic* (2012).

[ABB13] Federico Aschieri, Stefano Berardi, and Giovanni Birolo. “Realizability and Strong Normalization for a Curry-Howard interpretation of HA+ EM1”. In: *LIPIcs-Leibniz International Proceedings in Informatics*. Vol. 23. 2013.

[Aka+04] Y Akama et al. “An arithmetical hierarchy of the law of excluded middle and related principles”. In: *19Th Annual Ieee Symposium On Logic In Computer Science, Proceedings* (2004), pp. 192–201.

[Avi00] Jeremy Avigad. “Interpreting classical theories in constructive ones”. In: *The Journal of Symbolic Logic* 65.04 (2000), pp. 1785–1812.

[AZ14] Federico Aschieri and Margherita Zorzi. “A "Game Semantical" Intuitionistic Realizability Validating Markov’s Principle”. In: *LIPIcs-Leibniz International Proceedings in Informatics*. Vol. 26. 2014. DOI: 10.4230/LIPIcs.TYPES.2013.XXX.

[AZ16] Federico Aschieri and Margherita Zorzi. “On natural deduction in classical first-order logic: Curry-Howard correspondence, strong normalization and Herbrand’s theorem”. In: *Theoretical Computer Science* 625 (2016), pp. 125–146. DOI: 016/j.tcs.2016.02.028.

[Con13] Andrea Condoluci. “Interpretazioni computazionali della contronominale dell’assioma della scelta”. In: (2013).

[Fel88] Mattias Felleisen. “The Theory and Practice of First-class Prompts”. In: *Proceedings of the 15th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*. POPL ’88. San Diego, California, USA: ACM, 1988, pp. 180–190. ISBN: 0-89791-252-7. DOI: 10.1145/73560.73576. URL: http://doi.acm.org/10.1145/73560.73576.

[FO11] Gilda Ferreira and Paulo Oliva. “On various negative translations”. In: *arXiv preprint arXiv:1101.5442* (2011).

[Fri78] Harvey Friedman. “Classically and intuitionistically provably recursive functions”. In: *Higher set theory*. Springer, 1978, pp. 21–27.

[Gen35] Gerhard Gentzen. “Untersuchungen über das logische Schließen. I”. In: *Mathematische zeitschrift* 39.1 (1935), pp. 176–210.

[Gra13] Hans Bugge Grathwohl. “Programming with Classical Proofs”. MA thesis. Universiteit van Amsterdam, 2013.

[Gri89] Timothy G. Griffin. “A formulae-as-type notion of control”. In: *Proceedings of the 17th ACM SIGPLAN-SIGACT symposium on Principles of programming languages*. 1989, pp. 47–58.

[Gro01] Philippe de Groote. “Strong normalization of classical natural deduction with disjunction”. In: *International Conference on Typed Lambda Calculi and Applications*. 2001, pp. 182–196.

[Gro95] Philippe de Groote. “A simple calculus of exception handling”. In: *International Conference on Typed Lambda Calculi and Applications*. 1995, pp. 201–215.

[GTL89] Jean-Yves Girard, Paul Taylor, and Yves Lafont. *Proofs and types*. Vol. 7. Cambridge University Press, 1989.

[Göd33] Kurt Gödel. “Zur intuitionistischen arithmetik und zahlentheorie”. In: *Ergebnisse eines mathematischen Kolloquiums* 4.1933 (1933), pp. 34–38.

[Göd41] Kurt Gödel. “In what sense is intuitionistic logic constructive”. In: *Kurt Gödel: Collected Works (1995)* 3 (1941), pp. 189–200.

[Göd58] Kurt Gödel. “Über eine bisher noch nicht benützte Erweiterung des finiten Standpunktes”. In: *Dialectica* 12.3-4 (1958), pp. 280–287.

[Göd72] Kurt Gödel. “On an Extension of Finitary Mathematics Which has Not yet Been Used”. In: *Kurt Gödel: Collected Works Vol. II*. Ed. by Solomon Feferman, John Dawson, and Stephen Kleene. Vol. 12. 3-4. Oxford University Press, 1972, pp. 271–284.

[Her10] Hugo Herbelin. “An Intuitionistic Logic That Proves Markov’s Principle”. In: *25Th Annual Ieee Symposium On Logic In Computer Science (Lics 2010)* (2010), pp. 50–56. DOI: 109/LICS.2010.49.

[How69] William Howard. “The formulae-as-types notion of construction”. In: *To H. B. Curry: Essays on Combinatory Logic, Lambda Calculus and Formalism (1980)*. Ed. by J. Seldin and J. Hindley. 1969, pp. 480–490.

[Ili12] Danko Ilik. “Delimited control operators prove double-negation shift”. In: *Annals of Pure and Applied logic* 163.11 (2012), pp. 1549–1559.

[Kle45] S. C. Kleene. “On the interpretation of intuitionistic number theory”. In: *The Journal of Symbolic Logic* 10.04 (Dec. 1945), pp. 109–124. ISSN: 1943-5886. DOI: 10.2307/2269016. URL: http://journals.cambridge.org/article_S0022481200061363.

[Kle60] S.C. Kleene. “Realizability and Shanin’s algorithm for the constructive deciphering of mathematical sentences”. In: *Logique et Analyse, Nouvelle Série* 3 (1960), pp. 154–165.

[Koh08] Ulrich Kohlenbach. *Applied proof theory: proof interpretations and their use in mathematics*. Springer Science & Business Media, 2008.

[Kre59] Georg Kreisel. “Interpretation of Analysis by Means of Constructive Functionals of Finite Types”. In: *Constructivity in Mathematics*. Ed. by A. Heyting. Amsterdam, North-Holland Pub. Co., 1959, pp. 101–128.

[Kre62] G. Kreisel. “On Weak Completeness of Intuitionistic Predicate Logic”. In: *The Journal of Symbolic Logic* 27.2 (1962), pp. 139–158. ISSN: 00224812. URL: http://www.jstor.org/stable/2964110.

[Kri09] Jean-Louis Krivine. “Realizability in classical logic”. In: *Panoramas et synthèses* 27 (2009), pp. 197–229.

[Kri10] Jean-Louis Krivine. “Realizability algebras II: new models of ZF+ DC”. In: *arXiv preprint arXiv:1007.0825* (2010).

[MN54] A. A. Markov and N. M. Nagorny. “Algorithm theory”. In: *Trudy Mat. Inst. Akad. Nauk SSSR* 42 (1954), pp. 1–376.

[Par92] Michel Parigot. “$\lambda\mu$-Calculus: An algorithmic interpretation of classical natural deduction”. In: *Logic Programming and Automated Reasoning*. Ed. by Andrei Voronkov. Vol. 624. Berlin, Heidelberg: Springer Berlin Heidelberg, 1992. Chap. $\lambda\mu$-Calculus: An algorithmic interpretation of classical natural deduction, p. 190. ISBN: 978-3-540-47279-7. DOI: 10.1007/BFb0013061. URL: http://dx.doi.org/10.1007/BFb0013061.

[PG08] Jan von Plato and Gerhard Gentzen. “Gentzen’s Proof of Normalization for Natural Deduction”. In: *The Bulletin of Symbolic Logic* 14.2 (2008), pp. 240–257. ISSN: 10798986. URL: http://www.jstor.org/stable/20059973.

[Pla14] Jan von Plato. “The Development of Proof Theory”. In: *The Stanford Encyclopedia of Philosophy*. Ed. by Edward N. Zalta. Winter 2014. 2014.

[Pra06] Dag Prawitz. “Meaning Approached Via Proofs”. In: *Synthese* 148.3 (2006), p. 507. DOI: 10.1007/s11229-004-6295-2.

[Sel89] Jonathan P. Seldin. “Normalization and Excluded Middle. I”. In: *Studia Logica: An International Journal for Symbolic Logic* 48.2 (1989), pp. 193–217. ISSN: 00393215, 15728730. URL: http://www.jstor.org/stable/20015426.

[SU06] Morten Heine Sørensen and Pawel Urzyczyn. *Lectures on the Curry-Howard isomorphism*. Vol. 149. Elsevier, 2006.

[Tai06] W. W. Tait. “Gödel’s interpretation of intuitionism”. In: *Philosophia Mathematica* 14.2 (2006), pp. 208–228.

[TD88] Anne S. Troelstra and Dirk van Dalen. *Constructivism in Mathematics*. Vol. 1. Elsevier, 1988.

[Tro73] Anne S. Troelstra. *Metamathematical investigation of intuitionistic arithmetic and analysis*. Vol. 344. Springer Science & Business Media, 1973.

[Wad15] Philip Wadler. “Propositions as Types”. In: *Communications Of The Acm* 58 (2015), pp. 75–84. DOI: 145/2699407.