LINEAR SET THEORY

A DISSERTATION
SUBMITTED TO THE DEPARTMENT OF PHILOSOPHY
AND THE COMMITTEE ON GRADUATE STUDIES
OF STANFORD UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

By
Masaru Shirahata
February 1994

I certify that I have read this dissertation and that in my opinion it is fully adequate, in scope and in quality, as a dissertation for the degree of Doctor of Philosophy.

Grigori Mints
(Principal Advisor)

I certify that I have read this dissertation and that in my opinion it is fully adequate, in scope and in quality, as a dissertation for the degree of Doctor of Philosophy.

Solomon Feferman

I certify that I have read this dissertation and that in my opinion it is fully adequate, in scope and in quality, as a dissertation for the degree of Doctor of Philosophy.

John Etchemendy

Approved for the University Committee on Graduate Studies:

Abstract

In this thesis, we develop four systems of set theory based on linear logic. All of those systems have the principle of unrestricted comprehension but they are shown to be consistent. The consitency proofs are given by establishing the cut-elimination theorems.

Our first system of linear set theory SMALL is formulated in full linear logic, *i.e.*, with exponentials. However we do not allow exponentials to appear inside of set terms.

Secondly, we formulate a system of set theory in linear logic with infinitary additive conjunction and disjunction, instead of exponentials. This system is called AS^{∞}.

Thirdly, we present the system of linear set theory LZF which is a conservative extension of Zermelo-Fraenkel set theory without the axiom of regularity or ZF^{-}. The idea is to build up a linear set theory on top of ZF^{-} in a style similar to SMALL. We establish a partial cut-elimination result for LZF, and derive from it that LZF is a conservative extension of ZF^{-}, and therefore consistent relative to ZF^{-}.

Our last system of linear set theory AZF further extends LZF with weakening and the substitutivity principle, which are not available in LZF.

In addition, we present the phase-valued model of linear set theory which is an extension of the Boolean-valued model of classical set theory. This only gives a model of linear set theory with the axiom of separation and not with the unrestricted comprehension.

Finally, we explore possible applications of linear set theory, particularly to the foundations of category theory.

Preface

In this thesis, we develop systems of set theory with the unrestricted comprehension based on linear logic. The underlying idea is that we can avoid the set-theoretical paradoxes, normally created by the unrestricted comprehension, by restricting the use of the contraction rule. Linear logic is used precisely because it is the logic obtained by restricting the contraction rule.

The topic of the thesis is suggested to the author by Prof. Grigori Mints. The formulation of the first system SMALL is due to him. Other systems are developed under his suggestions.

The main result of the thesis is the system LZF, presented in Chapter 4, which is proved to be a conservative extension of Zermelo- Fraenkel set theory without the axiom of regularity.

The consistency result for SMALL was obtained in January, 1992. The phase-valued model was conceived in the spring of 1992, and worked out during the summer. The result about AS^{∞} was essentially obtained from late August to early September of 1992. The formulation of LZF was conceived in the winter of 1993, and the relevant proofs were worked out in the spring. The material on the foundations of category theory presented in Chapter 7 was initially studied in the summer of 1993. This led to the formulation of AZF, which was developed from October, 1993, to January, 1994.

Acknowledgements

First of all, I would like to thank my advisors Solomon Feferman and Grigori Mints.

Grigori Mints has been the driving force of this dissertation, which is based on his idea. Without his direction, this thesis would have never been completed.

Solomon Feferman shows me the standard of logic, which I would like to live up to. It has been a great pleasure and privilege for me to have the opportunity to participate in his seminar for the last three years.

I would also like to thank the following people.

John Etchemendy and John Perry helped me at the crucial stage of this work, by offering the financial support for me.

The seminars and talks by John Mitchell and Vaughan Pratt have been the invaluable resources to learn theoretical computer science and linear logic.

Tim Fernando, Ian Mason and Rick Sommer patiently taught me logic. In particular, Rick Sommer has always been helpful in many aspects of graduate study.

Munkew Leong and Emma Pease have helped me in various problems related to Unix and TeX.

Koji Nakatogawa and Yasushi Fujiwara have been willing to discuss my premature ideas and share their insights with me.

Thank you all.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Introduction

In this thesis, we develop and study systems of set theory based on linear logic. The main idea of the entire project is to avoid set-theoretical paradoxes by the restricted use of the contraction rule. Linear logic is used precisely for the reason that it is the logic obtained by restricting the use of contraction.

In this introduction, we first review one of the set-theoretical paradoxes, *i.e.*, Russell's paradox, to see that the contraction rule is essentially involved in its derivation. Secondly, we give an overview of linear logic and explain the basic intuition behind it. Thirdly, we give a preview of the systems of set theory developed in later chapters and sketch their consistency proofs. Finally, we place linear set theory in a broader context and give some thought on its philosophical meaning.

1.2 Russell's paradox and the contraction rule

1.2.1 Russell's paradox

Set-theoretical paradoxes appear in the pre-axiomatic set theory whose notion of sets is "naive". The fundamental principle of such a set theory is *the principle of unrestricted comprehension*, which says: For any predicate $P(x)$, there exists a set, denoted $\{x : P(x)\}$, such that

$$\forall x(x \in \{x : P(x)\} \leftrightarrow P(x)).$$

This principle is natural and in accord with our ordinary understanding of sets or classes, but it easily leads to contradiction. Russell's paradox shows this in a very simple and clear way.

Consider the predicate "not a member of itself", or "$x \notin x$". Then, the principle says that there exists a set consisting of exactly those objects which satisfy this predicate. Let's call this set R. We now ask if R is a member of itself or not.

1. Assume that R is a member of R. Then R satisfies the predicate, *i.e.*, R is not a member of R.

2. However, by the assumption, R is a member of R. Therefore we have both R is a member of R and R is not a member of R. This is a contradiction.

3. Since we have derived the contradiction from the assumption, we can conclude its negation. Hence R is not a member of R.

4. Then R satisfies the predicate. Therefore R is a member of R.

Note that the assumption "R is a member of R" is used *twice* in this derivation of the paradox, namely, at the step 1 for the first time, and at the step 2 for the second. This is exactly what the contraction rule amounts to.

1.2.2 Contraction in Russell's paradox

In short, the contraction rule says that you can use one assumption as many times as you like. In other words, several assumptions of the same proposition can be regarded as one assumption. Formally, this can be stated in the Gentzen-style sequent calculus as follows [9]:

$$\frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta} \qquad \frac{\Gamma \vdash A, A, \Delta}{\Gamma \vdash A, \Delta}$$

To make the use of contraction explicit, let's give the formal derivation of Russell's paradox in the Gentzen-style sequent calculus. We use the constant symbol $\perp$ for the contradiction, and the sentence $A \to \perp$ for the negation of the sentence A. Then R is denoted as $\{x : x \in$

$x \to \bot\}$, and the derivation is written as follows:

$$
\begin{array}{c}
\underline{R \in R \vdash R \in R \quad \bot \vdash \bot} \\
\underline{R \in R \to \bot, R \in R \vdash \bot} \\
\underline{R \in R, R \in R \vdash \bot} \\
\underline{R \in R \vdash \bot} \\
\underline{\vdash R \in R \to \bot} \\
\vdash R \in R
\end{array}
\quad (*)
$$

where the inference step marked with $(*)$ is an application of the contraction rule.

1.3 Linear logic

1.3.1 An overview

Linear logic is a new system of logic proposed by J.Y. Girard in the middle of 1980's [7], and has been the focus of intensive study in theoretical computer science since then. It is expected that linear logic gives a useful framework to describe dynamic computational processes, with a wide range of applications in functional programming, logic programming, object-oriented programming and concurrency [26].

Classical linear logic is obtained from the classical Gentzen-style sequent calculus by restricting the use of two structural rules, *contraction and weakening.* The two structural rules are no longer applicable to every formula, but only to those created by the new sentential operators, *exponentials.* In classical linear logic, we have the negation operation called *linear negation*, and the negation of the formula A is denoted $A^{\perp}$. All the De Morgan's laws and the law of double negation are assumed and built into the syntax. We will use the Tait-style one-side only presentation for classical linear logic [22].

There are other variants of linear logic. If we allow only one formula to appear on the right side of $\vdash$, the system is called intuitionistic. If we further restrict another structural rule, *exchange*, the system is called non-commutative. All the systems of set theory presented in this thesis are based on classical and commutative linear logic.

In general, the logics obtained by restricting some of the structural rules are called *substructural logics*, and linear logic is one of them. The other members of this family of logics include relevance logic (without weakening), affine logic (without contraction) and Lambek calculus (without weakening, contraction and exchange).

The syntax of linear logic

The restriction on weakening and contraction in linear logic makes it possible to distinguish two kinds of conjunction and disjunction. In classical logic, there are two equivalent ways to formulate the conjunction introduction rule:

$$\frac{\Gamma_1 \vdash A, \Delta_1 \quad \Gamma_2 \vdash B, \Delta_2}{\Gamma_1, \Gamma_2 \vdash A \wedge B, \Delta_1, \Delta_2} \qquad \frac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta}$$

However, they are not equivalent in linear logic, *i.e.*, without weakening and contraction. Therefore, we distinguish the two conjunctions introduced by the first rule and the second. The first type of conjunction is called *multiplicative*, and the second *additive*. The multiplicative conjunction of A and B is denoted $A \otimes B$, and the additive is $A \mathbin{\&} B$. By duality, we also have two types of disjunction. The multiplicative disjunction of A and B is denoted $A \mathbin{⅋} B$, and the additive is $A \oplus B$. The introduction rules for them are:

$$\frac{\vdash A, \Gamma \quad \vdash B, \Delta}{\vdash A \otimes B, \Gamma, \Delta} \qquad \frac{\vdash A, B, \Gamma}{\vdash A \mathbin{⅋} B, \Gamma}$$

$$\frac{\vdash A, \Gamma \quad \vdash B, \Gamma}{\vdash A \mathbin{\&} B, \Gamma} \qquad \frac{\vdash A, \Gamma}{\vdash A \oplus B, \Gamma} \quad \frac{\vdash B, \Gamma}{\vdash A \oplus B, \Gamma}$$

The introduction rule for $⅋$ indicates that the sequent $\vdash \Gamma$ should be interpreted as the multiplicative disjunction of the formulas in the list Γ. We also have the identity constants for each of those operations, *i.e.*, $\mathbf{1}$ for $\otimes$, $\perp$ for $⅋$, $\top$ for $\&$ and $\mathbf{0}$ for $\oplus$. We have the axioms for $\mathbf{1}$ and $\top$, the introduction rule for $\perp$, but none for $\mathbf{0}$:

$$\vdash \mathbf{1} \qquad \vdash \top, \Gamma \qquad \frac{\vdash \Gamma}{\vdash \perp, \Gamma}$$

As already stated, the weakening and contraction rules are applicable only to the formulas created by the exponentials. We have two such exponentials. One of them is the operator !, called *of course*, and the other is its dual ?, called *why not*. The operator ! makes it possible to have contraction and weakening on the left side of $\vdash$, and its dual ? has the same effect on the right side. Since we will use the right-side only presentation in this thesis, contraction and weakening are possible only on the formulas of the form $?A$, *i.e.*:

$$\frac{\vdash ?A, ?A, \Gamma}{\vdash ?A, \Gamma} \qquad \frac{\vdash \Gamma}{\vdash ?A, \Gamma}$$

However it seems pedagogically more useful to present the introduction rules for them in the two-sided way:

$$\frac{\Gamma, A \vdash \Delta}{\Gamma, \,!A \vdash \Delta} \qquad \frac{!\Gamma \vdash A}{!\Gamma \vdash \,!A}$$

where $!\Gamma$ is the list of formulas of the form $!B$ or the constant $\mathbf{1}$. The first rule essentially says that $!A$ entails A, and the second rule says that if A is entailed by the formulas of the form $!B$ or $\mathbf{1}$, then we can strengthen A to $!A$. In the one-sided presentation, those introduction rules become the following:

$$\frac{\vdash \Gamma, A}{\vdash \Gamma, \,?A} \qquad \frac{\vdash \,?\Gamma, A}{\vdash \,?\Gamma, \,!A}$$

where $?\Gamma$ is the list of formulas of the form $?B$ or the constant $\perp$.

The introduction rules for the first-order quantifiers in linear logic are as straightforward as follows:

$$\frac{\vdash A, \Gamma}{\vdash \bigwedge v.A, \Gamma} \qquad \frac{\vdash A[t/v], \Gamma}{\vdash \bigvee v.A, \Gamma}$$

where v is not free in Γ in the rule for the universal quantifier. We note that if we want to regard the universal and existential quantifications as the infinitary conjunction and disjunction, respectively, then they should be understood as additives. This should be obvious once we rewrite the introduction rule for the universal quantifier as the rule for the infinitary conjunction:

$$\frac{\vdash A_i, \Gamma \quad \ldots \quad \vdash A_k, \Gamma \quad \ldots}{\vdash \bigwedge\{A_j : j \in I\}, \Gamma}$$

where the same context Γ is used in all the premises.

Finally, we have the axioms

$$\vdash A, A^{\perp}$$

for any atomic formula A, and the cut rule:

$$\frac{\vdash A, \Gamma \quad \vdash A^{\perp}, \Delta}{\vdash \Gamma, \Delta}$$

This completes our overview of the syntax of linear logic.

The semantics of linear logic

The semantics of linear logic is not as clean as its syntax. In particular, it has been a big challenge to obtain an intuitive and useful semantics for classical linear logic. The difficulty is mainly due to its duality. It is only recently that the game semantics emerged as a strong candidate for this with the impressive application to the full abstraction problem for PCF [1]. However, if we restrict ourselves to intuitionistic linear logic, it is not difficult to give semantics by familiar category theoretic means. In the following, we briefly review the categorical semantics for linear logic [2].

In fact, the logic without contraction and weakening has been studied since the late 1960's exactly because of its neat correspondence with closed monoidal categories. Roughly speaking, a category is a collection of a certain kind of structures and structure-preserving maps between them. For example, the collection of all topological spaces and continuous functions forms a category. In more abstract terminology, strucrures and maps are called *objects* and *morphisms*, respectively. Now suppose that we have a category $\mathcal{C}$ with a commutative and associative binary operation $\otimes$ on its objects. If the category $\mathcal{C}$ has an object, denoted $B \multimap C$, for each pair of its objects B and C, and there is a natural bijection between the morphisms from $A \otimes B$ to C and the morphisms from A to $B \multimap C$, then $\mathcal{C}$ is called a closed monoidal category [17].

The logic without weakening and contraction can be regarded as a closed monoidal category, by interpreting propositions as objects, proofs as morphisms and the multiplicative conjunction as the binary operation $\otimes$. This was first pointed out by J. Lambek and applied in the proof of the coherence theorem for closed monoidal categories [16, 20].

We can also interpret the additive conjunction in the given category, if we add one more binary operation $\&$ which is a Cartesian product in the sense defined in category theory. Therefore, we can say that the intuitionistic linear logic without exponentials is a monoidal closed category with a Cartesian product.

We note that linear logic is not closed with respect to the Cartesian product. This is in sharp contrast to the intuitionistic logic which is a Cartesian closed category.

In addition, the exponential ! has a natural interpretation in category theory as a comonad.

The functions which map objects and morphisms of a category to those of another are called functors if they preserve the basic structural properties of category. A functor from a category $\mathcal{C}$ to $\mathcal{C}$ itself is called an endofunctor. A pair of functors $\mathcal{F}$ and $\mathcal{G}$, from a category $\mathcal{C}$

to $\mathcal{D}$ and from $\mathcal{D}$ to $\mathcal{C}$, respectively, form an *adjunction* if there is a natural bijection between morphisms from $\mathcal{F}A$ to B in $\mathcal{D}$ and morphisms from A to $\mathcal{G}B$ in $\mathcal{C}$ for any objects A in $\mathcal{C}$ and B in $\mathcal{D}$. $\mathcal{F}$ is called the left adjoint of $\mathcal{G}$, and $\mathcal{G}$ the right adjoint of $\mathcal{F}$. Furthermore, such a pair is called an adoint pair. The composition $\mathcal{F} \circ \mathcal{G}$ of such a pair is an endofunctor from $\mathcal{D}$ to $\mathcal{D}$. Comonads are those endofunctors which can be regarded as a composition of an adjoint pair [17].

The observation that ! is just a comonad is due to R. Seely [27]. Indeed, if we limit ourselves to a special case, ! can be described in a very neat way. In short, given a closed monoidal category $\mathcal{C}$, we pick up the objects which can be duplicated, *i.e.* the objects A such that there is a morphism f from A to $A \otimes A$. The pairs (A, f) of such objects and morphisms are called comonoids in $\mathcal{C}$. We then form the new category Com$\mathcal{C}$ from those comonoids and morphisms in $\mathcal{C}$ which commute over the morphisms in the comonoids. The objects in Com$\mathcal{C}$ are identical to the objects in the original category $\mathcal{C}$ except that the former carry the extra information about the duplicating morphisms. The morphisms in Com$\mathcal{C}$ are also morphisms in $\mathcal{C}$. Hence we have a functor from Com$\mathcal{C}$ to $\mathcal{C}$, which simply disregards the extra information about the duplicating morphisms. Such a functor is called the forgetful functor. Then the exponential ! is described as the functor from Com$\mathcal{C}$ to $\mathcal{C}$ such that there is a natural bijection between the morphisms from A to B in $\mathcal{C}$ and the morphisms from A to $!B$ in Com$\mathcal{C}$. In other words, ! is the right adjoint to the forgetful functor. Furthermore, the composition of ! and the forgetful functor is a comonad as it is always the case for adjunction.

To obtain the categorical semantics for classical linear logic, we need to have duals for $\otimes$, $\&$ and !, and the endofunctor which connects up the duals. This is indeed possible, and the category thus obtained is named $*$-autonomous category by M. Barr. However, the $*$-autonomous category does not seem to arise as naturally as the closed monoidal category, and the challenge is to find a natural and useful construction for it. In this respect, we only note that the ongoing works on Chu-construction by Pratt and Gupta, and game semantics by Abramsky and Jagadeesan seem to point to an interesting direction [1, 23].

1.3.2 Interpretation of linear logic

The meaning of a logical system is manifested most evidently in its entailment relation. We describe our intuitive understanding of the logical entailment in linear logic in terms of the useful analogy, *consumption*. This is in contrast to *accumulation*, which is a suitable analogy for intuitionistic logic. We also show that *accumulation* comes from *duplication*, and *vice versa*. Duplication is nothing but the meaning of contraction.

First let's review the meaning of the logical entailments in classical and intuitionistic logic. In classical logic, the entailment $A \vdash B$ means the preservation of truth, *i.e.*: If A is true in a structure (world) M, then B is also true in M. In intuitionistic logic, $A \vdash B$ means the acquisition of knowledge: If we have a justification (knowledge) d of A, then we can construct a justification $F(d)$ of B from d.

The logical entailment in linear logic strongly suggests the interpretation in terms of production from limited resources, *i.e.*, $A \vdash B$ means: If we have a resource r of type A, then we can produce the product $f(r)$ of type B by using r only once.

Note that this interpretation of $A \vdash B$ in linear logic shares the functional view of logical entailment with its intuitionistic counterpart. The difference is that the resource r is *consumed* and annihilated in producing $f(r)$, while the justification d is kept intact and *accumulated* in the construction of $F(d)$.

We want to elaborate this contrast of consumption and accumulation by considering a simple formal property. Let's assume $A \vdash B$. In intuitionistic logic, an object of type A is accumulated in the construction of an object of B so that we also have $A \vdash A \wedge B$. In linear logic, however, an object of type A is consumed in producing an object of B so that the object of type A no longer exist at the moment the object of B comes into existence, *i.e.*, $A \vdash A \otimes B$ does not hold. Diagrammatically, this is expressed as:

$$\begin{array}{rcl} A \vdash B & \Rightarrow & A \vdash A \wedge B \\ & \not\Rightarrow & A \vdash A \otimes B \end{array}$$

In fact, the rule of inference

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

is equivalent to the contraction rule. First, let's derive this rule by using contraction.

$$\cfrac{\cfrac{A \vdash A \quad \Gamma, A \vdash B}{\Gamma, A, A \vdash A \wedge B}}{\Gamma, A \vdash A \wedge B}$$

The other direction is also very easy.

$$\dfrac{\dfrac{A \vdash A}{A \vdash A \wedge A} \quad \dfrac{\Gamma, A, A \vdash B}{\Gamma, A \wedge A \vdash B}}{\Gamma, A \vdash B}$$

In a similar way, we can derive the accumulation from the axiom, *duplication*:

$$A \vdash A \wedge A$$

and *vice versa*. We have already seen that the duplication of A to $A \otimes A$ plays an important role in the categorical semantics of linear logic. This is indeed very satisfactory since contraction is essentially equivalent to duplication as shown below:

$$\dfrac{A \vdash A \otimes A \quad \dfrac{\Gamma, A, A \vdash \Delta}{\Gamma, A \otimes A \vdash \Delta}}{\Gamma, A \vdash \Delta} \qquad \dfrac{\dfrac{A \vdash A \quad A \vdash A}{A, A \vdash A \otimes A}}{A \vdash A \otimes A}$$

From the perspective of intuitionistic logic, accumulation is a natural and obvious principle. This is because the construction in intuitionistic logic is a method to discover a structural relationship between *mathematical patterns*. In other words, the construction has to do with the atemporal relationship between the *universals*, or so-called the *structural universals*, rather than between the *individuals*. The notion of causality, or change, has no place in such a relationship. In particular, nothing ever vanishes in the construction.

From the linear logic perspective, however, accumulation is not natural at all. The reason for this is that the objects involved in production are not mathematical patterns themselves, but their spatio-temporal occurrences, or individuals which exemplify mathematical patterns. Furthermore, the production has a causal character. In particular, resources are consumed in the production process, and no longer available after the production.

From the latter perspective, accumulation is only possible when we have resources which can be duplicated and multiplied by themselves. Then, intuitionistic logic may be interpreted as a special case of linear logic in which it is possible to duplicate everything.

1.4 Linear set theory

1.4.1 Sytems of linear set theory

In this thesis, we develop four systems of linear set theory: SMALL, AS^{∞} , LZF and AZF. All of those systems have the principle of unrestricted comprehension as rules of inference but they are all shown to be consistent. The basic idea is to restrict the use of the comprehension only to a certain type of formulas.

The unrestricted comprehension is formalized in the Gentzen-style sequent calculus by the following two rules of inference:

$$\frac{\Gamma \vdash A[t/x], \Delta}{\Gamma \vdash t \in \{x : A\}, \Delta} \qquad \frac{\Gamma, A[t/x] \vdash \Delta}{\Gamma, t \in \{x : A\}, \vdash \Delta}$$

To restate these rules in our Tait-style presentation of sequent calculus, we need to negate the formulas on the left side and move them to the right so that the rules become:

$$\frac{\vdash A[t/x], \Gamma}{\vdash t \in \{x : A\}, \Gamma} \qquad \frac{\vdash A[t/x]^{\perp}, \Gamma}{\vdash t \notin \{x : A\}, \Gamma}$$

Without any restriction on the application of those rules, Russell's paradox can be easily reproduced in linear logic. Let $R = \{x : ?\, x \notin x\}$. Then we have:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\vdash R \in R, R \notin R}{\vdash R \in R, ?\, R \notin R}}{\vdash !\, R \in R, ?\, R \notin R}}{\vdash R \notin R, ?\, R \notin R}}{\vdash ?\, R \notin R, ?\, R \notin R}}{\vdash ?\, R \notin R}}{\vdash R \in R}}{\vdash !\, R \in R}$$

where we have used $!\, R \in R \equiv (\, ?\, R \notin R)^{\perp}$. It should be clear that the use of exponentials is essential in this derivation. In order to obtain the consistent system, therefore, the use of exponentials has to be restricted in one way or another.

One of the possible ways for such restriction is not to use exponentials at all. In fact, such a system, with weakening, was proved to be consistent by V.N. Grishin in 1974 [12]. Our work extends Grishin's result in various ways.

Our first system of linear set theory SMALL is formulated in full linear logic, *i.e.*, with exponentials. However we do not allow exponentials to appear inside of set terms. In other words, the unrestricted comprehension rules in SMALL are only applicable to the formulas which do not contain exponentials at all. The formulation of SMALL was suggested to us by G. Mints. We prove the consistency of SMALL by establishing the cut-elimination theorem. This result is presented in Chapter 2.

Secondly, we extend Grishin's system by infinitary additive conjunction and disjunction, instead of exponentials. This new system is called AS^∞ since it is a system of set theory in infinitary affine logic. It is based on R.B. White's natural deduction system [30]. White proved the consistency of his system by a partial normalization result. We prove the complete cut-elimination theorem for AS^∞ and its consistency in Chapter 3.

Thirdly, we present a system of linear set theory which is a conservative extension of Zermelo-Fraenkel set theory without the axiom of regularity or ZF^-. The idea is to build up a linear set theory on top of ZF^- in a style similar to SMALL. For this, we first define a class of terms, called Z-terms, which correspond to definable sets in ZF^-. Then we define another class of terms, or S-terms, by induction starting with Z-terms as the basis and using no exponentials in the building up. The only essential restriction we need to impose is that only S-terms can appear in the axioms $\vdash A, A^\perp$. We have no restriction on the use of the unrestricted comprehension rules. This system is called LZF. We establish a partial cut-elimination result for LZF, and derive from it that LZF is a conservative extension of ZF^-, and therefore consistent relative to ZF^-. This is given in Chapter 4.

Our last system of linear set theory AZF further extends LZF with weakening and the substitutivity principle, which are not available in LZF. We establish the similar result for AZF as for LZF, by essentially the same method. However, the substitutivity makes the argument sufficiently complicated to deserve the independent treatment. This is Chapter 5.

Finally, we present our first attempt toward the semantics of systems of linear set theory in Chapter 6. The idea is to extend the Boolean-valued model of classical set theory to the phase-valued model of linear set theory. Unfortunately, this only gives a model of linear set theory with the axiom of separation and not with unrestricted comprehension. Hence the model does not give a semantics to any of our four systems, and this chapter can be read independently of others.

Chapter 7 is the conclusion of this thesis, in which we explore possible applications of linear set theory, particularly to the foundations of category theory.

1.4.2 The consistency proof of linear set theory

All of the consistency proofs presented in this thesis come from the cut-elimination theorems, and the latter are established by using the more or less same idea for all the systems. We briefly sketch the basic idea of cut-elimination for linear set theory.

The standard method to establish the cut-elimination result for a first-order system is by induction on the syntactic complexity of formulas, which is defined along the inductive definition of formulas. However, this method does not work for the second order logic since the elimination of cuts with the second-order quantification involve the substitution of a predicate for a second-order variable and this may increase the syntactic complexity of cut-formulas. We have the same situation in set theory. For example, suppose that t is a fairly complex term , say $\{z : \bigwedge v.(\bigvee w.(w \in v \otimes v \notin z))\}$. The proof on the left below reduces to the proof on the right in our cut-elimination process:

$$\dfrac{\dfrac{\dfrac{\vdots \pi_1}{\vdash x \in y, \Gamma}}{\vdash \bigwedge x.x \in y, \Gamma} \quad \dfrac{\dfrac{\vdots \pi_2}{\vdash t \notin y, \Delta}}{\vdash \bigvee x.x \notin y, \Delta}}{\vdash \Gamma, \Delta} \quad \rightsquigarrow \quad \dfrac{\dfrac{\vdots \pi_1[t/x]}{\vdash t \in y, \Gamma} \quad \dfrac{\vdots \pi_2}{\vdash t \notin y, \Delta}}{\vdash \Gamma, \Delta}$$

The cut with formulas $\bigwedge x.x \in y$ and $\bigvee x.x \notin y$ is replaced by a cut with formulas which contain a more complex term t. The next example shows that a cut with atomic formulas becomes a cut with logically complex formulas:

$$\dfrac{\dfrac{\dfrac{\vdots \pi_1}{\vdash x \notin y \otimes y \in w, \Gamma}}{\vdash x \in t, \Gamma} \quad \dfrac{\dfrac{\vdots \pi_2}{\vdash x \in y \parr y \notin w, \Delta}}{\vdash x \notin t, \Gamma}}{\vdash \Gamma, \Delta} \quad \rightsquigarrow \quad \dfrac{\dfrac{\vdots \pi_1}{\vdash x \notin y \otimes y \in w, \Gamma} \quad \dfrac{\vdots \pi_2}{\vdash x \in y \parr y \notin w, \Delta}}{\vdash \Gamma, \Delta}$$

where t is $\{z : z \notin y \otimes y \in w\}$. In general, the situation for set theory is much worse than for the second-order or higher-order logic, since we do not have any good hierarchy among set terms for doing induction.

The cut-elimination theorems for the second and higher-order logics are proved by the method now known as "candidates of reducibility". The same method can be used to establish a partial cut-elimination result for set theory, using a well-ordering built in the standard model of set theory. However, the complete cut-elimination is not possible even for a system of set theory in classical logic with only the principle of separation [14, 24].

Our proof of the cut-elimination theorem for linear set theory is, however, very simple. This is precisely because the use of contraction is restricted in linear logic. In fact, we can define a measure of the size of a proof in such a way that it decreases along with the cut-elimination process if no exponential is involved.

In short, we measure the size of a proof by summing up the lengths of all of its subproofs. For example, the size of a proof π

$$\dfrac{\overset{\vdots\,\pi_1}{\vdash A,\Gamma} \qquad \overset{\vdots\,\pi_2}{\vdash A^\perp,\Delta}}{\vdash \Gamma,\Delta}$$

is the sum of the sizes of its immediate subproofs π_1 and π_2. If a proof is obtained from its immediate subproof by one of the one-premiss rules, we simply increment the size by 1. If no exponential is involved, the size thus measured never increases in the cut-elimination process, and strictly decreases at the essential steps.

If we have exponentials, the size may increase because of contraction as can be seen below:

$$\dfrac{\dfrac{\overset{\vdots\,\pi_1}{\vdash\ ?A,\ ?A,\Gamma}}{\vdash\ ?A,\Gamma} \qquad \overset{\vdots\,\pi_2}{\vdash\ !A^\perp,\ ?\Delta}}{\vdash \Gamma,\ ?\Delta} \quad\rightsquigarrow\quad \dfrac{\dfrac{\dfrac{\overset{\vdots\,\pi_1}{\vdash\ ?A,\ ?A,\Gamma} \qquad \overset{\vdots\,\pi_2}{\vdash\ !A^\perp,\ ?\Delta}}{\vdash\ ?A,\Gamma,\ ?\Delta} \qquad \overset{\vdots\,\pi_2}{\vdash\ !A^\perp,\ ?\Delta}}{\vdash \Gamma,\ ?\Delta,\ ?\Delta}}{\vdash \Gamma,\ ?\Delta}$$

where we repeat applications of the contraction rule at the last step on the right. The subproof π_2 is duplicated in this cut-elimination process so that the size of the whole proof increases.

Another case where duplication is necessary is when we need to permute a cut with the introduction rule for the additive conjunction:

$$\dfrac{\overset{\vdots\,\pi_1}{\vdash C,\Gamma} \qquad \dfrac{\overset{\vdots\,\pi_2}{\vdash A,C^\perp,\Delta} \qquad \overset{\vdots\,\pi_3}{\vdash B,C^\perp,\Delta}}{\vdash A \mathbin{\&} B,C^\perp,\Delta}}{\vdash A \mathbin{\&} B,\Gamma,\Delta} \quad\rightsquigarrow\quad \dfrac{\dfrac{\overset{\vdots\,\pi_1}{\vdash C,\Gamma} \qquad \overset{\vdots\,\pi_2}{\vdash A,C^\perp,\Delta}}{\vdash A,\Gamma,\Delta} \qquad \dfrac{\overset{\vdots\,\pi_1}{\vdash C,\Gamma} \qquad \overset{\vdots\,\pi_3}{\vdash B,C^\perp,\Delta}}{\vdash B,\Gamma,\Delta}}{\vdash A \mathbin{\&} B,\Gamma,\Delta}$$

However, the increase in size can be avoided in this case by defining the size of a proof π

$$\dfrac{\begin{matrix}\vdots\pi_1 \\ \vdash A, \Gamma\end{matrix} \quad \begin{matrix}\vdots\pi_2 \\ \vdash B, \Gamma\end{matrix}}{\vdash A \,\&\, B, \Gamma}$$

to be the maximum of the sizes of π_1 and π_2 incremented by 1.

Once we obtain such a measure, we can proceed by induction on the size of a proof in our cut-elimination proofs. This method is used in the cut-elimination proofs for all of our four systems of linear set theory, in conjunction with the standard method.

1.5 The meaning of linear set theory

1.5.1 Linear logic as a research program

Linear logic has been studied not so much for its immediate success in applications as for its prospects. One of such prospects is to obtain a good abstract mathematical theory of computational processes.

Ever since Frege, the intensional and extensional aspects of language have been distinguished. The first has to do with *presentation* and *computation*, or how we conceive the world and how we manipulate the information. The second has to do with *denotation*, or what extra-linguistic entities are referred to in the use of the language. In Frege, intension *Sinn* and extension *Bedeutung* are separate kinds of *meaning*, and intension should not be identified with syntactic expressions.

Unfortunately, the only well-developed semantics as of today is a model-theoretic semantics, which reduces all meaning to denotation. In this framework, intension is either identified with a set of possible denotations, or neglected and relegated to syntax, which is regarded as manipulation of meaningless and arbitrarily chosen formal symbols. The limitation of this framework is ever more obvious today, particularly due to the problem of belief sentences in natural language semantics and the problem of full abstraction models in programming language.

On the other hand, there have been a few attempts to obtain semantics which take intension seriously into account. For example, Per Martin-Löf has been proposing for a long time the theory of meaning in terms of normalized proofs [19]. Another example is Moschovakis' intensional semantics of algorithms, which identifies the intension of an algorithm by its normalized definition as second-order recursive functionals [21].

The study of linear logic points to the same goal. The research program "Geometry of interaction", proposed by J.Y. Girard, purports to give an abstract mathematical modeling to the cut-elimination process of linear logic, and eventually to the computational process of lambda-calculus [8]. Another promising line of research in linear logic is game semantics of Abramsky and Jagadeesan, which extends the previous work by A. Blass [1]. As we have already seen, the behavior of linear logic strongly suggests the interpretation in terms of consumption and production. In the case of classical linear logic, they can be read as *communication* with the environment, in which a piece of information is consumed by the environment and a new piece of information is produced in return. This idea leads Abramsky and Jagadeesan to their game semantics. This semantics actually solves the problem of the full abstraction model for PCF.

1.5.2 Sets and processes

In the spirit of the above goal, the meaning of linear set theory should be given in terms of the dynamic constructive process of the classical universe of sets. Unfortunately, this is yet only a speculation, and it is a challenge to develop a mathematical theory based on this idea. Hence we only discuss two points relevant to the understanding of linear set theory.

First, the philosophical interpretation of intuitionistic set theory is established fairly well, and this should help us to understand the meaning of linear set theory. We have already described intuitionistic logic as accumulation, which is sometimes regarded as the accumulation of knowledge. This understanding can be extended to intuitionistic set theory under different guises of Kripke's possible world model, Cohen's forcing, and Lawvere's topos [18]. Sets are then regarded as incomplete objects, the extension of which are determined gradually, as it were, over time. In other words, a set encodes the process in which the knowledge about the set is gradually accumulated as time goes by.

If we extrapolate this understanding to linear set theory through the contrast between consumption and accumulation, we may say that a set encodes the process in which the information about a set is consumed and changed into the new information. In other words, sets are regarded as transient objects, the extension of which are changed according to the context. Let's consider Russell's paradox from this point of view. From the initially given information $R \in R$, the new information $R \notin R$ is produced. However, the initial information is consumed in the process. Hence two contradicting pieces of information do not coexist, and there is no contradiction.

Secondly, the transition from the transient world of linear logic to the stable intuitionistic world is carried out by the exponential !. In fact, ! is interpreted as the "storage" operator in the linear lambda calculus, which stores a term in memory so that it can be duplicated later by copying. In other words, transient information is regarded as knowledge when ! is applied to it.

In relation to Russell's paradox, then, we might say that the information $R \in R$ is harmless as long as it does not claim the status of knowledge.

It seems that the above extrapolation of understanding is reasonable and useful as a heuristic guide to semantics of linear set theory. Then one direction to go is to extend the semantics of intuitionistic set theory to linear logic. In fact, we have already carried this out to some extent, and the result is presented in Chapter 6. However, as we have already noted, the phase-valued semantics thus obtained does not give a model of the unrestricted comprehension. In this respect, semantics of linear set theory still poses a problem.

Chapter 2

Basic linear set theory

2.1 Introduction

This chapter presents our first system of linear set theory SMALL and proves its consistency by cut-elimination theorem.

SMALL is formulated in full classical linear logic with exponentials. However, the set terms of SMALL are formed by the unrestricted comprehension over only the formulas in the multiplicative additive fragment of linear logic, or MALL in short.

Our consistency proof of SMALL comes from the cut-elimination theorem. As in the second order case, the standard argument for cut-elimination in terms of the complexity of formulas does not work for SMALL. We overcome this problem by defining a suitable measure of the size of a proof which decreases along with the cut-elimination process for formulas without exponentials. In fact, we give two such measures, one of which is taken from Girard's small normalization theorem for proof nets [7], and the other is from the works of R.B. White and Schroeder-Heister [30, 25]. In later chapters, we will use only the second since it is much simpler than the first.

Given such a measure, we proceed as follows. First we eliminate the cuts down to the cuts over atomic formulas by the standard method, *i.e.* by induction on the formula complexity. Then we can show by induction on the measure of the size of a proof that the cut-elimination process for the remaining cuts will eventually halt since the process involve only the cuts over formulas without exponentials.

The expressive power of SMALL seems to be fairly weak. However SMALL gives a good starting point for our endeavour in the sense that its formulation is simple and the basic idea in its consistency proof will be used again and again in later chapters.

2.2 The formal system SMALL

2.2.1 The language of SMALL

In our formulation of set theory, atomic formulas are constructed from terms, and terms are from formulas. Hence we need to define both of them simultaneously. Besides, we need to distinguish from others a special type of formulas, *i.e.* the formulas which do not contain exponentials. This type of formulas is called *small*. The set terms are formed by the unrestricted comprehension over only small formulas.

Definition 2.1 *We define the terms and formulas of SMALL by simultaneuos induction as follows:*

- *Variables* $x, y, z \ldots$ *are terms*
- *If* s *and* t *are terms, then* $s \in t$ *and* $s \notin t$ *are small formulas*
- *If* $A(x)$ *is a small formula, then* $\{x : A(x)\}$ *is a term*
- $\mathbf{1}$, $\perp$,$\top$ *and* $\mathbf{0}$ *are small formulas*
- *If* A *and* B *are small formulas, then* $A \otimes B$, $A \parr B$, $A \,\&\, B$, $A \oplus B$, $\bigwedge x.A$ *and* $\bigvee x.A$ *are small formulas*
- *If* A *and* B *are formulas, then* $A \otimes B$, $A \parr B$, $A \,\&\, B$, $A \oplus B$, $\bigwedge x.A$ *and* $\bigvee x.A$ *are formulas*
- *If* A *is a formula, then* $!A$ *and* $?A$ *are formulas*

where all small formulas are formulas.

In our presentation, we assume the De Morgan dualities and build them into the definition of linear negation.

Definition 2.2 *The linear negations of formulas are defined inductively as follows:*

- $(s \in t)^\perp =_{def} s \notin t$
- $(s \notin t)^\perp =_{def} s \in t$
- $(A \otimes B)^\perp =_{def} A^\perp \mathbin{⅋} B^\perp$
- $(A \mathbin{⅋} B)^\perp =_{def} A^\perp \otimes B^\perp$
- $(A \mathbin{\&} B)^\perp =_{def} A^\perp \oplus B^\perp$
- $(A \oplus B)^\perp =_{def} A^\perp \mathbin{\&} B^\perp$
- $(\bigwedge x.A)^\perp =_{def} \bigvee x.A^\perp$
- $(\bigvee x.A)^\perp =_{def} \bigwedge x.A^\perp$
- $(\,!\,A)^\perp =_{def}\ ?\,A^\perp$
- $(\,?\,A)^\perp =_{def}\ !\,A^\perp$
- $(\mathbf{1})^\perp =_{def} \perp$
- $(\perp)^\perp =_{def} \mathbf{1}$
- $(\top)^\perp =_{def} \mathbf{0}$
- $(\mathbf{0})^\perp =_{def} \top$

2.2.2 The axioms and rules of inference of SMALL

The axioms and the rules of inference of SMALL are those of the Gentzen-style sequent calculus of classical linear logic and the introduction rules $(\in)$ and $(\notin)$ for set terms $\{x : A(x)\}$. In the following, the capital Greek letters Γ, Δ, ...stand for list of formulas. The formula $A[t/x]$ is the result of substitution of the term t for some occurrences of the variable x in a formula A. Furthermore we disregard the sequential order of formulas in sequents.

Axioms

$$(I) \quad \vdash A, A^\perp$$

$$(\mathbf{1}) \quad \vdash \mathbf{1} \qquad\qquad (\top) \quad \vdash \top, \Gamma$$

where A is atomic in (I).

Rules of inference

$$(\otimes)\ \frac{\vdash A, \Gamma \quad \vdash B, \Delta}{\vdash A \otimes B, \Gamma, \Delta} \qquad\qquad (⅋)\ \frac{\vdash A, B, \Gamma}{\vdash A \mathbin{⅋} B, \Gamma}$$

$$(\&)\ \frac{\vdash A, \Gamma \quad \vdash B, \Gamma}{\vdash A \mathbin{\&} B, \Gamma} \qquad (\oplus 1)\ \frac{\vdash A, \Gamma}{\vdash A \oplus B, \Gamma} \quad (\oplus 2)\ \frac{\vdash B, \Gamma}{\vdash A \oplus B, \Gamma}$$

$$(\bigwedge)\quad \frac{\vdash A, \Gamma}{\vdash \bigwedge x.A, \Gamma} \qquad (\bigvee)\quad \frac{\vdash A[t/x], \Gamma}{\vdash \bigvee x.A, \Gamma}$$

$$(\in)\quad \frac{\vdash A[t/x], \Gamma}{\vdash t \in \{x : A\}, \Gamma} \qquad (\notin Z)\quad \frac{\vdash A[t/x]^{\perp}, \Gamma}{\vdash t \notin \{x : A\}, \Gamma}$$

$$(W?)\quad \frac{\vdash \Gamma}{\vdash\ ?\,A, \Gamma} \qquad (D?)\quad \frac{\vdash A, \Gamma}{\vdash\ ?\,A, \Gamma}$$

$$(C?)\quad \frac{\vdash\ ?\,A,\ ?\,A, \Gamma}{\vdash\ ?\,A, \Gamma} \qquad (!)\quad \frac{\vdash A,\ ?\,\Gamma}{\vdash\ !\,A,\ ?\,\Gamma}$$

$$(\perp)\quad \frac{\vdash \Gamma}{\vdash \perp, \Gamma}$$

$$(cut)\quad \frac{\vdash A, \Gamma \quad \vdash A^{\perp}, \Delta}{\vdash \Gamma, \Delta}$$

where

- the variable x is not free in the context Γ in $(\bigwedge)$,
- the formula $A(t)$ is a small formula in $(\in)$ and $(\notin)$,
- the context $?\,\Gamma$ is the list of formulas of the form $?\,A$ or $\perp$ in $(!)$.

2.3 The cut-elimination procedures for SMALL

In order to prove the cut-elimation theorem, it is useful to augument SMALL with an extra rule, and prove the theorem for the new system, which we call SMALL^{+}. The extra rule combines contraction and cut:

$$(\,?\,cut)\quad \frac{\vdash\ ?\,A^{k}, \Gamma \quad \vdash\ !\,A^{\perp}, \Delta}{\vdash \Gamma, \Delta}$$

where $1 \leq k$ and $?\,A^{k}$ denotes k occurrences of the formula $?\,A$. If the cut formulas of the ordinary cut have the forms $?\,A$ and $!\,A^{\perp}$, then that cut will be regarded as an application of $(\,?\,cut)$ with $k = 1$.

Clearly any sequent provable in SMALL is also provable SMALL^{+}, and *vice versa* since

(? *cut*) is a derived rule of SMALL as follows:

$$\dfrac{\dfrac{\vdash \Gamma, ?\,A^k}{\vdash \Gamma, ?\,A} \quad \vdash \Delta, !\,A^\perp}{\vdash \Gamma, \Delta}$$

where we apply the contraction rule $k-1$ times and then use the ordinary cut. Furthermore, any proof in SMALL can be regarded as a proof in SMALL$^+$, and any proof in SMALL$^+$ without (*cut*) nor (? *cut*) is also a cut-free proof in SMALL. Hence, once we establish the cut-elimination theorem for SMALL$^+$, we also have the theorem for SMALL in the following way: Given a proof of Γ in SMALL, read it as a proof in SMALL$^+$, and obtain a cut-free proof of Γ in SMALL$^+$, which is also a cut-free proof in SMALL.

In our cut-elimination procedure, the cuts are eliminated by consecutive applications of one-step reductions of proofs. Consider the proof:

$$\dfrac{\begin{array}{c}\vdots\pi_1 \\ \vdash \Gamma, A\end{array} \quad \begin{array}{c}\vdots\pi_2 \\ \vdash \Delta, A^\perp\end{array}}{\vdash \Gamma, \Delta}\ (cut) \quad \text{or} \quad \dfrac{\begin{array}{c}\vdots\pi_1 \\ \vdash \Gamma, ?\,A^k\end{array} \quad \begin{array}{c}\vdots\pi_2 \\ \vdash \Delta, !\,A^\perp\end{array}}{\vdash \Gamma, \Delta}\ (?\,cut)$$

In general, we have two types of one-step reductions:

1. Symmetric reductions: A and $A^\perp$ are the main formulas of the last inferences π_1 and π_2, or, one of π_i's is an axiom (I) or $(\top)$.

2. Permutative reductions: A or $A^\perp$ is not the main formula. For (? *cut*), we further need to distinguish

   (a) Permutative reductions on !-branch: $!\,A^\perp$ is not the main formula of π_2.

   (b) Permutative reductions on ?-branch: $!\,A^\perp$ is the main formula of π_2 and $?\,A$ is not the main formula of π_1.

We need to pay special attention to the cases where any form of contraction is involved. Otherwise all the one-step reductions are standard.

2.3.1 Symmetric reductions

Symmetric reductions for (cut)

$(*/I)$

$$\dfrac{\vdash A, \Gamma \quad \vdash A^{\perp}, A}{\vdash A, \Gamma} \;\rightsquigarrow\; \vdash A, \Gamma$$

$(\perp/\mathbf{1})$

$$\dfrac{\dfrac{\vdash \Gamma}{\vdash \perp, \Gamma} \quad \vdash \mathbf{1}}{\vdash \Gamma} \;\rightsquigarrow\; \vdash \Gamma$$

$(*/\top)$

$$\dfrac{\vdash A, \Gamma \quad \vdash \top, A^{\perp}, \Delta}{\vdash \top, \Gamma, \Delta} \;\rightsquigarrow\; \vdash \top, \Gamma, \Delta$$

$(\otimes/\parr)$

$$\dfrac{\dfrac{\vdash A, \Gamma \quad \vdash B, \Delta}{\vdash A \otimes B, \Gamma, \Delta} \quad \dfrac{\vdash A^{\perp}, B^{\perp}, \Theta}{\vdash A^{\perp} \parr B^{\perp}, \Theta}}{\vdash \Gamma, \Delta, \Theta} \;\rightsquigarrow\; \dfrac{\vdash B, \Delta \quad \dfrac{\vdash A, \Gamma \quad \vdash A^{\perp}, B^{\perp}, \Theta}{\vdash B^{\perp}, \Gamma, \Theta}}{\vdash \Gamma, \Delta, \Theta}$$

$(\with/\oplus 1)$

$$\dfrac{\dfrac{\vdash A, \Gamma \quad \vdash B, \Gamma}{\vdash A \with B, \Gamma} \quad \dfrac{\vdash A^{\perp}, \Delta}{\vdash A^{\perp} \oplus B^{\perp}, \Delta}}{\vdash \Gamma, \Delta} \;\rightsquigarrow\; \dfrac{\vdash A, \Gamma \quad \vdash A^{\perp}, \Delta}{\vdash \Gamma, \Delta}$$

$(\with/\oplus 2)$

$$\dfrac{\dfrac{\vdash A, \Gamma \quad \vdash B, \Gamma}{\vdash A \with B, \Gamma} \quad \dfrac{\vdash \Delta, B^{\perp}}{\vdash \Delta, A^{\perp} \oplus B^{\perp}}}{\vdash \Gamma, \Delta} \;\rightsquigarrow\; \dfrac{\vdash B, \Gamma \quad \vdash B^{\perp}, \Delta}{\vdash \Gamma, \Delta}$$

$(\bigwedge / \bigvee)$

$$\dfrac{\dfrac{\vdash A, \Gamma}{\vdash \bigwedge x.A, \Gamma} \quad \dfrac{\vdash A[t/x]^{\perp}, \Delta}{\vdash \bigvee x A^{\perp}, \Delta}}{\vdash \Gamma, \Delta} \;\rightsquigarrow\; \dfrac{\vdash A[t/x], \Gamma \quad \vdash A[t/x]^{\perp}, \Delta}{\vdash \Gamma, \Delta}$$

$(\in / \notin)$

$$\dfrac{\dfrac{\vdash A[t/x], \Gamma}{\vdash t \in \{x : A\}, \Gamma} \quad \dfrac{\vdash A[t/x]^{\perp}, \Delta}{\vdash t \notin \{x : A\}, \Delta}}{\vdash \Gamma, \Delta} \;\rightsquigarrow\; \dfrac{\vdash A[t/x], \Gamma \quad \vdash A[t/x]^{\perp}, \Delta}{\vdash \Gamma, \Delta}$$

Symmetric reductions for $(\,?\,cut)$

$(W?/!)$

$$\dfrac{\dfrac{\vdash \Gamma}{\vdash\ ?A, \Gamma} \quad \dfrac{\vdash A^{\perp}, ?\Delta}{\vdash\ !A^{\perp}, ?\Delta}}{\vdash \Gamma, ?\Delta} \quad \leadsto \quad \dfrac{\vdash \Gamma}{\vdash \Gamma, ?\Delta}$$

$(D?/!)$

$$\dfrac{\dfrac{\vdash A, \Gamma}{\vdash\ ?A, \Gamma} \quad \dfrac{\vdash A^{\perp}, ?\Delta}{\vdash\ !A^{\perp}, ?\Delta}}{\vdash \Gamma, ?\Delta} \quad \leadsto \quad \dfrac{\vdash A, \Gamma \quad \vdash A^{\perp}, ?\Delta}{\vdash \Gamma, ?\Delta}$$

$(W?/!)$–?

$$\dfrac{\dfrac{\vdash\ ?A^{k}, \Gamma}{\vdash\ ?A^{k+1}, \Gamma} \quad \vdash\ !A^{\perp}, ?\Delta}{\vdash \Gamma, ?\Delta} \quad \leadsto \quad \dfrac{\vdash\ ?A^{k}, \Gamma \quad \vdash\ !A^{\perp}, ?\Delta}{\vdash \Gamma, ?\Delta}$$

$(D?/!)$–?

$$\dfrac{\dfrac{\vdash A, ?A^{k}, \Gamma}{\vdash\ ?A^{k+1}, \Gamma} \quad \dfrac{\vdash A^{\perp}, ?\Delta}{\vdash\ !A^{\perp}, ?\Delta}}{\vdash \Gamma, ?\Delta} \quad \leadsto \quad \dfrac{\dfrac{\dfrac{\vdash A, ?A^{k}, \Gamma \quad \vdash\ !A^{\perp}, ?\Delta}{\vdash A, \Gamma, ?\Delta} \qquad \vdash A^{\perp}, ?\Delta}{\vdash \Gamma, ?\Delta, ?\Delta}}{\vdash \Gamma, ?\Delta}$$

$(C\ ?\,/\,!\,)$–?

$$\dfrac{\dfrac{\vdash\ ?A^{k+1}, \Gamma}{\vdash\ ?A^{k}, \Gamma} \quad \vdash\ !A^{\perp}, ?\Delta}{\vdash \Gamma, ?\Delta} \quad \leadsto \quad \dfrac{\vdash\ ?A^{k+1}, \Gamma \quad \vdash A^{\perp}, ?\Delta}{\vdash \Gamma, ?\Delta}$$

2.3.2 Permutative reductions:

The inference rule (cut) is freely permutable except with $(\,!\,)$. This exceptional case is subsumed by the corresponding permutative reduction for $(\,?\,cut)$. All the other permutative reductions for (cut) and $(?cut)$ on !-branch are straightforward.

The permutative reductions for $(?cut)$ on ?-branch require more attention. The inference rules $(\otimes)$, (cut) and $(?cut)$ have two premisses and the permutative reductions for them depend on whether $?\,A^{k}$ have ancestors in both of the premisses or not.

Permutative reductions for (cut)

$(cut/\otimes)$

$$\dfrac{\vdash C,\Gamma \quad \dfrac{\vdash A, C^{\perp},\Delta \quad \vdash B,\Theta}{\vdash A\otimes B, C^{\perp},\Delta,\Theta}}{\vdash A\otimes B,\Gamma,\Delta,\Theta} \rightsquigarrow \dfrac{\dfrac{\vdash C,\Gamma \quad \vdash A,C^{\perp},\Delta}{\vdash A,\Gamma,\Delta} \quad \vdash B,\Theta}{\vdash A\otimes B,\Gamma,\Delta,\Theta}$$

$(cut/\parr)$

$$\dfrac{\vdash C,\Gamma \quad \dfrac{\vdash A, B, C^{\perp},\Delta}{\vdash A\parr B, C^{\perp},\Delta}}{\vdash A\parr B,\Gamma,\Delta} \rightsquigarrow \dfrac{\dfrac{\vdash C,\Gamma \quad \vdash A,B,C^{\perp},\Delta}{\vdash A,B,\Gamma,\Delta}}{\vdash A\parr B,\Gamma,\Delta}$$

$(cut/\&)$

$$\dfrac{\vdash C,\Gamma \quad \dfrac{\vdash A, C^{\perp},\Delta \quad \vdash B, C^{\perp},\Delta}{\vdash A\,\&\,B, C^{\perp},\Delta}}{\vdash A\,\&\,B,\Gamma,\Delta} \rightsquigarrow \dfrac{\dfrac{\vdash C,\Gamma \quad \vdash A,C^{\perp},\Delta}{\vdash A,\Gamma,\Delta} \quad \dfrac{\vdash C,\Gamma \quad \vdash B,C^{\perp},\Delta}{\vdash B,\Gamma,\Delta}}{\vdash A\,\&\,B,\Gamma,\Delta}$$

$(cut/\oplus 1)$

$$\dfrac{\vdash C,\Gamma \quad \dfrac{\vdash A, C^{\perp},\Delta}{\vdash A\oplus B, C^{\perp},\Delta}}{\vdash A\oplus B,\Gamma,\Delta} \rightsquigarrow \dfrac{\dfrac{\vdash C,\Gamma \quad \vdash A,C^{\perp},\Delta}{\vdash A,\Gamma,\Delta}}{\vdash A\oplus B,\Gamma,\Delta}$$

$(cut/\oplus 2)$

$$\dfrac{\vdash C,\Gamma \quad \dfrac{\vdash B, C^{\perp},\Delta}{\vdash A\oplus B, C^{\perp},\Delta}}{\vdash A\oplus B,\Gamma,\Delta} \rightsquigarrow \dfrac{\dfrac{\vdash C,\Gamma \quad \vdash B,C^{\perp},\Delta}{\vdash B,\Gamma,\Delta}}{\vdash A\oplus B,\Gamma,\Delta}$$

$(cut/\bigwedge)$

$$\dfrac{\vdash C,\Gamma \quad \dfrac{\vdash A, C^{\perp},\Delta}{\vdash \bigwedge x.A, C^{\perp},\Delta}}{\vdash \bigwedge x.A,\Gamma,\Delta} \rightsquigarrow \dfrac{\dfrac{\vdash C,\Gamma \quad \vdash A[y/x],C^{\perp},\Delta}{\vdash A[y/x],\Gamma,\Delta}}{\vdash \bigwedge y.A,\Gamma,\Delta}$$

$(cut/\bigvee)$

$$\dfrac{\vdash C,\Gamma \quad \dfrac{\vdash A[t/x], C^{\perp},\Delta}{\vdash \bigvee x.A, C^{\perp},\Delta}}{\vdash \bigvee x.A,\Gamma,\Delta} \rightsquigarrow \dfrac{\dfrac{\vdash C,\Gamma \quad \vdash A[t/x],C^{\perp},\Delta}{\vdash A[t/x],\Gamma,\Delta}}{\vdash \bigvee x.A,\Gamma,\Delta}$$

$(cut/\in)$

$$\dfrac{\vdash C,\Gamma \qquad \dfrac{\vdash A[t/x], C^\perp,\Delta}{\vdash t\in\{x:A\}, C^\perp,\Delta}}{\vdash t\in\{x:A\},\Gamma,\Delta} \rightsquigarrow \dfrac{\dfrac{\vdash C,\Gamma \qquad \vdash A[t/x],C^\perp,\Delta}{\vdash A[t/x],\Gamma,\Delta}}{\vdash t\in\{x:A\},\Gamma,\Delta}$$

$(cut/\notin)$

$$\dfrac{\vdash C,\Gamma \qquad \dfrac{\vdash A[t/x]^\perp, C^\perp,\Delta}{\vdash t\notin\{x:A\}, C^\perp,\Delta}}{\vdash t\notin\{x:A\},\Gamma,\Delta} \rightsquigarrow \dfrac{\dfrac{\vdash C,\Gamma \qquad \vdash A[t/x]^\perp,C^\perp,\Delta}{\vdash A[t/x]^\perp,\Gamma,\Delta}}{\vdash t\notin\{x:A\},\Gamma,\Delta}$$

$(cut/\perp)$

$$\dfrac{\vdash C,\Gamma \qquad \dfrac{\vdash C^\perp,\Delta}{\vdash \perp, C^\perp,\Delta}}{\vdash \perp,\Gamma,\Delta} \rightsquigarrow \dfrac{\dfrac{\vdash C,\Gamma \qquad \vdash C^\perp,\Delta}{\vdash \Gamma,\Delta}}{\vdash \perp,\Gamma,\Delta}$$

$(cut/W?)$

$$\dfrac{\vdash C,\Gamma \qquad \dfrac{\vdash C^\perp,\Delta}{\vdash\ ?A, C^\perp,\Delta}}{\vdash\ ?A,\Gamma,\Delta} \rightsquigarrow \dfrac{\dfrac{\vdash C,\Gamma \qquad \vdash C^\perp,\Delta}{\vdash \Gamma,\Delta}}{\vdash\ ?A,\Gamma,\Delta}$$

$(cut/D?)$

$$\dfrac{\vdash C,\Gamma \qquad \dfrac{\vdash A, C^\perp,\Delta}{\vdash\ ?A, C^\perp,\Delta}}{\vdash\ ?A,\Gamma,\Delta} \rightsquigarrow \dfrac{\dfrac{\vdash C,\Gamma \qquad \vdash A, C^\perp,\Delta}{\vdash A,\Gamma,\Delta}}{\vdash\ ?A,\Gamma,\Delta}$$

$(cut/C?)$

$$\dfrac{\vdash C,\Gamma \qquad \dfrac{\vdash\ ?A,\ ?A, C^\perp,\Delta}{\vdash\ ?A, C^\perp,\Delta}}{\vdash\ ?A,\Gamma,\Delta} \rightsquigarrow \dfrac{\dfrac{\vdash C,\Gamma \qquad \vdash\ ?A,\ ?A, C^\perp,\Delta}{\vdash\ ?A,\ ?A,\Gamma,\Delta}}{\vdash\ ?A,\Gamma,\Delta}$$

(cut/cut)

$$\dfrac{\vdash C,\Gamma \qquad \dfrac{\vdash A, C^\perp,\Delta \quad \vdash A^\perp,\Theta}{\vdash C^\perp,\Delta,\Theta}}{\vdash \Gamma,\Delta,\Theta} \rightsquigarrow \dfrac{\dfrac{\vdash C,\Gamma \quad \vdash A, C^\perp,\Delta}{\vdash A,\Gamma,\Delta} \qquad \vdash A^\perp,\Theta}{\vdash \Gamma,\Delta,\Theta}$$

$(cut/\ ?\,cut1)$

$$\dfrac{\vdash C,\Gamma \qquad \dfrac{\vdash\ ?A^k, C^\perp,\Delta \quad \vdash\ !A^\perp,\Theta}{\vdash C^\perp,\Delta,\Theta}}{\vdash \Gamma,\Delta,\Theta} \rightsquigarrow \dfrac{\dfrac{\vdash C,\Gamma \quad \vdash\ ?A^k, C^\perp,\Delta}{\vdash\ ?A^k,\Gamma,\Delta} \qquad \vdash\ !A^\perp,\Theta}{\vdash \Gamma,\Delta,\Theta}$$

$(cut/\ ?\,cut2)$

$$\dfrac{\vdash C,\Gamma \qquad \dfrac{\vdash\ ?A^k,\Delta \quad \vdash\ !A^\perp, C^\perp,\Theta}{\vdash C^\perp,\Delta,\Theta}}{\vdash \Gamma,\Delta,\Theta} \quad\leadsto\quad \dfrac{\dfrac{\vdash C,\Gamma \quad \vdash\ !A^\perp,C^\perp,\Theta}{\vdash\ !A^\perp,\Gamma,\Theta} \qquad \vdash\ ?A^k,\Delta}{\vdash \Gamma,\Delta,\Theta}$$

Permutative reductions for $(\,?\,cut)$ **on !–branch**

They are entirely similar to the permutations for (cut). This type of permutations are indicated by the suffix !.

$(\,?\,cut/\otimes)$–!

$$\dfrac{\vdash\ ?C^k,\Gamma \qquad \dfrac{\vdash A,\,!C^\perp,\Delta \quad \vdash B,\Theta}{\vdash A\otimes B,\,!C^\perp,\Delta,\Theta}}{\vdash A\otimes B,\Gamma,\Delta,\Theta} \quad\leadsto\quad \dfrac{\dfrac{\vdash\ ?C^k,\Gamma \quad \vdash A,\,!C^\perp,\Delta}{\vdash A,\Gamma,\Delta} \qquad \vdash B,\Theta}{\vdash A\otimes B,\Gamma,\Delta,\Theta}$$

$(\,?\,cut/\parr)$–!

$$\dfrac{\vdash\ ?C^k,\Gamma \qquad \dfrac{\vdash A,B,\,!C^\perp,\Delta}{\vdash A\parr B,\,!C^\perp,\Delta}}{\vdash A\parr B,\Gamma,\Delta} \quad\leadsto\quad \dfrac{\dfrac{\vdash\ ?C^k,\Gamma \quad \vdash A,B,\,!C^\perp,\Delta}{\vdash A,B,\Gamma,\Delta}}{\vdash A\parr B,\Gamma,\Delta}$$

$(\,?\,cut/\&)$–!

$$\dfrac{\vdash\ ?C^k,\Gamma \qquad \dfrac{\vdash A,\,!C^\perp,\Delta \quad \vdash B,\,!C^\perp,\Delta}{\vdash A\,\&\,B,\,!C^\perp,\Delta}}{\vdash A\,\&\,B,\Gamma,\Delta} \quad\leadsto\quad \dfrac{\dfrac{\vdash\ ?C^k,\Gamma \quad \vdash A,\,!C^\perp,\Delta}{\vdash A,\Gamma,\Delta} \qquad \dfrac{\vdash\ ?C^k,\Gamma \quad \vdash B,\,!C^\perp,\Delta}{\vdash B,\Gamma,\Delta}}{\vdash A\,\&\,B,\Gamma,\Delta}$$

$(\,?\,cut/\oplus 1)$–!

$$\dfrac{\vdash\ ?C^k,\Gamma \qquad \dfrac{\vdash A,\,!C^\perp,\Delta}{\vdash A\oplus B,\,!C^\perp,\Delta}}{\vdash A\oplus B,\Gamma,\Delta} \quad\leadsto\quad \dfrac{\dfrac{\vdash\ ?C^k,\Gamma \quad \vdash A,\,!C^\perp,\Delta}{\vdash A,\Gamma,\Delta}}{\vdash A\oplus B,\Gamma,\Delta}$$

$(\,?\,cut/\oplus 2)$–!

$$\dfrac{\vdash\ ?C^k,\Gamma \qquad \dfrac{\vdash B,\,!C^\perp,\Delta}{\vdash A\oplus B,\,!C^\perp,\Delta}}{\vdash A\oplus B,\Gamma,\Delta} \quad\leadsto\quad \dfrac{\dfrac{\vdash\ ?C^k,\Gamma \quad \vdash B,\,!C^\perp,\Delta}{\vdash B,\Gamma,\Delta}}{\vdash A\oplus B,\Gamma,\Delta}$$

$(?\, cut/ \bigwedge)$–!

$$\frac{\vdash\ ?C^k, \Gamma \qquad \dfrac{\vdash A, !C^\perp, \Delta}{\vdash \bigwedge x.A, !C^\perp, \Delta}}{\vdash \bigwedge x.A, \Gamma, \Delta} \rightsquigarrow \frac{\dfrac{\vdash\ ?C^k, \Gamma \quad \vdash A[y/x], !C^\perp, \Delta}{\vdash A[y/x], \Gamma, \Delta}}{\vdash \bigwedge y.A, \Gamma, \Delta}$$

$(?\, cut/ \bigvee)$–!

$$\frac{\vdash\ ?C^k, \Gamma \qquad \dfrac{\vdash A[t/x], !C^\perp, \Delta}{\vdash \bigvee x.A, !C^\perp, \Delta}}{\vdash \bigvee x.A, \Gamma, \Delta} \rightsquigarrow \frac{\dfrac{\vdash\ ?C^k, \Gamma \quad \vdash A[t/x], !C^\perp, \Delta}{\vdash A[t/x], \Gamma, \Delta}}{\vdash \bigvee x.A, \Gamma, \Delta}$$

$(?\, cut/ \in)$–!

$$\frac{\vdash\ ?C^k, \Gamma \qquad \dfrac{\vdash A[t/x], !C^\perp, \Delta}{\vdash t \in \{x : A\}, !C^\perp, \Delta}}{\vdash t \in \{x : A\}, \Gamma, \Delta} \rightsquigarrow \frac{\dfrac{\vdash\ ?C^k, \Gamma \quad \vdash A[t/x], !C^\perp, \Delta}{\vdash A[t/x], \Gamma, \Delta}}{\vdash t \in \{x : A\}, \Gamma, \Delta}$$

$(?\, cut/ \notin)$–!

$$\frac{\vdash\ ?C^k, \Gamma \qquad \dfrac{\vdash A[t/x]^\perp, !C^\perp, \Delta}{\vdash t \notin \{x : A\}, !C^\perp, \Delta}}{\vdash t \notin \{x : A\}, \Gamma, \Delta} \rightsquigarrow \frac{\dfrac{\vdash\ ?C^k, \Gamma \quad \vdash A[t/x]^\perp, !C^\perp, \Delta}{\vdash A[t/x]^\perp, \Gamma, \Delta}}{\vdash t \notin \{x : A\}, \Gamma, \Delta}$$

$(?\, cut/ \perp)$–!

$$\frac{\vdash\ ?C^k, \Gamma \qquad \dfrac{\vdash\ !C^\perp, \Delta}{\vdash \perp, !C^\perp, \Delta}}{\vdash \perp, \Gamma, \Delta} \rightsquigarrow \frac{\dfrac{\vdash\ ?C^k, \Gamma \quad \vdash\ !C^\perp, \Delta}{\vdash \Gamma, \Delta}}{\vdash \perp, \Gamma, \Delta}$$

$(?\, cut/ W?)$–!

$$\frac{\vdash\ ?C^k, \Gamma \qquad \dfrac{\vdash\ !C^\perp, \Delta}{\vdash\ ?A, !C^\perp, \Delta}}{\vdash\ ?A, \Gamma, \Delta} \rightsquigarrow \frac{\dfrac{\vdash\ ?C^k, \Gamma \quad \vdash\ !C^\perp, \Delta}{\vdash \Gamma, \Delta}}{\vdash\ ?A, \Gamma, \Delta}$$

$(?\, cut/ D?)$–!

$$\frac{\vdash\ ?C^k, \Gamma \qquad \dfrac{\vdash A, !C^\perp, \Delta}{\vdash\ ?A, !C^\perp, \Delta}}{\vdash\ ?A, \Gamma, \Delta} \rightsquigarrow \frac{\dfrac{\vdash\ ?C^k, \Gamma \quad \vdash A, !C^\perp, \Delta}{\vdash A, \Gamma, \Delta}}{\vdash\ ?A, \Gamma, \Delta}$$

$(\,?\,cut/C?)$–!

$$\frac{\vdash\, ?\,C^k, \Gamma \qquad \dfrac{\vdash\, ?\,A,\, ?\,A,\, !\,C^\perp, \Delta}{\vdash\, ?\,A,\, !\,C^\perp, \Delta}}{\vdash\, ?\,A, \Gamma, \Delta} \leadsto \frac{\dfrac{\vdash\, ?\,C^k, \Gamma \quad \vdash\, ?\,A,\, ?\,A,\, !\,C^\perp, \Delta}{\vdash\, ?\,A,\, ?\,A, \Gamma, \Delta}}{\vdash\, ?\,A, \Gamma, \Delta}$$

$(\,?\,cut/cut)$–!

$$\frac{\vdash\, ?\,C^k, \Gamma \qquad \dfrac{\vdash A,\, !\,C^\perp, \Delta \quad \vdash A^\perp, \Theta}{\vdash\, !\,C^\perp, \Delta, \Theta}}{\vdash \Gamma, \Delta, \Theta} \leadsto \frac{\dfrac{\vdash\, ?\,C^k, \Gamma \quad \vdash A,\, !\,C^\perp, \Delta}{\vdash A, \Gamma, \Delta} \qquad \vdash A^\perp, \Theta}{\vdash \Gamma, \Delta, \Theta}$$

$(\,?\,cut/\,?\,cut1)$–!

$$\frac{\vdash\, ?\,C^k, \Gamma \qquad \dfrac{\vdash\, ?\,A^k,\, !\,C^\perp, \Delta \quad \vdash\, !\,A^\perp, \Theta}{\vdash\, !\,C^\perp, \Delta, \Theta}}{\vdash \Gamma, \Delta, \Theta} \leadsto \frac{\dfrac{\vdash\, ?\,C^k, \Gamma \quad \vdash\, ?\,A^k,\, !\,C^\perp, \Delta}{\vdash\, ?\,A^k, \Gamma, \Delta} \qquad \vdash\, !\,A^\perp, \Theta}{\vdash \Gamma, \Delta, \Theta}$$

$(\,?\,cut/\,?\,cut2)$–!

$$\frac{\vdash\, ?\,C^k, \Gamma \qquad \dfrac{\vdash\, ?\,A^k, \Delta \quad \vdash\, !\,A^\perp,\, !\,C^\perp, \Theta}{\vdash\, !\,C^\perp, \Delta, \Theta}}{\vdash \Gamma, \Delta, \Theta} \leadsto \frac{\dfrac{\vdash\, ?\,C^k, \Gamma \quad \vdash\, !\,A^\perp,\, !\,C^\perp, \Theta}{\vdash\, !\,A^\perp, \Gamma, \Theta} \qquad \vdash\, ?\,A^k, \Delta}{\vdash \Gamma, \Delta, \Theta}$$

Permutative reductions for $(\,?\,cut)$ on ?–branch

We indicate this type of permutations with the suffix ?. Note that we are assuming that the cut formula $!\,C^\perp$ is the main formula of the !-branch.

$(\otimes/\,?\,cut1)$–?

$$\frac{\dfrac{\vdash A,\, ?\,C^k, \Gamma \quad \vdash B, \Delta}{\vdash A \otimes B,\, ?\,C^k, \Gamma, \Delta} \qquad \vdash\, !\,C^\perp,\, ?\,\Theta}{\vdash A \otimes B, \Gamma, \Delta, \Theta} \leadsto \frac{\dfrac{\vdash A,\, ?\,C^k, \Gamma \quad \vdash\, !\,C^\perp,\, ?\,\Theta}{\vdash A, \Gamma,\, ?\,\Theta} \qquad \vdash B, \Delta}{\vdash A \otimes B, \Gamma, \Delta,\, ?\,\Theta}$$

$(\otimes/\,?\,cut2)$–?

$$\frac{\dfrac{\vdash A,\, ?\,C^k, \Gamma \quad \vdash B,\, ?\,C^l, \Delta}{\vdash A \otimes B,\, ?\,C^{k+l}, \Gamma, \Delta} \qquad \vdash\, !\,C^\perp,\, ?\,\Theta}{\vdash A \otimes B, \Gamma, \Delta,\, ?\,\Theta} \leadsto \frac{\dfrac{\dfrac{\vdash A,\, ?\,C^k, \Gamma \quad \vdash\, !\,C^\perp,\, ?\,\Theta}{\vdash A, \Gamma,\, ?\,\Theta} \qquad \dfrac{\vdash B,\, ?\,C^l, \Delta \quad \vdash\, !\,C^\perp,\, ?\,\Theta}{\vdash B, \Delta,\, ?\,\Theta}}{\vdash A \otimes B, \Gamma, \Delta,\, ?\,\Theta,\, ?\,\Theta}}{\vdash A \otimes B, \Gamma, \Delta,\, ?\,\Theta}$$

$(\mathbin{\text{⅋}}/\ ?\,cut)$–?

$$\dfrac{\dfrac{\vdash A, B, ?\,C^k, \Gamma}{\vdash A \mathbin{\text{⅋}} B, ?\,C^k, \Gamma} \quad \vdash\, !\,C^\perp, ?\,\Delta}{\vdash A \mathbin{\text{⅋}} B, \Gamma, ?\,\Delta} \rightsquigarrow \dfrac{\dfrac{\vdash A, B, ?\,C^k, \Gamma \quad \vdash\, !\,C^\perp, ?\,\Delta}{\vdash A, B, \Gamma, ?\,\Delta}}{\vdash A \mathbin{\text{⅋}} B, \Gamma, \Delta}$$

$(\&/\ ?\,cut)$–?

$$\dfrac{\dfrac{\vdash A, ?\,C^k, \Gamma \quad \vdash B, ?\,C^k, \Gamma}{\vdash A \,\&\, B, ?\,C^k, \Gamma} \quad \vdash\, !\,C^\perp, ?\,\Delta}{\vdash A \,\&\, B, \Gamma, ?\,\Delta} \rightsquigarrow \dfrac{\dfrac{\vdash A, ?\,C^k, \Gamma \quad \vdash\, !\,C^\perp, ?\,\Delta}{\vdash A, \Gamma, ?\,\Delta} \quad \dfrac{\vdash B, ?\,C^k, \Gamma \quad \vdash\, !\,C^\perp, ?\,\Delta}{\vdash B, \Gamma, ?\,\Delta}}{\vdash A \,\&\, B, \Gamma, ?\,\Delta}$$

$(\oplus 1/\ ?\,cut)$–?

$$\dfrac{\dfrac{\vdash A, ?\,C^k, \Gamma}{\vdash A \oplus B, ?\,C^k, \Gamma} \quad \vdash\, !\,C^\perp, ?\,\Delta}{\vdash A \oplus B, \Gamma, ?\,\Delta} \rightsquigarrow \dfrac{\dfrac{\vdash A, ?\,C^k, \Gamma \quad \vdash\, !\,C^\perp, ?\,\Delta}{\vdash A, \Gamma, ?\,\Delta}}{\vdash A \oplus B, \Gamma, \Delta}$$

$(\oplus 2/\ ?\,cut)$–?

$$\dfrac{\dfrac{\vdash B, ?\,C^k, \Gamma}{\vdash A \oplus B, ?\,C^k, \Gamma} \quad \vdash\, !\,C^\perp, ?\,\Delta}{\vdash A \oplus B, \Gamma, ?\,\Delta} \rightsquigarrow \dfrac{\dfrac{\vdash B, ?\,C^k, \Gamma \quad \vdash\, !\,C^\perp, ?\,\Delta}{\vdash B, \Gamma, ?\,\Delta}}{\vdash A \oplus B, \Gamma, \Delta}$$

$(\bigwedge/\ ?\,cut)$–?

$$\dfrac{\dfrac{\vdash A, ?\,C^k, \Gamma}{\vdash \bigwedge x.A, ?\,C^k, \Gamma} \quad \vdash\, !\,C^\perp, ?\,\Delta}{\vdash \bigwedge x.A, \Gamma, ?\,\Delta} \rightsquigarrow \dfrac{\dfrac{\vdash A[y/x], ?\,C^k, \Gamma \quad \vdash\, !\,C^\perp, ?\,\Delta}{\vdash A[y/x], \Gamma, ?\,\Delta}}{\vdash \bigwedge y.A, \Gamma, \Delta}$$

$(\bigvee/\ ?\,cut)$–?

$$\dfrac{\dfrac{\vdash A[t/x], ?\,C^k, \Gamma}{\vdash \bigvee x.A, ?\,C^k, \Gamma} \quad \vdash\, !\,C^\perp, ?\,\Delta}{\vdash \bigvee x.A, \Gamma, ?\,\Delta} \rightsquigarrow \dfrac{\dfrac{\vdash A[t/x], ?\,C^k, \Gamma \quad \vdash\, !\,C^\perp, ?\,\Delta}{\vdash A[t/x], \Gamma, ?\,\Delta}}{\vdash \bigvee x.A, \Gamma, \Delta}$$

$(\in/\ ?\,cut)$–?

$$\dfrac{\dfrac{\vdash A[t/x], ?\,C^k, \Gamma}{\vdash t \in \{x : A\}, ?\,C^k, \Gamma} \quad \vdash\, !\,C^\perp, ?\,\Delta}{\vdash t \in \{x : A\}, \Gamma, ?\,\Delta} \rightsquigarrow \dfrac{\dfrac{\vdash A[t/x], ?\,C^k, \Gamma \quad \vdash\, !\,C^\perp, ?\,\Delta}{\vdash A[t/x], \Gamma, ?\,\Delta}}{\vdash t \in \{x : A\}, \Gamma, \Delta}$$

$(\notin /\ ?\, cut)$–?

$$\dfrac{\dfrac{\vdash A[t/x]^\perp, ?\,C^k, \Gamma}{\vdash t \notin \{x : A\}, ?\,C^k, \Gamma} \quad \vdash\ !\,C^\perp, ?\,\Delta}{\vdash t \notin \{x : A\}, \Gamma, ?\,\Delta} \leadsto \dfrac{\dfrac{\vdash A[t/x]^\perp, ?\,C^k, \Gamma \quad \vdash\ !\,C^\perp, ?\,\Delta}{\vdash A[t/x]^\perp, \Gamma, ?\,\Delta}}{\vdash t \notin \{x : A\}, \Gamma, \Delta}$$

$(\bot /\ ?\, cut)$–?

$$\dfrac{\dfrac{\vdash\ ?\,C^k, \Gamma}{\vdash \bot, ?\,C^k, \Gamma} \quad \vdash\ !\,C^\perp, ?\,\Delta}{\vdash \bot, \Gamma, ?\,\Delta} \leadsto \dfrac{\dfrac{\vdash\ ?\,C^k, \Gamma \quad \vdash\ !\,C^\perp, ?\,\Delta}{\vdash \Gamma, ?\,\Delta}}{\vdash \bot, \Gamma, \Delta}$$

$(W?/\ ?\, cut)$–?

$$\dfrac{\dfrac{\vdash\ ?\,C^k, \Gamma}{\vdash\ ?\,A, ?\,C^k, \Gamma} \quad \vdash\ !\,C^\perp, ?\,\Delta}{\vdash\ ?\,A, \Gamma, ?\,\Delta} \leadsto \dfrac{\dfrac{\vdash\ ?\,C^k, \Gamma \quad \vdash\ !\,C^\perp, ?\,\Delta}{\vdash \Gamma, ?\,\Delta}}{\vdash\ ?\,A, \Gamma, \Delta}$$

$(D?/\ ?\, cut)$–?

$$\dfrac{\dfrac{\vdash A, ?\,C^k, \Gamma}{\vdash\ ?\,A, ?\,C^k, \Gamma} \quad \vdash\ !\,C^\perp, ?\,\Delta}{\vdash\ ?\,A, \Gamma, ?\,\Delta} \leadsto \dfrac{\dfrac{\vdash A, ?\,C^k, \Gamma \quad \vdash\ !\,C^\perp, ?\,\Delta}{\vdash A, \Gamma, ?\,\Delta}}{\vdash\ ?\,A, \Gamma, \Delta}$$

$(C?/\ ?\, cut)$–?

$$\dfrac{\dfrac{\vdash\ ?\,A, ?\,A, ?\,C^k, \Gamma}{\vdash\ ?\,A, ?\,C^k, \Gamma} \quad \vdash\ !\,C^\perp, ?\,\Delta}{\vdash\ ?\,A, \Gamma, ?\,\Delta} \leadsto \dfrac{\dfrac{\vdash\ ?\,A, ?\,A, ?\,C^k, \Gamma \quad \vdash\ !\,C^\perp, ?\,\Delta}{\vdash\ ?\,A, ?\,A, \Gamma, ?\,\Delta}}{\vdash\ ?\,A, \Gamma, \Delta}$$

$(!/\ ?\, cut)$–?

$$\dfrac{\dfrac{\vdash A, ?\,C^k, ?\,\Gamma}{\vdash\ !\,A, ?\,C^k, ?\,\Gamma} \quad \vdash\ !\,C^\perp, ?\,\Delta}{\vdash\ !\,A, ?\,\Gamma, ?\,\Delta} \leadsto \dfrac{\dfrac{\vdash A, ?\,C^k, ?\,\Gamma \quad \vdash\ !\,C^\perp, ?\,\Delta}{\vdash\ !\,A, ?\,\Gamma, ?\,\Delta}}{\vdash\ !\,A, \Gamma, \Delta}$$

$(cut/\ ?\, cut1)$–?

$$\dfrac{\dfrac{\vdash A, ?\,C^k, \Gamma \quad \vdash A^\perp, \Delta}{\vdash\ ?\,C^k, \Gamma, \Delta} \quad \vdash\ !\,C^\perp\ ?\,\Theta}{\vdash \Gamma, \Delta, ?\,\Theta} \leadsto \dfrac{\dfrac{\vdash A, ?\,C^k, \Gamma \quad \vdash\ !\,C^\perp, ?\,\Theta}{\vdash A, \Gamma, ?\,\Theta} \quad \vdash A^\perp, \Delta}{\vdash \Gamma, \Delta, ?\,\Theta}$$

$(cut/\,?\,cut2)$–?

$$\dfrac{\dfrac{\vdash A, ?C^k, \Gamma \quad \vdash A^\perp, ?C^l, \Delta}{\vdash ?C^{k+l}, \Gamma, \Delta} \quad \vdash !C^\perp, ?\Theta}{\vdash \Gamma, \Delta, ?\Theta} \quad \leadsto \quad \dfrac{\dfrac{\dfrac{\vdash A, ?C^k, \Gamma \quad \vdash !C^\perp, ?\Theta}{\vdash A, ?\Theta, \Gamma} \quad \dfrac{\vdash A^\perp, ?C^l, \Delta \quad \vdash !C^\perp, ?\Theta}{\vdash A^\perp, \Delta, ?\Theta}}{\vdash \Gamma, \Delta, ?\Theta, ?\Theta}}{\vdash \Gamma, \Delta, ?\Theta}$$

$(\,?\,cut/\,?\,cut1)$–?

$$\dfrac{\dfrac{\vdash ?A^n, ?C^k, \Gamma \quad \vdash !A^\perp, \Delta}{\vdash ?C^k, \Gamma, \Delta} \quad \vdash !C^\perp, ?\Theta}{\vdash \Gamma, \Delta, ?\Theta} \quad \leadsto \quad \dfrac{\dfrac{\vdash ?A^n, ?C^k, \Gamma \quad \vdash !C^\perp, ?\Theta}{\vdash ?A^n, \Gamma, ?\Theta} \quad \vdash !A^\perp, \Delta}{\vdash \Gamma, \Delta, ?\Theta}$$

$(\,?\,cut/\,?\,cut2)$–?

$$\dfrac{\dfrac{\vdash ?A^n, \Gamma \quad \vdash !A^\perp, ?C^k, \Delta}{\vdash ?C^k, \Gamma, \Delta} \quad \vdash !C^\perp, ?\Theta}{\vdash \Gamma, \Delta, ?\Theta} \quad \leadsto \quad \dfrac{\vdash ?A^n, \Gamma \quad \dfrac{\vdash !A^\perp, ?C^k, \Delta \quad \vdash !C^\perp, ?\Theta}{\vdash !A^\perp, \Delta, ?\Theta}}{\vdash \Gamma, \Delta, ?\Theta}$$

$(\,?\,cut/\,?\,cut3)$–?

$$\dfrac{\dfrac{\vdash ?A^n, ?C^k, \Gamma \quad \vdash !A^\perp, ?C^l, \Delta}{\vdash ?C^{k+l}, \Gamma, \Delta} \quad \vdash !C^\perp, ?\Theta}{\vdash \Gamma, \Delta, ?\Theta} \quad \leadsto \quad \dfrac{\dfrac{\dfrac{\vdash ?A^n, ?C^k, \Gamma \quad \vdash !C^\perp, ?\Theta}{\vdash ?A^n, \Gamma, ?\Theta} \quad \dfrac{\vdash !A^\perp, ?C^l, \Delta \quad \vdash !C^\perp, ?\Theta}{\vdash !A^\perp, \Delta, ?\Theta}}{\vdash \Gamma, \Delta, ?\Theta, ?\Theta}}{\vdash \Gamma, \Delta, ?\Theta}$$

2.4 The cut-elimination theorem for SMALL

In this section, we prove the cut-elimination theorem for SMALL$^+$, and hence for SMALL. The proof has two parts. To explain them, we need to fix the terminology. The word *cut* is used as a generic term for application of (cut) as well as $(\,?\,cut)$. If the cut formulas of a cut are atomic, we call the cut *atomic*. Otherwise cuts are *non-atomic*. Then we proceed as follows:

1. We show that all the non-atomic cuts can be eliminated by the standard method, *i.e.*, by induction on the syntactic complexity of formulas.

2. We then show that all the atomic cuts can be eliminated by induction on the size of a proof.

In the cut-elimination process of atomic cuts, we may create non-atomic cuts. However, note that those cuts never involve exponentials.

2.4.1 The elimination of non-atomic cuts

The cut-elimination of non-atomic cuts is obtained by the standard method, *i.e.*, by induction on the syntactic complexity, or *degree* $\partial(A)$, of formulas A. We start with the definition of degrees.

Definition 2.3 *The degree $\partial(A)$ of a formula A is defined inductively as follows:*

- *If A is atomic, then $\partial(A) = 1$*
- $\partial(A \otimes B) = \partial(A \parr B) = \partial(A \mathbin{\&} B) = \partial(A \oplus B) = max(\partial(A) + \partial(B)) + 1$
- $\partial(\,!\,A) = \partial(\,?\,A) = \partial(A) + 1$

In addition, we define the degree $\partial(\pi)$ of a proof π to be the supremum of the degrees of the cut formulas in π.

Note that the degrees of a formula A and its $A^{\perp}$ are always the same. This can be shown immediately by induction on the definition of linear negation.

Furthermore, we introduce two measures of the size of a proof, the first of which we call *Girard-size*, and the second simply *size*. In fact, we need only one of them in our proofs of the cut-elimination theorems, and we will use only the second in later chapters. The size is much cleaner than the Girard size, and sufficient for our purpose. On the other hand, the Girard-size is rather interesting for its own sake, and we can actually obtain a stronger result with it. This is our justification for presenting both of them. First, we give the definition of the Girard-size $\varsigma(\pi)$ of a proof π.

Definition 2.4 *The Girard-size $\varsigma(\pi)$ of a proof π is defined inductively as follows:*

- *If π is one of the axioms (I), then $\varsigma(\pi) = 2 \cdot 2 = 4$*
- *If π is the axiom $(\mathbf{1})$, then $\varsigma(\pi) = 2$*
- *If π is one of the axioms $(\top)$ of the form $\vdash \top, C^1 \ldots C^n$, then $\varsigma(\pi) = 2 + n$*
- *If π is obtained from τ by one of the rules of inference $(\perp)$, $(W?)$, $(\bigwedge)$, $(\in)$ and $(!)$, then $\varsigma(\pi) = \varsigma(\tau) + 1$*

- *If π is obtained from π_1 and π_2 by the rule of inference* ($\&$), *then* $\varsigma(\pi) = \varsigma(\pi_1)+\varsigma(\pi_2)+1$
- *If π is obtained from τ by one of the rules of inference* ($⅋$), ($\oplus 1$), ($\oplus 2$), ($\bigvee$), ($\notin$), ($D?$) *and* ($C?$), *then* $\varsigma(\pi) = \varsigma(\tau) \cdot 2$
- *If π is obtained from π_1 and π_2 by the rule of inference* ($\otimes$), *then* $\varsigma(\pi) = \varsigma(\pi_1) \cdot \varsigma(\pi_2) \cdot 2$
- *If π is obtained from π_1 and π_2 by one of* (cut) *and* ($?\,cut$), *then* $\varsigma(\pi) = \varsigma(\pi_1) \cdot \varsigma(\pi_2)$

The definition of the size $\sigma(\pi)$ of a proof π is more straightforward:

Definition 2.5 *The size $\sigma(\pi)$ of a proof π is defined inductively as follows:*

- *If π is an axiom, then* $\sigma(\pi) = 1$
- *If π is obtained from τ by one of the one-premiss rules of inference* ($⅋$), ($\oplus 1$), ($\oplus 2$), ($\bigwedge$), ($\bigvee$), ($\in$), ($\notin$), ($W?$), ($D?$), ($C?$) *and* ($!$), *then* $\sigma(\pi) = \sigma(\tau) + 1$
- *If π is obtained from π_1 and π_2 by one of the rules of inference* ($\otimes$), (cut) *and* ($?\,cut$), *then* $\sigma(\pi) = \sigma(\pi_1) + \sigma(\pi_2)$
- *If π is obtained from π_1 and π_2 by* ($\&$), *then* $\sigma(\pi) = max(\sigma(\pi_1), \sigma(\pi_2)) + 1$

In the cut-elimination of non-atomic cuts, we reduce the maximal degree of the cut-formulas as usual. We first show that the uppermost cut with the maximal degree of formulas can be eliminated. In the proof, we use the size $\sigma(\pi)$ of a proof π for induction. In fact, there are two cases since we have ($?\,cut$) as well as (cut). We begin with the former.

Proposition 2.6 *Consider the proof π*

$$\dfrac{\dfrac{\vdots \pi_1}{\vdash \Gamma, ?\,A^k} \qquad \dfrac{\vdots \pi_2}{\vdash \Delta, !\,A^{\perp}}}{\vdash \Gamma, \Delta}\ (?\,cut)$$

and suppose that the degrees $\partial(\pi_1)$ and $\partial(\pi_2)$ of the proofs π_1 and π_2 are strictly less than the degree $\partial(?\,A)$ of the formula $?\,A$. Then there exists a proof τ with the same conclusion $\vdash \Gamma, \Delta$ such that π reduces τ and $\partial(\tau)$ is strictly less than $\partial(?\,A)$.

Proof
The proof is by induction on $\sigma(\pi_1) + \sigma(\pi_2)$.

Case 1 The last inference of π_2 is not $(\,!\,)$.

1.1 π_2 is an axiom $(\top)$. Then π reduces to the same type of axiom.

1.2 Otherwise, we apply one of the permutative reductions and use the inductive hypothesis.

Case 2 The last inference of π_2 is $(\,!\,)$.

2.1 π_1 is an axiom $(\top)$. Then π reduces to the same type of axiom.

2.2 The main formula of the last inference of π_1 is not one of $?\,A^k$. Then we apply one of the permutative reductions and use the inductive hypothesis.

2.3 The main formula of the last inference of π_1 is one of $?\,A^k$ and $2 \leq k$. Then we apply one of the symmetric reductions and use the inductive hypothesis.

2.4 The main formula of the last inference is one of $?\,A^k$ and $k = 1$. Then we apply one of the symmetric reductions.

■

The case for (cut) is essentially the same.

Proposition 2.7 *Consider the proof* π

$$\dfrac{\begin{array}{c}\vdots\pi_1\\ \vdash \Gamma, A\end{array} \quad \begin{array}{c}\vdots\pi_2\\ \vdash \Delta, A^\perp\end{array}}{\vdash \Gamma, \Delta}$$

where the formula A is not of the form $?\,C$ nor $!\,C$. Suppose that the degrees $\partial(\pi_1)$ and $\partial(\pi_2)$ are strictly less than the degree $\partial(A)$ of the formula A and $2 \leq \partial(A)$. Then there exists a proof τ with the same conclusion $\vdash \Gamma, \Delta$ such that π reduces to τ and $\partial(\tau)$ is strictly less than $\partial(A)$.

Proof

The proof is by induction on $\sigma(\pi_1) + \sigma(\pi_2)$

2.1 One of π_1 and π_2 is $\top$-axiom. Then π reduces to the same kind of axiom.

2.2 One of A and $A^\perp$ is not the main formula of the last rule of inference in π_1 or π_2. Then we apply one of the permutative reduction and use the inductive hypothesis.

2.3 A and $A^{\perp}$ are the main formulas of the last rules of inference. We then apply the symmetric reduction. Note that we do not use the symmetric reduction ($\in$ / $\notin$) since $2 \leq \partial(A)$. Hence the degree decreases.

∎

We can now prove:

Lemma 2.8 *For any proof π of the sequent $\vdash \Gamma$ with $2 \leq \partial(\pi)$, there exists a proof τ of the same conclusion $\vdash \Gamma$ such that π reduces to τ and $\partial(\tau)$ is strictly less than $\partial(\pi)$.*

Proof

The proof is by induction on $\sigma(\pi)$. Consider the lowermost cut with the formulas of the maximum degree in π. Apply the inductive hypothesis to both of the branches. Then eliminate the remaining cut by the previous propositions. ∎

From this lemma, the following result is obtained immediately by induction on the degree $\partial(\pi)$ of a proof π.

Corollary 2.9 *For any proof π of the sequent $\vdash \Gamma$ with $2 \leq \partial(\pi)$, there exists a proof τ of the same conclusion $\vdash \Gamma$ such that π reduces to τ and $\partial(\tau)$ is less than or equal to 1.*

In other words, any proof π can be reduced to another proof τ which contains either only atomic cuts or none.

2.4.2 The elimination of atomic cuts

The cut-elimination of atomic cuts is by induction on the size of a proof. For this, the Girard-size $\varsigma(\pi)$ of a proof π as well well as the size $\sigma(\pi)$ can be used.

So far, we have shown that we can eliminate all the non-atomic cuts. In the process of eliminating the remaining atomic cuts, we create new cuts which may not be atomic. However, the cut-formulas of the new cuts never contain any exponentials, due to our definition of terms. Therefore, no symmetric or permutative reductions for ($?\,cut$) needs to be used anymore.

The symmetric and permutative reductions for (cut) have a good property with respect to the size of a proof. The Girard-size $\varsigma(\pi)$ of a proof π strictly decreases by any of the symmetric reductions for (cut), and does not increase by the permutative reductions for (cut). The same property holds with the size $\sigma(\pi)$ instead of $\varsigma(\pi)$.

For the Girard-size, we need the lemma:

Lemma 2.10 *The Girard-size $\varsigma(\pi)$ of a proof π of the sequent $\vdash C_1, \ldots, C_n$ is greater than or equal to 2, and strictly greater than n.*

Proof

The proof is by induction on the construction of a proof.

Case 1 π is (I). Then $\varsigma(\pi) = 4$ which is greater than 2.

Case 2 π is $(\mathbf{1})$. Then $\varsigma(\pi) = 2 > 1$.

Case 3 π is $(\top)$. Then $\varsigma(\pi) = 2 + n \geq 2$ and $\varsigma(\pi) > n$.

Case 4 π is obtained from τ by one of $(\bot)$ and $(W?)$. By the inductive hypothesis, $\varsigma(\tau) \geq 2$ and $\varsigma(\tau) > m$ where $n = m + 1$. Hence $\varsigma(\pi) = \varsigma(\tau) + 1 \geq 2$ and $\varsigma(\pi) > m + 1 = n$.

Case 5 π is obtained from τ by one of $(\bigwedge)$, $(\in)$ and $(!)$. Then $\varsigma(\tau) \geq 2$ and $\varsigma(\tau) > n$ by the inductive hypothesis. Therefore $\varsigma(\pi) = \varsigma(\tau) + 1 \geq 2$ and $\varsigma(\pi) > n$.

Case 6 π is obtained from π_1 and π_2 by the rule of inference $(\&)$. Then $\varsigma(\pi_1) > m_1$ and $\varsigma(\pi_2) > m_2$ where $n = m_1 + m_2 - 1$. Hence $\varsigma(\pi) = \varsigma(\pi_1) + \varsigma(\pi_2) + 1 > m_1 + m_2 > n$. Similarly $\varsigma(\pi) \geq 2 + 2 + 1 > 2$.

Case 7 π is obtained from τ by one of $(\oplus 1)$, $(\oplus 2)$, $(\bigvee)$, $(\notin)$ and $(D?)$. Then $\varsigma(\tau) > n$ and $\varsigma(\pi) = \varsigma(\tau) \cdot 2 > 2n > n$. Similarly $\varsigma(\pi) \geq 2 \cdot 2 = 4 > 2$.

Case 8 π is obtained from τ by one of $(\invamp)$ and $(C?)$. Then $\varsigma(\tau) > m$ where $m = n + 1$. Hence $\varsigma(\pi) = \varsigma(\tau) \cdot 2 > 2m = 2n + 2 > 2$.

Case 9 π is obtained from π_1 and π_2 by $(\otimes)$. Then $\varsigma(\pi_1) > m_1$ and $\varsigma(\pi_2) > m_2$ where $n = m_1 + m_2 - 1$. Hence $\varsigma(\pi) = \varsigma(\pi_1) \cdot \varsigma(\pi_2) \cdot 2 > 2m_1 m_2$. Now m_1 and m_2 are greater than or equal to 1 since otherwise the rule $(\otimes)$ would not be applicable. Hence $m_1 m_2 \geq m_1$ and $m_1 m_2 \geq m_2$. Therefore $2m_1 m_2 \geq m_1 + m_2 > n$. Similarly $\varsigma(\pi) \geq 2 \cdot 2 \cdot 2 > 2$.

Case 10 π is obtained from π_1 and π_2 by (cut). Then $\varsigma(\pi_1) > m_1$ and $\varsigma(\pi_2) > m_2$ where $n = m_1 + m_2 - 2$. Hence $\varsigma(\pi) = \varsigma(\pi_1) \cdot \varsigma(\pi_2) \cdot 2 > 2m_1 m_2 \geq m_1 + m_2 > n$ for the same reason as above. Similarly $\varsigma(\pi) \geq 2 \cdot 2 \cdot 2 > 2$.

Case 11 π is obtained from π_1 and π_2 by $(\,?\,cut)$. This is the same as above except $n = m_1 + m_2 - k - 1$.

∎

We now prove the essential lemmas for the cut-elimination theorem.

Lemma 2.11 *All the symmetric reductions for (cut) strictly decrease the Girard-size of a proof.*

Proof

The proof is by simple computation. We show in a diagrammatical way how the size of a proof changes.

The symmetric reduction $(*/I)$

$$\frac{\vdash \alpha \quad \vdash 4}{\vdash 4\alpha} \quad \rightsquigarrow \quad \vdash \alpha$$

where $4\alpha > \alpha$ since α is non-zero.

The symmetric reduction $(\perp/\mathbf{1})$

$$\frac{\dfrac{\vdash \alpha}{\vdash \alpha + 1} \quad \vdash 2}{\vdash 2(\alpha + 1)} \quad \rightsquigarrow \quad \vdash \alpha$$

The symmetric reduction $(*/\top)$

$$\frac{\vdash \alpha \quad \vdash 2 + n}{\vdash \alpha(2 + n)} \quad \rightsquigarrow \quad \vdash m + (2 + n) - 2$$

where m is the number of the formula occurrences of the last sequent of the left branch. As we have seen, $\alpha > m$ and $\alpha \geq 2$. Hence $\alpha(2 + n) = 2\alpha + \alpha n > 2m + 2n > m + n$.

The symmetric reduction $(\otimes/\wp)$

$$\frac{\dfrac{\vdash \alpha \quad \vdash \beta}{\vdash 2\alpha\beta} \quad \dfrac{\vdash \gamma}{\vdash 2\gamma}}{\vdash 4\alpha\beta\gamma} \quad \rightsquigarrow \quad \frac{\vdash \beta \quad \dfrac{\vdash \alpha \quad \vdash \gamma}{\vdash \alpha\gamma}}{\vdash \alpha\beta\gamma}$$

where $4\alpha\beta\gamma > \alpha\beta\gamma$ since α, β and γ are non-zero.

The symmetric reductions $(\&/\oplus 1)$ **and** $(\&/\oplus 2)$ For $(\&/\oplus 1)$, we have the following.

$$\dfrac{\dfrac{\vdash \alpha \quad \vdash \beta}{\vdash \alpha+\beta+1} \quad \dfrac{\vdash \gamma}{\vdash 2\gamma}}{\vdash 2\gamma(\alpha+\beta+1)} \quad \leadsto \quad \dfrac{\vdash \alpha \quad \vdash \gamma}{\vdash \alpha\gamma}$$

where the inequality holds since α and γ are non-zero. The case for $(\&/\oplus 2)$ is entirely similar.

The symmetric reductions $(\bigwedge / \bigvee)$ **and** $(\in / \notin)$

$$\dfrac{\dfrac{\vdash \alpha}{\vdash \alpha+1} \quad \dfrac{\vdash \beta}{\vdash 2\beta}}{\vdash 2\beta(\alpha+1)} \quad \leadsto \quad \dfrac{\vdash \alpha \quad \vdash \beta}{\vdash \alpha\beta}$$

where the inequality holds since α and β are non-zero. ∎

Lemma 2.12 *The permutative reductions* $(cut/\&)$, $(cut/\bigwedge)$, $(cut/\in)$ *and* $(cut/W?)$ *for* (cut) *strictly decreases the Girard-size of a proof. The rest of the permutative reductions for* (cut) *preserve the Girard-size.*

Proof

The proof is by computation and from the previous lemma.

The permutative reduction $(cut/\&)$

$$\dfrac{\vdash \alpha \quad \dfrac{\vdash \beta \quad \vdash \gamma}{\vdash \beta+\gamma+1}}{\vdash \alpha(\beta+\gamma+1)} \quad \leadsto \quad \dfrac{\dfrac{\vdash \alpha \quad \vdash \beta}{\vdash \alpha\beta} \quad \dfrac{\vdash \alpha \quad \vdash \gamma}{\vdash \alpha\gamma}}{\vdash \alpha\beta+\alpha\gamma+1}$$

where $\alpha(\beta+\gamma+1) = \alpha\beta+\alpha\gamma+\alpha > \alpha\beta+\alpha\gamma+1$ since $\alpha \geq 2$.

The permutative reductions $(cut/\bigwedge)$, $(cut/\in)$ **and** $(cut/W?)$

$$\dfrac{\vdash \alpha \quad \dfrac{\vdash \beta}{\vdash \beta+1}}{\vdash \alpha(\beta+1)} \quad \leadsto \quad \dfrac{\dfrac{\vdash \alpha \quad \vdash \beta}{\vdash \alpha\beta}}{\vdash \alpha\beta+1}$$

where $\alpha(\beta+1) = \alpha\beta+\alpha > \alpha\beta+1$ since $\alpha \geq 2$.

The permutative reduction $(cut/\otimes)$

$$\dfrac{\vdash \alpha \qquad \dfrac{\vdash \beta \quad \vdash \gamma}{\vdash 2\beta\gamma}}{\vdash 2\alpha\beta\gamma} \quad \leadsto \quad \dfrac{\dfrac{\vdash \alpha \quad \vdash \beta}{\vdash \alpha\beta} \qquad \vdash \gamma}{\vdash 2\alpha\beta\gamma}$$

The permutative reductions (cut/cut)**,** $(cut/\,?\,cut1)$ **and** $(cut/\,?\,cut2)$ For (cut/cut) and $(cut/\,?\,cut1)$, we have the following.

$$\dfrac{\vdash \alpha \qquad \dfrac{\vdash \beta \quad \vdash \gamma}{\vdash \beta\gamma}}{\vdash \alpha\beta\gamma} \quad \leadsto \quad \dfrac{\dfrac{\vdash \alpha \quad \vdash \beta}{\vdash \alpha\beta} \qquad \vdash \gamma}{\vdash \alpha\beta\gamma}$$

The case for $(cut/\,?\,cut2)$ is entirely similar.

The permutative reductions $(cut/\parr)$**,** $(cut/\oplus 1)$**,** $(cut/\oplus 2)$**,** $(cut/\bigvee)$**,** $(cut/\not\in)$**,** $(cut/D?)$ **and** $(cut/C?)$

$$\dfrac{\vdash \alpha \qquad \dfrac{\vdash \beta}{\vdash 2\beta}}{\vdash 2\alpha\beta} \quad \leadsto \quad \dfrac{\dfrac{\vdash \alpha \quad \vdash \beta}{\vdash \alpha\beta}}{\vdash 2\alpha\beta}$$

∎

In fact, these nice properties hold also with most of the reductions for $(\,?\,cut)$. However there are notable exceptions, *i.e.*, the symmetric reduction $(D?/!)$–?, and the permutative reductions $(\otimes/\,?\,cut2)$–?, $(cut/\,?\,cut2)$–? and $(\,?\,cut/\,?\,cut3)$–?. These are the cases where we need to duplicate subproofs in the reduction processes.

The Girard size of a proof is changed by the symmetric reduction $(D?/!)$–? as follows:

$$\dfrac{\dfrac{\vdash \alpha}{\vdash 2\alpha} \qquad \dfrac{\vdash \beta}{\vdash \beta + 1}}{\vdash 2\alpha(\beta+1)} \quad \leadsto \quad \dfrac{\dfrac{\dfrac{\vdash \alpha \quad \vdash \beta + 1}{\vdash \alpha(\beta+1)} \qquad \vdash \beta}{\vdash \alpha(\beta+1)\beta}}{\vdash 2^m\alpha(\beta+1)\beta}$$

where m is the number of formulas occurrences in the context $?\Delta$. For the permutative reduction $(\otimes/\,?\,cut2)$–?, we have

$$\dfrac{\dfrac{\vdash \alpha \quad \vdash \beta}{\vdash 2\alpha\beta} \qquad \vdash \gamma}{\vdash 2\alpha\beta\gamma} \quad \leadsto \quad \dfrac{\dfrac{\dfrac{\vdash \alpha \quad \vdash \gamma}{\vdash \alpha\gamma} \qquad \dfrac{\vdash \beta \quad \vdash \gamma}{\vdash \beta\gamma}}{\vdash 2\alpha\beta\gamma^2}}{\vdash 2\alpha\beta\gamma^2 + m}$$

and for the permutative reductions $(cut/\ ?\,cut2)$–? and $(\ ?\,cut/\ ?\,cut3)$–?,

$$\dfrac{\dfrac{\vdash \alpha \quad \vdash \beta}{\vdash \alpha\beta} \quad \vdash \gamma}{\vdash \alpha\beta\gamma} \quad \rightsquigarrow \quad \dfrac{\dfrac{\dfrac{\vdash \alpha \quad \vdash \gamma}{\vdash \alpha\gamma} \quad \dfrac{\vdash \beta \quad \vdash \gamma}{\vdash \beta\gamma}}{\vdash \alpha\beta\gamma^2}}{\vdash \alpha\beta\gamma^2 + m}$$

where m is the same as above.

Instead of the Girard-size $\varsigma(\pi)$ of a proof π, we can also use the size $\sigma(\pi)$. The only significant difference is that the Girard-size strictly decreases in some of the permutative reductions for (cut), while all the permutative reductions for (cut) only preserves the size of a proof. For the normalization of a proof net, we only need those permutative reductions which strictly decrease the Girard-size. This means that all the reduction steps for proof nets, symmetric as well as permutative, strictly decrease the Girard-size of a proof. In fact, Girard defined the Girard-size for proof nets precisely to achieve this effect.

However, our cut-elimination proof only requires that all the permutative reductions at least preserve the size of a proof. For this, the much simpler measure of size $\sigma(\pi)$ suffices, and we will use only this measure in later chapters. The relevant lemmas are also simplified.

Lemma 2.13 *All the symmetric reductions for (cut) strictly decrease the size $\sigma(\pi)$ of a proof π.*

Proof

The proof is by simple computation.

The symmetric reduction $(*/I)$

$$\dfrac{\vdash \alpha \quad \vdash 1}{\vdash \alpha} \quad \rightsquigarrow \quad \vdash \alpha$$

The symmetric reduction $(\perp/\mathbf{1})$

$$\dfrac{\dfrac{\vdash \alpha}{\vdash \alpha + 1} \quad \vdash 1}{\vdash \alpha + 2} \quad \rightsquigarrow \quad \vdash \alpha$$

The symmetric reduction $(*/\top)$

$$\frac{\vdash \alpha \quad \vdash 1}{\vdash \alpha + 1} \quad \leadsto \quad \vdash 1$$

The symmetric reduction $(\otimes/\invamp)$

$$\frac{\dfrac{\vdash \alpha \quad \vdash \beta}{\vdash \alpha + \beta} \quad \dfrac{\vdash \gamma}{\vdash \gamma + 1}}{\vdash \alpha + \beta + \gamma + 1} \quad \leadsto \quad \frac{\vdash \beta \quad \dfrac{\vdash \alpha \quad \vdash \gamma}{\vdash \alpha + \gamma}}{\vdash \alpha + \beta + \gamma}$$

The symmetric reductions $(\&/\oplus 1)$ **and** $(\&/\oplus 2)$

$$\frac{\dfrac{\vdash \alpha \quad \vdash \beta}{\vdash max(\alpha,\beta) + 1} \quad \dfrac{\vdash \gamma}{\vdash \gamma + 1}}{\vdash max(\alpha,\beta) + \gamma + 2} \quad \leadsto \quad \frac{\vdash \alpha \quad \vdash \gamma}{\vdash \alpha + \gamma}$$

The symmetric reductions $(\bigwedge / \bigvee)$ **and** $(\in / \notin)$

$$\frac{\dfrac{\vdash \alpha}{\vdash \alpha + 1} \quad \dfrac{\vdash \beta}{\vdash \beta + 1}}{\vdash \alpha + \beta + 2} \quad \leadsto \quad \frac{\vdash \alpha \quad \vdash \beta}{\vdash \alpha + \beta}$$

∎

Lemma 2.14 *All the permutative reductions for* (cut) *preserve the size* $\sigma(\pi)$ *of a proof* π*.*

Proof

The proof is by computation.

The permutative reduction $(cut/\&)$

$$\frac{\vdash \alpha \quad \dfrac{\vdash \beta \quad \vdash \gamma}{\vdash max(\beta,\gamma) + 1}}{\vdash \alpha + max(\beta,\gamma) + 1} \quad \leadsto \quad \frac{\dfrac{\vdash \alpha \quad \vdash \beta}{\vdash \alpha + \beta} \quad \dfrac{\vdash \alpha \quad \vdash \gamma}{\vdash \alpha + \gamma}}{\vdash max(\alpha\beta, \alpha\gamma) + 1}$$

where $\alpha + max(\beta,\gamma) + 1 = max(\alpha + \beta, \alpha + \gamma) + 1$.

The permutative reductions $(cut/\bigwedge)$, $(cut/\in)$ **and** $(cut/W?)$

$$\dfrac{\vdash \alpha \qquad \dfrac{\vdash \beta}{\vdash \beta + 1}}{\vdash \alpha + \beta + 1} \quad \leadsto \quad \dfrac{\dfrac{\vdash \alpha \quad \vdash \beta}{\vdash \alpha + \beta}}{\vdash \alpha + \beta + 1}$$

The permutative reduction $(cut/\otimes)$, (cut/cut), $(cut/\ ?\,cut1)$ **and** $(cut/\ ?\,cut2)$

$$\dfrac{\vdash \alpha \qquad \dfrac{\vdash \beta \quad \vdash \gamma}{\vdash \beta + \gamma}}{\vdash \alpha + \beta + \gamma} \quad \leadsto \quad \dfrac{\dfrac{\vdash \alpha \quad \vdash \beta}{\vdash \alpha + \beta} \qquad \vdash \gamma}{\vdash \alpha + \beta + \gamma}$$

∎

Given these lemmas, we can now proceed by induction on the size of a proof.

Theorem 2.15 *Let π be a proof which contains no application of* $(\ ?\,cut)$*. Then there exists a proof τ of the same conclusion such that*

- *π reduces to τ,*
- *$\varsigma(\tau)$ is less than or equal to $\varsigma(\pi)$,*
- *τ contains no application of* (cut) *or* $(\ ?\,cut)$*.*

The similar results also holds for $\sigma(\pi)$.

Proof

The proof is by induction on the Girard-size $\varsigma(\pi)$ of a proof π. The similar proof also can be given by induction on $\sigma(\pi)$. First suppose that the last inference rule of π is not (cut). Then the result is obtained immediately by the inductive hypothesis. Therefore, let's suppose that π ends with a (cut). We consider reductions applicable to this cut. There are three cases.

Case 1 One of the symmetric reductions is applicable. Then we perform the symmetric reduction. The resulting proof contains no application of $(\ ?\,cut)$ due to the construction of set terms, and its Girard-size is strictly less than the original's. Hence we can apply the inductive hypotheisis to this new proof.

Case 2 One of the permutative reductions except (cut/cut) is applicable. Then we perform the permutative reduction and apply the inductive hypothesis to the immediate subproofs of the result.

Case 3 The permutative reduction (cut/cut) is applicable. Then we can apply the inductive hypothesis to the immediate subproof so that we obtain a proof ending with only one (cut). Furthermore the inductive hypothesis assures that the Girard-size of the new proof is not greater than the original one. Therefore we can proceed from here as in the two other cases.

■

As a corollary, we have the cut-elimination theorem for SMALL.

Theorem 2.16 *For any proof π of SMALL, there exists a proof τ of the same conclusion such that π reduces to τ and τ contains no application of the rule of inference (cut).*

Proof

First, we read π as a proof in SMALL$^+$. We then eliminate all non-atomic cuts. The resulting proof does not contain $(\,?\,cut)$ since the cut-formulas of $(\,?\,cut)$ are not atomic. Hence we can eliminate all the remaining cuts by the previous theorem. The result is a proof of SMALL. ■

From this, the consistency of SMALL follows immediately.

Corollary 2.17 *SMALL is consistent, i.e., there is no formula A such that both $\vdash A$ and $\vdash A^\perp$ are provable in SMALL.*

Proof

Suppose otherwise. Then we would have a proof of the empty sequent obtained by one application of (cut) from the proofs of $\vdash A$ and $\vdash A^\perp$. By the cut-elimination theorem, then, there would be a cut-free proof of the empty sequent, which is impossible. ■

Chapter 3

Infinitary linear set theory

3.1 Introduction

In this chapter, we develop our second system of linear set theory AS^{∞} based on infinitary linear logic with weakening, or infinitary affine logic, which has the infinitary additive conjunction and disjunction instead of exponentials.

AS^{∞} is a sequent-calculus version of White's natural deduction system CG [30]. The infinitary additive conjunction and disjunction are introduced by him to recover some of the uses of contraction, and the consistency of CG is proved through the normalization of *contradictive proofs*, or closed derivations of $\perp$. We extend his result by using Gentzen-style sequent calculus and establish the full cut-elimination theorem. Furthermore, we study connections between infinitary additives and exponentials.

3.2 The formal system of AS^{∞}

3.2.1 The language of AS^{∞}

The language of AS^{∞} is very similar to that of SMALL. However, we use no exponetials and have no restriction on the formation of set terms. In other words, we no longer need to distinguish a special type of formulas to which the unrestricted comprehension is applicable.

Definition 3.1 *We define the terms and formulas of AS^{∞} inductively as follows:*

- *Variables x,y,z,... are terms*
- *If $A(x)$ is a formula, then $\{x : A(x)\}$ is a term*

- *If t and u are terms, then $t \in u$ and $t \notin u$ are formulas*
- $\mathbf{1}$, $\perp$, $\top$ *and* $\mathbf{0}$ *are formulas*
- *If A and B are formulas, then $A \otimes B$ and $A \mathbin{⅋} B$ are formulas*
- *If A_i's are formulas for all $i \in I$ with an index set I, then $\bigcap\{A_i \mid i \in I\}$ and $\bigoplus\{A_i \mid i \in I\}$ are formulas*
- *If A is a formula and x a variable, then $\bigwedge x.A$ and $\bigvee x.A$ are formulas*

The formulas of the form $t \in u$ or $t \notin u$ are called atomic.

The definition of linear negation is extended so that we have two additional clauses:

- $(\bigcap\{A_i \mid i \in I\})^{\perp} =_{def} \bigoplus\{A^{\perp}{}_i \mid i \in I\}$
- $(\bigoplus\{A_i \mid i \in I\})^{\perp} =_{def} \bigcap\{A^{\perp}{}_i \mid i \in I\}$

3.2.2 The axioms and rules of inference of AS$^{\infty}$

The axioms and rules of inference of AS$^{\infty}$ are similar to those of SMALL. However, the rules for additive conjunction and disjunction are generalized to infinitary cases. Furthermore, we have the weakening rule but no rules for exponentials in AS$^{\infty}$. Finally, we no longer need to restrict the uses of the unrestricetd comprehension rules.

Axioms

$$(I) \quad \vdash A, A^{\perp}$$

$$(\mathbf{1}) \quad \vdash \mathbf{1}$$

$$(\top) \quad \vdash \top, \Gamma$$

where A and $A^{\perp}$ are atomic in (I).

Rules of Inference

$$(\otimes) \quad \frac{\vdash A, \Gamma \quad \vdash B, \Delta}{\vdash A \otimes B, \Gamma, \Delta} \qquad\qquad (⅋) \quad \frac{\vdash A, B, \Gamma}{\vdash A \mathbin{⅋} B, \Gamma}$$

$$(\bigcap) \quad \frac{\vdash A_i, \Gamma \quad (all\ i \in I)}{\vdash \bigcap\{A_i \mid i \in I\}, \Gamma} \qquad\qquad (\bigoplus) \quad \frac{\vdash A_i, \Gamma \quad (some\ i \in I)}{\vdash \bigoplus\{A_i \mid i \in I\}, \Gamma}$$

$$(\bigwedge)\ \frac{\vdash A, \Gamma}{\vdash \bigwedge x.A, \Gamma} \qquad (\bigvee)\ \frac{\vdash A[t/x], \Gamma}{\vdash \bigvee x.A, \Gamma}$$

$$(\in)\ \frac{\vdash A(t), \Gamma}{\vdash t \in \{x : A(x)\}, \Gamma} \qquad (\notin)\ \frac{\vdash A(t)^{\perp}, \Gamma}{\vdash (t \in \{x : A(x)\})^{\perp}, \Gamma}$$

$$(W)\ \frac{\vdash \Gamma}{\vdash \Delta, \Gamma}$$

$$(cut)\ \frac{\vdash A, \Gamma \quad \vdash A^{\perp}, \Delta}{\vdash \Gamma, \Delta}$$

where the free variable x does not appear in Γ in $(\bigwedge)$.

3.3 The weak implication

The infinitary additives are introduced by White to recover some uses of contraction. This is accomplished by defining the new implication, called the *weak implication*, by means of the infinitary additive disjunction. We review the definition of the weak implication and its properties.

First, the definition of the weak implication $A \Rightarrow B$ is given by White as follows:

- $A \Rightarrow B =_{def} \bigoplus\{A^n \multimap B : n \in \omega\}$.

where $A^0 \multimap B$ is $\mathbf{1} \multimap B$ and $A^{n+1} \multimap B$ is $A \multimap (A^n \multimap B)$. More intuitively, $A \Rightarrow B$ can be read as $(A^0 \multimap B) \oplus (A^1 \multimap B) \oplus \ldots \oplus (A^n \multimap B) \oplus \ldots$.

To state the properties of the weak implication, we use the two-sided presentation of our sequent calculus AS^{∞} to make the meanings of those properties more perspicuous. The conversion between the one-sided and the two-sided versions is so straightforward that we simply assume it.

The weak implication has three notable properties. First of all, the linear implication entails the weak implication, *i. e.*, the sequents

$$A \multimap B \vdash A \Rightarrow B$$

are provable in AS^{∞}. Secondly, the antecedent of the weak implication can be contracted in some cases, or the sequents

$$A \Rightarrow (B \multimap C), A \Rightarrow B \vdash A \Rightarrow C$$

are provable in AS^∞. Finally, we have the derived rule

$$\frac{A \multimap B \vdash C_1 \multimap (\ldots(C_n \multimap B)\ldots)}{A \Rightarrow B \vdash C_1 \Rightarrow (\ldots(C_n \Rightarrow B)\ldots)}$$

in AS^∞.

The first property is immediate as shown below:

$$\frac{A \multimap B \vdash A \multimap B}{A \multimap B \vdash \bigoplus\{A^n \multimap B : n \in \omega\}}$$

For the second, we need to piece together the weak implications of the form $A^p \multimap (B)$ for all natural numbers p in the same context $A^m \multimap (B \multimap C), \ldots \vdash \bigoplus\{A^n \multimap C : n \in \omega\}$ with a fixed m, and then piece together $A^m \multimap (B \multimap C)$ for all natural numbers m in the context $\ldots, \bigoplus\{A^n \multimap B : n \in \omega\} \vdash \bigoplus\{A^n \multimap C : n \in \omega\}$:

$$\cfrac{\cfrac{\cfrac{A^m \multimap (B \multimap C), A^p \multimap B \vdash A^{m+p} \multimap C}{\ldots A^m \multimap (B \multimap C), A^p \multimap B \vdash \bigoplus\{A^n \multimap C : n \in \omega\} \ldots}}{\ldots A^m \multimap (B \multimap C), \bigoplus\{A^n \multimap B : n \in \omega\} \vdash \bigoplus\{A^n \multimap C : n \in \omega\} \ldots}}{\bigoplus\{A^n \multimap (B \multimap C) : n \in \omega\}, \bigoplus\{A^n \multimap B : n \in \omega\} \vdash \bigoplus\{A^n \multimap C : n \in \omega\}}$$

The derivation of the last is more complicated. Given $A \multimap B \vdash C_1 \multimap (\ldots(C_n \multimap B)\ldots)$, we first derive $A^m \multimap B, C_1, \ldots \vdash C_n^m \multimap B$, where we have m occurrences of C_1 through C_{n-1} on the left. For this, we supply m occurrences of A to the left side to obtain

$$A^m \multimap B, A, \ldots, A \vdash B$$

and drop one occurrence of A to the right:

$$A^m \multimap B, A, \ldots \vdash A \multimap B$$

By cut, then we have:

$$A^m \multimap B, A, \ldots \vdash C_1 \multimap (\ldots(C_n \multimap B)\ldots)$$

Discharging the antecedents C's by supplying C's to the left, we have:

$$A^m \multimap B, A, \ldots, C_1, \ldots, C_n \vdash B$$

Then we drop one more A to the right and repeat the same operation m times. In the process, we accumulate C's on the left m times. Dropping all the occurrences of C_n to the right, we finally have:

$$A^m \multimap B, C_1, \ldots \vdash C_n^m \multimap B$$

For the case $m = 2$ and $n = 1$, the formal derivation is as follows:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A^2 \multimap B, A \vdash A \multimap B \quad A \multimap B \vdash C \multimap B}{A^2 \multimap B, A \vdash C \multimap B} \quad C, C \multimap B \vdash B}{A^2 \multimap B, A, C \vdash B}}{A^2 \multimap B, C \vdash A \multimap B \quad A \multimap B \vdash C \multimap B}}{A^2 \multimap B, C \vdash C \multimap B}}{A^2 \multimap B \vdash C^2 \multimap B}$$

Then we simply introduce the infinitary additive disjunction on the right, drop the occurrences of C_{n-1} to the right and make it infinitary additive again. By repeating this operation n times, we have:

$$A^m \multimap B \vdash C_1 \Rightarrow (\ldots(C_n \Rightarrow B)\ldots)$$

This is the case for any natural number m. Hence we can piece them together to obtain:

$$A \Rightarrow B \vdash C_1 \Rightarrow (\ldots(C_n \Rightarrow B)\ldots)$$

3.4 The cut-elimination theorem for AS$^\infty$

The cut-elimination theorem for AS$^\infty$ is proved in a similar manner as for SMALL. However, there are a few changes. First, we do not need to consider (? *cut*) anymore since there is no exponential in AS$^\infty$. Secondly, however, we need to extend the measure $\sigma(\pi)$ of the size of a proof π from natural numbers to ordinals. This forces us to use the natural sum instead of arithmetic addition.

3.4.1 The cut-elimination procedure for $\mathbf{AS}^\infty$

We use the same symmetric and permutative reductions as before for all the axioms and the rules of inference ($\otimes$), ($\parr$), ($\bigwedge$), ($\bigvee$), ($\in$) and ($\notin$). In addition, we have three new symmetric reductions and three new permutative reductions.

symmetric reductions

($\bigcap / \bigoplus$)

$$\dfrac{\dfrac{\vdash A_i, \Gamma \ (all\ i \in I)}{\vdash \bigcap\{A_i \mid i \in I\}, \Gamma} \quad \dfrac{\vdash {A_j}^\perp, \Delta \ (some\ j \in I)}{\vdash \bigoplus\{{A_i}^\perp : i \in I\}, \Delta}}{\vdash \Gamma, \Delta} \quad \rightsquigarrow \quad \dfrac{\vdash A_j, \Gamma \quad \vdash A_j^\perp, \Delta}{\vdash \Gamma, \Delta}$$

($*/W1$)

$$\dfrac{\vdash A \quad \dfrac{\vdash \Delta}{\vdash A^\perp, \Delta}}{\vdash \Delta} \quad \rightsquigarrow \quad \vdash \Delta$$

($*/W2$)

$$\dfrac{\vdash A, \Gamma \quad \dfrac{\vdash \Delta}{\vdash A^\perp, \Theta, \Delta}}{\vdash \Gamma, \Theta, \Delta} \quad \rightsquigarrow \quad \dfrac{\vdash \Delta}{\vdash \Gamma, \Theta, \Delta}$$

Permutative reductions

($cut/\bigcap$)

$$\dfrac{\vdash C, \Gamma \quad \dfrac{\vdash C^\perp, A_i, \Delta \ (all\ i \in I)}{\vdash C^\perp, \bigcap\{A_i \mid i \in I\}, \Delta}}{\vdash \bigcap\{A_i \mid i \in I\}, \Gamma, \Delta} \quad \rightsquigarrow \quad \dfrac{\dfrac{\vdash C, \Gamma \quad \vdash C^\perp, A_i, \Delta}{\vdash A_i, \Gamma, \Delta}\ (all\ i \in I)}{\vdash \bigcap\{A_i \mid i \in I\}, \Gamma, \Delta}$$

($cut/\bigoplus$)

$$\dfrac{\vdash C, \Gamma \quad \dfrac{\vdash A_i, C^\perp, \Delta \ (some\ i \in I)}{\vdash \bigoplus\{A_i \mid i \in I\}, C^\perp, \Delta}}{\vdash \bigoplus\{A_i \mid i \in I\}, \Gamma, \Delta} \quad \rightsquigarrow \quad \dfrac{\dfrac{\vdash C, \Gamma \quad \vdash A_i, C^\perp, \Delta}{\vdash A_i, \Gamma, \Delta}\ (some\ i \in I)}{\vdash \bigoplus\{A_i \mid i \in I\}, \Gamma, \Delta}$$

(cut/W)

$$\dfrac{\vdash C, \Gamma \quad \dfrac{\vdash C^{\perp}, \Delta}{\vdash \Theta, C^{\perp}, \Delta}}{\vdash \Theta, \Gamma, \Delta} \quad \rightsquigarrow \quad \dfrac{\dfrac{\vdash C, \Gamma \quad \vdash C^{\perp}, \Delta}{\vdash \Gamma, \Delta}}{\vdash \Theta, \Gamma, \Delta}$$

3.4.2 The cut-elimination theorem for AS$^{\infty}$

We start with the extended definition of the size $\sigma(\pi)$ of a proof π.

Definition 3.2 *We define the the size $\sigma(\pi)$ of a proof π inductively as follows:*

- *If π is one of the axioms, then $\sigma(\pi) = 1$*
- *If π is obtained from τ by one of the rules of inference ($\parr$), ($\bigoplus$), ($\bigwedge$), ($\bigvee$), ($\in$), ($\notin$) and (W), then $\sigma(\pi) = \sigma(\tau)\#1$*
- *If π is obtained from π_1 and π_2 by one of the rules of inference ($\otimes$) and (cut), then $\sigma(\pi) = \sigma(\pi_1)\#\sigma(\pi_2)\#1$*
- *If π is obtained from π_i's ($i \in I$) by the rule of inference ($\bigwedge$), then $\sigma(\pi) = sup\{\sigma(\pi_i)\#1 : i \in I\}$*

where $\#$ is the natural sum in the ordinal arithmetic.

We note that the natural sum has the following property:

Proposition 3.3 *For any ordinals α_i ($i \in I$) and β,*

$$sup\{\alpha_i\#\beta : i \in I\} \leq sup\{\alpha_i : i \in I\}\#\beta$$

Proof

Clearly, $\alpha_i \leq sup\{\alpha_i : i \in I\}$ for all $i \in I$. Hence, $\alpha_i\#\beta \leq sup\{\alpha_i : i \in I\}\#\beta$ for all $i \in I$. Since $sup\{\alpha_i\#\beta : i \in I\}$ is the least upper bound of $\{\alpha_i\#\beta : i \in I\}$, we have $sup\{\alpha_i\#\beta : i \in I\} \leq sup\{\alpha_i : i \in I\}\#\beta$. ∎

As before, we prove that the symmetric reductions strictly decrease the size of a proof and the permutative reductions preserve the size.

Lemma 3.4 *Suppose that a proof π ends with cut. Let τ be the proof obtained from π by applying one of the symmetric reductions to the cut. Then $\sigma(\tau)$ is strictly less than $\sigma(\pi)$.*

Proof

The proof is by computation as before. We only need to check three additional cases.

The symmetric reduction $(\bigcap / \bigoplus)$

$$\frac{\dfrac{\vdash \alpha_i \;\; (i \in I)}{\vdash sup\{\alpha_i\#1 : i \in I\}} \quad \dfrac{\vdash \beta}{\vdash \beta\#1}}{\vdash sup\{\alpha_i\#1 : i \in I\}\#\beta\#1} \quad \leadsto \quad \frac{\vdash \alpha_j \quad \vdash \beta}{\vdash \alpha_j\#\beta\#1}$$

where

$$\begin{aligned} \sigma(\pi) &= sup\{\alpha_i\#1 : i \in I\}\#\beta\#1 \\ &\geq sup\{\alpha_i\#\beta\#2 : i \in I\} \\ &\geq \alpha_j\#\beta\#2 \\ &> \alpha_j\#\beta\#1 \\ &= \sigma(\tau) \end{aligned}$$

The symmetric reduction $(*/W1)$

$$\frac{\vdash \alpha \quad \dfrac{\vdash \beta}{\vdash \beta\#1}}{\vdash \alpha\#\beta\#1} \quad \leadsto \quad \vdash \beta$$

The symmetric reduction $(*/W2)$

$$\frac{\vdash \alpha \quad \dfrac{\vdash \beta}{\vdash \beta\#1}}{\vdash \alpha\#\beta\#1} \quad \leadsto \quad \frac{\vdash \beta}{\vdash \beta\#1}$$

where $\beta\#1 < \alpha\#\beta\#1$ since α is non-zero. ∎

Lemma 3.5 *Suppose that a proof π ends with a cut. Let τ be the proof obtained from π by applying one of permutative reductions to the cut. Then $\sigma(\tau) \leq \sigma(\pi)$.*

Proof

The proof is by computation. We only need to check three additional cases.

The permutative reduction $(cut/\bigcap)$

$$\frac{\vdash \alpha \quad \dfrac{\vdash \beta_i \;\; (i \in I)}{\vdash sup\{\beta_i\#1 : i \in I\}}}{\vdash \alpha\#sup\{\beta_i\#1 : i \in I\}} \quad \leadsto \quad \frac{\dfrac{\vdash \alpha \quad \vdash \beta_i}{\vdash \alpha\#\beta_i} \;\; (i \in I)}{\vdash sup\{\alpha\#\beta_i\#1 : i \in I\}}$$

where

$$\begin{aligned}\sigma(\pi) &= \alpha\#sup\{\beta_i\#1 : i \in I\}\\ &\geq sup\{\alpha\#\beta_i\#1 : i \in I\}\\ &= \sigma(\tau)\end{aligned}$$

The permutative reduction $(cut/\bigoplus)$

$$\dfrac{\vdash \alpha \quad \dfrac{\vdash \beta}{\vdash \beta\#1}}{\vdash \alpha\#\beta\#1} \quad \leadsto \quad \dfrac{\dfrac{\vdash \alpha \quad \vdash \beta}{\vdash \alpha\#\beta}}{\vdash \alpha\#\beta\#1}$$

The permutative reduction (cut/W)

$$\dfrac{\vdash \alpha \quad \dfrac{\vdash \beta}{\vdash \beta\#1}}{\vdash \alpha\#\beta\#1} \quad \leadsto \quad \dfrac{\dfrac{\vdash \alpha \quad \vdash \beta}{\vdash \alpha\#\beta}}{\vdash \alpha\#\beta\#1}$$

∎

From those two lemmas, we infer the cut-elimination theorem. First, we need to make sure that the size of a proof is monotonic under substitution.

Proposition 3.6 *Let π_i and τ_i be proofs such that π_i and τ_i have the same conclusion and $l(\tau_i) \leq l(\pi_i)$ for all $i \in I$. Suppose τ is obtained from π by replacing the subproofs π_i in π by τ_i for $i \in I$. Then the size $\sigma(\tau)$ of the proof τ is less than or equal to the size $\sigma(\pi)$ of π.*

Proof

The proof is by induction on the construction of proofs.

Case 1 π is one of the axioms. Then π has no subproof except itself. If π is identical to π_i, then τ is τ_i and $\sigma(\tau) = \sigma(\tau_i) \leq \sigma(\pi_i) \leq \sigma(\pi)$. Otherwise τ is π.

Case 2 π is obtained from π' by one of the rules of inference $(\invamp)$, $(\bigoplus)$, $(\bigwedge)$, $(\bigvee)$, $(\in)$, $(\notin)$ and (W). If π is identical to π_i, then τ is τ_i and $\sigma(\tau) = \sigma(\tau_i) = \sigma(\pi_i) = \sigma(\pi)$. Otherwise we have the immediate subproof τ' of τ by the inductive hypothesis such that $\sigma(\tau') \leq \sigma(\pi)$ and $\sigma(\tau) = \sigma(\tau')\#1 \leq \sigma(\pi')\#1 = \sigma(\pi)$.

Case 3 π is obtained from π'_1 and π'_2 by one of the rules of inference $(\otimes)$ and (cut). If π is identical to π_i, then the conclusion is immediate. Otherwise we have the immediate subproofs τ'_1 and τ'_2 of τ by the inductive hypothesis such that $\sigma(\tau) = \sigma(\tau'_1)\#\sigma(\tau'_2) = \sigma(\pi'_1)\#\sigma(\pi'_2) = \sigma(\pi)$.

Case 4 π is obtained from π'_j 's $(i \in I)$ by the rule of inference $(\bigwedge)$. If π is identical to π_1, then the conclusion is immediate. Otherwise we have the immediate subproofs $\tau' j$'s of τ by the inductive hypothesis such that

$$\sigma(\tau) = sup\{\sigma(\tau'_j)\#1 : j \in J\}$$

and $\tau'_j \leq \pi'_j$ for $j \in J$. Then

$$\begin{array}{rcl} \tau'_j\#1 & \leq & \pi'_j\#1 \\ & \leq & sup\{\pi'_j\#1 : j \in J\} \\ & = & \sigma(\pi) \end{array}$$

Since $sup\{\sigma(\tau'_j)\#1 : j \in J\}$ is the least upper bound of $\{\sigma(\tau'_j)\#1 : j \in J\}$, we have $\sigma(\tau) \leq \sigma(\pi)$.

∎

Theorem 3.7 *For any proof π, there exists a cut-free proof τ such that π reduces to τ and $\sigma(\tau) \leq \sigma(\pi)$.*

Proof

The proof is by the induction on the length. Suppose that the last inference rule of π is not a cut. Then we can apply the inductive hypothesis to the immediate subproofs of π and we have $\sigma(\tau) \leq \sigma(\pi)$ by the previous proposition. Hence suppose otherwise. We consider reductions applicable to the cut. There are three cases.

Case 1 The cut is reducible by one of the symmetric reductions. Then we perform the symmetric reduction and apply the inductive hypothesis.

Case 2 The cut is reducible by one of the permutative reductions except (cut/cut). Then we perform the permutative reduction and apply the inductive hypothesis to the immediate subproofs of the result. The size does not increase by the previous proposition.

Case 3 Otherwise. Then we have two consecutive applications of cut at the end of π. We apply the inductive hypothesis to the immediate subproof of π. Since the size of the whole proof does not increase in the process, we can eliminate the remaining cut as in the other two cases.

∎

As a corollary to the cut-elimination theorem, we have the consistency of AS$^\infty$.

Corollary 3.8 *AS^∞ is consistent.*

Proof
The empty sequent is not provable without cut. ∎

3.5 Infinitary Additives and Exponentials

The cut-elimination theorem makes it easy to establish some connections between infinitary additives and exponentials. For reminder, let's state the rules of inference for exponentials again:

$$(D?)\ \frac{\vdash A, \Gamma}{\vdash\ ?A, \Gamma} \qquad (W?)\ \frac{\vdash \Gamma}{\vdash\ ?A, \Gamma}$$

$$(C?)\ \frac{\vdash\ ?A,\ ?A, \Gamma}{\vdash\ ?A, \Gamma} \qquad (!)\ \frac{\vdash A,\ ?\Gamma}{\vdash\ !A,\ ?\Gamma}$$

We show that the behaviours of exponentials can be imitated in AS$^\infty$ to some extent by the use of infinitary additives.

Definition 3.9 *We define $\otimes A^n$ and $⅋ A^n$ for $n \in \omega$ inductively as follows:*

$$\otimes A^n =_{def} \begin{cases} \mathbf{1} & \textit{if } n = 0 \\ A \otimes (\otimes A^{n-1}) & \textit{otherwise} \end{cases}$$

and

$$⅋ A^n =_{def} \begin{cases} \bot & \textit{if } n = 0 \\ A ⅋ (⅋ A^{n-1}) & \textit{otherwise} \end{cases}$$

The idea is to use $\bigcap\{\otimes A^n : n \in \omega\}$ for $!A$ and $\bigoplus\{\invamp A^n : n \in \omega\}$ for $?A$. Under this translation, the rule $(D?)$ is clearly a valid rule and $(W?)$ is also valid even without the weakening (W) in AS^∞.

However, the contraction rule $(C?)$ and the rule $(!)$ are valid only under limited circumstances. In fact, it is the use of $(!)$ that makes the translation far less than perfect. We therefore restrict ourselves to the formulas which does not contain the symbol $\bigcap$.

Definition 3.10 *A formula A is $\bigcap$-free if A contains no occurrence of the symbol $\bigcap$ within it. A list Γ of formulas is $\bigcap$-free if all the formulas in Γ are $\bigcap$-free.*

We first show the disjunction property of AS^∞.

Proposition 3.11 *Suppose Γ is $\bigcap$-free. Then,*

$$\vdash \bigoplus\{\invamp A^n : n \in \omega\}, \Gamma$$

is provable if and only if

$$\vdash \invamp A^m, \Gamma$$

is provable for some $m \in \omega$.

Proof

The direction from the right to the left is immediate by one application of the rule of inference $(\bigoplus)$. The other direction is proved by induction on the construction of cut-free proofs π.

Case 1 π is one of the axioms $(\top)$. Then $\top$ is in Γ, and the sequent $\vdash \invamp A^m, \Gamma$ is also one of the axioms $(\top)$.

Case 2 $\bigoplus\{\invamp A^n : n \in \omega\}$ is not the main formula of the last inference rule in π. Then we apply the inductive hypothesis to the immediate subproof of π, and use the same rule of inference to recover the context Γ.

Case 3 $\bigoplus\{\invamp A^n : n \in \omega\}$ is the main formula of the last inference rule in π. Then the last inference is either (W) or $(\bigoplus)$. In the former case, we simply replace $\bigoplus\{\invamp A^n : n \in \omega\}$ with $\invamp A^n$. In the latter, the immediate subproof is exactly what we need.

∎

It is worth noting why the above proof does not work in the presence of $\bigcap$. Suppose that the context Γ were not $\bigcap$-free. Then we would have to deal with the proof

$$\dfrac{\begin{array}{c}\vdots\pi_i\\ \vdash B_i, \bigoplus\{\invamp A^n : n \in \omega\}\end{array}}{\vdash \bigwedge\{B_i : i \in I\}, \bigoplus\{\invamp A^n : n \in \omega\}}$$

in the inductive step. By the inductive hypothesis, we could obtain the proof

$$\begin{array}{c}\vdots{\pi_i}'\\ \vdash B_i, \invamp A^{m_i}\end{array}$$

for each $i \in I$. However, we could not apply the rule $(\bigcap)$ anymore to recover the context, since n_i's may be different from each other and there may not exist a finite bound for them. Notice that this problem does not occur when I is finite. In that case, we can always find a finite bound and increase each n_i by (W) and $(\invamp)$ so that all the premisses have the same context.

From this, it follows that the contraction rule $(C?)$ can be imitated to some extent by the infinitary additive disjunction.

Theorem 3.12 *Suppose that A and Γ are $\bigcap$-free. Then,*

$$\vdash \bigoplus\{\invamp A^n : n \in \omega\}, \bigoplus\{\invamp A^n : n \in \omega\}, \Gamma$$

is provable if and only if

$$\vdash \bigoplus\{\invamp A^n : n \in \omega\}, \Gamma$$

is provable.

Proof

The direction from the right to the left is immediate since we have weakening. For the other direction, we use the previous proposition twice so that we have:

$$\vdash \invamp A^n, \invamp A^m, \Gamma$$

By the rule of inference ($\parr$), we then have

$$\vdash \parr A^{n+m}, \Gamma$$

and by the rule ($\bigoplus$), we obtain

$$\vdash \bigoplus\{\parr A^n : n \in \omega\}, \Gamma$$

∎

Furthermore, the rule of inference (!) can be imitated similarly.

Theorem 3.13 *Suppose that B, $A_o \ldots A_i$ are all $\bigcap$-free. Then,*

$$\vdash B, \bigoplus\{\parr {A_0}^n : n \in \omega\}, \ldots \bigoplus\{\parr {A_i}^n : n \in \omega\}$$

is provable if and only if

$$\vdash \bigcap\{\otimes B^n : n \in \omega\}, \bigoplus\{\parr {A_0}^n : n \in \omega\}, \ldots \bigoplus\{\parr {A_i}^n : n \in \omega\}.$$

is provable.

Proof

For the direction from the right to the left, note that $\vdash B, \bigoplus\{\parr {B^\perp}^n : n \in \omega\}$ is provable by one application of the rule ($\bigoplus$) from the axiom $\vdash B, B^\perp$. Then the conclusion is immediate by cut.

For the other direction, we use the disjunction property again. From a proof of

$$\vdash \bigcap\{\otimes B^n : n \in \omega\}, \bigoplus\{\parr {A_0}^n : n \in \omega\}, \ldots \bigoplus\{\parr {A_i}^n : n \in \omega\}$$

we first obtain the proof of

$$\vdash B, \parr A_0^{p_0}, \ldots A_i^{p_i}$$

We then show by induction on $n \geq 1$ that $\vdash \otimes B^n, \parr A_0^{np_0}, \ldots A_i^{np_i}$ is provable.

Case 1 $n = 1$. This is already given.

Case 2 $n = m + 1$. By the inductive hypothesis, we have a proof of the sequent

$$\vdash \otimes B^m, \parr A_0^{mp_0}, \ldots A_i^{mp_i}$$

and we are given the proof of

$$\vdash B, \parr A_0^{p_0}, \ldots A_i^{p_i}$$

An application of the rule $(\otimes)$ then yields

$$\vdash \otimes B^{m+1}, \parr A_0^{mp_0}, \parr A_0^{p_0}, \ldots A_i^{mp_i}, A_i^{p_i}$$

and several applications of the rule $(\parr)$ give us:

$$\vdash \otimes B^{m+1}, \parr A_0^{(m+1)p_0}, \ldots A_i^{(m+1)p_i}$$

Hence we have proofs of

$$\vdash \otimes B^n, \bigoplus\{\parr A_0{}^n : n \in \omega\}, \ldots \bigoplus\{\parr A_i{}^n : n \in \omega\}$$

for all $n \geq 1$ by the rule $(\bigoplus)$. Also, a proof of

$$\vdash \mathbf{1}, \bigoplus\{\parr A_0{}^n : n \in \omega\}, \ldots \bigoplus\{\parr A_i{}^n : n \in \omega\}$$

is immediate from the axiom **1** and the weakening rule (W). Piecing them together by the rule of inference $(\bigcap)$, Hence we finally have the proof of the sequent

$$\vdash \bigcap\{\otimes B^n : n \in \omega\}, \bigoplus\{\parr A_0{}^n : n \in \omega\}, \ldots \bigoplus\{\parr A_i{}^n : n \in \omega\}$$

∎

However, a good correspondence stops immediately. For example, consider the proof:

$$\dfrac{\begin{array}{c}\vdots\tau\\ \vdash C, \bigoplus\{\parr A^n : n \in \omega\}\end{array} \quad \dfrac{\begin{array}{c}\vdots\pi_i\\ \vdash B_i, \bigoplus\{\parr A^n : n \in \omega\}\end{array}}{\vdash \bigwedge\{B_i : i \in I\}, \bigoplus\{\parr A^n : n \in \omega\}}}{\vdash C \otimes \bigwedge\{B_i : i \in I\}, \bigoplus\{\parr A^n : n \in \omega\}, \bigoplus\{\parr A^n : n \in \omega\}}$$

Contraction is no longer possible for this proof since we cannot apply the previous proposition anymore. On the other hand, It is certainly possible to extend the correspondence to the cases where all the $\bigoplus\{\parr A^n : n \in \omega\}$'s are introduced before the application of the rule $(\bigcap)$. These cases are left to the reader as exercises.

Chapter 4

Extension of Zermelo-Fraenkel set theory

4.1 Introduction

In this chapter, we present our third system of linear set theory LZF which is a conservative extension of the classical Zermelo-Fraenkel set theory, or ZF in short, without the axiom of regularity.

LZF has two special types of terms, *i.e.*, S-terms and Z-terms. We first reformulate ZF in the formalism with set terms $\{x : A\}$ in classical logic. We then translate into linear logic the terms which correspond to the axioms of ZF. Those translated terms are called Z-terms. The other terms of LZF are built on top of the Z-terms. Among them, the terms constructed from Z-terms without using exponentials are called S-terms. This is similar to the definition of terms in SMALL. Note that Z-terms are also S-terms.

LZF is based on the standard full linear logic, *i.e.*, linear logic with exponentials and finite additives. In LZF, the quantifications over S-terms and over Z-terms are both available. However, we cannot quantify over all terms. Similarly, the unrestricted comprehensions are with respect to S-terms and Z-terms, although the set terms created by the comprehension do not have to be either S-terms or Z-terms.

LZF is a conservative extension of ZF without the axiom of regularity. This is proved by establishing the partial cut-elimination theorem, which ensures that all the remaining cut-formulas contain only Z-terms. Hence, if the translation of a classical formula A is provable in LZF, we only need for its proof the uses of comprehension which correspond to the axioms of ZF without the regularity. Since any proof in linear logic can be read as a proof in classical logic, this shows that A is provable in ZF, *i.e.*, LZF is a conservative extension of ZF without the regularity. We then have the consistency of LZF as a corollary.

The omission of the axiom of regularity is only to simplify the argument, and our system can be easily extended to contain it by taking it as one of the axioms.

4.2 Preliminary

We review some of the basics about ZF and the translation of classical logic into linear logic.

4.2.1 Axioms of ZF

The axiomatic system of ZF consists of:

(Ext) $\forall u \forall v[\forall w(w \in u \leftrightarrow w \in v) \to u = v]$

(Empty) $\exists u \forall v(v \notin u)$

(Pair) $\forall u_1 \forall u_2 \exists v \forall w(w \in v \leftrightarrow w = u_1 \vee w = u_2)$

(Union) $\forall u \exists v \forall w[w \in v \leftrightarrow \exists w_1(w \in w_1 \wedge w_1 \in u)]$

(Power) $\forall u \exists v \forall w[w \in v \leftrightarrow \forall w_1(w_1 \in w \to w_1 \in u)]$

(Separation) $\forall u_1 \ldots \forall u_k \forall v \exists w \forall w_1(w_1 \in w \leftrightarrow w_1 \in v \wedge A(w_1, v, u_1, \ldots, u_k))$

(Infinity) $\exists u[\emptyset \in u \wedge \forall v(v \in u \to v \cup \{v\} \in u)]$

(Regularity) $\forall u[u \neq \emptyset \to \exists v(v \in u \wedge v \cap u = \emptyset)]$

(Replacement) $\forall u[\forall w(w \in u \to \forall w_1 \forall w_2(F(w, w_1) \wedge F(w, w_2) \to w_1 = w_2)) \to \exists v \forall w(w \in v \leftrightarrow \exists w_1(w_1 \in u \wedge F(w_1, w)))]$

Our first task is to reformulate ZF in the language of linear logic with set terms $\{x : A\}$ [24, 14]. For the sake of simplicity, we will omit the regularity axiom. Hence our target theory is ZF without the regularity, or ZF$^-$.

In ZF, the use of an set term is acceptable only when we can show the existence and uniqueness of the set denoted by the term. In the cases of (Empty), (Pair), (Union), (Power) and (Separation), we simply introduce the set terms for the sets which are said to exist by the axioms.

It is not immediately clear how we should introduce the terms for the sets given by (Infinity) and (Replacement), since they do not have the form:

$$\exists u \forall w (w \in u \leftrightarrow \varphi(w))$$

However we have the equivalent formulations of those axioms as follows:

(Infinity*) $\exists u \forall w [w \in u \leftrightarrow \forall v (Ind(v) \rightarrow w \in v)]$

(Replacement*) $\forall u \exists v \forall w [w \in v \leftrightarrow \exists w_1 (w_1 \in u \wedge Fun(F, w_1) \wedge F(w_1, w))]$

where

- $Ind(v) =_{def} \emptyset \in v \wedge \forall w_1 (w_1 \in v \rightarrow w_1 \cup \{w_1\} \in v)$
- $Fun(F, w_1) =_{def} \forall u_1 \forall u_2 (F(w_1, u_1) \wedge F(w_1, u_2) \rightarrow u_1 = u_2)$

The equivalence between (Infinity) and (Infinity*) is proved as follows:

1. (Infinity)$\Rightarrow$(Infinity*)
   This is immediate by the usual definition of ω.

2. (Infinity*)$\Rightarrow$(Infinity)
   Let ω be the witness of (Infinity*).
   - Suppose $Ind(v)$. Then $\emptyset \in v$. Hence, $\forall v (Ind(v) \rightarrow \emptyset \in v)$. Therefore $\emptyset \in \omega$.
   - Suppose $w_1 \in \omega$. Then $\forall v (Ind(v) \rightarrow w_1 \in v)$. In particular, $Ind(v) \rightarrow w_1 \in v$. Assume $Ind(v)$. Then $w_1 \in v$. Furthermore, $w_1 \in v \rightarrow w_1 \cup \{w_1\} \in v$. Hence $w_1 \cup \{w_1\} \in v$. Therefore $\forall v (Ind(v) \rightarrow w_1 \cup \{w_1\} \in v)$. Hence $w_1 \cup \{w_1\} \in \omega$.

The equivalence between (Replacement) and (Replacement*) is shown as follows:

1. (Replacement)$\Rightarrow$(Replacement*)
   Define the subset $u^* = \{w \in u : Fun(F, w)\}$. Then the set obtained by (Replacemnt) from u^* is the witness of (Replacement*).

2. (Replacement*)$\Rightarrow$(Replacement)
   Assume $\forall w (w \in u \leftrightarrow Fun(F, w))$. Then the set obtained by (Replacement*) from u witnesses (Replacement).

Hence we are justified in using the following set terms:

- $\emptyset =_{def} \{w : \perp\}$
- $\mathcal{P}(u_1, u_2) =_{def} \{w : w = u_1 \vee w = u_2\}$
- $\bigcup u =_{def} \{w : \exists v(w \in v \wedge v \in u)\}$
- $\wp u =_{def} \{w : \forall v(v \in w \rightarrow v \in u)\}$
- $\mathcal{S}(u, A) =_{def} \{w : w \in u \wedge A(w, u_1, \ldots, u_k)\}$
- $\omega =_{def} \{w : \forall v(Ind(v) \rightarrow w \in v)\}$
- $\Re(u, F) =_{def} \{w : \exists v(v \in u \wedge Fun(F, v) \wedge F(v, w))\}$

4.2.2 Translation of classical logic into linear logic

Our next task is to embed the terms and formulas of classical logic into those of linear logic. For this purpose, we use the following translation $(\ )^+$ proposed by Girard [7]:

- $A^+ \equiv\ ?\,!A$ where A is atomic
- $(A \vee B)^+ \equiv A^+ \parr B^+$
- $(\neg A)^+ \equiv\ ?\,(A^{+\perp})$
- $(\forall x A)^+ \equiv\ ?\,!\bigwedge x A^+$

Accordingly, we have:

- $(A \wedge B)^+ \equiv (\neg(\neg A \vee \neg B))^+ \equiv\ ?\,!(A^+ \,\&\, B^+)$
- $(A \rightarrow B)^+ \equiv (\neg A \vee B)^+ \equiv\ ?\,(A^{+\perp}) \parr B^+ \equiv\ !A^+ \multimap B^+$
- $(\exists x A)^+ \equiv (\neg \forall x \neg A)^+ \equiv\ ?\,!\,?\bigvee x\ !A^+ \equiv\ ?\bigvee x\ !A$

Note that we are using the same propositional letters both for classical logic and linear logic. In fact, the specific choice of translation has no particular importance for our purpose and other translations should work as well.

For the translation of schematic expressions, it is convenient to introduce placeholders φ for formulas and α for terms with $\varphi^+ \equiv \varphi$. Then we can define the translation of the constants and abstraction schemas straightforwardly:

- $\emptyset^+ =_{def} \{w : \bot\}$
- $\mathcal{P}^+(\alpha_1, \alpha_2) =_{def} \{w : (w = \alpha_1 \vee w = \alpha_2)^+\}$
- $\bigcup^+(\alpha) =_{def} \{w : [\exists v(w \in v \wedge v \in \alpha)]^+\}$
- $\wp^+(\alpha) =_{def} \{w : [\forall v(v \in w \rightarrow v \in \alpha)]^+\}$
- $\mathcal{S}^+(\alpha, \varphi) =_{def} \{w : (w \in \alpha \wedge \varphi)^+\}$
- $\omega^+ =_{def} \{w : [\forall v(Ind(v) \rightarrow w \in v)]^+\}$
- $\Re^+(\alpha, \varphi) =_{def} \{w : [\exists v(v \in \alpha \wedge Fun(\varphi, v) \wedge F(v, w))]^+\}$

4.3 The formal system of LZF

4.3.1 The language of LZF

In the language of LZF, terms are variables and set terms constructed freely from formulas by the unrestricted comprehension. There are two subclasses of terms: Z-terms and S-terms. Z-terms are the terms which correspond to the definable sets in ZF^- and S-terms are the terms obtained by comprehension over formulas which contain no exponential. Roughly speaking, the terms of LZF in general correspond to *classes* in the Bernays-Gödel set theory [11]. Among them, Z-terms are also *sets*. S-terms comprise all sets and some of the *proper classes* such that the arguments about them should not use the contraction rule.

Definition 4.1 *We define terms and formulas of LZF inductively as follows:*

- *Z-variables* u, v, w, ... *are terms*
- *S-variables* $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}$, ... *are terms*
- *If* A *is a formula, then* $\{u : A\}$ *and* $\{\mathbf{x} : A\}$ *are terms*
- *If* s *and* t *are terms, then* $s \in t$, $s \notin t$, $s = t$ *and* $s \neq t$ *are formulas*
- $\mathbf{1}$, $\bot$, $\top$ *and* $\mathbf{0}$ *are formulas*
- *If* A *is a formula, then* $\bigwedge \mathbf{x}.A$, $\bigvee \mathbf{x}.A$, $\bigwedge u.A$, $\bigvee u.A$, $!A$ *and* $?A$ *are formulas*
- *If* A *and* B *are formulas, then* $A \otimes B$, $A \parr B$, $A \,\&\, B$ *and* $A \oplus B$ *are formulas*

The formulas of the form $s \in t$, $s \notin t$, $s = t$ or $s \neq t$ are called atomic.

The definition of linear negation is extended accordingly to include the additional clauses:

- $(s = t)^\perp =_{def} s \neq t$
- $(s \neq t)^\perp =_{def} s = t$
- $(\bigwedge \mathbf{x}.A)^\perp =_{def} \bigvee \mathbf{x}.A^\perp$
- $(\bigwedge u.A)^\perp =_{def} \bigvee u.A^\perp$

Definition 4.2 *Z-terms and Z-formulas are defined as follows:*

- *Z-variables are Z-terms*
- *$\emptyset^+$ and ω^+ are Z-terms*
- *If s_1 and s_2 are Z-terms, then $\mathcal{P}^+(s_1, s_2)$ is a Z-term*
- *If s is a Z-term, then $\bigcup^+ s$ and $\wp^+ s$ are Z-terms*
- *If s is a Z-term and A is a Z-formula, then $\mathcal{S}^+(s, A)$ is a Z-term with the abstraction over a Z-variable*
- *If s is a Z-term and F is a Z-formula with precisely two parameters, then $\Re^+(s, F)$ is a Z-term*
- *Z-formulas are those formulas in which only Z-terms occur*

where all the variables occurring the schemas are understood as Z-variables.

Definition 4.3 *S-terms and S-formulas are defined as follows:*

- *S-variables are S-terms*
- *Z-terms are S-terms*
- *If A is an S-formula, then $\{\mathbf{x} : A\}$ is an S-term*
- *If s and t are S-terms, then $s \in t$ and $s \notin t$ are S-formula*

- *$\mathbf{1}$, $\bot$, $\top$ and $\mathbf{0}$ are S-formulas*
- *If A is an S-formula, then $\bigwedge \mathbf{x}.A$ and $\bigvee \mathbf{x}.A$ are S-formulas*
- *If A and B are S-formulas, then $A \otimes B$, $A \parr B$, $A \mathbin{\&} B$ and $A \oplus B$ are S-formulas*

We denote the classes of Z-terms and S-terms by $\mathcal{ZT}$ and $\mathcal{ST}$, respectively.

4.3.2 The axioms and rules of inference of LZF

In the axiomatic system of LZF, there is only one critical restriction: *The atomic formulas of the form $s \in t$ in the axioms for atomic formulas contain only S-terms.* We have two types of quantifier and abstraction introduction rules according to the two types of variables. Otherwise all the rules of inferences are standard. Note that the abstraction terms newly introduced by the rules of inference are not necessarily S-terms. Furthermore we do not impose any restriction on terms in the abstraction with S-variable. In fact terms which are not S-terms can be regarded as "syntactic sugar", which are eliminable if necessary.

Definition 4.4 *Atomic formulas are admissible if they have one of the forms*

- *$s \in t$ or $s \notin t$ where s and t are S-terms*
- *$s = t$ or $s \neq t$ where s and t are Z-terms*

Axioms

$$(I) \quad \vdash A, A^\bot$$

where A and $A^\bot$ are admissible atomic formulas.

$$(E) \quad \vdash s = s$$

where $s = s$ is admissible.

$$(\mathbf{1}) \quad \vdash \mathbf{1}$$

$$(\top) \quad \vdash \top, \Gamma$$

Rules of inference

$$(\otimes)\ \frac{\vdash A, \Gamma \quad \vdash B, \Delta}{\vdash A \otimes B, \Gamma, \Delta} \qquad (⅋)\ \frac{\vdash A, B, \Gamma}{\vdash A ⅋ B, \Gamma}$$

$$(\&)\ \frac{\vdash A, \Gamma \quad \vdash B, \Gamma}{\vdash A \& B, \Gamma} \qquad (\oplus 1)\ \frac{\vdash A, \Gamma}{\vdash A \oplus B, \Gamma} \quad (\oplus 2)\ \frac{\vdash B, \Gamma}{\vdash A \oplus B, \Gamma}$$

$$(\bigwedge Z)\ \frac{\vdash A, \Gamma}{\vdash \bigwedge u.A, \Gamma} \qquad (\bigvee Z)\ \frac{\vdash A[s/u], \Gamma}{\vdash \bigvee u.A, \Gamma}$$

where the Z-variable u is not free in the context Γ in $(\bigwedge Z)$, and the term s is a Z-term in $(\bigvee Z)$.

$$(\bigwedge S)\ \frac{\vdash A, \Gamma}{\vdash \bigwedge \mathbf{x}.A, \Gamma} \qquad (\bigvee S)\ \frac{\vdash A[s/\mathbf{x}], \Gamma}{\vdash \bigvee \mathbf{x}.A, \Gamma}$$

where the S-variable $\mathbf{x}$ is not free in the context Γ in $(\bigwedge S)$, and the term s is an S-term in $(\bigvee S)$.

$$(\in Z)\ \frac{\vdash A[s/u], \Gamma}{\vdash s \in \{u : A\}, \Gamma} \qquad (\notin Z)\ \frac{\vdash A[s/u]^{\perp}, \Gamma}{\vdash s \notin \{u : A\}, \Gamma}$$

where the term S is a Z-term in both $(\in Z)$ and $(\notin Z)$.

$$(\in S)\ \frac{\vdash A[s/\mathbf{x}], \Gamma}{\vdash s \in \{\mathbf{x} : A\}, \Gamma} \qquad (\notin S)\ \frac{\vdash A[s/\mathbf{x}]^{\perp}, \Gamma}{\vdash s \notin \{\mathbf{x} : A\}, \Gamma}$$

where the term s *does not have to be an S-term.* In other words, we have no restriction on this type of unrestricted comprehension.

$$(= E)\ \frac{\vdash v \in s, v \notin t, \Gamma \quad \vdash v \notin s, v \in t, \Delta}{\vdash s = t, \Gamma, \Delta} \qquad (\neq S)\ \frac{\vdash A, \Gamma}{\vdash s \neq t, A[s/t], \Gamma}$$

where the Z-variable v is not free in s, t, Γ and Δ, the terms s and t are Z-terms, and the formula A is a Z-formula.

$$(W\ ?)\ \frac{\vdash \Gamma}{\vdash\ ?\, A, \Gamma} \qquad (D\ ?)\ \frac{\vdash A, \Gamma}{\vdash\ ?\, A, \Gamma}$$

$$(C\ ?)\ \frac{\vdash\ ?\,A,\ ?\,A,\Gamma}{\vdash\ ?\,A,\Gamma} \qquad\qquad (\,!\,)\ \frac{\vdash A,\ ?\,\Gamma}{\vdash\ !\,A,\ ?\,\Gamma}$$

$$(\bot)\ \frac{\vdash \Gamma}{\vdash \bot, \Gamma}$$

$$(cut)\ \frac{\vdash A, \Gamma \quad \vdash A^{\bot}, \Delta}{\vdash \Gamma, \Delta}$$

4.4 The cut-elimination procedure for LZF

Our idea of the consistency proof of LZF is to reduce it to the consistency of ZF^{-}. This is accomplished by removing all the cuts which involve the terms other than Z-terms. In other words, we are not interested in eliminating the cuts whose cut-formulas are Z-formulas.

Since the formulas of the form $s = t$ or $s \neq t$ only appear as Z-formulas in LZF, we do not need to give any symmetric reductions for them. In addition, the formulas $A[s/t]$ obtained from A by the substitution rule $(\neq S)$ are always Z-formulas by definition, and therefore the cuts involving them need not be eliminated.

The distinction between two types of quantification and comprehension in LZF makes it necessary to duplicate the reductions involving them. However, they are exactly similar to those in SMALL, and we do not need to repeat them.

This leaves us only the permutative reductions with $(= E)$ and $(\neq S)$ as additional reductions to be given.

4.4.1 Permutative reductions

Permutative reductions for (cut)

$(cut/=E)$

$$\frac{\vdash C, \Gamma \qquad \dfrac{\vdash u \in s, u \notin t, C^{\bot}, \Delta \quad \vdash u \notin s, u \in t, \Theta}{\vdash s = t, C^{\bot}, \Delta, \Theta}}{\vdash s = t, \Gamma, \Delta, \Theta} \rightsquigarrow \frac{\dfrac{\vdash C, \Gamma \quad \vdash v \in s, v \notin t, C^{\bot}, \Delta}{\vdash v \in s, v \notin t, \Gamma, \Delta} \qquad \vdash v \notin s, v \in t, \Theta}{\vdash s = t, \Gamma, \Delta, \Theta}$$

$(cut/\neq S)$

$$\frac{\vdash C, \Gamma \qquad \dfrac{\vdash A, C^{\bot}, \Delta}{\vdash s \neq t, A[s/t], C^{\bot}, \Delta}}{\vdash s \neq t, A[s/t], \Gamma, \Delta} \rightsquigarrow \frac{\dfrac{\vdash C, \Gamma \quad \vdash A, C^{\bot}, \Delta}{\vdash A, \Gamma, \Delta}}{\vdash s \neq t, A[s/t], \Gamma, \Delta}$$

Permutative reductions for $(\,?\,cut)$ on !–branch

$(\,?\,cut/=E)$–!

$$\dfrac{\vdash\ ?\,C^k,\Gamma \qquad \dfrac{\vdash u\in s, u\notin t,\,!\,C^{\perp},\Delta \quad \vdash u\notin s, u\in s,\Theta}{\vdash s=t,\,!\,C^{\perp},\Delta,\Theta}}{\vdash s=t,\Gamma,\Delta,\Theta} \rightsquigarrow \dfrac{\dfrac{\vdash\ ?\,C^k,\Gamma \quad \vdash v\in s, v\notin t,\,!\,C^{\perp},\Delta}{\vdash v\in s, v\notin t,\Gamma,\Delta} \qquad \vdash v\notin s, v\in t,\Theta}{\vdash s=t,\Gamma,\Delta,\Theta}$$

$(\,?\,cut/\neq S)$–!

$$\dfrac{\vdash\ ?\,C^k,\Gamma \qquad \dfrac{\vdash A,\,!\,C^{\perp},\Delta}{\vdash s\neq t, A[s/t],\,!\,C^{\perp},\Delta}}{\vdash s\neq t, A[s/t],\Gamma,\Delta} \rightsquigarrow \dfrac{\dfrac{\vdash\ ?\,C^k,\Gamma \quad \vdash A,\,!\,C^{\perp},\Delta}{\vdash A,\Gamma,\Delta}}{\vdash s\neq t, A[s/t],\Gamma,\Delta}$$

Permutative reductions for $(\,?\,cut)$ on ?–branch

$(=E/\,?\,cut1)$–?

$$\dfrac{\dfrac{\vdash u\in s, u\notin t,\,?\,C^k,\Gamma \quad \vdash u\notin s, u\in t,\Delta}{\vdash s=t,\,?\,C^k,\Gamma,\Delta} \qquad \vdash\ !\,C^{\perp},\,?\,\Theta}{\vdash s=t,\Gamma,\Delta,\Theta} \rightsquigarrow$$

$$\dfrac{\dfrac{\vdash v\in s, v\notin t,\,?\,C^k,\Gamma \quad \vdash\ !\,C^{\perp},\,?\,\Theta}{\vdash v\in s, v\notin t,\Gamma,\,?\,\Theta} \qquad \vdash v\notin s, v\in t,\Delta}{\vdash s=t,\Gamma,\Delta,\,?\,\Theta}$$

$(=E/\,?\,cut2)$–?

$$\dfrac{\dfrac{\vdash u\in s, u\notin t,\,?\,C^k,\Gamma \quad \vdash u\notin s, u\in t,\,?\,C^l,\Delta}{\vdash s=t,\,?\,C^{k+l},\Gamma,\Delta} \qquad \vdash\ !\,C^{\perp},\,?\,\Theta}{\vdash s=t,\Gamma,\Delta,\,?\,\Theta} \rightsquigarrow$$

$$\dfrac{\dfrac{\dfrac{\vdash v\in s, v\notin t,\,?\,C^k,\Gamma \quad \vdash\ !\,C^{\perp},\,?\,\Theta}{\vdash v\in s, v\notin t,\Gamma,\,?\,\Theta} \qquad \dfrac{\vdash v\notin s, v\in t,\,?\,C^l,\Delta \quad \vdash\ !\,C^{\perp},\,?\,\Theta}{\vdash v\notin s, v\in t,\Delta,\,?\,\Theta}}{\vdash s=t,\Gamma,\Delta,\,?\,\Theta,\,?\,\Theta}}{\overline{\vdash s=t,\Gamma,\Delta,\,?\,\Theta}}$$

$(\neq S/\,?\,cut)$–?

$$\dfrac{\dfrac{\vdash A,\,?\,C^k,\Gamma}{\vdash s\neq t, A[s/t],\,?\,C^k,\Gamma} \qquad \vdash\ !\,C^{\perp},\,?\,\Delta}{\vdash s\neq t, A[s/t],\Gamma,\,?\,\Delta} \rightsquigarrow \dfrac{\dfrac{\vdash A,\,?\,C^k,\Gamma \quad \vdash\ !\,C^{\perp},\,?\,\Delta}{\vdash A,\Gamma,\,?\,\Delta}}{\vdash s\neq t, A[s/t],\Gamma,\Delta}$$

4.5 The cut-elimination for LZF

Our proof of the cut-elimination theorem proceeds in three steps:

1. First of all, we eliminate the non-atomic cuts by induction on the degrees of formulas.

2. We then eliminate the atomic cuts which do not involve axioms.

3. Finally, we eliminate the remaining atomic cuts by induction on the size of a proof.

In this cut-elimination process, we only eliminate cuts whose formulas are not Z-formulas. The first and last steps are essentially the same as in SMALL. Therefore, we do not give too many details on them. The second step is achieved by induction on the *abstraction depth* $\delta(A)$ of an formula occurrence A, which will be defined shortly.

We use the essentially the same definitions for the degree $\partial(A)$ of a formula A and the size $\sigma(\pi)$ of a proof π as before. However, we need two additional clauses for size:

- If π is obtained from π_1 and π_2 by the rule of inference $(= E)$, then $\sigma(\pi) = \sigma(\pi_1) + \sigma(\pi_2)$

- If π is obtained from τ by the rule of inference $(\neq S)$, then $\sigma(\pi) = \sigma(\tau) + 1$

Furthermore, note that the old definitions involving quantifiers and set terms should now be read to cover both types of quantifiers and set terms.

4.6 The elimination of non-atomic cuts

We first eliminate all the non-atomic cuts whose cut-formulas are not Z-formulas. This is accomplished by the standard method, *i.e.*, by induction on the degrees of formulas. As in SMALL, we extend the system by $(\,?\,cut)$ and prove the cut-elimination for that extended system. All the proofs in this first step are entirely similar to the corresponding results for SMALL. Therefore, we only give them in a sketchy manner. In the following, we redefine the degree $\partial(\pi)$ of a proof π to be the maximal degree of the cut-formulas in π which are not Z-formulas.

Proposition 4.5 *Consider the proof* π

$$\dfrac{\begin{array}{c}\vdots\pi_1\\ \vdash \Gamma, ?\,A^k\end{array} \qquad \begin{array}{c}\vdots\pi_2\\ \vdash \Delta, !\,A^\perp\end{array}}{\vdash \Gamma, \Delta}\ (\,?\,cut)$$

and suppose that the formulas $?\,A$ *and* $!\,A^{\perp}$ *are not Z-formulas, and the degrees* $\partial(\pi_1)$ *and* $\partial(\pi_2)$ *of the proofs* π_1 *and* π_2 *are strictly less than the degree* $\partial(\,?\,A)$ *of* $?\,A$*. Then there exists a proof* τ *with the same conclusion* $\vdash \Gamma, \Delta$ *such that* π *reduces* τ *and* $\partial(\tau)$ *is strictly less than* $\partial(\,?\,A)$*.*

Proof
The proof is by induction on $\sigma(\pi_1) + \sigma(\pi_2)$ and entirely similar to the one for SMALL. Note that neither of the cut-formulas $?\,A$ and $!\,A^{\perp}$ is obtained by ($\neq S$) since they are not Z-formulas. ∎

Proposition 4.6 *Consider the proof* π

$$\dfrac{\begin{array}{c}\vdots\pi_1\\ \vdash \Gamma, A\end{array} \quad \begin{array}{c}\vdots\pi_2\\ \vdash \Delta, A^{\perp}\end{array}}{\vdash \Gamma, \Delta}$$

where the formulas A *and* $A^{\perp}$ *are not Z-formulas, and they are not of the form* $?\,C$ *nor* $!\,C$*. Suppose that the degrees* $\partial(\pi_1)$ *and* $\partial(\pi_2)$ *are strictly less than the degree* $\partial(A)$ *of the formula* A *and* $2 \leq \partial(A)$*. Then there exists a proof* τ *with the same conclusion* $\vdash \Gamma, \Delta$ *such that* π *reduces to* τ *and* $\partial(\tau)$ *is strictly less than* $\partial(A)$*.*

Proof
The proof is by induction on $\sigma(\pi_1) + \sigma(\pi_2)$ and entirely similar to the one for SMALL. Note that A and $A^{\perp}$ are not of the form $s = t$ nor $s \neq t$ since they are not Z-formulas. Furthermore, they are not obtained by ($\neq S$) for the same reason. ∎

Then the next lemma and corollary follow as before.

Lemma 4.7 *For any proof* π *of the sequent* $\vdash \Gamma$ *with* $2 \leq \partial(\pi)$*, there exists a proof* τ *of the same conclusion* $\vdash \Gamma$ *such that* π *reduces to* τ *and* $\partial(\tau)$ *is strictly less than* $\partial(\pi)$*.*

Corollary 4.8 *For any proof* π *of the sequent* $\vdash \Gamma$ *with* $2 \leq \partial(\pi)$*, there exists a proof* τ *of the same conclusion* $\vdash \Gamma$ *such that* π *reduces to* τ *and* $\partial(\tau)$ *is less than or equal to* 1*.*

4.7 The elimination of atomic cuts

The second step of our cut-elimination theorem is to eliminate all the cuts with atomic formulas which do not originate in axioms. For this, we need to introduce the *abstraction* *depth* $\delta(A)$ of occurrences of formulas A, and the *abstraction indices* (i,j) for the cuts with the occurrences of the formulas of abstraction depth i and j.

In contrast to the degree, the abstraction depth of an occurrence of a formula has to do with the place and role of the formula occurrence in a proof. Hence we give the definition of abstraction depth in accordance with the axioms and rules of inferences. In the following, we indicate the assignment of abstraction depth to the occurrences of the formulas in sequents to the right of the axioms and the rules of inference. The abstraction depth increases when one of the comprehension rules is used. When two formula occurrences are combined by one of the inference rules, we take the maximum of the abstraction depths of the two formula occurrences.

First we introduce several useful notations:

Definition 4.9 *Let p's and q's be natural numbers;*

- $\rho(p_1, \dots, p_k) =_{def} max\{p_1, \dots, p_k\}$
- $\overline{p} =_{def}$ *the list of* p_1, ..., p_k *for some* k
- $\overline{\rho}(\overline{p}, \overline{q}) =_{def}$ *the list of* $\rho(p_1, q_1)$, ..., $\rho(p_k, q_k)$ *where* $\overline{p}$ *and* $\overline{q}$ *have the same length* k

Now we define the way how to assign the abstraction depth to each occurrence of a formula in a proof.

Definition 4.10 *The abstraction depth* $\delta(A)$ *of a formula occurrence* A *and the abstraction index of a cut are given inductively as in the following table.*

Axioms

$$(I) \quad \vdash A, A^{\perp} \quad \vdash 0, 0$$

$$(E) \quad \vdash s = s \quad \vdash 0$$

$$(\mathbf{1}) \quad \vdash \mathbf{1} \quad \vdash 0$$

$$(\top) \quad \vdash \top, A_1, \dots, A_k \quad \vdash 0, 0, \dots, 0$$

Rules of inference

$$(\otimes)\ \frac{\vdash A,\Gamma \quad \vdash B,\Delta}{\vdash A\otimes B,\Gamma,\Delta}\ \frac{\vdash i,\overline{p} \quad \vdash j,\overline{q}}{\vdash \rho(i,j),\overline{p},\overline{q}} \qquad (\parr)\ \frac{\vdash A,B,\Gamma}{\vdash A\parr B,\Gamma}\ \frac{\vdash i,j,\overline{p}}{\vdash \rho(i.j),\overline{p}}$$

$$(\&)\ \frac{\vdash A,\Gamma \quad \vdash B,\Gamma}{\vdash A\mathbin{\&} B,\Gamma}\ \frac{\vdash i,\overline{p} \quad \vdash j,\overline{q}}{\vdash \rho(i,j),\overline{p}(\overline{p},\overline{q})} \qquad (\oplus i)\ \frac{\vdash A_i,\Gamma}{\vdash A_1\oplus A_2,\Gamma}\ \frac{\vdash i,\overline{p}}{\vdash i,\overline{p}}$$

$$(\bigwedge Z)\ \frac{\vdash A,\Gamma}{\vdash \bigwedge u.A,\Gamma}\ \frac{\vdash i,\overline{p}}{\vdash i,\overline{p}} \qquad (\bigvee Z)\ \frac{\vdash A[s/u],\Gamma}{\vdash \bigvee u.A,\Gamma}\ \frac{\vdash i,\overline{p}}{\vdash i,\overline{p}}$$

$$(\bigwedge S)\ \frac{\vdash A,\Gamma}{\vdash \bigwedge \mathbf{x}.A,\Gamma}\ \frac{\vdash i,\overline{p}}{\vdash i,\overline{p}} \qquad (\bigvee S)\ \frac{\vdash A[s/\mathbf{x}],\Gamma}{\vdash \bigvee \mathbf{x}.A,\Gamma}\ \frac{\vdash i,\overline{p}}{\vdash i,\overline{p}}$$

$$(\in Z)\ \frac{\vdash A[s/u],\Gamma}{\vdash s\in\{u:A\},\Gamma}\ \frac{\vdash i,\overline{p}}{\vdash i+1,\overline{p}} \qquad (\notin Z)\ \frac{\vdash A[s/u]^{\perp},\Gamma}{\vdash s\notin\{u:A\},\Gamma}\ \frac{\vdash i,\overline{p}}{\vdash i+1,\overline{p}}$$

$$(\in S)\ \frac{\vdash A[s/\mathbf{x}],\Gamma}{\vdash s\in\{\mathbf{x}:A\},\Gamma}\ \frac{\vdash i,\overline{p}}{\vdash i+1,\overline{p}} \qquad (\notin S)\ \frac{\vdash A[s/\mathbf{x}]^{\perp},\Gamma}{\vdash s\notin\{\mathbf{x}:A\},\Gamma}\ \frac{\vdash i,\overline{p}}{\vdash i+1,\overline{p}}$$

$$(=E)\ \frac{\vdash v\in s, v\notin t,\Gamma \quad \vdash v\notin s, v\in t,\Delta}{\vdash s=t,\Gamma,\Delta}\ \frac{\vdash i,j,\overline{p} \quad \vdash k,l,\overline{q}}{\vdash \rho(i,j,k,l),\overline{p},\overline{q}} \qquad (\neq S)\ \frac{\vdash A,\Gamma}{\vdash s\neq t, A[s/t],\Gamma}\ \frac{\vdash i,\overline{p}}{\vdash 0,i,\overline{p}}$$

$$(W\ ?)\ \frac{\vdash \Gamma}{\vdash\ ?A,\Gamma}\ \frac{\vdash \overline{p}}{\vdash 0,\overline{p}} \qquad (D\ ?)\ \frac{\vdash A,\Gamma}{\vdash\ ?A,\Gamma}\ \frac{\vdash i,\overline{p}}{\vdash i,\overline{p}}$$

$$(C\ ?)\ \frac{\vdash\ ?A,\ ?A,\Gamma}{\vdash\ ?A,\Gamma}\ \frac{\vdash i,j,\overline{p}}{\vdash \rho(i,j),\overline{p}} \qquad (\,!\,)\ \frac{\vdash A,\ ?\Gamma}{\vdash\ !A,\ ?\Gamma}\ \frac{\vdash i,\overline{p}}{\vdash i,\overline{p}}$$

$$(\perp)\ \frac{\vdash \Gamma}{\vdash \perp,\Gamma}\quad \frac{\vdash \overline{p}}{\vdash 0,\overline{p}}$$

$$(cut)\ \frac{\vdash A,\Gamma \quad \vdash A^{\perp},\Delta}{\vdash \Gamma,\Delta}\quad \frac{\vdash i,\overline{p} \quad \vdash j,\overline{q}}{\vdash \overline{p},\overline{q}}\ (i,j)$$

$$(\,?\,cut)\ \frac{\vdash\ ?A^{k},\Gamma \quad \vdash\ !A^{\perp},\Delta}{\vdash \Gamma,\Delta}\quad \frac{\vdash \overline{i},\overline{p} \quad \vdash j,\overline{q}}{\vdash \overline{p},\overline{q}}\ (\rho(\overline{i}),j)$$

Furthermore, we define the abstraction depth of a proof in terms of the abstraction indices of the cuts in it.

Definition 4.11 *The cut with the abstraction depth (i, j) is called an (i, j)-cut. We define the abstraction depth $\delta(\pi)$ of a proof π to be the maximum of the numbers $k = i \cdot j$ where (i, j) is the abstraction index of a cut in π whose cut formulas are not Z-formulas. If there is no such cut in π, the abstraction depth of π is set to 0.*

We now show that we can eliminate the atomic cuts whose cut formulas are obtained by the comprehension rules. The intuitive idea is as follows. Consider the occurrence of a formula A in a proof π. By tracing back how the occurrence of A is generated in π, we can talk about its ancestral formula occurrences. It should be clear that the abstraction depths of the ancestral formula occurrences are equal or smaller than that of the occurrence A. In the cut-elimination process except that for axioms, we replace a cut with the occurrence A by other cuts with itself or its ancestral formula occurrences. Therefore $\delta(\pi)$ remains the same or decreases in the cut-elimination process up to the axioms. In this way we can eliminate the cuts with the maximal abstraction depth one by one.

Proposition 4.12 *None of the reductions except the symmetric reduction $(*/I)$ increase the abstraction depth of a formula occurrence in the conclusion and the abstraction depth of a proof. Furthermore, the symmetric reductions $(\in S/\notin S)$ and $(\in Z/\notin Z)$ strictly decrease the abstraction depth of a proof.*

Proof

The proof is by inspection.

The symmetric reduction $(\perp/1)$

$$\dfrac{\dfrac{\vdash \overline{p}}{\vdash 0, \overline{p}} \quad \vdash 0}{\vdash \overline{p}}\ (0,0) \ \rightsquigarrow\ \vdash \overline{p}$$

The symmetric reduction $(*/\top)$

$$\dfrac{\vdash i, \overline{p}, i \quad \vdash 0, 0, \ldots, 0, 0}{\vdash 0, \overline{p}, 0, \ldots 0}\ (i, 0) \ \rightsquigarrow\ \vdash 0, 0, \ldots, 0, 0, \ldots, 0$$

The symmetric reduction ($\otimes$/⅋)

$$\frac{\dfrac{\vdash i,\overline{p} \quad \vdash j,\overline{q}}{\vdash \rho(i,j),\overline{p},\overline{q}} \quad \dfrac{\vdash k,l,\overline{r}}{\vdash \rho(k,l),\overline{r}}}{\vdash \overline{p},\overline{q},\overline{r}}\,(\rho(i,j),\rho(k,l)) \;\rightsquigarrow\; \frac{\vdash j,\overline{q} \quad \dfrac{\vdash i,\overline{p} \quad \vdash k,l,\overline{r}}{\vdash l,\overline{p},\overline{r}}\,(i,k)}{\vdash \overline{p},\overline{q},\overline{r}}\,(j,l)$$

The symmetric reduction (&/$\oplus$)

$$\frac{\dfrac{\vdash i,\overline{p} \quad \vdash j,\overline{q}}{\vdash \rho(i,j),\overline{\rho}(\overline{p},\overline{q})} \quad \dfrac{\vdash k,\overline{r}}{\vdash k,\overline{r}}}{\vdash \overline{\rho}(\overline{p},\overline{q}),\overline{r}}\,(\rho(i,j),k) \;\rightsquigarrow\; \frac{\vdash i,\overline{p} \quad \vdash k,\overline{r}}{\vdash \overline{p},\overline{r}}\,(i,k)$$

The symmetric reductions ($\bigwedge Z/\bigvee Z$), ($\bigwedge S/\bigvee S$) and (! /D ?)

$$\frac{\dfrac{\vdash i,\overline{p}}{\vdash i,\overline{p}} \quad \dfrac{\vdash j,\overline{q}}{\vdash j,\overline{q}}}{\vdash \overline{p},\overline{q}}\,(i,j) \;\rightsquigarrow\; \frac{\vdash i,\overline{p} \quad \vdash j,\overline{q}}{\vdash \overline{p},\overline{q}}\,(i,j)$$

The symmetric reductions ($\in Z/\notin Z$) and ($\in S/\notin S$)

$$\frac{\dfrac{\vdash i,\overline{p}}{\vdash i+1,\overline{p}} \quad \dfrac{\vdash j,\overline{q}}{\vdash j+1,\overline{q}}}{\vdash \overline{p},\overline{q}}\,(i+1,j+1) \;\rightsquigarrow\; \frac{\vdash i,\overline{p} \quad \vdash j,\overline{q}}{\vdash \overline{p},\overline{q}}\,(i,j)$$

The symmetric reduction (! /W ?)

$$\frac{\dfrac{\vdash i,\overline{p}}{\vdash i,\overline{p}} \quad \dfrac{\vdash \overline{q}}{\vdash 0,\overline{q}}}{\vdash \overline{p},\overline{q}}\,(i,0) \;\rightsquigarrow\; \frac{\vdash \overline{q}}{\vdash 1,\ldots 1,\overline{q}}$$

The symmetric reduction (W ? / !)–?

$$\frac{\dfrac{\vdash \overline{m},\overline{p}}{\vdash 0,\overline{m},\overline{p}} \quad \vdash j,\overline{q}}{\vdash \overline{p},\overline{q}}\,(\rho(\overline{m}),j) \;\rightsquigarrow\; \frac{\vdash \overline{m},\overline{p} \quad \vdash j,\overline{q}}{\vdash \overline{p},\overline{q}}\,(\rho(\overline{m}),j)$$

The symmetric reduction $(D\ ?\,/\,!\,)$**–?**

$$\dfrac{\dfrac{\vdash i,\overline{m},\overline{p}}{\vdash i,\overline{m},\overline{p}} \quad \dfrac{\vdash j,\overline{q}}{\vdash j,\overline{q}}}{\vdash \overline{p},\overline{q}}\,(\rho(\overline{m},i),j) \;\leadsto\; \dfrac{\dfrac{\dfrac{\vdash i,\overline{m},\overline{p} \quad \vdash j,\overline{q}}{\vdash i,\overline{p},\overline{q}}\,(\rho(\overline{m}),j) \qquad \vdash j,\overline{q}}{\vdash \overline{p},\overline{q},\overline{q}}\,(i,j)}{\vdash \overline{p},\overline{q}}$$

The symmetric reduction $(C\ ?\,/\,!\,)$**–?**

$$\dfrac{\dfrac{\vdash i,m_1,\ldots,m_n,\ldots,m_k,\overline{p}}{\vdash m_1,\ldots,\rho(m_n,i),\ldots,m_k,\overline{p}} \quad \vdash j,\overline{q}}{\vdash \overline{p},\overline{q}}\,(\rho(\overline{m},i),j) \;\leadsto\; \dfrac{\vdash i,\overline{m},\overline{p} \quad \vdash j,\overline{q}}{\vdash \overline{p},\overline{q}}\,(\rho(\overline{m},i),j)$$

The permutative reduction $(cut/\otimes)$

$$\dfrac{\vdash k,\overline{p} \quad \dfrac{\vdash i,l,\overline{q} \quad \vdash j,\overline{r}}{\vdash \rho(i,j),l,\overline{q},\overline{r}}}{\vdash \rho(i,j),\overline{p},\overline{q},\overline{r}}\,(k,l) \;\leadsto\; \dfrac{\dfrac{\vdash k,\overline{p} \quad \vdash i,l,\overline{q}}{\vdash i,\overline{p},\overline{q}}\,(k,l) \qquad \vdash j,\overline{r}}{\vdash \rho(i,j),\overline{p},\overline{q},\overline{r}}$$

The permutative reduction $(cut/\&)$

$$\dfrac{\vdash k,\overline{p} \quad \dfrac{\vdash i,l_1,\overline{q} \quad \vdash j,l_2,\overline{r}}{\vdash \rho(i,j),\rho(l_1,l_2),\overline{\rho}(\overline{q},\overline{r})}}{\vdash \rho(i,j),\overline{p},\overline{\rho}(\overline{q},\overline{r})}\,(k,\rho(l_1,l_2)) \;\leadsto\; \dfrac{\dfrac{\vdash k,\overline{p} \ \vdash i,l_1,\overline{q}}{\vdash i,\overline{p},\overline{q}}\,(k,l_1) \quad \dfrac{\vdash k,\overline{p} \ \vdash j,l_2,\overline{r}}{\vdash j,\overline{r},\overline{p}}\,(k,l_2)}{\vdash \rho(i,j),\overline{p},\overline{\rho}(\overline{q},\overline{r})}$$

The permutative reduction (cut/cut)

$$\dfrac{\vdash \overline{p},k \quad \dfrac{\vdash \overline{q},l,i \quad \vdash \overline{r},j}{\vdash \overline{q},\overline{r},l}\,(i,j)}{\vdash \overline{p},\overline{q},\overline{r}}\,(k,l) \;\leadsto\; \dfrac{\dfrac{\vdash \overline{p},k \quad \vdash \overline{q},l,i}{\vdash \overline{p},\overline{q},i}\,(k,l) \qquad \vdash \overline{r},j}{\vdash \overline{p},\overline{q},\overline{r}}\,(i,j)$$

The permutative reductions $(cut/\parr)$ **and** $(cut/C\ ?)$

$$\frac{\vdash k,\overline{p} \quad \dfrac{\vdash i,j,l,\overline{q}}{\vdash \rho(i,j),l,\overline{r}}}{\vdash \rho(i,j),\overline{p},\overline{q}}\,(k,l) \quad\leadsto\quad \frac{\dfrac{\vdash k,\overline{p},k \quad \vdash i,j,l,\overline{q}}{\vdash i,j,\overline{p},\overline{q}}\,(k,l)}{\vdash \rho(i,j),\overline{p},\overline{q}}$$

The permutative reductions $(cut/\oplus)$, $(cut/\bigwedge Z)$, $(cut/\bigvee Z)$, $(cut/\bigwedge S)$, $(cut/\bigvee S)$ **and** $(cut/D\ ?)$

$$\frac{\vdash k,\overline{p} \quad \dfrac{\vdash i,l,\overline{q}}{\vdash i,l,\overline{q}}}{\vdash i,\overline{p},\overline{q}}\,(k,l) \quad\leadsto\quad \frac{\dfrac{\vdash k,\overline{p} \quad \vdash i,l,\overline{q}}{\vdash i,\overline{p},\overline{q}}\,(k,l)}{\vdash i,\overline{p},\overline{q}}$$

The permutative reductions $(cut/\in Z)$, $(cut/\notin Z)$, $(cut/\in S)$ **and** $(cut/\notin S)$

$$\frac{\vdash k,\overline{p} \quad \dfrac{\vdash i,l,\overline{q}}{\vdash i+1,l,\overline{r}}}{\vdash i+1,\overline{p},\overline{q}}\,(k,l) \quad\leadsto\quad \frac{\dfrac{\vdash k,\overline{p} \quad \vdash i,l,\overline{q}}{\vdash i,\overline{p},\overline{q}}\,(k,l)}{\vdash i+1,\overline{p},\overline{q}}$$

The permutative reduction $(cut/=E)$

$$\frac{\vdash k,\overline{p} \quad \dfrac{\vdash i_1,i_2,l,\overline{q} \quad \vdash j_1,j_2,\overline{r}}{\vdash \rho(i_1,i_2,j_1,j_2),l,\overline{p},\overline{q}}}{\vdash \rho(i_1,i_2,j_1,j_2,\overline{p},\overline{q},\overline{r}}\,(k,l) \leadsto \frac{\dfrac{\vdash k,\overline{p} \quad \vdash i_1,i_2,l,\overline{q}}{\vdash i_1,i_2,\overline{p},\overline{q}}\,(k,l) \qquad \vdash j_1,j_2,\overline{r}}{\vdash \rho(i_1,i_2,j_1,j_2),\overline{p},\overline{q},\overline{r}}$$

The permutative reduction $(cut/\neq S)$

$$\frac{\vdash k,\overline{p} \quad \dfrac{\vdash i,l,\overline{q}}{\vdash 0,i,l,\overline{q}}}{\vdash 0,i,\overline{p},\overline{q}}\,(k,l) \quad\leadsto\quad \frac{\dfrac{\vdash k,\overline{p} \quad \vdash i,l,\overline{q}}{\vdash i,\overline{p},\overline{q}}\,(k,l)}{\vdash 0,i,\overline{p},\overline{q}}$$

The permutative reductions $(cut/W\ ?)$ **and** $(cut/\perp)$

$$\frac{\vdash k,\overline{p} \quad \dfrac{\vdash l,\overline{q}}{\vdash 0,l,\overline{r}}}{\vdash 0,\overline{p},\overline{q}}\,(k,l) \quad\leadsto\quad \frac{\dfrac{\vdash k,\overline{p} \quad \vdash l,\overline{q}}{\vdash \overline{p},\overline{q}}\,(k,l)}{\vdash 0,\overline{p},\overline{q}}$$

The permutative reductions for ($?\,cut$ on !-branch They are entirely similar to the permutations for the permutative reductions for (cut) except that we have to replace $\overline{k}$ and $(\rho(\overline{k}), l)$ for k and (k, l), respectively.

The permutative reduction $(\otimes/\ ?\,cut1)$**–?**

$$\dfrac{\dfrac{\vdash i,\overline{m},\overline{p} \quad \vdash j,\overline{q}}{\vdash \rho(i,j),\overline{m},\overline{p},\overline{q}} \quad \vdash l,\overline{r}}{\vdash \rho(i,j),\overline{p},\overline{q},\overline{r}}\,(\rho(\overline{m}),l) \;\rightsquigarrow\; \dfrac{\dfrac{\vdash i,\overline{m},\overline{p} \quad \vdash l,\overline{r}}{\vdash i,\overline{p},\overline{r}}\,(\rho(\overline{m}),l) \quad \vdash j,\overline{q}}{\vdash \rho(i,j),\overline{p},\overline{q},\overline{r}}$$

The permutative reduction $(\otimes/\ ?\,cut2)$**–?**

$$\dfrac{\dfrac{\vdash i,\overline{m},\overline{p} \vdash j,\overline{n},\overline{q}}{\vdash \rho(i,j),\overline{m},\overline{n},\overline{p},\overline{q}} \quad \vdash l,\overline{r}}{\vdash \rho(i,j),\overline{p},\overline{q},\overline{r}}\,(\rho(\overline{m},\overline{n}),l) \;\rightsquigarrow\; \dfrac{\dfrac{\dfrac{\vdash i,\overline{m},\overline{p} \vdash l,\overline{r}}{\vdash i,\overline{p},\overline{r}}\,(\rho(\overline{m}),l) \quad \dfrac{\vdash j,\overline{n},\overline{q} \vdash l,\overline{r}}{\vdash j,\overline{q},\overline{r}}\,(\rho(\overline{n}),l)}{\vdash \rho(i,j),\overline{p},\overline{q},\overline{r},\overline{r}}}{\vdash \rho(i,j),\overline{p},\overline{q},\overline{r}}$$

The permutative reduction $(\&/\ ?\,cut)$**–?**

$$\dfrac{\dfrac{\vdash i,\overline{m},\overline{p} \vdash j,\overline{n},\overline{q}}{\vdash \rho(i,j),\overline{\rho}(\overline{m},\overline{n}),\overline{\rho}(\overline{p},\overline{q})} \quad \vdash l,\overline{r}}{\vdash \rho(i,j),\overline{\rho}(\overline{p},\overline{q}),\overline{r}}\,(\rho(\overline{m},\overline{n}),l) \;\rightsquigarrow\; \dfrac{\dfrac{\vdash i,\overline{m},\overline{p} \vdash l,\overline{r}}{\vdash i,\overline{p},\overline{r}}\,(\rho(\overline{m}),l) \quad \dfrac{\vdash j,\overline{n},\overline{q} \vdash l,\overline{r}}{\vdash j,\overline{q},\overline{r}}\,(\rho(\overline{n}),l)}{\vdash \rho(i,j),\overline{\rho}(\overline{p},\overline{q}),\overline{r}}$$

The permutative reduction $(=E/\ ?\,cut1)$**–?**

$$\dfrac{\dfrac{\vdash i_1,i_2,\overline{m},\overline{p} \quad \vdash j_1,j_2,\overline{q}}{\vdash \rho(i_1,i_2,j_1,j_2),\overline{m},\overline{p},\overline{q}} \quad \vdash k,\overline{r}}{\vdash \rho(i_1,i_2,j_1,j_2),\overline{p},\overline{q},\overline{r}}\,(\rho(\overline{m}),k) \;\rightsquigarrow$$

$$\dfrac{\dfrac{\vdash i_1,i_2,\overline{m},\overline{p} \quad \vdash k,\overline{r}}{\vdash i_1,j_2,\overline{p},\overline{r}}\,(\rho(\overline{m}),k) \quad \vdash j_1,j_2,\overline{q}}{\vdash \rho(i_1,i_2,j_1,j_2),\overline{p},\overline{q},\overline{r}}$$

The permutative reduction $(= E/\ ?\,cut2)$**–?**

$$\frac{\dfrac{\vdash i_1,i_2,\overline{m},\overline{p} \quad \vdash j_1,j_2,\overline{n},\overline{r}}{\vdash \rho(i_1,i_2,j_1,j_2),\overline{m},\overline{n},\overline{p},\overline{q}} \quad \vdash k,\overline{r}}{\vdash \rho(i_1,i_2,j_1,j_2),\overline{p},\overline{q},\overline{r}}\,(\rho(\overline{m},\overline{n}),k) \ \rightsquigarrow$$

$$\frac{\dfrac{\vdash i_1,i_2,\overline{m},\overline{p} \quad \vdash k,\overline{r}}{\vdash i_1,i_2,\overline{p},\overline{r}}\,(\rho(\overline{m}),k) \quad \dfrac{\vdash j_1,j_2,\overline{n},\overline{q} \quad \vdash k,\overline{r}}{\vdash j_1,j_2,\overline{q},\overline{r}}\,(\rho(\overline{n}),k)}{\dfrac{\vdash \rho(i_1,i_2,j_1,j_2),\overline{p},\overline{q},\overline{r},\overline{r}}{\vdash \rho(i_1,i_2,j_1,j_2),\overline{p},\overline{q},\overline{r}}}$$

The permutative reduction $(cut/\ ?\,cut1)$**–?**

$$\frac{\dfrac{\vdash i,\overline{m},\overline{p} \quad \vdash j,\overline{q}}{\vdash \overline{m},\overline{p},\overline{q}}\,(i,j) \quad \vdash l,\overline{r}}{\vdash \rho(i,j),\overline{p},\overline{q},\overline{r}}\,(\rho(\overline{m}),l) \ \rightsquigarrow \ \frac{\dfrac{\vdash i,\overline{m},\overline{p} \quad \vdash l,\overline{r}}{\vdash i,\overline{p},\overline{r}}\,(\rho(\overline{m}),l) \quad \vdash j,\overline{q}}{\vdash \overline{p},\overline{q},\overline{r}}\,(i,j)$$

The permuative reduction $(cut/\ ?\,cut2)$**–?**

$$\frac{\dfrac{\vdash i,\overline{m},\overline{p} \vdash j,\overline{n},\overline{q}}{\vdash \overline{m},\overline{n},\overline{p},\overline{q}}\,(i,j) \quad \vdash l,\overline{r}}{\vdash \overline{p},\overline{q},\overline{r}}\,(\rho(\overline{m},\overline{n}),l) \ \rightsquigarrow \ \frac{\dfrac{\vdash i,\overline{m},\overline{p} \vdash l,\overline{r}}{\vdash i,\overline{p},\overline{r}}\,(\rho(\overline{m}),l) \quad \dfrac{\vdash j,\overline{n},\overline{q} \vdash l,\overline{r}}{\vdash j,\overline{q},\overline{r}}\,(\rho(\overline{n}),l)}{\dfrac{\vdash \overline{p},\overline{q},\overline{r},\overline{r}}{\vdash \overline{p},\overline{q},\overline{r}}}\,(i,j)$$

The permutative reduction $(\ ?\,cut/\ ?\,cut1)$**–?**

$$\frac{\dfrac{\vdash \overline{i},\overline{m},\overline{p} \quad \vdash j,\overline{q}}{\vdash \overline{m},\overline{p},\overline{q}}\,(\rho(\overline{i}),j) \quad \vdash l,\overline{r}}{\vdash \overline{p},\overline{q},\overline{r}}\,(\rho(\overline{m}),l) \ \rightsquigarrow \ \frac{\dfrac{\vdash \overline{i},\overline{m},\overline{p} \quad \vdash l,\overline{r}}{\vdash \overline{i},\overline{p},\overline{r}}\,(\rho(\overline{m}),l) \quad \vdash j,\overline{q}}{\vdash \overline{p},\overline{q},\overline{r}}\,(\rho(\overline{i}),j)$$

The permutative reduction $(\ ?\,cut/\ ?\,cut2)$**–?**

$$\frac{\dfrac{\vdash \overline{i},\overline{m},\overline{p} \vdash j,\overline{q},\overline{n}}{\vdash \overline{m},\overline{n},\overline{p},\overline{q}}\,(\rho(\overline{i}),j) \quad \vdash l,\overline{r}}{\vdash \overline{p},\overline{q},\overline{r}}\,(\rho(\overline{m},\overline{n}),l) \ \rightsquigarrow \ \frac{\dfrac{\vdash \overline{i},\overline{m},\overline{p} \vdash l,\overline{r}}{\vdash \overline{i},\overline{p},\overline{r}}\,(\rho(\overline{m}),l) \quad \dfrac{\vdash j,\overline{n},\overline{q} \vdash l,\overline{r}}{\vdash j,\overline{q},\overline{r}}\,(\rho(\overline{n}),l)}{\dfrac{\vdash \overline{p},\overline{q},\overline{r},\overline{r}}{\vdash \overline{p},\overline{q},\overline{r}}}\,(\rho(\overline{i}),j)$$

The permutative reductions $(\,?\,cut/\parr)$**–?**, $(\oplus 1/\,?\,cut)$**–?**, $(\oplus 2/\,?\,cut)$**–?**, $(\bigwedge S/\,?\,cut)$**–?**, $(\bigvee S/\,?\,cut)$**–?**, $(\bigwedge Z/\,?\,cut)$**–?**, $(\bigvee Z/\,?\,cut)$**–?**, $(\in\ S/\,?\,cut)$**–?**, $(\notin\ S/\,?\,cut)$**–?**, $(\in\ Z/\,?\,cut)$**–?**, $(\notin\ Z/\,?\,cut)$**–?**, $(\neq\ S/\,?\,cut)$, $(\perp\ /\,?\,cut)$**–?**, $(W?/\,?\,cut)$**–?**, $(D?/\,?\,cut)$**–?**, **and** $(C?/\,?\,cut)$**–?** They are exactly similar to the corresponding permutative reductions for (cut) except that we have to replace $\overline{k}$ and $\rho(\overline{k},l)$ for k and (k,l), respectively.

The permutative reduction $(\,!\,/\,?\,cut)$**–?**

$$\dfrac{\dfrac{\vdash i,\overline{m},\overline{p}}{\vdash i,\overline{m},\overline{p}} \quad \vdash l,\overline{q}}{\vdash i,\overline{p},\overline{q}}\,(\rho(\overline{m}),l) \quad \leadsto \quad \dfrac{\dfrac{\vdash i,\overline{m},\overline{p} \quad \vdash l,\overline{q}}{\vdash i,\overline{p},\overline{q}}\,(\rho(\overline{m}),l)}{\vdash i,\overline{p},\overline{q}}$$

∎

Notice that the use of $(*/I)$ can indeed lead to the increase of the abstraction index as shown below:

$$(*/I) \qquad \dfrac{\dfrac{\vdash i,\overline{p} \quad \vdash j,k}{\vdash k,\overline{p}}\,(i,j) \qquad \vdash l,\overline{q}}{\vdash \overline{p},\overline{q}}\,(k,l) \quad \leadsto \quad \dfrac{\vdash i,\overline{p} \quad \vdash l,\overline{q}}{\vdash \overline{p},\overline{q}}\,(i,l)$$

where $k < i$.

Proposition 4.13 *Suppose the proof π reduces to a proof τ without the use of $(*/I)$. Then the abstraction depth of each formula occurrence in the conclusion sequent of π is less than or equal to the corresponding formula occurrence in τ, and the abstraction depth $\delta(\pi)$ of π is less than or equal to $\delta(\tau)$ of τ.*

Proof

When one of the reductions is applied to a subproof τ of a proof π, the abstraction indices of the cuts outside τ remain unchanged or decrease since the abstraction depth of each formula occurrence in the conclusion sequent of π does not increase by the reduction. Given this, the result is immediate by induction on the number of one-step reductions. ∎

Proposition 4.14 *Consider the proof π*

$$\dfrac{\begin{array}{c}\vdots\pi_1\\ \vdash A,\Gamma\end{array} \quad \begin{array}{c}\vdots\pi_2\\ \vdash A^{\perp},\Delta\end{array}}{\vdash \Gamma,\Delta}$$

and suppose that π contains only atomic cuts and cuts over Z-formulas, and the formulas A and $A^\perp$ are not Z-formulas. Furthermore suppose that the abstraction depth $\delta(\pi_1)$ and $\delta(\pi_2)$ are strictly less than the abstraction depth $\delta(\pi) = \delta(A) \times \delta(A^\perp)$. Then there exists a proof τ such that

- *π reduces to τ*
- *the degree $\partial(\tau)$ of τ is less than or equal to 1*
- *the abstraction depth $\delta(\tau)$ of τ is strictly less than the abstraction depth $\delta(\pi)$ of π.*

Proof

Note that the abstraction depth $\delta(\pi)$ is strictly greater than 0 since $\delta(\pi_1)$ and $\delta(\pi_2)$ are at least equal to 0. The proof is by induction on $\sigma(\pi)$.

Case 1 One of the cut formulas is not the main formula. Then apply one of the permutative reductions and use the inductive hypothesis.

Case 2: Otherwise we apply one of the symmetric reductions $(\in S/ \notin S)$ or $(\in Z/ \notin Z)$. This may create new cuts with formulas which are not atomic. However the abstraction indices of those newly created cuts are strictly less than $\delta(\pi)$ and they can be eliminated by repeating the first step of our cut-elimination without increasing the abstraction depth of the proof.

∎

Lemma 4.15 *Suppose that the abstraction depth $\delta(\pi)$ and degree $\partial(\pi)$ of a proof π is greater than or equal to 1. Then π reduces to a proof τ such that the degree $\partial(\tau)$ of τ is less than or equal to 1 and the abstraction depth $\delta(\tau)$ of τ is strictly less than the abstraction depth $\delta(\pi)$ of π.*

Proof

The proof is by induction on $\sigma(\pi)$. Consider the lowermost cut of the maximal abstraction index whose cut formulas are not Z-formulas. We first apply the inductive hypothesis to both branches above the cut and eliminate the cut by the previous lemma. ∎

Theorem 4.16 *Let π be a proof. Then π reduces to a proof τ such that the degree $\partial(\tau)$ of τ is less than or equal to 1 and the abstraction depth $\delta(\tau)$ of τ is 0.*

Proof
First eliminate all the atomic cuts whose cut-formulas are not Z-formulas. Then reduce the theorem follows from the previous lemma by induction on $\delta(\pi)$. ∎

4.8 The elimination of atomic cuts involving axioms

In the previous two steps, we have reduced a proof π to a proof τ such that τ contains only cuts over Z-formulas and atomic cuts whose cut formulas are obtained by the comprehension rules. The last step of our cut-elimination is to eliminate all the remaining atomic cuts whose cut formulas are not Z-formulas. This is achieved again in the same way as in SMALL. However, we need to make sure for this that the exponentials in Z-terms do not intervene in the size decrease through the cut-elimination process.

Let's consider what kind of cuts still remain in the proof. First of all, we have cuts whose cut formulas are Z-formulas. As we have already emphasized, we are not interested in eliminating those cuts. Secondly, we have cuts whose cut formulas are constants $\mathbf{1}$ and $\perp$, or $\top$ and $\mathbf{0}$. Those cuts can be eliminated easily without creating any new cuts. Thirdly, we have cuts whose cut formulas are of the form $s \in t$ and $s \notin t$, and both of them are originated in axioms (I) or one of them is originated in an axiom $\top$. They can be also eliminated without new cuts. Finally, we have the most interesting case in which the cut formulas are of the form $s \in t$ and $s \notin t$ and one of them is created by a comprehension rule and the other originated in an axiom (I).

In the last case, we have a cut

$$\frac{\stackrel{\vdots\pi}{\vdash s \in t, \Gamma} \quad \vdash s \notin t, s \in t}{\vdash s \in t, \Gamma} \quad \text{or} \quad \frac{\stackrel{\vdots\pi}{\vdash s \notin t, \Gamma} \quad \vdash s \in t, s \notin t}{\vdash s \notin t, \Gamma}$$

where $s \in t$ or $s \notin t$ on the left branch is created by one of the comprehension rules in the subproof π. We can assume that $s \in t$ and $s \notin t$ are not Z-formulas since otherwise we would not have to eliminate the cut. Furthermore, we know that the terms s and t are S-terms since otherwise $s \in t$ and $s \notin t$ would not be admissible. From this, we can conclude that t is not a Z-term as follows.

First, suppose that $s \in t$ is created by the comprehension rule $(\in Z)$ in the subproof π. Then s is a Z-term, and t has the form $\{v : A\}$. Among S-terms, only Z-terms have the form $\{v : A\}$, *i.e.*, abstraction over Z-variables. Hence t is a Z-term. Then both s and t are Z-terms, and we have already excluded this case from our consideration.

Therefore suppose that $s \in t$ is created by the rule $(\in S)$. Then t has the form $\{\mathbf{x} : A\}$ and hence it is not a Z-term. Similarly for the case where $s \notin t$ is created by a comprehension rule.

This observation ensures that we never encounter the exponetials in further rewinding the set terms through the cut-elimination of the remaining atomic formulas. Therefore, we can use the same argument for our last step of cut-elimination as we did in SMALL.

Proposition 4.17 *All the symmetric reductions for* (cut) *strictly decrease the size of a proof.*

Proof

Since we have essentially no new symmetric reductions in LZF, the proof is the same as the one for SMALL. We only note that two kinds of quantification and comprehension rules in LZF behave in a completely similar way. ∎

Proposition 4.18 *All the permutative reductions for* (cut) *do not increase the size of a proof.*

Proof

We only need to check two new permutative reductions.

The permutative reduction $(cut/=E)$

$$\dfrac{\vdash \alpha \quad \dfrac{\vdash \beta \quad \vdash \gamma}{\vdash \beta + \gamma}}{\vdash \alpha + \beta + \gamma} \rightsquigarrow \dfrac{\dfrac{\vdash \alpha \quad \vdash \beta}{\vdash \alpha + \beta} \quad \vdash \gamma}{\vdash \alpha + \beta + \gamma}$$

The permutative reduction $(cut/\neq S)$

$$\dfrac{\vdash \alpha \quad \dfrac{\vdash \beta}{\vdash \beta + 1}}{\vdash \alpha + \beta + 1} \rightsquigarrow \dfrac{\dfrac{\vdash \alpha \quad \vdash \beta}{\vdash \alpha + \beta}}{\vdash \alpha + \beta + 1}$$

∎

Lemma 4.19 *Suppose that a proof π only contains cuts over Z-formulas and atomic cuts whose cut formulas are S-formulas. Then π reduces to a proof τ such that the size $\sigma(\tau)$ of τ is less than or equal to $\sigma(\pi)$ of π and τ only contains cuts over Z-formulas.*

Proof

The proof is by induction on $\sigma(\pi)$. Suppose that the last inference of π is either not cut or a cut over Z-formula. Then the conclusion follows immediately by the inductive hypothesis. Hence we suppose otherwise.

Furthermore, we can exclude the case where the symmetric reduction ($\in Z / \notin Z$) is applicable to the cut at the bottom. In this case, the term s in the cut formula $s \in t$ and $s \notin t$ should be a Z-term, and t be of the form $\{v : A\}$. Since t is also a S-term, it could only be a Z-term. Hence $s \in t$ and $s \notin t$ should be Z-formulas.

Then there remain only four cases.

Case 1 The symmetric reduction ($\in S / \notin S$) is applicable to the cut at the bottom. Then we perform the symmetric reduction. The newly created cut is again a cut over S-formulas by the construction of S-terms. Furthermore, the size of a proof strictly decreases. Therefore we can apply the inductive hypothesis to the result.

Case 2 One of the symmetric reductions other than ($\in S / \notin S$) is applicable. Then we perform the symmetric reduction. By construction of S-formulas, the cut formulas of the newly created cuts are again S-formulas. Since the reduction strictly decreases the size of a proof, we can apply the inductive hypothesis to the result.

Case 3 One of the permutative reductions except (cut/cut) is applicable. Then we perform the permutative reduction and then apply the inductive hypothesis.

Case 4 The permutation (cut/cut) is applicable. If the upper cut is over Z-formulas, apply the permutation and use the inductive hypothesis. Otherwise apply the inductive hypothesis to the upper cut. This reduction does not increase the size of the proof and leads to the situation to which the other cases are applicable.

∎

Theorem 4.20 *For any proof π, there exists a proof τ such that π reduces to τ and τ only contains cuts over Z-formulas.*

Proof

In the second step of our cut-elimination, we have already reduced a proof π to another proof which only contains cuts over Z-formulas and atomic cuts one of whose cut formulas is originated in axioms. By induction on the size of a proof, we eliminate all the atomic cuts which do not involve a cut formula created by one of the comprehension rules. Then we have a proof which only contains cuts over Z-formulas and atomic cuts one of whose cut formula is created by a comprehension rule and the other originated in an axion (I). Hence the cut formulas of the remaining atomic cuts have the form $s \in t$ or $s \notin t$ where the terms s and t are S-terms. In other words, all the remaining atomic cuts are over S-formulas. The conclusion then follows from the previous lemma. ∎

4.9 Consistency of LZF

Given all the previous results at hand, we can now prove that LZF is a conservative extension of ZF$^-$.

Theorem 4.21 *Let A^+ be the translation of a formula A in ZF$^-$. If A^+ is provable in LZF, then so is A in ZF$^-$.*

Proof

Suppose that there is a proof π of the formula A^+ in LZF. Then there is a proof τ of A^+ which only contains Z-terms. Ignoring all the occurrences of $!$ and $?$, we can read the proof τ as a proof in ZF$^-$. ∎

Theorem 4.22 *LZF is consistent relative to ZF$^-$.*

Proof

If A and $A^\perp$ were both provable in LZF, then any formula of the form $?C$ would be provable. In particular, $?\,u \neq u$ would be provable in LZF and hence $u \neq u$ provable in ZF$^-$. ∎

Chapter 5

Further extension

5.1 Introduction

In this chapter, we further extend our linear set theory LZF by adjoining the substitutivity for all S-terms and the weakening. The extended system is our fourth system of linear set theory AZF.

In LZF, we have the equality relation for Z-terms, which satisfies the extensionality $(= E)$ and the substitutivity $(\neq S)$. We now extend only the substitutivity to cover all S-terms. We do not extend the extensionality since Grishin has shown that linear set theory with both the substitutivity and extensionality is inconsistent [13].

Grishin has also shown that we can recover the left-side contraction for equations $s = t$. Given this, we decide to incorporate this type of contraction in AZF from the beginning. This contraction rule is in fact necessary to obtain the cut-elimination result.

5.2 Grishin's paradox

We start by reviewing Grishin's result about the incompatibility of the substitutivity and the extensionality in linear set theory.

5.2.1 Contraction and weakening

We first show that the right-side contraction and weaking rules are derivable for the atomic sentences of the form $s \neq t$ by the use of of the substitutivity principle:

$$(\neq S) \quad \frac{\vdash A, \Gamma}{\vdash s \neq t, A[s/t], \Gamma}$$

The contraction rule is derived from this as follows

$$\frac{\dfrac{\dfrac{\vdash t = t \quad \vdash t = t}{\vdash t = t \otimes t = t}}{\vdash s \neq t, s = t \otimes s = t} \quad \dfrac{\vdash s \neq t, s \neq t, \Gamma}{\vdash s \neq t \parr s \neq t, \Gamma}}{\vdash s \neq t, \Gamma}$$

and the weakning is derived trivially:

$$\frac{\vdash A, \Gamma}{\vdash s \neq t, A, \Gamma}$$

where no occurrence of t in A is substituted by s. This shows that the formulas of the form $s \neq t$ behave in a similar way as the formulas of the form $?A$.

5.2.2 Grishin's paradox

Grishin obtained his inconsistency result in linear set theory with the weakening rule, or affine set theory. Assuming the extensionality principle

$$\frac{\vdash x \in s, x \notin t, \Gamma \quad \vdash x \notin s, x \in t, \Delta}{\vdash s = t, \Gamma, \Delta}$$

we construct the terms s and t for any formula A such that $s = t$ is logically equivalent to A, *i.e.*

$$\vdash s \neq t, A \qquad \text{and} \qquad \vdash s = t, A^{\perp}$$

are both provable. Let w be any term. We define $s =_{def} \{x : x = w\}$ and $t =_{def} \{x : x = w \otimes A\}$. Then the following derivations show that they satisfy the required properties.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\vdash x = w, x \neq w}{\vdash A^{\perp}, x = w, x \neq w}}{\vdash x \neq w \parr A^{\perp}, x = w}}{\vdash x \notin \{x : x = w \otimes A\}, x = w}}{\vdash x \in s, x \notin t} \qquad \dfrac{\dfrac{\dfrac{\vdash A, A^{\perp} \quad \vdash x = w, x \neq w}{\vdash x = w \otimes A, A^{\perp}, x \neq w}}{\vdash x \in t, A^{\perp}, x \neq w}}{\vdash x \notin s, x \in t, A^{\perp}}}{\vdash s = t, A^{\perp}}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\vdash A, A^{\perp}}{\vdash w \neq w, A, A^{\perp}}}{\vdash w \neq w \parr A^{\perp}, A}}{\vdash w \notin t, A}}{\vdash s \neq t, w \notin s, A} \qquad \dfrac{\vdash w = w}{\vdash w \in s}}{\vdash s \neq t, A}$$

Combined with the contraction for the equations, we can derive the contraction rule for any formula $C =_{def} A^{\perp}$ as follows:

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdash C, C, \Gamma \quad \vdash s \neq t, A}{\vdash s \neq t, C, \Gamma} \qquad \vdash s \neq t, A}{\vdash s \neq t, s \neq t, \Gamma}}{\vdash s \neq t, \Gamma} \qquad \vdash s = t, C}{\vdash C, \Gamma}$$

Hence the derivation of the Russell's paradox goes through.

5.3 The formal system of AZF

5.3.1 The axioms and rules of inference of AZF

The language of AZF is the same as that of LZF. The axioms and rules of inference of AZF is obtained by extending those of LZF to include the substitutivity for all S-terms, the contraction for $s \neq t$ and the weakening.

Rules of inference

$$(S \neq) \quad \dfrac{\vdash A, \Gamma}{\vdash s \neq t, A[s/t], \Gamma}$$

where s and t are S-terms, and the formula A contains only S-terms.

$$(C \neq) \quad \frac{\vdash s \neq t, s \neq t, \Gamma}{\vdash s \neq t, \Gamma} \qquad\qquad (W) \quad \frac{\vdash \Gamma}{\vdash A, \Gamma}$$

5.3.2 Additional rules of inference

For the cut-eliminatiion proof, we use additional rules of infererece as we did for SMALL. In the following, the Greek lower case letters θ, η, ξ, ... are used to denote lists of the formulas $s \neq t$. Furthermore, we write $A[\theta]$ for $(\ldots(A[s_1/t_1])\ldots)[s_n/t_n])$ when θ is the list $s_1 \neq t_1$, ..., $s_n \neq t_n$.

Given this notational convention, our first additional rule is written as follows

$$(RS \neq) \quad \frac{\vdash A, \Gamma}{\vdash A[\theta], \theta, \Gamma}$$

which combines repetitive uses of $(S \neq)$ as a single rule of inference.

Secondly, we combine substitution and cut into a single rule of inference. For this, we need a definition.

Definition 5.1 *The formulas A and A' are substitutionally identical under the list of formulas θ if there are two lists of formulas η and ξ such that*

- *θ is a permutation of the concatenation of η and ξ*
- *$A[\eta]$ is identical to $A[\xi]$.*

The substitutional identity for terms is defined in a similar way.

In short, A and A' are identical under $s_1 \neq t_1$, ..., $s_n \neq t_n$ if we can make A and A' identical by substitution, using the equations in the list. Then our second additional rule of inference is formulated as follows:

$$(\neq cut) \quad \frac{\vdash A, \Gamma \quad \vdash A'^{\perp}, \Delta}{\vdash \theta, \Gamma, \Delta}$$

where the formulas A and A' are substitutionally identical under the list θ. We regard (cut) as a special case of $(\neq cut)$ where θ is empty. Note that the substitutional identity has the following property.

Proposition 5.2 *Suppose that A is substitutionally identical to A' under θ. Then we can make A identical to A' by substituting the terms only in A, using the equations in θ. Similarly for terms.*

Proof

By the definition of substitutional identity, we have η and ξ such that $A[\eta]$ is identical to $A'[\xi]$ and θ is a permutation of their concatenation. Let ξ^{-1} be the list of formulas obtained by reversing the order of ξ. Then we can recover the formula A' by the reverse substitution as $A'[\xi][\xi^{-1}]$. Hence A' is identical to $A[\eta][\xi^{-1}]$. Note that θ is again a permutation of the concatenation of η and ξ^{-1}. Similarly for terms. ∎

Finally, cut and contraction are combined as before. However, we now also incorporate the repetitive substitution and modify $(\,?\,cut)$ as follows:

$$(?\neq cut)\quad \frac{\vdash (C_i)^k,\Gamma \quad \vdash C^{\perp},\Delta}{\vdash (\theta_i)^k,\Gamma,\Delta}$$

where $(C_i)^k$ and $(\theta_i)^k$ are the lists $C_1, \ldots, C_k$ and $\theta_1, \ldots, \theta_k$, respectively, and the formula C_i is substitutionally identical to C under θ_i. Note that the formula C is of the form either $?\,A$ or $s \neq t$, since we have the contraction rule for $s \neq t$ as well as $?\,A$.

All of those additional rules of inference are derivable in AZF and any sequent provable in this extended system is also provable in AZF. The rule $(RS \neq)$ is simply the repetition of $(S \neq)$. The rule $(\neq cut)$ is derived as follows:

$$\frac{\dfrac{\vdash A,\Gamma}{\vdash \eta, A[\eta],\Gamma} \quad \dfrac{\vdash A'^{\perp},\Gamma}{\vdash \xi, A'[\xi]^{\perp},\Delta}}{\vdash \theta,\Gamma,\Delta}$$

where η and ξ are the lists obtained by the definition of substitutional identity of A and A' so that $A[\eta]$ is identical to $A[\xi]$. The rule $(?\neq cut)$ is obtained as below.

$$\frac{\dfrac{\vdash (C_i)^k,\Gamma}{\vdash C^k,(\theta_i)^k,\Gamma} \quad \vdash C^{\perp},\Delta}{\vdash (\theta_i)^k,\Gamma,\Delta}$$

5.4 The cut-elimination procedure for AZF

The equality relation makes the cut-elimination slightly more complicated than before. As usual, we use symmetric and permutative reductions to eliminate cuts. However, we now have to consider the symmetric and permutative reductions for $(\neq cut)$ as well as for (cut) and $(?cut)$. Furthermore, there are cases where we cannot eliminate the cut.

For example, consider the following cut

$$\dfrac{\dfrac{\vdash A[r/x], \Gamma}{\vdash r \in \{x : A\}, \Gamma} \quad \dfrac{\vdash B[r/x]^{\perp}, \Delta}{\vdash r \notin \{x : B\}, \Delta}}{\vdash s \neq t, \Gamma, \Delta}$$

where s and t are $\{x : A\}$ and $\{x : B\}$, respectively, which are trivially brought to the identical formula through $s \neq t$, but $A[r/x]$ and $B[r/x]$ are not substitutionally identical under $s \neq t$. In this case, we cannot reduce the cut to another cut whose cut formulas are $A[r/x]$ and $B[r/x]$ as before.

The above is an example of the cases where one of the cut formulas is an atomic formulas $r \in t$ or $r \notin t$ and the substitution of the whole term t by another term s is involved. This type of substitution distracts the correspondence between the way $s \in t$ or $s \notin t$ is created and the internal structure of t. Hence we first need to distinguish non-distractive applications of $(S \neq)$ from distractive ones.

Definition 5.3 *The substitution of the term s_1 by s_2 in an atomic formula $r \in s_1$ or $r \notin s_1$, resulting in $r \in s_2$ or $r \notin s_2$ respectively, is called irregular. Suppose that the two atomic formulas of the form $s \in t$ or $s \notin t$ are substituionally identical. If any irregular substitution is involved in making the two formulas identical, then the substitutional identity between them is irregular. Otherwise the substitutional identity is regular.*

The point of the above definition is that an atomic cut using $(\neq cut)$ is eliminable if the substitution identity involved in it is regular. We now give the symmetric and permutative reductions which are new for AZF.

5.4.1 Symmetric reductions

Symmetric reductions for $(\neq\ cut)$

$(*/I)$–$\neq$

$$\dfrac{\vdash A,\Gamma \quad \vdash {A'}^{\perp}, A'}{\vdash \theta, A', \Gamma} \leadsto \dfrac{\vdash A,\Gamma}{\vdash \theta, A', \Gamma}$$

$(*/\top)$–$\neq$

$$\dfrac{\vdash A,\Gamma \quad \vdash \top, {A'}^{\perp}, \Delta}{\vdash \theta, \top, \Gamma, \Delta} \leadsto \vdash \theta, \top, \Gamma, \Delta$$

$(S\neq/E)$–$\neq$

$$\dfrac{\dfrac{\vdash A,\Gamma}{\vdash s_1 \neq s_2, A[s_1/s_2], \Gamma} \quad \vdash s = s}{\vdash \theta, A[s_1/s_2], \Gamma} \leadsto \dfrac{\dfrac{\vdash A,\Gamma}{\vdash \theta, \theta, A[\theta_2][\theta_1], \Gamma}}{\vdash \theta, A[s_1/s_2], \Gamma}$$

where θ_1 and θ_2 are appropriate permutations of θ which make $s_2[\theta_2]$ identical to s and $s[\theta_1]$ identical to s_1, respectively. In other words, we first change A to $A[s/s_2]$ through θ_2, and then to $A[s/s_2][s_1/s]$ through θ_1, which is identical to $A[s_1/s_2]$.

$(\otimes/\parr)$–$\neq$

$$\dfrac{\dfrac{\vdash A,\Gamma \quad \vdash B,\Delta}{\vdash A\otimes B, \Gamma, \Delta} \quad \dfrac{\vdash {A'}^{\perp}, {B'}^{\perp}, \Theta}{\vdash {A'}^{\perp} \parr {B'}^{\perp}, \Theta}}{\vdash \theta, \Gamma, \Delta, \Theta} \leadsto \dfrac{\dfrac{\vdash B,\Delta \quad \dfrac{\vdash A,\Gamma \quad \vdash {A'}^{\perp}, {B'}^{\perp}, \Theta}{\vdash \theta, {B'}^{\perp}, \Gamma, \Theta}}{\vdash \theta, \theta, \Gamma, \Delta, \Theta}}{\vdash \theta, \Gamma, \Delta, \Theta}$$

$(\&/\oplus 1)$–$\neq$

$$\dfrac{\dfrac{\vdash A,\Gamma \quad \vdash B,\Gamma}{\vdash A \mathbin{\&} B, \Gamma} \quad \dfrac{\vdash {A'}^{\perp}, \Delta}{\vdash {A'}^{\perp} \oplus {B'}^{\perp}, \Delta}}{\vdash \theta, \Gamma, \Delta} \leadsto \dfrac{\vdash A,\Gamma \quad \vdash {A'}^{\perp}, \Delta}{\vdash \theta, \Gamma, \Delta}$$

$(\&/\oplus 2)$–$\neq$

$$\dfrac{\dfrac{\vdash A,\Gamma \quad \vdash B,\Gamma}{\vdash A \mathbin{\&} B, \Gamma} \quad \dfrac{\vdash {B'}^{\perp}, \Delta}{\vdash {A'}^{\perp} \oplus {B'}^{\perp}, \Delta}}{\vdash \theta, \Gamma, \Delta} \leadsto \dfrac{\vdash B,\Gamma \quad \vdash {B'}^{\perp}, \Delta}{\vdash \theta, \Gamma, \Delta}$$

$(\bigwedge S/\bigvee S)$–$\neq$

$$\dfrac{\dfrac{\vdash A,\Gamma}{\vdash \bigwedge \mathbf{x}.A, \Gamma} \quad \dfrac{\vdash A'[t/\mathbf{x}]^{\perp}, \Delta}{\vdash \bigvee \mathbf{x}.{A'}^{\perp}, \Delta}}{\vdash \theta, \Gamma, \Delta} \leadsto \dfrac{\vdash A[t/\mathbf{x}], \Gamma \quad \vdash A'[t/\mathbf{x}]^{\perp}, \Delta}{\vdash \theta, \Gamma, \Delta}$$

$(\bigwedge Z/\bigvee Z)$–$\neq$

$$\dfrac{\dfrac{\vdash A,\Gamma}{\vdash \bigwedge v.A,\Gamma} \quad \dfrac{\vdash A'[t/v]^{\perp},\Delta}{\vdash \bigvee v.A'^{\perp},\Delta}}{\vdash \theta,\Gamma,\Delta} \quad \leadsto \quad \dfrac{\vdash A[t/v],\Gamma \quad \vdash A'[t/v]^{\perp},\Delta}{\vdash \theta,\Gamma,\Delta}$$

$(\in S/\notin S)$–$\neq$

$$\dfrac{\dfrac{\vdash A[t/\mathbf{x}],\Gamma}{\vdash t\in\{\mathbf{x}:A\},\Gamma} \quad \dfrac{\vdash A'[t'/\mathbf{x}]^{\perp},\Delta}{\vdash t'\notin\{\mathbf{x}:A'\},\Delta}}{\vdash \theta,\Gamma,\Delta} \quad \leadsto \quad \dfrac{\vdash A[t/\mathbf{x}],\Gamma \quad \vdash A'[t'/\mathbf{x}]^{\perp},\Delta}{\vdash \theta,\Gamma,\Delta}$$

where the substitutional identity under θ is regular.

$(\in Z/\notin Z)$–$\neq$

$$\dfrac{\dfrac{\vdash A[t/v],\Gamma}{\vdash t\in\{v:A\},\Gamma} \quad \dfrac{\vdash A'[t'/v]^{\perp},\Delta}{\vdash t'\notin\{v:A'\},\Delta}}{\vdash \theta,\Gamma,\Delta} \quad \leadsto \quad \dfrac{\vdash A[t/v],\Gamma \quad \vdash A'[t'/v]^{\perp},\Delta}{\vdash \theta,\Gamma,\Delta}$$

where the substitutional identity under θ is regular.

$(RS\neq/*)$–$\neq$

$$\dfrac{\dfrac{\vdash A,\Gamma}{\vdash A[\eta],\eta,\Gamma} \quad \vdash A',\Delta}{\vdash \theta,\eta,\Gamma,\Delta} \quad \leadsto \quad \dfrac{\vdash A,\Gamma \quad \vdash A',\Delta}{\vdash \theta,\eta,\Gamma,\Delta}$$

$(W/*)$–$\neq$

$$\dfrac{\dfrac{\vdash \Gamma}{\vdash A,\Gamma} \quad \vdash A'^{\perp},\Delta}{\vdash \theta,\Gamma,\Delta} \quad \leadsto \quad \dfrac{\vdash \Gamma}{\vdash \theta,\Gamma,\Delta}$$

Symmetric reductions for $(?\neq cut)$

$(*/RS\neq)$

$$\dfrac{\vdash (C_i)^k,\Gamma \quad \dfrac{\vdash C'^{\perp},\Delta}{\vdash \xi, C'[\xi]^{\perp},\Delta}}{\vdash (\theta_i)^k,\xi,\Gamma,\Delta} \quad \leadsto \quad \dfrac{\dfrac{\vdash (C_i)^k,\Gamma \quad \vdash C'^{\perp},\Delta}{\vdash (\theta_i*\xi)^k,\Gamma,\Delta}}{\vdash (\theta_i)^k,\xi,\Gamma,\Delta}$$

where $\theta_i * \xi$ is the concatenation of θ_i and ξ.

$(D?/!)$–$?\neq$

$$\dfrac{\dfrac{\vdash A,\Gamma}{\vdash ?A,\Gamma} \quad \dfrac{\vdash A'^{\perp}, ?\Delta}{\vdash !A'^{\perp}, ?\Delta}}{\vdash (\theta_i)^{k+1}, \Gamma^-, ?\Delta} \quad \rightsquigarrow \quad \dfrac{\dfrac{\dfrac{\vdash A,\Gamma \quad \vdash !A'^{\perp}, ?\Delta}{\vdash (\theta_i)^k, A, \Gamma^-, ?\Delta} \quad \vdash A^{\perp}, ?\Delta}{\vdash (\theta_i)^{k+1},\Gamma^-,?\Delta,?\Delta}}{\vdash (\theta_i)^{k+1},\Gamma^-,?\Delta}$$

where Γ^- is the result of removing some of the formula occurrences from Γ which are cut out.

$(C?/!)$–$?\neq$

$$\dfrac{\dfrac{\vdash ?A,\Gamma}{\vdash \Gamma} \quad \vdash !A^{\perp}, ?\Delta}{\vdash (\theta_i)^k,\Gamma^-,?\Delta} \quad \rightsquigarrow \quad \dfrac{\dfrac{\vdash ?A,\Gamma \quad \vdash A^{\perp},?\Delta}{\vdash (\theta_i)^{k+1},\Gamma^-,?\Delta}}{\vdash(\theta_i)^k,\Gamma^-,?\Delta}$$

$(RS\neq/!)$–$?\neq$

$$\dfrac{\dfrac{\vdash ?A,\Gamma}{\vdash \xi, ?A[\xi],\Gamma} \quad \vdash !A'^{\perp},?\Delta}{\vdash \xi,(\theta_i)^{k+1},\Gamma^-,?\Delta} \quad \rightsquigarrow \quad \dfrac{\vdash ?A,\Gamma \quad \vdash !A'^{\perp},?\Delta}{\vdash (\theta_i)^k,\theta_{k+1},\xi,\Gamma^-,?\Delta}$$

$(C\neq/E)$–$?\neq$

$$\dfrac{\dfrac{\vdash s\neq t,\Gamma}{\vdash\Gamma}\quad \vdash r=r}{\vdash(\theta_i)^k,\Gamma^-} \quad \rightsquigarrow \quad \dfrac{\dfrac{\vdash s\neq t,\Gamma \quad \vdash r=r}{\vdash(\theta_i)^k,\theta_{k+1},\Gamma^-,\Delta}}{\vdash(\theta_i)^k,\Gamma^-,\Delta}$$

$(RS\neq/E1)$–$?\neq$

$$\dfrac{\dfrac{\vdash A,\Gamma}{\vdash\eta,A[\eta],\Gamma}\quad\vdash s=s}{\vdash \eta^-,(\theta_i)^k,(\xi_i)^l,A[\eta],\Gamma^-} \quad \rightsquigarrow \quad \dfrac{\dfrac{\dfrac{\vdash A,\Gamma\quad\vdash s=s}{\vdash(\theta_i)^k,A,\Gamma^-}}{\vdash\eta^-,(\xi_i)^l,(\xi_i)^l,(\theta_i)^k,A[\eta],\Gamma^-}}{\vdash\eta^-,(\theta_i)^k,(\xi_i)^l,A[\eta],\Gamma^-}$$

This reduction is justified for the same reason as $(S\neq/E)$–$?\neq$, *i.e*, instead of using $s_1\neq s_2$ in η for substitution, we first change s_2 to s and then to s_1 by using one of ξ_i twice.

$(RS\neq/E2)$–$?\neq$

$$\dfrac{\dfrac{\vdash s\neq t,\Gamma}{\vdash\eta,s[\eta]\neq t[\eta],\Gamma}\quad\vdash r=r}{\vdash\eta^-,(\theta_i)^{k+1},(\xi_i)^l,\Gamma^-} \quad \rightsquigarrow \quad \dfrac{\dfrac{\vdash s\neq t,\Gamma\quad\vdash r=r}{\vdash(\theta_i)^k,\theta_k,\eta^-,(\xi_i)^l,(\xi_i)^l,\Gamma^-}}{\vdash(\theta_i)^{k+1},(\xi_i)^l,\eta^-,\Gamma^-}$$

where $t[\eta] \neq r[\eta]$ is cut out. This reduction is justified for the same reason as $(RS \neq /E1)$–$? \neq$.

$(\neq cut/E)$–$? \neq$

$$\dfrac{\dfrac{\vdash A, \Gamma \quad \vdash A'^{\perp}, \Delta}{\vdash \eta, \Gamma, \Delta} \quad \vdash s = s}{\vdash \eta^-, (\theta_i)^k, (\xi_i)^l, ({\xi'}_i)^m, \Gamma^-, \Delta^-} \leadsto \dfrac{\dfrac{\dfrac{\vdash A, \Gamma \quad \vdash s = s}{\vdash (\xi_i)^l, A, \Gamma^-} \quad \dfrac{\vdash A'^{\perp}, \Delta \quad \vdash s = s}{\vdash ({\xi'}_i)^m, A'^{\perp}, \Delta^-}}{\vdash \eta^-, (\theta_i)^k, (\theta_i)^k, (\xi_i)^l, ({\xi'}_i)^m, \Gamma^-, \Delta^-}}{\vdash \eta^-, (\theta_i)^k, (\xi_i)^l, ({\xi'}_i)^m, \Gamma^-, \Delta^-}$$

When none of the formula occurrences in Γ or Δ are cut out, we do not need to use a cut on that branch. The reduction is justified for the same reason as before.

$(? \neq cut/E)$–$? \neq$

$$\dfrac{\dfrac{\vdash (C_i)^k, \Gamma \quad \vdash C^{\perp}, \Delta}{\vdash (\eta_i)^k, \Gamma, \Delta} \quad \vdash s = s}{\vdash (\eta_i^-)^k, (\theta_i)^{k'}, (\xi_i)^l, ({\xi'}_i)^m, \Gamma^-, \Delta^-} \leadsto \dfrac{\dfrac{\dfrac{\vdash (C_i)^k, \Gamma \quad \vdash s = s}{\vdash (\xi_i)^m, (C_i)^k, \Gamma^-} \quad \dfrac{\vdash C^{\perp}, \Delta \quad \vdash s = s}{\vdash ({\xi'}_i)^m, C^{\perp}, \Delta^-}}{\vdash (\eta_i^-)^k, (\theta_i)^{k'}, (\theta_i)^{k'}, (\xi_i)^l, ({\xi'}_i)^m, \Gamma^-, \Delta^-}}{\vdash (\eta_i^-)^k, (\theta_i)^{k'}, (\xi_i)^l, ({\xi'}_i)^m, \Gamma^-, \Delta^-}$$

When none of the formula occurrences in η, Γ or Δ are cut out, we do not need to use a cut on that branch. The reduction is justified for the same reason as before.

$(W/*)$–$? \neq$

$$\dfrac{\dfrac{\vdash \Gamma}{\vdash C, \Gamma} \quad \vdash C'^{\perp}, \Delta}{\vdash (\theta_i)^{k+l}, \Gamma^-, \Delta} \leadsto \dfrac{\dfrac{\vdash \Gamma \quad \vdash C^{\perp}, \Delta}{\vdash (\theta_i)^k, \Gamma^-, \Delta}}{\vdash (\theta_i)^{k+l}, \Gamma^-, \Delta}$$

Permutative reductions for $(\neq cut)$

$(\neq cut/\otimes)$

$$\dfrac{\vdash C, \Gamma \quad \dfrac{\vdash A, C'^{\perp}, \Delta \quad \vdash B, \Theta}{\vdash A \otimes B, C'^{\perp}, \Delta, \Theta}}{\vdash \theta, A \otimes B, \Gamma, \Delta, \Theta} \leadsto \dfrac{\dfrac{\vdash C, \Gamma \quad \vdash A, C'^{\perp}, \Delta}{\vdash \theta, A, \Gamma, \Delta} \quad \vdash B, \Theta}{\vdash \theta, A \otimes B, \Gamma, \Delta, \Theta}$$

$(\neq cut/⅋)$

$$\dfrac{\vdash C, \Gamma \quad \dfrac{\vdash A, B, C'^{\perp}, \Delta}{\vdash A ⅋ B, C'^{\perp}, \Delta}}{\vdash \theta, A ⅋ B, \Gamma, \Delta} \leadsto \dfrac{\dfrac{\vdash C, \Gamma \quad \vdash A, B, C'^{\perp}, \Delta}{\vdash \theta, A, B, \Gamma, \Delta}}{\vdash \theta, A ⅋ B, \Gamma, \Delta}$$

$(\neq cut/\&)$

$$\dfrac{\vdash C, \Gamma \quad \dfrac{\vdash A, C'^{\perp}, \Delta \quad \vdash B, C'^{\perp}, \Delta}{\vdash A \& B, C'^{\perp}, \Delta}}{\vdash \theta, A \& B, \Gamma, \Delta} \leadsto \dfrac{\dfrac{\vdash C, \Gamma \quad \vdash A, C'^{\perp}, \Delta}{\vdash \theta, A, \Gamma, \Delta} \quad \dfrac{\vdash C, \Gamma \quad \vdash B, C'^{\perp}, \Delta}{\vdash \theta, B, \Gamma, \Delta}}{\vdash \theta, A \& B, \Gamma, \Delta}$$

$(\neq cut/\oplus 1)$

$$\dfrac{\vdash C, \Gamma \quad \dfrac{\vdash A, C'^{\perp}, \Delta}{\vdash A \oplus B, C'^{\perp}, \Delta}}{\vdash \theta, A \oplus B, \Gamma, \Delta} \leadsto \dfrac{\dfrac{\vdash C, \Gamma \quad \vdash A, C'^{\perp}, \Delta}{\vdash \theta, A, \Gamma, \Delta}}{\vdash \theta, A \oplus B, \Gamma, \Delta}$$

$(\neq cut/\oplus 2)$

$$\dfrac{\vdash C, \Gamma \quad \dfrac{\vdash B, C'^{\perp}, \Delta}{\vdash A \oplus B, C'^{\perp}, \Delta}}{\vdash \theta, A \oplus B, \Gamma, \Delta} \leadsto \dfrac{\dfrac{\vdash C, \Gamma \quad \vdash B, C'^{\perp}, \Delta}{\vdash \theta, B, \Gamma, \Delta}}{\vdash \theta, A \oplus B, \Gamma, \Delta}$$

$(\neq cut/\bigwedge S)$

$$\dfrac{\vdash C, \Gamma \quad \dfrac{\vdash A, C'^{\perp}, \Delta}{\vdash \bigwedge \mathbf{x}.A, C'^{\perp}, \Delta}}{\vdash \theta, \bigwedge \mathbf{x}.A, \Gamma, \Delta} \leadsto \dfrac{\dfrac{\vdash C, \Gamma \quad \vdash A[\mathbf{y}/\mathbf{x}], C'^{\perp}, \Delta}{\vdash \theta, A[\mathbf{y}/\mathbf{x}], \Gamma, \Delta}}{\vdash \theta, \bigwedge \mathbf{y}.A, \Gamma, \Delta}$$

$(\neq cut/\bigvee S)$

$$\dfrac{\vdash C, \Gamma \quad \dfrac{\vdash A[s/\mathbf{x}], C'^{\perp}, \Delta}{\vdash \bigvee \mathbf{x}.A, C'^{\perp}, \Delta}}{\vdash \theta, \bigvee \mathbf{x}.A, \Gamma, \Delta} \leadsto \dfrac{\dfrac{\vdash C, \Gamma \quad \vdash A[s/\mathbf{x}], C'^{\perp}, \Delta}{\vdash \theta, A[s/\mathbf{x}], \Gamma, \Delta}}{\vdash \theta, \bigvee \mathbf{x}.A, \Gamma, \Delta}$$

$(\neq cut/\bigwedge Z)$

$$\dfrac{\vdash C, \Gamma \quad \dfrac{\vdash A, C'^{\perp}, \Delta}{\vdash \bigwedge v.A, C'^{\perp}, \Delta}}{\vdash \theta, \bigwedge v.A, \Gamma, \Delta} \leadsto \dfrac{\dfrac{\vdash C, \Gamma \quad \vdash A[u/v], C'^{\perp}, \Delta}{\vdash \theta, A[u/v], \Gamma, \Delta}}{\vdash \theta, \bigwedge u.A, \Gamma, \Delta}$$

$(\neq cut/\bigvee Z)$

$$\dfrac{\vdash C, \Gamma \quad \dfrac{\vdash A[t/v], C'^{\perp}, \Delta}{\vdash \bigvee v.A, C'^{\perp}, \Delta}}{\vdash \theta, \bigvee v.A, \Gamma, \Delta} \leadsto \dfrac{\dfrac{\vdash C, \Gamma \quad \vdash A[t/v], C'^{\perp}, \Delta}{\vdash \theta, A[t/v], \Gamma, \Delta}}{\vdash \theta, \bigvee v.A, \Gamma, \Delta}$$

$(\neq cut/\in S)$

$$\dfrac{\vdash C,\Gamma \quad \dfrac{\vdash A[t/\mathbf{x}], {C'}^{\perp}, \Delta}{\vdash t \in \{\mathbf{x} : A\}, {C'}^{\perp}, \Delta}}{\vdash \theta, t \in \{\mathbf{x} : A\}, \Gamma, \Delta} \quad \leadsto \quad \dfrac{\dfrac{\vdash C,\Gamma \quad \vdash A[t/\mathbf{x}], {C'}^{\perp}, \Delta}{\vdash \theta, A[t/\mathbf{x}], \Gamma, \Delta}}{\vdash \theta, t \in \{\mathbf{x} : A\}, \Gamma, \Delta}$$

$(\neq cut/\notin S)$

$$\dfrac{\vdash C,\Gamma \quad \dfrac{\vdash A[t/\mathbf{x}]^{\perp}, {C'}^{\perp}, \Delta}{\vdash t \notin \{\mathbf{x} : A\}, {C'}^{\perp}, \Delta}}{\vdash \theta, t \notin \{\mathbf{x} : A\}, \Gamma, \Delta} \quad \leadsto \quad \dfrac{\dfrac{\vdash C,\Gamma \quad \vdash A[t/\mathbf{x}]^{\perp}, {C'}^{\perp}, \Delta}{\vdash \theta, A[t/\mathbf{x}]^{\perp}, \Gamma, \Delta}}{\vdash \theta, t \notin \{\mathbf{x} : A\}, \Gamma, \Delta}$$

$(\neq cut/=E)$

$$\dfrac{\vdash C,\Gamma \quad \dfrac{\vdash u \in s, u \notin t, {C'}^{\perp}, \Delta \quad \vdash v \notin s, v \in t, \Pi}{\vdash s = t, {C'}^{\perp}, \Delta, \Pi}}{\vdash \theta, s = t, \Gamma, \Delta, \Pi} \quad \leadsto \quad \dfrac{\dfrac{\vdash C,\Gamma \quad \vdash u \in s, u \notin t, {C'}^{\perp}, \Delta}{\vdash \theta, u \in s, u \notin t, \Gamma, \Delta} \quad \vdash v \notin s, v \in t, \Pi}{\vdash s = t, \theta, \Gamma, \Delta, \Pi}$$

$(\neq cut/RS\neq)$

$$\dfrac{\vdash C,\Gamma \quad \dfrac{\vdash A, {C'}^{\perp}, \Delta}{\vdash \eta, A[\eta], {C'}^{\perp}, \Delta}}{\vdash \theta, \eta, A[\eta], \Gamma, \Delta} \quad \leadsto \quad \dfrac{\dfrac{\vdash C,\Gamma \quad \vdash {C'}^{\perp}, A, \Delta}{\vdash \theta, A, \Gamma, \Delta}}{\vdash \theta, \eta, A[\eta], \Gamma, \Delta}$$

$(\neq cut/D?)$

$$\dfrac{\vdash C,\Gamma \quad \dfrac{\vdash A, {C'}^{\perp}, \Delta}{\vdash\, ?A, {C'}^{\perp}, \Delta}}{\vdash \theta,\, ?A, \Gamma, \Delta} \quad \leadsto \quad \dfrac{\dfrac{\vdash C,\Gamma \quad \vdash A, {C'}^{\perp}, \Delta}{\vdash \theta, A, \Gamma, \Delta}}{\vdash \theta,\, ?A, \Gamma, \Delta}$$

$(\neq cut/C?)$

$$\dfrac{\vdash C,\Gamma \quad \dfrac{\vdash\, ?A,\, ?A, {C'}^{\perp}, \Delta}{\vdash\, ?A, {C'}^{\perp}, \Delta}}{\vdash \theta,\, ?A, \Gamma, \Delta} \quad \leadsto \quad \dfrac{\dfrac{\vdash C,\Gamma \quad \vdash\, ?A,\, ?A, {C'}^{\perp}, \Delta}{\vdash \theta,\, ?A,\, ?A, \Gamma, \Delta}}{\vdash \theta,\, ?A, \Gamma, \Delta}$$

$(\neq cut/C\neq)$

$$\dfrac{\vdash C,\Gamma \quad \dfrac{\vdash s \neq t, s \neq t, {C'}^{\perp}, \Delta}{\vdash s \neq t, {C'}^{\perp}, \Delta}}{\vdash \theta, s \neq t, \Gamma, \Delta} \quad \leadsto \quad \dfrac{\dfrac{\vdash C,\Gamma \quad \vdash s \neq t, s \neq t, {C'}^{\perp}, \Delta}{\vdash \theta, s \neq t, s \neq t, \Gamma, \Delta}}{\vdash \theta, s \neq t, \Gamma, \Delta}$$

$(\neq cut/W)$

$$\dfrac{\vdash C,\Gamma \qquad \dfrac{\vdash {C'}^{\perp},\Delta}{\vdash A,{C'}^{\perp},\Delta}}{\vdash \theta,A,\Gamma,\Delta} \rightsquigarrow \dfrac{\dfrac{\vdash C,\Gamma \quad \vdash {C'}^{\perp},\Delta}{\vdash \theta,\Gamma,\Delta}}{\vdash \theta,A,\Gamma,\Delta}$$

$(\neq cut/\neq cut)$

$$\dfrac{\vdash C,\Gamma \qquad \dfrac{\vdash A,{C'}^{\perp},\Delta \quad \vdash {A'}^{\perp},\Theta}{\vdash \eta,{C'}^{\perp},\Delta,\Theta}}{\vdash \theta,\eta,\Gamma,\Delta,\Theta} \rightsquigarrow \dfrac{\dfrac{\vdash C,\Gamma \quad \vdash A,{C'}^{\perp},\Delta}{\vdash \theta,A,\Gamma,\Delta} \qquad \vdash {A'}^{\perp},\Theta}{\vdash \theta,\eta,\Gamma,\Delta,\Theta}$$

$(\neq cut/?\neq cut1)$

$$\dfrac{\vdash C,\Gamma \qquad \dfrac{\vdash (D_i)^k,{C'}^{\perp},\Delta \quad \vdash D^{\perp},\Theta}{\vdash (\eta_i)^k,{C'}^{\perp},\Delta,\Theta}}{\vdash \theta,(\eta_i)^k,\Gamma,\Delta,\Theta} \rightsquigarrow \dfrac{\dfrac{\vdash C,\Gamma \quad \vdash (D_i)^k,{C'}^{\perp},\Delta}{\vdash \theta,(D_i)^k,\Gamma,\Delta} \qquad \vdash D^{\perp},\Theta}{\vdash (\eta_i)^k,\theta,\Gamma,\Delta,\Theta}$$

$(\neq cut/?\neq cut2)$

$$\dfrac{\vdash C,\Gamma \qquad \dfrac{\vdash (D_i)^k,\Delta \quad \vdash D^{\perp},{C'}^{\perp},\Theta}{\vdash (\eta_i)^k,{C'}^{\perp},\Delta,\Theta}}{\vdash \theta,(\eta_i)^k,\Gamma,\Delta,\Theta} \rightsquigarrow \dfrac{\dfrac{\vdash C,\Gamma \quad \vdash D^{\perp},{C'}^{\perp},\Theta}{\vdash \theta,D^{\perp},\Gamma,\Theta} \qquad \vdash (D_i)^k,\Delta}{\vdash \theta,(\eta_i)^k,\Gamma,\Delta,\Theta}$$

Permutative reductions for $(?\neq cut)$ on !–branch

They are entirely similar to the permutative reductions for $(\neq cut)$ with $(\theta_i)^k$ instead of θ.

Permutative reductions for $(?\neq cut)$ on ?–branch

They are also similar to the permutative reductions for $(\neq cut)$. Hence we only give the rules which are new to $(?\neq cut)$. As before, we only consider the cases where the cut formula C is the main formula on the right branch.

$(!/?\neq cut1)$

$$\dfrac{\dfrac{\vdash A,(s_i\neq t_i)^k,?\Gamma}{\vdash\ !A,(s_i\neq t_i)^k,?\Gamma} \qquad \vdash s=s}{\vdash\ !A,(\theta_i)^k,?\Gamma} \rightsquigarrow \dfrac{\dfrac{\vdash A,(s_i\neq t_i)^k,?\Gamma \quad \vdash s=s}{\vdash A,(\theta_i)^k,?\Gamma}}{\vdash\ !A,(\theta_i)^k,?\Gamma}$$

$(!/? \neq cut2)$

$$\dfrac{\dfrac{\vdash A,\ ?\,\Gamma}{\vdash\ !A,\ ?\,\Gamma} \qquad \dfrac{\vdash C^{\perp},\ ?\,\Delta}{\vdash\ !C^{\perp},\ ?\,\Delta}}{\vdash\ !A, (\theta_i)^k,\ ?\,\Gamma^{-},\ ?\,\Delta} \;\rightsquigarrow\; \dfrac{\dfrac{\vdash A,\ ?\,\Gamma \quad \vdash\ !C^{\perp},\ ?\,\Delta}{\vdash A, (\theta_i)^k,\ ?\,\Gamma^{-},\ ?\,\Delta}}{\vdash\ !A, (\theta_i)^k,\ ?\,\Gamma^{-},\ ?\,\Delta}$$

$(\otimes/? \neq cut1)$–?

$$\dfrac{\dfrac{\vdash A, \Gamma \quad \vdash B, \Delta}{\vdash A \otimes B, \Gamma, \Delta} \qquad \vdash s = s}{\vdash A \otimes B, (\theta_i)^k, (\xi_i)^l, \Gamma^{-}, \Delta^{-}} \;\rightsquigarrow\; \dfrac{\dfrac{\vdash A, \Gamma \quad \vdash s = s}{\vdash A, (\theta_i)^k, \Gamma^{-}} \qquad \dfrac{\vdash B, \Delta \quad \vdash s = s}{\vdash B, (\xi_i)^l, \Delta^{-}}}{\vdash A \otimes B, (\theta_i)^k, (\xi_i)^l, \Gamma^{-}, \Delta^{-}}$$

$(\otimes/? \neq cut2)$–?

$$\dfrac{\dfrac{\vdash A, \Gamma \quad \vdash B, \Delta}{\vdash A \otimes B, \Gamma, \Delta} \qquad \dfrac{\vdash C^{\perp},\ ?\,\Theta}{\vdash\ !C^{\perp},\ ?\,\Theta}}{\vdash A \otimes B, (\theta_i)^k, (\xi_i)^l, \Gamma^{-}, \Delta^{-},\ ?\,\Theta} \;\rightsquigarrow\; \dfrac{\dfrac{\dfrac{\vdash A, \Gamma \quad \vdash C^{\perp},\ ?\,\Theta}{\vdash A, (\theta_i)^k, \Gamma^{-},\ ?\,\Theta} \qquad \dfrac{\vdash B, \Delta \quad \vdash C^{\perp},\ ?\,\Theta}{\vdash B, (\xi_i)^l, \Delta^{-},\ ?\,\Theta}}{\vdash A \otimes B, (\theta_i)^k, (\xi_i)^l, \Gamma^{-}, \Delta^{-},\ ?\,\Theta,\ ?\,\Theta}}{\vdash A \otimes B, (\theta_i)^k, (\xi_i)^l, \Gamma^{-}, \Delta^{-},\ ?\,\Theta}$$

$(\neq cut/? \neq cut1)$–?

$$\dfrac{\dfrac{\vdash A, \Gamma \quad \vdash A'^{\perp}, \Delta}{\vdash \eta, \Gamma, \Delta} \qquad \vdash s = s}{\vdash \eta, (\theta_i)^k, (\xi_i)^l, \Gamma^{-}, \Delta^{-}} \;\rightsquigarrow\; \dfrac{\dfrac{\vdash A, \Gamma \quad \vdash s = s}{\vdash A, (\theta_i)^k, \Gamma^{-}} \qquad \dfrac{\vdash A'^{\perp}, \Delta \quad \vdash s = s}{\vdash A'^{\perp}, (\xi_i)^l, \Delta^{-}}}{\vdash \eta, (\theta_i)^k, (\xi_i)^l, \Gamma^{-}, \Delta^{-}}$$

$(\neq cut/? \neq cut2)$–?

$$\dfrac{\dfrac{\vdash A, \Gamma \quad \vdash A'^{\perp}, \Delta}{\vdash \eta, \Gamma, \Delta} \qquad \dfrac{\vdash C^{\perp},\ ?\,\Theta}{\vdash\ !C^{\perp},\ ?\,\Theta}}{\vdash \eta, (\theta_i)^k, (\xi_i)^l, \Gamma^{-}, \Delta^{-},\ ?\,\Theta} \;\rightsquigarrow\; \dfrac{\dfrac{\dfrac{\vdash A, \Gamma \quad \vdash\ !C^{\perp},\ ?\,\Theta}{\vdash A, (\theta_i)^k, \Gamma^{-},\ ?\,\Theta} \qquad \dfrac{\vdash A'^{\perp}, \Delta \quad \vdash\ !C^{\perp},\ ?\,\Theta}{\vdash A'^{\perp}, (\xi_i)^l, \Delta^{-},\ ?\,\Theta}}{\vdash \eta, (\theta_i)^k, (\xi_i)^l, \Gamma^{-}, \Delta^{-},\ ?\,\Theta,\ ?\,\Theta}}{\vdash \eta, (\theta_i)^k, (\xi_i)^l, \Gamma^{-}, \Delta^{-},\ ?\,\Theta}$$

$(? \neq cut/? \neq cut1)$–?

$$\dfrac{\dfrac{\vdash (D_j)^m, \Gamma \quad \vdash D^{\perp}, \Delta}{\vdash (\eta_i)^m, \Gamma, \Delta} \qquad \vdash s = s}{\vdash (\eta_i)^m, (\theta_i)^k, (\xi_i)^l, \Gamma^{-}, \Delta^{-}} \;\rightsquigarrow\; \dfrac{\dfrac{\vdash (D_j)^m, \Gamma \quad \vdash s = s}{\vdash (D_j)^m, (\theta_i)^k, \Gamma^{-}} \qquad \dfrac{\vdash D^{\perp}, \Delta \quad \vdash s = s}{\vdash D^{\perp}, (\xi_i)^l, \Delta^{-}}}{\vdash (\eta_i)^m, (\theta_i)^k, (\xi_i)^l, \Gamma^{-}, \Delta^{-}}$$

$(? \neq cut/? \neq cut2)$–?

$$\dfrac{\dfrac{\vdash (D_j)^m, \Gamma \quad \vdash D^\perp, \Delta}{\vdash (\eta_i)^m, \Gamma, \Delta} \quad \dfrac{\vdash C^\perp, ?\,\Theta}{\vdash\, !C^\perp, ?\,\Theta}}{\vdash (\eta_i)^m, (\theta_i)^k, (\xi_i)^l, \Gamma^-, \Delta^-, ?\,\Theta} \quad \leadsto \quad \dfrac{\dfrac{\dfrac{\vdash (D_j)^m, \Gamma \quad \vdash\, !C^\perp, ?\,\Theta}{\vdash (D_j)^m, (\theta_i)^k, \Gamma^-, ?\,\Theta} \quad \dfrac{\vdash D^\perp, \Delta \quad \vdash\, !C^\perp, ?\,\Theta}{\vdash D^\perp, (\xi_i)^l, \Delta^-, ?\,\Theta}}{\vdash (\eta_i)^m, (\theta_i)^k, (\xi_i)^l, \Gamma^-, \Delta^-, ?\,\Theta, ?\,\Theta}}{\vdash (\eta_i)^m, (\theta_i)^k, (\xi_i)^l, \Gamma^-, \Delta^-, ?\,\Theta}$$

5.5 The cut-elimination for AZF

The equality relation creates new complexities in the cut-elimination process of AZF. In particular, there are two novel features.

First, the elimination of atomic cuts over equations increases the size of a proof. This is due to the contraction of equations $(C \neq)$ and the duplication of the substitution θ involved in the symmetric reduction $(S \neq /E)$.

Secondly, some of the non-eliminable cuts with irregular substitutions may become eliminable after the elimination of atomic cuts over equalities, since it may remove the irregular substitutions which previously blocked the cut-elimination.

Those two features imply that we can no longer use the simple induction on the size to prove the termination of the cut-elimination process. The second feature requires that the elimination of atomic cuts over $s \in t$ be interwoven with the elimination of atomic cuts over $s = t$, and this whole process increases the size of a proof due to the first feature.

Fortunately, however, we do not need to change the basic idea of our previous method. We only need to examine carefully what is really necessary for proving the cut-elimination, and refine the method accordingly.

Note that the elimination of cuts over complex formulas can always proceed by the induction on the degree of formula complexity. The induction on the size was necessary to take care of the elimination of the atomic cuts over $s \in t$, or the symmetric reduction $(S \in /S \notin)$. Then the only thing we need to do is to find a measure which decreases at each application of $(S \in /S \notin)$ and does not increase in the elimination of cuts over complex formulas.

Indeed, such a measure is easy to find, *i.e.*, the number of applications of comprehension rules $(S \in)$ and $(S \notin)$. Surely, the same kind of care is needed for the use of this idea as for the definition of the size, because of the additive conjunction. Therefore, we will call this new measure *abstraction weight* , to distinguish it from the simple total sum.

5.5.1 The definition of abstraction weight

We start by extending the definitions of size and abstraction depth for AZF. They are entirely straightforward.

Definition 5.4 *The size $\sigma(\pi)$ of a proof π is defined in the same way as before with the following additional clauses:*

- *If π if obtained from τ by one of $(S \neq)$, $(RS \neq)$ or $(C \neq)$, then $\sigma(\pi) =_{def} \sigma(\tau) + 1$*
- *If π is obtained from π_1 and π_2 by $(\neq cut)$ or $(? \neq cut)$, then $\sigma(\pi) =_{def} \sigma(\pi_1) + \sigma(\pi_2)$*

Definition 5.5 *the abstraction depth $\delta(A)$ of a formula occurrence A is defined in the same way as before with the following additional rules:*

$$(S \neq) \ \frac{\vdash i, \overline{p}}{\vdash 0, i, \overline{p}} \qquad (RS \neq) \ \frac{\vdash i, \overline{p}}{\vdash 0, \ldots 0, i, \overline{p}}$$

$$(W) \ \frac{\vdash \overline{p}}{\vdash 0, \overline{p}} \qquad (C \neq) \ \frac{\vdash i, j, \overline{p}}{\vdash \rho(i,j), \overline{p}}$$

$$(\neq cut) \ \frac{\vdash i, \overline{p} \quad \vdash j, \overline{q}}{\vdash 0, \overline{p}, \overline{q}} \ (i, j)$$

$$(? \neq cut) \ \frac{\vdash i_1, \ldots, i_k, \overline{p} \quad \vdash j, \overline{q}}{\vdash 0, \ldots 0, \overline{p}, \overline{q}} \ \rho(i_1, \ldots, i_k, j)$$

Finally, we define the abstraction weight $\lambda(\pi)$ of a proof π, which is essentially the total number of the applications of comprehension rules $(S \in)$ and $(S \not in)$ in π.

Definition 5.6 *The abstraction weight $\lambda(\pi)$ of a proof π is defined inductively as follows:*

- *If π is an axiom, then $\lambda(\pi) =_{def} 0$*
- *If π is obtained from τ by one of the one-premiss rules other than $(S \in)$ and $(S \notin)$, then $\lambda(\pi) =_{def} \lambda(\tau)$*
- *If π is obtained from τ by one of $(S \in)$ and $(S \notin)$, then $\lambda(\pi) =_{def} \lambda(\tau) + 1$*
- *If π is obtained from π_1 and π_2 by one of $(\otimes)$, $(= E)$, $(\neq cut)$ and $(? \neq cut)$, then $\lambda(\pi) =_{def} \lambda(\pi_1) + \lambda(\pi_2)$*
- *If π is obtained from π_1 and π_2 by $(\&)$, then $\lambda(\pi) =_{def} max(\lambda(\pi_1), \lambda(\pi_2))$.*

5.5.2 The elimination of non-atomic cuts

We first eliminate all the cuts over non-Z complex formulas by the induction on the degree.

Lemma 5.7 *Consider the proof π*

$$\dfrac{\dfrac{\vdots\pi_1}{\vdash (\,?\,C_i)^k, \Gamma} \quad \dfrac{\vdots\pi_2}{\vdash\, !\,C'^{\perp}, \Delta}}{\vdash (\theta_i)^k, \Gamma, \Delta}$$

where the degrees of the proofs π_1 and π_2 are strictly less than the degree $\partial(\,?\,C_i)$ of the cut formulas $?\,C_i$. Then π reduces to a proof τ such that the degree of τ is strictly less than the degree of the cut formulas.

Proof

The proof is by induction on the size of a proof, and essentially the same as before.

Case 1 Either π_1 or π_2 is an axiom $(\top)$. Then π reduces to another $(\top)$.

Case 2 One of the permutative reductions is applicable. Then we perform it and use the inductive hypothesis.

Case 3 One of the symmetric reductions $(C?/*)$–$? \neq$, $(RS \neq /!)$–$? \neq$ and $(*/RS \neq)$–$? \neq$ is applicable. Then we perform it and use the inductive hypothesis since the size is reduced by the reduction.

Case 4 The symmetric reduction $(D?/!)$–$? \neq$ is applicable. Then we perform it and use the inductive hypothesis to the upper cut. The degree is the cut formula of the lower cut is already decreased.

Case 5 The symmetric reduction $(W/*)$–$? \neq$ is applicable. Then we simply perform the reduction.

∎

Lemma 5.8 *Consider the proof π*

$$\dfrac{\dfrac{\vdots\pi_1}{\vdash A, \Gamma} \quad \dfrac{\vdots\pi_2}{\vdash A'^{\perp}, \Delta}}{\vdash (\theta_i)^k, \Gamma, \Delta}$$

where the degrees of the proofs π_1 and π_2 is strictly less than the degree $\sigma(A)$ of the cut formulas. Furthermore $\sigma(A)$ is strictly greater than 1, but neither of A or ${A'}^{\perp}$ is of the form $?C$. Then π reduces to a proof τ such that the degree of τ is strictly less than **A** *and the abstraction weight $\lambda(\tau)$ is less than or equal to $\lambda(\pi)$.*

Proof

The proof is by induction on the size of a proof as before. We only note that no new application of $(S \in)$ or $(S \notin)$ is created and the abstraction weight never increases in the relevant permutative and symmetric reductions since we take the maximum for the permutations with the additives. ∎

From them, we can obtain the cut-elimination as before.

Corollary 5.9 *Let π be a proof whose degree is strictly greater than 1. Then π reduces to a proof τ such that the degree of τ is strictly less than the degree of π.*

Proof

By induction on the size of a proof as before. ∎

Corollary 5.10 *For any proof π, there exists a proof τ such that π reduces to τ and the degree of τ is equal to 1.*

Proof

By induction on the degree. ∎

Furthermore, we can obtain the following.

Corollary 5.11 *Suppose that all the cut formulas in a proof π are S-formulas, and the degree of π is stricly greater than 1. Then π reduces to a proof τ such that the abstraction weight $\lambda(\tau)$ of τ is less than or equal to $\lambda(\pi)$, and the degree of τ is equal to 1.*

Proof

This is immediate from the second lemma. ∎

5.5.3 The elimination of non-S atomic cuts

The elimination of non-S atomic cuts proceeds by induction on the abstraction index as before. We note that the substitution

$$\frac{\vdash A, \Gamma}{\vdash \theta, A[\theta], \Gamma}$$

is possible only when all of the terms in A and θ are S-terms. Due to this restriction, we can exclude the case where the elimination of the cut over non-S atomic formulas

$$\frac{\vdash s \in t, \Gamma \quad \vdash s' \notin t', \Delta}{\vdash \theta, \Gamma, \Delta}$$

is blocked because of the irregularity of the substitution θ.

We start by defining a useful terminology.

Definition 5.12 *consider the cut*

$$\frac{\begin{matrix} \vdots\pi_1 \\ \vdash s \in t, \Gamma \end{matrix} \quad \begin{matrix} \vdots\pi_2 \\ \vdash s' \notin t', \Gamma \end{matrix}}{\vdash \theta, \Gamma, \Delta}$$

where the cut formulas $s \in t$ and $s \notin t$ are S-formulas created by $(S \in)$ and $(S \notin)$ as the main formulas of π_1 and π_2, respectively. This type of cuts are called A-cuts.

Definition 5.13 *The cuts over equalities created by (E) and $(S \neq)$ are called E-cuts.*

When we refer to abstraction indices from now on, we only take into account the abstraction indices of non-S atomic cuts.

Lemma 5.14 *Suppose that the proof π is obtained from π_1 and π_2 by the non-S atomic cut with the abstraction index (i, j) and the abstraction indices of π_1 and π_2 are strictly less than $i \cdot j$. Then π reduces to a proof τ such that the abstraction index of τ is strictly less than $i \cdot j$.*

Proof

By induction on the size of a proof. If one of the permutative reductions is applicable, we perform it and use the inductive hypotheis. Otherwise we perform the symmetric reduction which decreases the abstraction index. ∎

Lemma 5.15 *Let π be a proof such that its abstraction index is strictly greater than 1 and it contains only atomic cuts. Then π reduces to a proof τ such that the abstraction index of τ is strictly less than that of π and τ contains only atomic cuts.*

Proof

By induction on the size of a proof. We take the lowermost cut of the maximal abstraction index and use the inductive hypothesis to both of the subproofs. We then use the previous lemma to decrease the abstraction index. Finally, we eliminate all the newly created complex cuts as before. ∎

Corollary 5.16 *For any proof π, there exists a proof τ such that π reduces to τ and τ contains only E-cuts, A-cuts and Z-cuts.*

Proof

We first eliminate all complex cuts. Then all non-S atomic cuts are eliminated by induction on the abstraction index. Finally, we bring all the cuts upward as much as possible and eliminate all the atomic cuts orginated from (I), $(\top)$ and (W) by induction on the size. In particluar, notice that the permutation of a cut with an A-cut does not make the latter a non-A cut since the former will be moved upward again by the permutation with $(S \in)$ or $(S \notin)$. ∎

5.5.4 The elimination of E-cuts

E-cuts are eliminated by the induction on the size. The critical observation is that if two terms used in substitution can be brought to be identical to each other, then the substitution itself can be carried out without using those two terms. This is the content of the symmetric reduction $(S \neq /E)$.

Lemma 5.17 *Suppose that the proof π is obtained from π_1 and π_2 by an E-cut and neither of π_1 or π_2 contains E-cuts. Then π reduces to a proof τ which contains no E-cuts. Furthermore, the abstraction weight does not increase in the reduction process, and no new cuts are created in τ.*

Proof

The proof is by induction on the size of a proof. If one of the permutative reduction is applicable, we perform it and use the inductive hypothesis. Otherwise, we apply one of the symmetric reductions and use the inductive hypothesis. Note that none of the relevant permutative and symmetric reductions create any application of $(S \in)$ or $(S \notin)$, and all the new cuts created in the middle of the reduction process are eventually eliminated. ∎

Lemma 5.18 *Suppose that the proof π contains only E-cuts, A-cuts and Z-cuts. Then π reduces to a proof π which contains only A-cuts and Z-cuts.*

Proof

The proof is by induction on the size of a proof. If the last rule of inference of π is not an E-cut, the conclusion follows immediately from the inductive hypotheis. Hence we suppose that π ends with an E-cut. By the inductive hypothesis, we can assume that the last cut is the only E-cut in π. By the previous proposition, we can eliminate this last E-cut. ∎

5.5.5 The elimination of A-cuts

The basic idea to eliminate A-cuts is as follows. Suppose that we have a proof π which contains only A-cuts and Z-cuts. Some of the A-cuts are eliminable while others are not. We take the lowermost eliminable A-cut and eliminate it with the decrease of the abstraction weight. Certainly this elimination creates new cuts. However they can be eliminated without increasing the abstraction weight until we have a new proof which contains only A-cuts and Z-cuts. We then can use the inductive hypothesis on the abstraction weight.

Before starting the proof, it is worth noting when a non-eliminable A-cut become eliminable after the elimination of another A-cut. Assuming that we have already eliminated all E-cuts, this can only happen when one of the irregular inequality in θ created in the A-cut is later used in a comprehension rule and placed inside an S-term, and another A-cut involving this S-term is eliminated, leading to the elimination of the irregular substitution. This means that we do not need to worry about non-eliminable A-cuts below the lowermost eliminable A-cut, since the former will never become eliminable.

Lemma 5.19 *Suppose that the proof π contains only A-cuts and Z-cuts, and π is obtained from π_1 and π_2 by an eliminable direct A-cut. Then π reduces to a proof τ such that τ contains only A-cuts and Z-cuts, and the abstraction weight $\lambda(\tau)$ is strictly less than $\lambda(\pi)$.*

Proof

We simply perform the symmetric reduction with the decrease of the abstraction weight and eliminate the newly created cuts down A-cuts and Z-cuts. In the latter process, the abstraction weight does not increase. ∎

Lemma 5.20 *Suppose that the proof π contains only A-cuts and Z-cuts. Then π reduces to a proof τ such that τ contains only non-eliminable direct A-cuts and Z-cuts.*

Proof

The proof is by induction on $\lambda(\pi)$. We take the lowermost eliminable A-cut and apply the previous lemma to it. Then we can use the inductive hypotheis since the abstraction weight of the subproof is decreased. ∎

Theorem 5.21 *For any proof π, there exists a proof τ such that π reduces to τ and τ contains only non-eliminable A-cuts and Z-cuts.*

Proof

First we obtain from π a proof which contains only E-cuts, A-cuts and Z-cuts. We then eliminate all E-cuts. Finally we use the previous lemma. ∎

5.6 The consistency of AZF

We can now prove that AZF is a conservative extension of ZF^- and therefore consistent. The proof method is essentially the same as before.

Lemma 5.22 *Suppose that the conclusion Γ of a proof π contains only Z-terms. Then π reduces to a proof τ such that τ contains only Z-cuts.*

Proof

We first use our cut-elimination theorem and obtain from π a proof which contains only non-eliminable A-cuts and Z-cuts. The proof then proceeds by the induction on the size of a proof. When the proof is just an axiom or obtained by one of the rules of inference other than (*cut*), the conclusion follows immediately from the inductive hypothesis. Hence we assume otherwise.

Case 1 The last rule of inference is a Z-cut. Then the conclusion follows immediately from the inductive hypotheis.

Case 2 The last rule of inference is an non-eliminable A-cut:

$$\frac{\vdash s \in t, \Gamma \quad \vdash s' \notin t', \Delta}{\vdash \theta, \Gamma, \Delta}$$

By the assumption, all the equations in the substitution θ are Z-formulas. Suppose that one of t and t' is not a Z-term. Since the substitutions with Z-terms do not change non-Z terms into Z-terms, they are then both non-Z terms. Furthermore, then, the irregular substitution cannot happen for the same reason. This contradicts the definition of non-eliminable A-cuts. Hence both t and t' are Z-terms. If both s and s' are Z-terms, then the conclusion follows immediately by the inductive hypothesis. Otherwise both s and s' are non-Z terms since they are identical under the substitution of Z-terms. Then the formula occurrence $s \in t$ must come from (I), $(\top)$ or (W). Therefore this cut is not an A-cut and should have been eliminated. This is a contradiction.

∎

Chapter 6

Phase-valued models of linear set theory

6.1 Introduction

In this chapter, we will extend Boolean-valued models for classical set theory to linear logic [29, 15]. This is in analogy to Heyting-valued models for intuitionistic set theory and Takeuti's ortholattice-valued models for quantum set theory [6, 28]. The general idea is as follows. Given a propositional logic and its algebraic model, we can regard an element of the algebra as a (non-standard) truth value. Then we can extend the notion of characteristic functions, or sets, so that their ranges become the sets of the extended truth values.

In the case of linear logic, such an underlying set of truth values is given by the objects of a symmetric monoidal closed category which contains its own dual category. In particular, we will use the phase-space model of linear logic as defined by Girard [7]. The set of truth values is then given by the set of *facts* in a phase space.

It is worth noting the similarity of the set of facts with the ortholattice in quantum logic. In short, the ortholattice is the lattice of closed subspaces of a Hilbert space orderd by inclusion. To each Hilbert space corresponds a physical system. Each vector in the space represents a state that a physical system can assume and each closed subspace represents an observable property of the physical system. Duals are defined by orthogonality in the Hilbert space. Then, the correspondence is:

- phase space/Hilbert space

- facts/closed subspaces
- phase/vector

In fact, this is not at all surprising since Girard clearly modelled his phase spaces on Hilbert spaces. The point stating the similarity explicitly is to give the reader some assurance that the approach taken in quantum set theory can be transfered to linear set theory, at least to some extent.

6.2 Preliminary

In this section, we review the semantics of linear logic and the construction of Boolean-valued models for classical set theory.

6.2.1 The semantics of linear logic

We first review the categorical model of linear logic and then the phase space model as a special case.

In short, the categorical model of linear logic is given as a symmetric monoidal closed category with:

- Cartesian products
- involutive self-dual endofunctor
- comonad

The very close connection between contraction-free logic and closed monoidal category was first noticed by Lambek. The idea of a category with a self-dual endofunctor, or $*$-autonomous category, was formulated by Barr. Finally the observation that the exponential ! is just a comonad is due to Seely. Our presentation is based on the exposition by Asperti and Longo [2]. We now give the precise definitions.

Definition 6.1 *Let $\mathcal{C}$ be a symmetric monoidal closed category. A functor $F : \mathcal{C} \to \mathcal{C}$ is closed if for every pair of objects $A, B \in \mathcal{C}$ there exists an arrow*

$$B^A \stackrel{f_{AB}}{\to} FB^{FA}$$

such that for every arrow $A \xrightarrow{g} B$

$$\Lambda(Fg \circ e_{FA}) = f_{AB} \circ \Lambda(g \circ e_A)$$

where the family of the arrows $A \otimes \mathbf{1} \xrightarrow{e_A} A$ *is the natural isomorphism for the identity* $\mathbf{1}$ *and* Λ *is the bijection for the adjunction* $Hom(C \otimes A \to B) \cong Hom(C \to B^A)$.

Writing $A \multimap B$ for B^A, we can represent the above condition in the following quasi sequent calculus which says that the arrows constructed at the bottom are equal.

$$\frac{\dfrac{A \xrightarrow{g} B}{FA \xrightarrow{Fg} FB}}{\mathbf{1} \to FA \multimap FB} = \frac{\dfrac{A \xrightarrow{g} B}{\mathbf{1} \to A \multimap B} \quad A \multimap B \xrightarrow{f_{AB}} FA \multimap FB}{\mathbf{1} \to FA \multimap FB}$$

Definition 6.2 *A* $*$*-autonomous category* $\mathcal{K}$ *is a symmetric closed monoidal category with a contravariant closed functor* $(\ )^* : \mathcal{K} \to \mathcal{K}$ *such that*

- *There exists a natural isomorphism*

$$Id \overset{d}{\cong} (\ )^{**}$$

- *The two arrows constructed at the bottom are equal*

$$\frac{\dfrac{A \xrightarrow{g} B}{B^* \xrightarrow{g^*} A^*}}{A^{**} \xrightarrow{g^{**}} B^{**}} = \frac{A^{**} \xrightarrow{d_A^{-1}} A \quad \dfrac{A \xrightarrow{g} B \quad B \xrightarrow{d_B} B^{**}}{A \to B^{**}}}{A^{**} \to B^{**}}$$

A $*$*-autonomous category is linear if it is also Cartesian.*

Definition 6.3 *A* $!$*-model is a linear category* $\mathcal{C}$ *with a comonad* $(!, \delta, \varepsilon)$ *such that there exist natural isomprphisms*

- $!(A \,\&\, B) \overset{i}{\cong}\ !A \otimes !B$
- $!\top \overset{j}{\cong} \mathbf{1}$

Definition 6.4 *Let* $\mathcal{C}$ *be a linear category and* $U : \mathbf{CoMon}_{\mathcal{C}} \to \mathcal{C}$ *the forgetful functor from the category of comonoids in* $\mathcal{C}$ *to* $\mathcal{C}$*. Then we say* $\mathcal{C}$ *is a free* $!$*-model if there exists the right adjoint* $!$ *to* U*.*

Proposition 6.5 *A free* $!$ *is indeed a* $!$*-model with* $U \circ\, !$ *as the comonad.*

Proof
See Asperti and Longo [2]. ∎

So far we have obtained enough machinery to interpret the full propositional linear logic. The tensor $\otimes$, the additive product $\&$ and the linear implication $\multimap$ are interpreted in the obvious way. The linear negation $(\ )^{\perp}$ is $(\ )^{*}$. Then the rest of logical connectives are defined by:

- $A \parr B =_{def} A^{\perp} \multimap B$
- $A \oplus B =_{def} (A^{\perp} \,\&\, B^{\perp})^{\perp}$
- $?\,A =_{def} (!\,A^{\perp})^{\perp}$

The standard way to interpret quantifiers in categorical logic is through an indexed category and adjunction. However it is useful for our purpose just to have infinitary product and interpret the universal quantification as the infinitary additive conjunction.

Definition 6.6 *A free* $!$*-model* $\mathcal{G}$ *is a first-order model if* $\mathcal{G}$ *has arbitrary Cartesian products.*

An example of a first-order model is provided by a phase space.

Definition 6.7 *A phase space is a quadraple* $(P, 1, \cdot, \perp)$ *where*

- $(P, 1, \cdot)$ *is a commutative monoid*
- $\perp \subset P$.

We will abbreviate $p \cdot q$ by pq.

Definition 6.8 *Given a subset* A *of* P*, the dual of* A*, denoted* $A^{\perp}$*, is defined by* $A^{\perp} = \{p \in P \mid \forall(q \in A)pq \in \perp\}$.

Definition 6.9 *A subset* A *of* P *is a fact if* $A = A^{\perp\perp}$*. The set of facts in* P *is denoted* $FACT_P$.

Definition 6.10 *A fact* A *is valid if* $1 \in A$.

Proposition 6.11 *Facts are closed under arbitrary intersection.*

Proof

First of all, $A \subset A^{\perp\perp}$. So. we only need to show the other direction. Let $\{F_i\}_{i \in I}$ be a family of facts and $A = \bigcap F_i$. Suppose $p \in A^{\perp\perp}$. We want to show $p \in F_i^{\perp\perp}$ for all $i \in I$. Let $q \in F_i^{\perp}$. Take any $r \in A$. Then $r \in F_i$. So, $qr \in \perp$. Therefore, $q \in A^{\perp}$. Hence, $pq \in \perp$. That is to say, $p \in F_i^{\perp\perp}$. ∎

Proposition 6.12 *Given a subset A of P, $A^{\perp\perp}$ is the smallest fact containing A.*

Proof

First, we show $A^{\perp} = A^{\perp\perp\perp}$. One direction is trivial. So let $p \in A^{\perp\perp\perp}$. Take any $q \in A$. Then, $q \in A^{\perp\perp}$. So, $pq \in \perp$.

Then $A^{\perp\perp\perp\perp} = A^{\perp\perp}$. Hence $A^{\perp\perp}$ is a fact.

Now suppose $A \subset B$ and B is a fact. Let $p \in B^{\perp}$ and take any $q \in A$. Then $q \in B$ so that $pq \in \perp$. Hence $B^{\perp} \subset A^{\perp}$. Then, by the same argument, $A^{\perp\perp} \subset B^{\perp\perp} = B$. ∎

Definition 6.13 *We define multicative operations on the set of facts in P as follows:*

- $A \otimes B = (AB)^{\perp\perp}$
- $A \vee B = (A^{\perp}B^{\perp})^{\perp}$
- $A \multimap B = (AB^{\perp})^{\perp}$

where A and B are facts in P and $AB = \{pq \mid p \in A \text{ and } q \in B\}$.

Definition 6.14 *We define additive operations on the set of facts in P as follows:*

- $A \& B = A \cap B$
- $A \oplus B = (A \cup B)^{\perp\perp}$

Definition 6.15 *We deine constants in the set of facts in P as follows:*

- $\mathbf{1} = \perp^{\perp}$
- $T = \emptyset^{\perp}$
- $\mathbf{0} = T^{\perp}$

Note that $\perp$ and all other constants are facts in P.

Now we define semantics for the multiplicative-additive fragment of linear logic, or MALL.

Definition 6.16 *A phase structure for MALL is a phase space with a function which assigns a fact to each propositional letter. The interpretation of a sentence is a fact assigned to the sentence by extending the function inductively.*

Definition 6.17 *A sentence is valid if the identity 1 is in its interpretation. A sentence is a linear tautology if it is valid in any phase structure.*

Proposition 6.18 *MALL is sound and complete with respect to the validity in phase structure.*

For the proof of the proposition, we refer the reader to Girard's original paper [7].

The phase semantics can be easily extended to predicate logic. We simply interpret quantifications as infinitary additive conjunction and disjunction. For exponentials, we need to extend the phase space.

Definition 6.19 *A topolinear space is a phase space paired with the set F of the closed facts such that:*

(i) *F is closed under arbitrary intersection (additive conjunction)*

(ii) *F is closed under finite multiplicative disjunction*

(iii) *$\perp$ is the smallest fact in F*

(iv) *For all $A \in F$, $A \vee A = A$.*

The linear negations of closed facts are called open facts.

Definition 6.20 *We define the exponential operations on the set of facts as follows:*

- $!A$ = *the greatest open fact included in A*
- $?A$ = *the smallest closed fact containing A*

where the order is with respect to set inclusion.

Proposition 6.21 *Linear logic is sound and complete with respect to the validity in the topolinear spaces.*

The following proposition is useful.

Proposition 6.22 *Let A and B be facts in P. Then, $1 \in A \to B$ if and only if $A \subset B$.*

Proof

First, assume $1 \in A \to B = (A \cdot B^{\perp})^{\perp}$. Then $\{1\} \cdot (A \cdot B^{\perp}) = A \cdot B^{\perp} \in \perp$. Hence $A \subset B^{\perp\perp} = B$. Secondly, assume $A \subset B$. Then $B^{\perp} \subset A^{\perp}$ so that $A \cdot B^{\perp} \subset A \cdot A^{\perp} \subset \perp$. Hence, $\{1\} \cdot (A \cdot B^{\perp}) \subset \perp$. Therefore $1 \in (A \cdot B^{\perp})^{\perp} = A \to B$. ∎

6.2.2 The boolean-valued models of classical set theory

We turn our attention to Boolean-valued models [29, 15]. Let $\mathcal{B}$ be a complete Boolean algebra. We first define the $\mathcal{B}$-valued universe $V^{\mathcal{B}}$.

Definition 6.23 *We define $V^{\mathcal{B}}_{\alpha}$ and $V^{\mathcal{B}}$ by the transfinite induction on ordinals α as follows:*

- $V^{\mathcal{B}}_0 = \emptyset$
- $V^{\mathcal{B}}_{\alpha+1} = \{u \mid u \textit{ is a function with } dom(u) \subset V^{\mathcal{B}}_a \textit{ and } ran(u) \subset \mathcal{B}\}$
- $V^{\mathcal{B}}_{\lambda} = \bigcup_{\alpha<\lambda} V^{\mathcal{B}}_{\alpha}$ *where* $\lambda \in LIM$.
- $V^{\mathcal{B}} = \bigcup_{\alpha \in ON} V^{\mathcal{B}}_{\alpha}$.

Next we define the interpretation of "atomic propositions". Note that we can assign the rank $\rho(u)$ to each $u \in V^{\mathcal{B}}$ by defining:

$$\rho(u) = \textit{ the least } \alpha \textit{ such that } u \in V^{\mathcal{B}}_{\alpha+1}.$$

Definition 6.24 *For $u, v \in V^{\mathcal{B}}$, we define $[\![u = v]\!], [\![u \subset v]\!]$ and $[\![u \in v]\!]$ by transfinite induction on $(\rho(u), \rho(v))$ as follows:*

- $[\![u \in v]\!] = \bigvee_{x \in dom(v)} (v(x) \wedge [\![x = u]\!])$
- $[\![u \subset v]\!] = \bigwedge_{x \in dom(u)} (u(x) \to [\![x \in v]\!])$ *where* $a \to b = \neg a \vee b$

- $[\![u = v]\!] = [\![u \subset v]\!] \wedge [\![v \subset u]\!]$

The idea behind the above definition is the following translation:

- $u \in v \iff \exists(x \in v)(x = u)$
- $u \subset v \iff \forall(x \in u)(x \in v)$
- $u = v \iff u \subset v$ *and* $v \subset u$

Notice that universal and existential quantifications are interpreted as infinitary conjunction (meet) and disjunction (join) respectively.

Proposition 6.25 *For every* $u, v \in V^{\mathcal{B}}$*,*

(i) $[\![u = u]\!] = 1$

(ii) $[\![u = v]\!] = [\![v = u]\!]$

(iii) $[\![u = v]\!] \wedge [\![v = w]\!] \leq [\![u = w]\!]$

(iv) $[\![u \in v]\!] \wedge [\![w = u]\!] \wedge [\![t = v]\!] \leq [\![w \in t]\!]$

The proof is by the induction on ranks. Now we extend this assignment to every sentence.

Definition 6.26 *For every formula* $\varphi(x_1, \ldots, x_n)$*, we define the Boolean value of* φ

$$[\![\varphi(u_1, \ldots, u_n)]\!] \qquad\qquad (u_1, \ldots, u_n \in V^{\mathcal{B}})$$

as follows:

(a) *If* φ *is an atomic formula, the assignment is as we defined above*

(b) *If* φ *is a negation, conjunction, etc.,*

$$\begin{array}{rcl}
[\![\neg\psi(u_1, \ldots, u_n)]\!] & = & \neg[\![\psi(u_1, \ldots, u_n)]\!] \\
[\![\psi \wedge \chi(u_1, \ldots, u_n)]\!] & = & [\![\psi(u_1, \ldots, u_n)]\!] \wedge [\![\chi(u_1, \ldots, u_n)]\!] \\
[\![\psi \vee \chi(u_1, \ldots, u_n)]\!] & = & [\![\psi(u_1, \ldots, u_n)]\!] \vee [\![\chi(u_1, \ldots, u_n)]\!] \\
[\![\psi \rightarrow \chi(u_1, \ldots, u_n)]\!] & = & [\![\psi(u_1, \ldots, u_n)]\!] \rightarrow [\![\chi(u_1, \ldots, u_n)]\!] \\
[\![\psi \leftrightarrow \chi(u_1, \ldots, u_n)]\!] & = & [\![\psi \rightarrow \chi(u_1, \ldots, u_n)]\!] \wedge [\![\chi \rightarrow \psi(u_1, \ldots, u_n)]\!]
\end{array}$$

(c) *If φ is $\exists x\psi$ or $\forall x\psi$*

$$\begin{aligned}
[\![\exists x\psi(x, u_1, \ldots, u_n]\!] &= \bigcup_{v\in V^{\mathcal{B}}} [\![\psi(v, u_1, \ldots, u_n]\!] \\
[\![\forall x\psi(x, u_1, \ldots, u_n]\!] &= \bigcap_{v\in V^{\mathcal{B}}} [\![\psi(v, u_1, \ldots, u_n]\!]
\end{aligned}$$

Definition 6.27 *A sentence φ is* valid *in $V^{\mathcal{B}}$ if $[\![\varphi]\!] = 1$.*

Proposition 6.28 *Every axiom of ZFC is valid in $V^{\mathcal{B}}$.*

6.3 The Phase-valued Model $V^{\mathcal{P}}$

We now define our first model $V^{\mathcal{P}}$. The construction is essentially the same as that of $V^{\mathcal{B}}$ except that we will use the set of facts in a phase space instead of the boolean algebra.

Definition 6.29 *We define $V^{\mathcal{P}}_\alpha$ and $V^{\mathcal{P}}$ by the transfinite induction on ordinals α as follows:*

- $V^{\mathcal{P}}_0 = \emptyset$
- $V^{\mathcal{P}}_{\alpha+1} = \{u \mid u \text{ is a function with } dom(u) \subset V^{\mathcal{P}}_\alpha \text{ and } ran(u) \subset FACT_{\mathcal{P}}\}$
- $V^{\mathcal{P}}_\lambda = \bigcup_{\alpha<\lambda} V^{\mathcal{P}}_\alpha$ *where* $\lambda \in LIM$.
- $V^{\mathcal{P}} = \bigcup_{\alpha\in ON} V^{\mathcal{P}}_\alpha$.

Definition 6.30 *For $u, v \in V^{\mathcal{B}}$, we define $[\![u = v]\!], [\![u \subset v]\!]$ and $[\![u \in v]\!]$ by transfinite induction on $(\rho(u), \rho(v))$ as follows:*

- $[\![u \in v]\!] = (\bigcup_{x\in dom(v)}(v(x) \cdot [\![x = u]\!])^{\perp\perp})^{\perp\perp}$
- $[\![u \subset v]\!] = \bigcap_{x\in dom(u)}(u(x) \cdot [\![x \in v]\!]^{\perp})^{\perp}$
- $[\![u = v]\!] = (![\![u \subset v]\!] \cdot ![\![v \subset u]\!])^{\perp\perp}$

Proposition 6.31 *For every $u, v \in V^{\mathcal{P}}$,*

(i) $1 \in (u(x) \cdot [\![x \in u]\!]^{\perp})^{\perp}$ *for all* $x \in dom(u)$

(ii) $1 \in [\![u = u]\!]$

(iii) $1 \in ((\llbracket u = v \rrbracket \cdot \llbracket v = u \rrbracket^{\perp})^{\perp} \cdot (\llbracket v = u \rrbracket \cdot \llbracket u = v \rrbracket^{\perp})^{\perp})^{\perp\perp}$

Proof

We prove (i) and (ii) together by the simultaneous induction on ranks.

(i) It suffices to show that for all $x \in dom(u)$,

$$u(x) \cdot \llbracket x \in u \rrbracket^{\perp} \subset \perp .$$

By the inductive hypothesis, $1 \in \llbracket x = x \rrbracket$. Then $u(x) = u(x) \cdot \{1\} \subset (u(x) \cdot \{1\})^{\perp\perp} \subset \bigcup_{y \in dom(u)} (u(y) \cdot \llbracket x = y \rrbracket)^{\perp\perp}$. Hence

$$\begin{aligned} u(x) \cdot \llbracket x \in u \rrbracket^{\perp} &= u(x) \cdot (\bigcup_{y \in dom(u)} (u(y) \cdot \llbracket x = y \rrbracket)^{\perp\perp})^{\perp\perp\perp} \\ &= u(x) \cdot (\bigcup_{y \in dom(u)} (u(y) \cdot \llbracket x = y \rrbracket)^{\perp\perp})^{\perp} \subset \perp . \end{aligned}$$

(ii) It suffices to show $1 \in !\llbracket u \subset u \rrbracket$. Now $\llbracket u \subset u \rrbracket = \bigcap_{x \in dom(u)} (u(x) \cdot \llbracket x \in u \rrbracket^{\perp})^{\perp}$. By (i), $u(x) \cdot \llbracket x \in u \rrbracket^{\perp} \subset \perp$ for all $x \in dom(u)$ so that $T = \perp^{\perp} \subset \bigcap_{x \in dom(u)} (u(x) \cdot \llbracket x \in u \rrbracket^{\perp})^{\perp}$. Since $\perp$ is the smallest closed fact, T is the greatest open fact. Hence $T = !\llbracket u \subset u \rrbracket$ and clearly $1 \in T$.

(iii) It suffices to show that $1 \in (\llbracket u = v \rrbracket \cdot \llbracket v = u \rrbracket^{\perp})^{\perp}$ and $1 \in (\llbracket v = u \rrbracket \cdot \llbracket u = v \rrbracket^{\perp})^{\perp}$. Now

$$1 \in (\llbracket u = v \rrbracket \cdot \llbracket v = u \rrbracket)^{\perp} \iff \llbracket u = v \rrbracket \cdot \llbracket v = u \rrbracket^{\perp} \subset \perp .$$

Since $\llbracket u = v \rrbracket = (!\llbracket u \subset v \rrbracket \cdot !\llbracket v \subset u \rrbracket)^{\perp\perp} = (!\llbracket v \subset u \rrbracket \cdot !\llbracket u \subset v \rrbracket)^{\perp\perp} = \llbracket v = u \rrbracket$, we have $\llbracket u = v \rrbracket \cdot \llbracket v = u \rrbracket^{\perp} = \llbracket u = v \rrbracket \cdot \llbracket u = v \rrbracket^{\perp} \subset \perp$. Similarly, $\llbracket v = u \rrbracket \cdot \llbracket v = u \rrbracket^{\perp} \subset \perp$. ∎

Proposition 6.32 *For every* $u, v, w \in V^{\mathcal{P}}$,

(i) $1 \in ((\llbracket u = v \rrbracket \cdot \llbracket v = w \rrbracket)^{\perp\perp} \cdot \llbracket u = w \rrbracket^{\perp})^{\perp}$

(ii) $1 \in ((\llbracket u \in v \rrbracket \cdot \llbracket w = u \rrbracket)^{\perp\perp} \cdot \llbracket w \in v \rrbracket^{\perp})^{\perp}$

(iii) $1 \in ((\llbracket u \in v \rrbracket \cdot \llbracket w = v \rrbracket)^{\perp\perp} \cdot \llbracket u \in w \rrbracket^{\perp})^{\perp}$

Proof

By the simultaneous induction on $(\rho(u), \rho(v), \rho(w))$.

(i) First we show $[\![u \subset v]\!] \otimes [\![v = u]\!] \subset [\![u \subset w]\!]$. Now

$$\begin{aligned}
[\![u \subset v]\!] \otimes [\![v = w]\!] &= \bigcap_{x \in dom(u)} (u(x) \cdot [\![x \in v]\!]^{\perp})^{\perp} \otimes [\![v = w]\!] \\
&= (\bigcap_{x \in dom(u)} (u(x) \cdot [\![x \in v]\!]^{\perp})^{\perp} \cdot [\![v = w]\!])^{\perp\perp}
\end{aligned}$$

Let $p \in \bigcap_{x \in dom(u)} (u(x) \cdot [\![x \in v]\!]^{\perp})^{\perp}$. Then for all $x \in dom(u), s \in u(x)$ and $s' \in [\![x \in v]\!]^{\perp}$, we have $pss' \in \perp$ so that $ps \in [\![x \in v]\!]^{\perp\perp} = [\![x \in v]\!]$.

Now we want to show that for any $q \in [\![v = w]\!]$, we have $pq \in \bigcap_{x \in dom(u)} (u(x) \cdot [\![x \in w]\!]^{\perp})^{\perp}$. Let's fix $y \in dom(u)$ and let $r \in u(y) \cdot [\![y \in w]\!]^{\perp}$. Then $r = tt'$ where $t \in u(y)$ and $t' \in [\![y \in w]\!]^{\perp}$. Then $pt \in [\![y \in v]\!]$. By the inductive hypothesis, $[\![y \in v]\!] \cdot [\![v = w]\!] \subset [\![y \in v]\!] \otimes [\![v = w]\!] \subset [\![y \in w]\!]$. Hence $ptq \in [\![y \in w]\!]$. Therefore $pqr = ptqt' \in \perp$.

Similarly, we can show $[\![w \subset v]\!] \otimes [\![u = v]\!] \subset [\![w \subset u]\!]$.

Next we show $[\![u = v]\!] \otimes [\![v = w]\!] \subset [\![u = w]\!]$. Note that $!A \subset A$ since $!A$ is the greatest open fact included in A. Also for any open fact A, we have $A \otimes A = A$ since closed facts are idempotent with respect to multiplicative disjunction. Then

$$\begin{aligned}
[\![u = v]\!] \otimes [\![v = w]\!] &= ![\![u \subset v]\!] \otimes ![\![v \subset u]\!] \otimes ![\![v \subset w]\!] \otimes ![\![w \subset v]\!] \\
&= ![\![u \subset v]\!] \otimes ![\![u \subset v]\!] \otimes ![\![v \subset u]\!] \otimes ![\![w \subset v]\!] \otimes ![\![v \subset w]\!] \otimes ![\![w \subset v]\!] \\
&= ![\![u \subset v]\!] \otimes [\![w = v]\!] \otimes ![\![w \subset v]\!] \otimes [\![u = v]\!]
\end{aligned}$$

Now $![\![u \subset v]\!] \otimes [\![w = v]\!] \subset [\![u \subset v]\!] \otimes [\![w = v]\!] \subset [\![u \subset w]\!]$. Furthermore, since open sets are closed under finite multiplicative conjunction, $![\![u \subset v]\!] \otimes [\![w = v]\!]$ is open. Therefore, we have $![\![u \subset v]\!] \otimes [\![w = v]\!] \subset ![\![u \subset w]\!]$. Similarly, $![\![w \subset v]\!] \otimes [\![u = v]\!] \subset ![\![w \subset u]\!]$. Hence,$[\![u = v]\!] \otimes [\![v = w]\!] \subset [\![u = w]\!]$.

(ii) We want to show $([\![u \in v]\!] \cdot [\![u = w]\!])^{\perp\perp} \subset [\![w \in v]\!]$. Now

$$\begin{aligned}
([\![u \in v]\!] \cdot [\![u = w]\!])^{\perp\perp} &= ((\bigcup_{x \in dom(v)} (v(x) \cdot [\![x = u]\!])^{\perp\perp})^{\perp\perp} \cdot [\![u = w]\!])^{\perp\perp} \\
&= (\bigcup_{x \in dom(v)} (v(x) \cdot [\![x = u]\!] \cdot [\![u = w]\!])^{\perp\perp})^{\perp\perp}
\end{aligned}$$

By the inductive hypothesis, $[\![x = u]\!] \cdot [\![u = w]\!] \subset [\![x = u]\!] \otimes [\![u = w]\!] \subset [\![x = w]\!]$. Hence $([\![u \in v]\!] \cdot [\![v = w]\!])^{\perp\perp} \subset (\bigcup_{x \in dom(v)}(\cdot [\![x = w]\!])^{\perp\perp})^{\perp\perp} = [\![w \in v]\!]$.

(iii) We want to show $([\![u \in v]\!] \cdot [\![v = w]\!])^{\perp\perp} \subset [\![u \in w]\!]$. We know

$$\begin{aligned}
([\![u \in v]\!] \cdot [\![v = w]\!])^{\perp\perp} &= ((\bigcup_{x \in dom(v)} (v(x) \cdot [\![x = u]\!])^{\perp\perp})^{\perp\perp} \cdot [\![v = w]\!])^{\perp\perp} \\
&= (\bigcup_{x \in dom(v)} (v(x) \cdot ![\![v \subset w]\!] \cdot ![\![w \subset v]\!] \cdot [\![x = u]\!])^{\perp\perp})^{\perp\perp}
\end{aligned}$$

Now fix $y \in dom(v)$. Let $p \in v(x) \cdot ![\![v \subset w]\!] \cdot ![\![w \subset v]\!] \cdot [\![x = u]\!]$. We have

$$\begin{aligned}
v(y) \cdot ![\![v \subset w]\!] &\subset v(y) \cdot [\![v \subset w]\!] \\
&= v(y) \cdot \bigcap_{x \in dom(v)} (v(x) \cdot [\![x \in w]\!]^{\perp})^{\perp}
\end{aligned}$$

We show $v(y) \cdot \bigcap_{x \in dom(v)}(v(x) \cdot [\![x \in w]\!]^{\perp})^{\perp} \subset [\![y \in w]\!]$. Let $q \in \bigcap_{x \in dom(v)}(v(x) \cdot [\![x \in w]\!]^{\perp})^{\perp}$. Then for any $x \in dom(v), r \in v(x)$ and $s \in [\![x \in w]\!]^{\perp}$, we have $qrs \in \perp$ so that $qr \in [\![x \in w]\!]^{\perp\perp} = [\![x \in w]\!]$. In particular, for any $r' \in v(y)$, we have $qr' \in [\![y \in w]\!]$. Hence $v(y) \cdot [\![v \subset w]\!] \subset [\![y \in w]\!]$.

Therefore it suffices to show $[\![y \in w]\!] \cdot ![\![w \subset v]\!] \cdot [\![y = u]\!] \subset (\bigcap_{z \in dom(w)}(w(z) \cdot [\![z = u]\!])^{\perp\perp})^{\perp\perp}$. By the inductive hypothesis, $[\![z = y]\!] \cdot [\![y = u]\!] \subset [\![z = y]\!] \otimes [\![y = u]\!] \subset [\![z = u]\!]$ for all $z \in dom(w)$. Then

$$\begin{aligned}
[\![y \in w]\!] \cdot [\![y = u]\!] &= (\bigcap_{z \in dom(w)} (w(z) \cdot [\![z = y]\!])^{\perp\perp})^{\perp\perp} \cdot [\![y = u]\!] \\
&\subset (\bigcap_{z \in dom(w)} (w(z) \cdot [\![z = y]\!] \cdot [\![y = u]\!])^{\perp\perp})^{\perp\perp} \\
&\subset (\bigcap_{z \in dom(w)} (w(z) \cdot [\![z = u]\!])^{\perp\perp})^{\perp\perp} \\
&= [\![u \in w]\!]
\end{aligned}$$

Now we show that for any open set C, if $A \subset B$, then $A \cdot C \subset B$. Assume $A \subset B$. Then $A \cdot B^{\perp} \subset \perp$. Then $A \cdot C \cdot B^{\perp} \subset \perp \cdot C$. So we want to show $\perp \cdot C \subset \perp$. Let $p \in \perp$ and $q \in C = D^{\perp}$ where D is closed. Then for any $r \in D$, we have $qr \in \perp$. In particular, $p \in \perp \subset D$ so that $pq \in \perp$. Hence $[\![y \in w]\!] \cdot ![\![w \subset v]\!] \cdot [\![y = u]\!] \subset (\bigcap_{z \in dom(w)}(w(z) \cdot$

$[\![z = u]\!])^{\perp\perp})^{\perp\perp}$.

∎

Definition 6.33 *For every formula $\varphi(x_1, \ldots, x_n)$, we define the* phase value *of φ*

$$[\![\varphi(u_1, \ldots, u_n)]\!] \qquad\qquad (u_1, \ldots, u_n \in V^{\mathcal{P}})$$

as follows:

(a) *If φ is an atomic formula, the assignment is as we defined above*

(b) *If φ is a linear negation, multiplicative conjunction, etc.,*

$$\begin{aligned}
[\![\psi(u_1, \ldots, u_n^{\perp})]\!] &= [\![\psi(u_1, \ldots, u_n)]\!]^{\perp} \\
[\![\psi \otimes \chi(u_1, \ldots, u_n]\!] &= ([\![\psi(u_1, \ldots, u_n)]\!] \cdot [\![\chi(u_1, \ldots, u_n)]\!])^{\perp\perp} \\
[\![\psi \vee \chi(u_1, \ldots, u_n]\!] &= ([\![\psi(u_1, \ldots, u_n)]\!]^{\perp} \cdot [\![\chi(u_1, \ldots, u_n)]\!]^{\perp})^{\perp} \\
[\![\psi \rightarrow \chi(u_1, \ldots, u_n)]\!] &= ([\![\psi(u_1, \ldots, u_n)]\!] \cdot [\![\chi(u_1, \ldots, u_n)]\!])^{\perp} \\
[\![\psi \& \chi(u_1, \ldots, u_n]\!] &= [\![\psi(u_1, \ldots, u_n)]\!] \cap [\![\chi(u_1, \ldots, u_n)]\!] \\
[\![\psi \oplus \chi(u_1, \ldots, u_n]\!] &= ([\![\psi(u_1, \ldots, u_n)]\!] \cup [\![\chi(u_1, \ldots, u_n)]\!])^{\perp\perp}
\end{aligned}$$

(c) *If φ is $\exists x \psi$ or $\forall x \psi$,*

$$\begin{aligned}
[\![\exists x \psi(x, u_1, \ldots, u_n)]\!] &= (\bigcup_{v \in V^{\mathcal{B}}} [\![\psi(v, u_1, \ldots, u_n)]\!])^{\perp\perp} \\
[\![\forall x \psi(x, u_1, \ldots, u_n)]\!] &= \bigcap_{v \in V^{\mathcal{B}}} [\![\psi(v, u_1, \ldots, u_n)]\!]
\end{aligned}$$

(d) *If φ is $!\psi$ or $?\psi$,*

$$\begin{aligned}
[\![!\psi(u_1, \ldots, u_n)]\!] &= ![\![\psi(u_1, \ldots, u_n)]\!] \\
[\![?\psi(u_1, \ldots, u_n)]\!] &= ?[\![\psi(u_1, \ldots, u_n)]\!]
\end{aligned}$$

We now start checking the validity of the basic set-theoretical principles.

Proposition 6.34 **(a)** $[\![(\exists y \in x)\phi(y)]\!] = (\bigcup_{y \in dom(x)} (x(y) \otimes [\![\phi(y)]\!]))^{\perp\perp}$

(b) $[\![(\forall y \in x)\phi(y)]\!] = \bigcap_{y \in dom(x)}(x(y) \rightarrow [\![\phi(y)]\!])$

Proof

(a)

$$\begin{aligned}
[\![(\exists y \in x)\phi(y)]\!] &= [\![\exists y(y \in x \otimes \phi(y)]\!] \\
&= (\bigcup_{y \in V^P} [\![y \in x \otimes \phi(y)]\!])^{\perp\perp} \\
&= (\bigcup_{y \in V^P} ([\![y \in x]\!] \otimes [\![\phi(y)]\!]))^{\perp\perp} \\
&= (\bigcup_{y \in V^P} [(\bigcup_{z \in dom(x)} (x(z) \otimes [\![y = z]\!]))^{\perp\perp} \otimes [\![\phi(y)]\!]])^{\perp\perp} \\
&\subset (\bigcup_{y \in V^P} [(\bigcup_{z \in dom(x)} (x(z) \otimes [\![y = z]\!] \otimes [\![\phi(y)]\!]))^{\perp\perp}])^{\perp\perp} \\
&\subset (\bigcup_{z \in dom(x)} (x(z) \otimes [\![\phi(z)]\!]))^{\perp\perp}
\end{aligned}$$

Also,

$$\begin{aligned}
(\bigcup_{y \in dom(x)} (x(y) \otimes [\![\phi(y)]\!]))^{\perp\perp} &\subset (\bigcup_{y \in dom(x)} ([\![y \in x]\!] \otimes [\![\phi(y)]\!]))^{\perp\perp} \\
&\subset (\bigcup_{y \in V^P} ([\![y \in x]\!] \otimes [\![\phi(y)]\!]))^{\perp\perp} \\
&= [\![\exists y(y \in x \otimes \phi(y)]\!]
\end{aligned}$$

(b) By duality from (a).

∎

Definition 6.35 *A phase-valued set $u \in V^P$ is* static *if $u(v)$ is open for all $v \in dom(u)$. We denote the class of static phase-valued set by $STAT$.*

Proposition 6.36 *Let $u \in V^P$ be static. Then $[\![x \in u]\!]$ is open for all $x \in V^P$.*

Proof

$[\![x \in u]\!] = (\bigcup_{z \in dom(u)}(u(z) \otimes [\![x = z]\!]))^{\perp\perp}$. Since open facts are closed under finite multiplicative conjunction, $[\![x = z]\!]$ is open. Furthermore, open facts are closed under arbitrary union. Hence, $[\![x \in u]\!]$ is open. ∎

Definition 6.37

- $\forall x^{STAT}\phi(x) =_{def} \bigcap_{x\in STAT}\phi(x)$
- $\exists x^{STAT}\phi(x) =_{def} (\bigcup_{x\in STAT}\phi(x))^{\perp\perp}$

Now, we formulate the axiomatic system ZFL of linear set theory as follows:

(Empty Set): $\exists Y\forall x(x\in Y)^{\perp}$

(Extensionality): $\forall X\forall Y(!\forall u(u\in X\to u\in Y)\otimes !\forall u(u\in Y\to u\in X)\to X=Y)$

(Pair): $\forall u\forall v\exists a\forall x(x=u\oplus x=v\to x\in a)$

(Union): $\forall X\exists Y\forall u(\exists z(z\in X\otimes u\in z)\to u\in Y)$

(Separation): $\forall X\forall p\exists Y\forall u(u\in Y\leftrightarrow u\in X\otimes\phi(u,p))$

(Static Power Set): $\forall u^{STAT}\exists v\forall x^{STAT}(!x\subset u\to x\in v)$

(Collection): $\forall u(\forall x\in u\exists y\phi(x,y)\to\exists v\forall x\in u\exists y\in v\phi(x,y))$

(Infinity): $\exists Y(\emptyset\in Y\otimes\forall x(x\in Y\to x\cup\{x\}\in Y)$

Theorem 6.38 *All the axioms of ZFL are valid in V^P.*

Proof

(Empty Set): Let $Y\in V^P$ be such that $dom(Y)=\emptyset$.Then, for any $x\in V^P$, we have $\bigcup_{v\in dom(Y)}(Y(v)\otimes [\![x=v]\!])=$ so that $(\bigcup_{v\in dom(Y)}(Y(v)\otimes [\![x=v]\!]))^{\perp}=\{p\in P\mid\forall q\in P(q\in\emptyset\Rightarrow pq\in\perp)\}=P$. Hence, $[\![(x\in Y)^{\perp}]\!]=P$ and $[\![\forall x(x\in Y)^{\perp}]\!]=P$. Obviously, $1\in P$.

(Extensionality): By the definition, $[\![X=Y]\!]=![\![X\subset Y]\!]\otimes ![\![Y\subset X]\!]$. Then, the axiom holds by the above proposition.

(Pair): Let $a\in V^P$ be such that $dom(a)=\{u,v\}$ and $1\in a(u)=a(v)$. Then, $1\in[\![u\in a]\!]$ and $1\in[\![v\in a]\!]$. Now for any $x\in V^P$, we have $[\![x=u]\!]\otimes[\![u\in a]\!]\subset[\![x\in a]\!]$ so that $[\![x=u]\!]\subset[\![x\in a]\!]$. Similarly, $[\![x=v]\!]\subset[\![x\in a]\!]$. Hence $[\![x=u\oplus x=v]\!]=([\![x=u]\!]\cup[\![x=v]\!])^{\perp\perp}\subset[\![x\in a]\!]^{\perp\perp}=[\![x\in a]\!]$.

(Union): Let $Y \in V^P$ be such that $dom(Y) = \bigcup\{dom(z) \mid z \in dom(X)\}$ and $Y(u) = \bigcup_{z \in \{z \mid u \in dom(z) \ and \ z \in dom(X)\}}(X(z) \otimes z(u))$. Then for any $z \in dom(X)$ and $u \in dom(z)$, we have $X(z) \otimes z(u) \subset Y(u) \subset [\![u \in Y]\!]$ so that $X(z) \subset z(u) \to [\![u \in Y]\!]$. Hence, $X(z) \subset [\![\forall w(w \in z \to w \in Y)]\!]$. This means that $1 \in [\![\forall z(z \in X \to \forall w(w \in z \to w \in Y))]\!]$, which is equivalent to the validity of the axiom.

(Separation): Let $Y \in V^P$ be such that $dom(Y) = dom(X)$ and $Y(u) = X(u) \otimes [\![\varphi(u,p)]\!]$ for all $u \in dom(Y)$. Then, we have $Y(u) \subset [\![u \in X \otimes \varphi(u,p)]\!]$ for all $u \in dom(Y)$ so that $1 \in [\![\forall u(u \in Y \to u \in X \otimes \varphi(u,p))]\!]$. Also, $X(u) \otimes [\![\varphi(u,p)]\!] \subset Y(u) \subset [\![u \in Y]\!]$ for all $u \in dom(X)$ so that $X(u) \subset [\![\varphi(u,p)]\!] \to [\![u \in Y]\!]$. Hence, $1 \in [\![\forall u(u \in X \to (\varphi(u,p) \to u \in Y))]\!] = [\![\forall u(u \in X \otimes \varphi(u,p) \to u \in Y)]\!]$.

(Static Power Set): Let $v \in STAT \subset V^P$ be such that

$$dom(v) = \{f \mid f \ is \ a \ function \ with \ dom(f) = dom(u) \ and \ ran(f) \subset OPEN\}$$

where OPEN is the set of all open facts in P, and $1 \in v(x)$ for all $x \in dom(v)$. We want to show $1 \in [\![\forall x(!x \subset u \to x \in v)]\!]$. For this, we define $x' \in dom(v)$ for each $x \in STAT \subset V^P$ which satisfies $[\![!x \subset u]\!] \subset [\![x' = x]\!]$. Given such an x', the validity of the axiom immediately follows since $1 \in [\![x' \in v]\!]$ and $[\![!x \subset u]\!] \subset [\![x' = x]\!] \subset [\![x' = x]\!] \otimes [\![x' \in v]\!] \subset x \in v$ for all $x \in V^P$.

The definition is as follows. Given $x \in STAT$, let $x' \in V^P$ be such that $dom(x') = dom(u)$ and $x'(y) = [\![y \in x]\!]$ for all $y \in dom(x')$. Clearly, $x' \in dom(v)$. Now for any $y \in V^P$,

$$\begin{aligned} [\![y \in x']\!] &= (\bigcup_{z \in dom(u)} x'(z) \otimes [\![z = y]\!])^{\perp\perp} \\ &= (\bigcup_{z \in dom(u)} [\![z \in x]\!] \otimes [\![z = y]\!])^{\perp\perp} \\ &\subset [\![y \in x]\!] \end{aligned}$$

Hence $1 \in [\![x' \subset x]\!]$. Next for any $y \in V^P$,

$$[\![y \in u \otimes y \in x]\!] = (\bigcup_{z \in dom(u)} (u(z) \otimes [\![z = y]\!] \otimes [\![y \in x]\!]))^{\perp\perp}$$

$$\begin{aligned}
&\subset (\bigcup_{z\in dom(u)} ([\![z = y]\!] \otimes [\![z \in x]\!]))^{\perp\perp} \; since\ u(z)\ is\ open \\
&= (\bigcup_{z\in dom(u)} ([\![z = y]\!] \otimes x'(z)))^{\perp\perp} \\
&= [\![y \in x']\!]
\end{aligned}$$

Then for any $y \in V^P$,

$$\begin{aligned}
[\![y \in x]\!] \otimes [\![y \in x]\!] \otimes [\![x \subset u]\!] &\subset [\![y \in x]\!] \otimes [\![x \subset u]\!] \; since\ x \in STAT \\
&\subset [\![y \in x']\!]
\end{aligned}$$

Hence $[\![x \subset u]\!] \subset [\![x \subset x']\!]$. Then we have $[\![!x \subset u]\!] \subset [\![!x \subset x']\!] \subset [\![!x \subset x']\!] \otimes [\![!x' \subset x]\!] = [\![x = x']\!]$.

(Collection): We assume that the set of all facts in P is a set. Given $x \in V^P$, let $F_x = \{s \mid s\ is\ a\ fact\ in\ P\ and\ \exists y \in V^P([\![\varphi(x,y)]\!] = s)\}$. Then F_x is a set and $\forall s \in F_x \exists\alpha\exists y([\![\varphi(x,y)]\!] = s\ and\ \rho(y) = \alpha)$. Hence by the Collection principle in ZF, $\exists v \forall s \in F_x \exists \alpha \in v \exists y([\![\varphi(x,y)]\!] = s\ and\ \rho(y) = \alpha)$. Let $\alpha_x = \bigcup\{\alpha \mid \alpha \in v\ and\ \alpha \in Ord\}$. Then $\exists v \forall s \in F_x \exists \alpha \in \alpha_x \exists y([\![\varphi(x,y)]\!] = s\ and\ \rho(y) = \alpha)$. That is to say, $F_x = \{s \mid s\ is\ a\ fact\ in\ P\ and\ \exists y \in V^P_{\alpha_x}([\![\varphi(x,y)]\!] = s)\}$. Hence $\bigcup_{y\in V^P}[\![\varphi(x,y)]\!] = \bigcup_{y\in V^P_{\alpha_x}}[\![\varphi(x,y)]\!]$. We let $\beta = \bigcup\{\alpha_x \mid x \in dom(u)\}$. Then

$$\begin{aligned}
[\![\forall x \in u \exists y \varphi(x,y)]\!] &= \bigcap_{x\in dom(u)} (u(x) \to (\bigcup_{y\in V^P} [\![\varphi(x,y)]\!])^{\perp\perp}) \\
&= \bigcap_{x\in dom(u)} (u(x) \to (\bigcup_{y\in V^P_{\alpha_x}} [\![\varphi(x,y)]\!])^{\perp\perp}) \\
&\subset \bigcap_{x\in dom(u)} (u(x) \to (\bigcup_{y\in V^P_{\beta}} [\![\varphi(x,y)]\!])^{\perp\perp})
\end{aligned}$$

Now let $v \in V^P$ be such that $dom(v) = V^P_\beta$ and $1 \in v(t)$ for all $t \in dom(v)$. Then

$$\begin{aligned}
(\bigcup_{y\in V^P_\beta} [\![\varphi(x,y)]\!])^{\perp\perp} &\subset (\bigcup_{y\in dom(v)} (v(y) \otimes [\![\varphi(x,y)]\!]))^{\perp\perp} \\
&= [\![\exists y \in v(\varphi(x,y))]\!]
\end{aligned}$$

Hence $\bigcup_{x\in dom(u)}(u(x) \to (\bigcup_{y\in V^P_\beta}[\![\varphi(x,y)]\!])^{\perp\perp}) \subset \bigcup_{x\in dom(u)}(u(x) \to [\![\exists y \in v(\varphi(x,y))]\!])$.

(Infinity): Define $Y \in V^P$ in such a way that

- $\emptyset \in dom(Y)$
- If $x \in dom(Y)$, then $x \cup \{x\} \in Y$
- $1 \in Y(\emptyset)$
- $Y(x) \subset Y(x \cup \{x\})$ for all $x \in dom(Y)$

Notice that if $\rho(x) = \alpha$, then $\rho(\{x\}) = \alpha + 1$ and $\rho(\{x, \{x\}\}) = \alpha + \omega + 1$. Also, $\rho(x \cup \{x\}) = \rho(\bigcup\{x, \{x\}\}) \leq \rho(\{x, \{x\}\})$. Hence, given $\emptyset \in V^P_\alpha$, we can have $Y \in V^P_{\alpha+\omega\cdot\omega}$. Therefore, $Y \in V^P$.

Since $1 \in Y(\emptyset) \subset [\![\emptyset \in Y]\!]$, it suffices to show $1 \in [\![\forall x(x \in Y \to x \cup \{x\} \in Y)]\!] = \bigcap_{x \in dom(Y)}(Y(x) \to (\bigcup_{z \in dom(Y)}(Y(z) \otimes [\![z = x \cup \{x\}]\!]))^{\perp\perp})$. Now for any $x \in dom(Y)$,

$$\begin{aligned}
Y(x) &\subset Y(x \cup \{x\}) \\
&\subset Y(x \cup \{x\}) \otimes [\![x \cup \{x\} = x \cup \{x\}]\!] \\
&\subset \bigcup_{z \in dom(Y)} (Y(z) \otimes [\![z = x \cup \{x\}]\!]) \\
&\subset (\bigcup_{z \in dom(Y)} (Y(z) \otimes [\![z = x \cup \{x\}]\!]))^{\perp\perp}
\end{aligned}$$

∎

Theorem 6.39 *ZFL is consistent.*

Proof

Let V^P be based on the phase space P such that $1 \notin \perp$. All the axioms in ZFL are valid in V^P and validity is preserved under inference rules of linear logic. Suppose $\vdash_{ZFL} A$ and $\vdash_{ZFL} A^\perp$. Then $1 \in [\![A]\!]$ and $1 \in [\![A^\perp]\!] = ([\![A]\!])^\perp$. From the latter, we have $[\![A]\!] = \{1\} \cdot [\![A]\!] \in \perp$. Hence $1 \in \perp$. This is a contradiction. ∎

Chapter 7

Conclusion

7.1 Introduction

In this chapter, we will discuss the application of linear set theory to the foundations of category theory. The work is still in progress, and we will be content with working out enough detail so that we can see clearly the problems to be overcome.

The foundations of category theory is particularly suitable as the benchmark of the usefulness of linear set theory. This is because category theory provides numerous examples of self-referential mathematical propositions which are evidently true on the intuitive ground but cannot be formalized in the standard set theories due to the set-theoretical paradoxes.

We do not believe that category theory is the only place where we can find the application of linear set theory. On the contrary, the strong connection of linear logic with computer science suggests that linear set theory may find a niche in some areas of computer science, for example, as the logical framework for concurrent processes. However, the elaboration of this idea is reserved for another occasion.

7.2 The foundations of category theory

7.2.1 The foundational problem of category theory

We first review the problem in the foundations of category theory, and the standard solutions to it.

In category theory and universal algebra, we often talk as if we assume totalities of certain kinds of structures, such as groups, topological spaces or even plain sets. For example, we talk about the category of groups, consisting of the collections of all groups and homomorphism, or even the category of sets, consisting of the collections of all sets and functions.

However, if we understand them literally, we cannot have such collections, or totalities, as sets in the standard Zermelo-Fraenkel set theory ZF. In fact, we can prove that the set of all sets does not exist, since we can derive contradiction from assuming its existence.

One way to deal with this problem is to introduce the universe set V, which is a model of ZF, and call a set A small if A belongs to V. We then interpret the totalities as the totalities of all small sets satisfying a certain condition. Another way is to use the Gödel-Bernays set theory. The totalities then become proper classes [17].

In either of the solutions, however, a totality thus interpreted cannot be a member of itself. The set of all small sets, for example, is just the universe set V itself, which is not a small set. Similarly, no proper class can be a member of another class, let alone itself.

From the point of view of the foundations of mathematics, this is not a very satisfactory situation. There are indeed numerous self-referential propositions, which are evident on the intuitive ground but cannot be formalized due to the above restriction. The following are typical examples of this kind [4].

- The collection of all partially ordered sets is a partially ordered set with the substructure relation.
- The collection of all pre-well-ordered sets is a pre-well-ordered set with the embedding relation.
- The collections of all categories and functors itself form a category.
- The collections of all functors and natural transformations form a category.

In this context, many people favors Quine's NF, or more precisely NFU, which has the unrestricted comprehension over stratified formulas. The consistency of NFU was shown by Jensen, and we can prove the above propositions as theorems in a suitable consistent extension of NFU.

We believe, however, that linear set theory will give yet another possibility for the foundations of category theory and universal algebra. In fact, AZF is developed with this specific application in mind. Unfortunately, we find that AZF is not yet sufficiently useful for the natural formalization of category theory. In the following, we will report our findings about pros and cons of linear set theory towards this goal. Our focus is in particular on the third proposition above, *i.e.* , the category of all categories and functors.

7.2.2 Basic mathematical construction in AZF

We start by exhibiting that most of the basic mathematical constructions can be carried out in AZF in the exactly the same way as in ZF. However, we need to modify the definition of domain and range of a function in a way suitable to linear logic. Since most of the proofs are straightforforward, we often state results only.

First of all, we define ordered pairs by using the additive disjunction, which can be shown to have the required property or pairing by the straightforward argument by cases.

Definition 7.1 *Let s and t be any terms. Then the ordered pair $\langle s, t\rangle$ is defined as follows:*

1. $\{s, t\} =_{def} \{\mathbf{x} : \mathbf{x} = s \oplus \mathbf{x} = t\}$
2. $\{s\} =_{def} \{s, s\}$
3. $\langle s, t\rangle =_{def} \{\{s\}, \{s, t\}\}$

Proposition 7.2 *For any S-terms s, t, s' and t'*

1. $\langle s, t\rangle = \langle s', t'\rangle \vdash s = s'$
2. $\langle s, t\rangle = \langle s', t'\rangle \vdash t = t'$
3. $\langle s, t\rangle = \langle s', t'\rangle \vdash s = s' \otimes t = t'$
4. $s = s', t = t' \vdash \langle s, t\rangle = \langle s', t'\rangle$

are all provable in AZF.

We note that the additive disjunction behaves in a similar way as the intuitionistic disjunction so that we cannot use the excluded middle in the proof. Furthermore, it is important to notice that we can obtain the above result since we have the contraction over equalities in AZF.

The flexibility given by the contraction to the equality thus make it possible to define the ordered pairs. However, our equality is not flexible enough since it lacks the extensionality. According to our diagnosis, this is the most serious defect of linear set theory, which will be discussed more extensively later. At this moment, we only need to define a new predicate to say that two sets are extensionally equivalent.

Definition 7.3 *We define the extensional equivalence $s \simeq t$ of two terms as follows:*

- $s \simeq t \Leftrightarrow_{def} \bigwedge \mathbf{x}.(\mathbf{x} \in s \multimap \mathbf{x} \in t) \,\&\, \bigwedge \mathbf{y}.(\mathbf{y} \in t \multimap \mathbf{y} \in s)$

Now we proceed to define relations, functions and their compositions in linear set theory.

Definition 7.4 *Let A and B be any sets.*

1. $A \times B =_{def} \{\mathbf{x} : \bigvee \mathbf{yz}.(\mathbf{x} = \langle \mathbf{y}, \mathbf{z} \rangle \otimes \mathbf{y} \in A \otimes \mathbf{z} \in B)\}$
2. $rel(A) \Leftrightarrow_{def} \bigwedge \mathbf{x}.(\mathbf{x} \in A \multimap \bigvee \mathbf{yz}(\mathbf{x} = \langle \mathbf{y}, \mathbf{z} \rangle \otimes \langle \mathbf{y}, \mathbf{z} \rangle \in A))$
3. $A \subseteq B \Leftrightarrow_{def} \bigwedge \mathbf{x}.(\mathbf{x} \in A \multimap \mathbf{y} \in B)$
4. $uniA \Leftrightarrow_{def} \bigwedge \mathbf{xyz}.(\langle \mathbf{x}, \mathbf{y} \rangle \in A \otimes \langle \mathbf{x}, \mathbf{z} \rangle \in A \multimap y = z)$
5. $fun(A) \Leftrightarrow_{def} rel(A) \otimes uni(A)$
6. $B \circ A =_{def} \{\mathbf{x} : \bigvee \mathbf{ywz}(\mathbf{x} = \langle \mathbf{y}, \mathbf{z} \rangle \otimes \langle \mathbf{y}, \mathbf{w} \rangle \in A \otimes \langle \mathbf{w}, \mathbf{z} \rangle \in B)\}$

Proposition 7.5 *Let A and B be any sets. Then*

1. $\vdash rel(B \circ A)$
2. $uni(A) \otimes uni(B) \vdash uni(B \circ A)$
3. $fun(A) \otimes fun(B) \vdash fun(B \circ A)$

are all provable in AZF.

However, we need to modify the standard definition of the domain and the range of a function. The standard definition is as follows:

Definition 7.6 *Let A, B and C be any sets.*

1. $dom(A) =_{def} \{\mathbf{x} : \bigvee \mathbf{y}.(\langle \mathbf{x}, \mathbf{y} \rangle \in A)\}$
2. $ran(A) =_{def} \{\mathbf{y} : \bigvee \mathbf{x}.(\langle \mathbf{x}, \mathbf{y} \rangle \in A)\}$
3. $A : B \to C \Leftrightarrow_{def} fun(A) \otimes dom(A) \simeq B \otimes ran(A) \subseteq C$

The problem occurs from this standard definition when we make the composition $B \circ A$ of two functions $A : C \to D$ and $B : D \to E$ and consider its domain and range. In classical logic, we can easily show $B \circ A : C \to E$. In linear logic, however, this is not the case.

In fact, we can easily show:

Proposition 7.7 *Let A and B be any sets. Then*

1. $\vdash dom(B \circ A) \subseteq dom(A)$
2. $\vdash ran(B \circ A) \subseteq ran(B)$

are provable in AZF.

However, we cannot obtain $\vdash dom(A) \subseteq dom(B \circ A)$ for $A : C \to D$ and $B : D \to E$. To see this, let's try to prove it in the standard way. First we assume $\langle \mathbf{x}, \mathbf{w} \rangle \in A$. Our goal is to derive $\langle \mathbf{x}, \mathbf{w} \rangle \in A \otimes \langle \mathbf{w}, \mathbf{y} \rangle$. From the assumption, we have $\mathbf{w} \in ran(A)$. Since $ran(A) \subseteq D$, we then have $\mathbf{w} \in D$ and hence $\mathbf{w} \in dom(B)$. Therefore $\langle \mathbf{w}, \mathbf{y} \rangle \in B$ for some $\mathbf{y}$. Hence we have

$$\langle \mathbf{x}, \mathbf{w} \rangle \in A \vdash \langle \mathbf{w}, \mathbf{y} \rangle \in B$$

In order to obtain our goal, however, we need one more assumption $\langle \mathbf{x}, \mathbf{w} \rangle \in A$ and use contraction, which is not in general possible.

Our solution to this problem is to use the weaker notion of domain and range, which is defined as follows.

Definition 7.8 *Let A, B and C any sets.*

$$A : B \circ\!\!\!\rightarrow C \Leftrightarrow_{def} fun(A) \otimes \bigwedge \mathbf{x}.(\mathbf{x} \in B \multimap \bigvee \mathbf{y}.(\langle \mathbf{x}, \mathbf{y} \rangle \in A \otimes \mathbf{y} \in C))$$

Construed in classical logic, $A : B \to C$ implies $A : B \circ\!\!\!\rightarrow C$. On the other hand, $A : B \circ\!\!\!\rightarrow C$ only implies that A is defined over B, or $B \subseteq dom(A)$, and the image of B under A is a subset of C. In linear logic, this weaker notion of domain and range behaves nicely with respect to composition.

Proposition 7.9 *Let A, B, C, D and E be any sets. Then,*

$$A : C \circ\!\!\!\rightarrow D \otimes B : D \circ\!\!\!\rightarrow E \vdash B \circ A : C \circ\!\!\!\rightarrow E$$

is provable in AZF.

Proof

Since $fun(A)$ and $fun(B)$ implies $fun(B \circ A)$, it suffices to derive $\bigvee \mathbf{z}.(\langle \mathbf{x}, \mathbf{z} \rangle \in B \circ A \otimes \mathbf{z} \in E)$ from the assumptions:

1. $\mathbf{x} \in C$
2. $\bigwedge \mathbf{x}.(\mathbf{x} \in C \multimap \bigvee \mathbf{y}.(\langle \mathbf{x}, \mathbf{y} \rangle \in A \otimes \mathbf{y} \in D))$
3. $\bigwedge \mathbf{x}.(\mathbf{x} \in D \multimap \bigvee \mathbf{y}.(\langle \mathbf{x}, \mathbf{y} \rangle \in B \otimes \mathbf{y} \in E))$

From the first and second assumptions, we have $\langle \mathbf{x}, \mathbf{y} \rangle \in A$ and $\mathbf{y} \in D$. Using the latter and the third assumption, we have $\langle \mathbf{y}, \mathbf{z} \rangle \in B$ and $\mathbf{z} \in E$ together with $\langle \mathbf{x}, \mathbf{y} \rangle \in A$. Hence $\langle \mathbf{x}, \mathbf{z} \rangle \in B \circ A$ and $\mathbf{z} \in E$. The conclusion follows immediately from this. ∎

Furthermore, we obtain certain flexibility in defining useful functions.

Definition 7.10 *We define the identity function I as follows:*

$$I =_{def} \{\mathbf{x} : \bigvee \mathbf{y}.(\mathbf{x} = \langle \mathbf{y}, \mathbf{y} \rangle)\}$$

Proposition 7.11 *For any set A,*

$$\vdash I : A \circ\!\!\rightarrow A$$

is provable in AZF.

Proposition 7.12 *For any set A,*

1. $\vdash A \circ I \subseteq A$
2. $\vdash \bigwedge \mathbf{xy}.(\langle \mathbf{x}, \mathbf{y} \rangle \in A \multimap \langle \mathbf{x}, \mathbf{y} \rangle \in A \circ I)$
3. $\vdash I \circ A \subseteq A$
4. $\vdash \bigwedge \mathbf{xy}.(\langle \mathbf{x}, \mathbf{y} \rangle \in A \multimap \langle \mathbf{x}, \mathbf{y} \rangle \in I \circ A)$

are all provable in AZF.

7.2.3 Categories and functors

We now review the definitions of categories and functors. A category is a collection of objects and arrows together with the identity arrows and the associative composition operation.

Each arrow f is equiped with a unique domain A and codomain B. This is denoted $A \xrightarrow{f} B$. For each object A, there is a unique identity arrow $A \xrightarrow{1_A} A$.

In order to specify a category $\mathcal{C}$, hence, we need the following information:

- The collection O of the objects in $\mathcal{C}$
- The collection A of the arrows in $\mathcal{C}$
- The function D which maps an arrow to an object as its domain
- The function C which maps an arrow to an object as its codomain
- The function E which maps an object to an arrow as its identity
- The function M which maps a composable pair of arrows to an arrow as their composition

where a pair of arrows f and g are composable if the codomain of f is the domain of g. Furthermore, they need to satisfy the following commutativity conditions:

(Com1) The domain of the identity for an object A is A and so is its codomain

(Com2) The composition of an arrow f with an identity is identical to f itself

(Com3) The domain of the composition of the two arrows f and g is the domain of f, and its codomain is the codomain of g

(Com4) The composition operation is associative

A functor $\mathcal{F}$ from a category $\mathcal{C}$ to $\mathcal{D}$ is a pair of maps FO and FA such that FO is a map from the objects of $\mathcal{C}$ to the objects of $\mathcal{D}$ and FA is from the arrows of $\mathcal{C}$ to the arrows of $\mathcal{D}$. Furthermore, they together preserve

(Pres1) identity, *i.e*, $FA(1_A) = 1_{FO(A)}$

(Pres2) domain and codomain, *i.e.*, FA sends $A \xrightarrow{f} B$ to $FO(A) \xrightarrow{FA(f)} FO(B)$

(Pres3) composition, *i.e.*, $FA(g \circ f) = FA(g) \circ FA(f)$

In classical mathematics, it is easy to show that the composition of two functors is again a functor with the appropriate domain and range. Furthermore, the identity functor for a category $\mathcal{C}$ is just a pair of identity functions. Since the composition of two functions is always associative, we can easily see that the collection of functors satisfy the conditions (Com1)-(Com4), under whatever interpretation we may have for this collection. This implies that the collections of all categories and functors together form a category.

In linear logic, however, things do not move as smoothly as in classical logic. Interestingly, most of the problems happen where we would say they are trivial if we were in classical logic. In fact, it is not difficult to show in linear logic:

Proposition 7.13 *The composition of two functors satisfies the preservation conditions (Pres1)-(Pres3).*

Furthermore, this can be shown by using only the information that the two functors to be composed satisfy the preservation conditions.

7.2.4 The problems

As far as we can see, there are three main problems in developing category theory in linear logic. They are:

- The domain and range of the composition of two functions
- The domain and range of the identity functor
- The lack of extensionality

The first two are surmountable. However, the last seems to pose a real problem

The domain and range of the funtorial composition

This problem was already pointed out when we developed basic mathematical constructions in linear set theory, *i.e.* we cannot show in linear logic that the composition of two functions has the same domain as its first component function.

Our solution to this problem was to modify the definition of domain and range of a functions so that it becomes "lean" and we can prove the required property for it in linear logic. However, the question to be asked is what kind of effects this modifictaion has in the overall development of mathematics.

As we have seen in the definition of the identity I, the new definition seems to have favorable effects in some situations. Combined with the use of unrestricted comprehension, it indeed gives us more flexibility in defining function that the standard one.

On the other hand, we cannot read off the domain of a function from the function itself. One consequence of this is that we need to deal with the triple of a function, its domain and range as one package if we want to talk about a function with specific domain and range.

In relation to category theory, this means that we need to define functors as a pair of functions together with the two categories, which are the domain and codomain of the functor, *i.e.*, as the tuple $\langle FO, FA, \mathcal{C}, \mathcal{D} \rangle$. Otherwise, we cannot have the functions D and C which assign the domain and codomain to arrows, when we want to talk about the category of all categories and functors. In conjunction with the lack of extensionality, this brings in a certain difficulty in our project.

In fact, it is not unlikely that some unexpected problems occur in developing mathematics due to our new definition of domain and range. This gives us a good reason to keep alert on the use of this new definition.

The domain and range of identity functors

This problem occurs when we define the function E for the category of all categories and functors. We define this function simply as the S-set which sends a category $\mathcal{C}$ to the tuple $\langle I, I, \mathcal{C}, \mathcal{C} \rangle$. We then need to show that this tuple is indeed a functor, and for that , we need to show that $\mathcal{C}$ is a category for both of the occurrences of $\mathcal{C}$. In other words, we need to show twice that $\mathcal{C}$ is a category. Since the information that $\mathcal{C}$ is a category is available only once, this is not feasible.

However, there is a solution to this problem. We just use the additive conjunction to say that both $\mathcal{C}$ and $\mathcal{D}$ must be categories for the tuple $\langle FO, FA, \mathcal{C}, \mathcal{D} \rangle$ to be a functor. Then we do not need to use the information that $\mathcal{C}$ is category twice, to show that $\mathcal{C}$ and $\mathcal{C}$ are categories. Indeed, we can in general show $A \vdash A \,\&\, A$.

As far as the proof of the category of all categories and functors is concerned, this trick does not impede other definitions and proofs, although unexpected effects may be lurking again in the further development.

The lack of extensionality

This problem again involves composition. The commutativity conditions (Com2) says that the composition of an arrow with the appropriate identity is identical to the arrow itself. The condition (Com4) says that the composition of three arrows is always unique reagrdless the order of composition. For the proof of category of all categories and functors, we need to show those properties for the functors, and eventually for two component functions FO and FA.

The problem is that if we understand the identity of two functions as the equality, we have no way to prove it for the lack of extensionality. We can certainly prove that the composition of a function with the identity is extensionally equivalent to the function itself, or the composition $f \circ (g \circ h)$ to $(f \circ g) \circ h$, but this is as far as we can go.

One obvious way out from this is to understand the identity of two functions as their extensional equivalence. In fact, this is the way we first pursue this project. However, there are at least two reasons to doubt the plausibility of this approach.

One reason is rather philosophical. The use of extensional equivalence in place of equality limits the capacity of category theory as an equation theory. Certainly we do have the extensionality for Z-terms in AZF, and it seems possible to argue that this delimitation is only for S-terms, which are peculiar objects anyway. However convincing this argument may be, it seems certain that no one would prefer this heterogeneous approach to the uniform one, if the latter is obtainable.

The other reason is more technical. Recall that we need to encode functors as tuples $\langle FO, FA, \mathcal{C}, \mathcal{D}\rangle$. It is easy to show that the associativity in the sense of extensional equivalence for the two function parts FO and FA. However, this does not lead to the associativity of the whole tuples, since pairing blocks the transition. Therefore, we cannot prove the associativity of functor compositions even under the extensional equivalence.

As a matter of fact, it is possible to define pairs such that two pairs are extensional equivalent if all of their corresponding components are extensionally equivalent, or even pairs which mix equality and extensional equivalence. However, this maneuver distracts the proof that the compostion operation of functors is a function. It seems feasible to relax the definition of function only for this specific case and regard the composition operation as a special type of function, but this move looks too *ad hoc*.

7.3 The extensionality in linear set theory

The diagnosis of linear set theory in the previous section indicates that it is necessary to have the extensionality at least for some limited cases, in order for linear set theory to be useful. Surely, we have already seen Grishin's result that linear set theory becomes inconsistent if both the substitutivity and the extensionality are present. However, we believe that there is a good reason for not taking Grishin's result as the final word on the issue.

In this section, we first give our analysis of Grishin's result, particularly with respect to the plausibiliy of consistent extension of linear set theory with the extensionality. We then make specific proposals and conjectures.

7.3.1 Grishin's paradox revisited

Let's recall that Grishin's result rests on the combination of two points:

1. The substitutivity implies the contraction over equalities
2. The extensionalty implies the existence of an equality formula $s = t$ for each formula A such that $s = t$ is logically equivalent to A in linear logic

We find that the first point is indisputable. It is true that the substitutivity allows the duplication of terms in substitution, which is reponsible for the contraction over equalities, and this seems to violate the spirit of linear logic. However, the same is true for the comprehension, which allows us to abstract over multiple occurrences of a variable at once. In fact, it is no use to prohibit the duplication in substitution without changing the comprehension at the same time, since the former can be recovered through the latter. We simply abstract over the multiple occurrences of a term t in a formula A so that we have the formula $t \in \{\mathbf{x} : A[\mathbf{x}/t]\}$, and substitute t on the left by s. We then move the term s back inside A. Hence, unless we want to make a change in the comphension, we have to accept the first point.

The second point consists of two derivations, *i.e.*, the derivation of the sequent $s = t \vdash A$ and that of $A \vdash s = t$. The first derivation is obtained essentially by the weakening, and we do not consider it problematic. The second derivation, however, makes an essential use of the extensionality, and this is the place where we find most critical.

We now reproduce the second derivation, using the double-sided formulation.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{x = w \vdash x = w}{x = w, A \vdash x = w}}{x = w \otimes A \vdash x = w}}{x \in \{x : x = w \otimes A\} \vdash x = w}}{x \in t \vdash x \in s} \qquad \dfrac{\dfrac{\dfrac{A \vdash A \quad x = w \vdash x = w}{A, x = w \vdash x = w \otimes A}}{A, x = w \vdash x \in t}}{A, x \in s \vdash x \in t}}{A \vdash s = t}$$

where s is $\{x : x = w\}$ and t is $\{x : x = w \otimes A\}$. As before, we are ignoring the distinction between S-variables and Z-variables since the issue is not specific to our LZF or AZF.

In this derivation, the extensionality is used at the last step, with the formula A as the parametric formula or the context. We believe that this use of A as the context of the extensionality is the main cause of the inconsistency. To put it differently, the context with which the extensionality is applicable should be restricted.

In fact, we have already encountered a similar situation to this in the introduction rule for the exponential !. In the double-sided formulation, it could be as follows:

$$\dfrac{!\Gamma \vdash A}{!\Gamma \vdash\, !A}$$

This rule is saying that we can make a formula A left-side contractible only when all the formulas in the context are also left-side contractible. We can indeed make this ideas as the general principle:

- For any rule of inference which introduces a left-side contractible formula, all the formulas in the context must also be left-side contractible.

This general principle makes sense particularly in relation to cut-elimination. Suppose that we have a new rule of inference $(*)$ which introduces a left-side contractible formula C. Consider the following proof which ends with a cut:

$$\dfrac{\begin{matrix}\vdots\pi_1 \\ \Gamma \vdash C\end{matrix} \qquad \begin{matrix}\vdots\pi_2 \\ C, \Delta \vdash \Theta\end{matrix}}{\Gamma, \Delta \vdash \Theta}$$

Let's suppose that the last rule of inference of π_1 is $(*)$ with the formula C as the main formula to exclude the possibility of permutation, and the formula C in π_2 is obtained as the result of left-side contraction. Then the cut-elimination would duplicate π_1 and hence

Γ, and we need to use contraction over Γ to cancel out the duplication. For example, we would have a pattern as follows:

$$\dfrac{\dfrac{\dfrac{\vdots\pi_1}{\Gamma \vdash C} \qquad \dfrac{\dfrac{\vdots\pi_1}{\Gamma \vdash C} \quad C, C, \Delta \vdash \Theta}{C, \Gamma, \Delta \vdash \Theta}}{\Gamma, \Gamma, \Delta \vdash \Theta}}{\Gamma, \Delta \vdash \Theta}$$

This demonstrates that the context Γ for the rule $(*)$ need to be left-side contractible in the first place to carry out the above reduction.

7.3.2 The proper formulation of the extensionality for linear set theory

The preceding discussion gives us a good reason to hope that we can have a consistent extension of AZF with the extensionality properly formulated. We now make two specific proposals about the proper formulation of the extensionality.

The first proposal is to restrict the context of the extensionality rule to formulas of the form $!A$ or $s = t$ on the left, both of which are evidently left-side contractible. Then the rule would be written as follows:

$$(EXT) \quad \frac{!\Gamma, \mathbf{x} \in s \vdash \mathbf{x} \in t \quad !\Delta, \mathbf{y} \in t \vdash \mathbf{y} \in s}{!\Gamma, !\Delta \vdash s = t}$$

where $!\Gamma$ is understood as described above. It is certainly possible to conceive the additive version of this, but we prefer the multiplicative version at this moment since the former is derived from the latter.

We find this formulation of the extensionality very natural, given our general principle. However, it seems that (EXT) brings in a fair amount of complexity in the system and we need to find a new method for the consistency proof. For this reason, we propose another formulation of the extensionality, which completely dispenses with the context:

$$(EXT^*) \quad \frac{\mathbf{x} \in s \vdash \mathbf{x} \in t \quad \mathbf{y} \in t \vdash \mathbf{y} \in s}{\vdash s = t}$$

In fact, this much weaker version of the extensionality is sufficiently useful for the problem that we have encountered in proving the category of all ctagories and functors. The associativity of functional composition can be proved easily without using any contexts. The composition of a function with the identity is also proved to be equal to itself by (EXT^*), although we need to modify the definition of relation slightly.

Our method of consistency proof in terms of size is not directly applicable even to a system with (EXT^*), since we no longer have a good control over duplication created in the cut-elimination process. This is in contrast to AZF where only equalities proliferate by the duplication.

Therfore, it may be necessary to impose further restriction on (EXT^*) if we want to obtain the consistency result by our method. However, we should note that we tried various restrictions and none of them has worked so far.

It is also worth noting that the method of *candidat de réducibilité* has only a limited success in the normalization of set theory, since it requires a well-ordering among terms. However we should not exclude the possibility that things might be easier in linear set theory.

In any case, the consistency of the system of linear set theory extended with either (EXT) or (EXT^*) is an open problem. We conclude our discussion on this issue by stating our conjectures explicitly.

Conjecture 7.14 *AZF extended with* (EXT) *is consistent.*

Conjecture 7.15 *AZF extended with* (EXT^*) *is consistent.*

7.4 Conclusion

Finally, we give a summary of what has been accomplished in this dissertation and indicate directions of further research.

7.4.1 Summary

The dissertation is mainly devoted to the proof-theoretic study of various systems of set theory based on linear logic. The main advantage of the use of linear logic is that we can have the unrestricted comprehension without making systems inconsistent.

In chapters 2 and 3, we present the systems SMALL and AS^∞ and prove their consistency by the cut-elimination method. SMALL is based on full linear logic, *i.e.*, with the exponentials, and AS^∞ is based on linear logic with the infinitary additives and the weakening, but without the exponentials. In both of the cases, the cut-elimination theorem is proved by induction on the size of a proof, defined in an appropriate way.

The main result of the dissertation is LZF, a system of linear set theory presented in chapter 4, which is a conservative extension of the Zermelo-Fraenkel set theory without the axiom of regularity. The proof of this result is by establishing the partial cut-elimination theorem, which is again proved by induction on the size. We further extend this system in chapter 5 to AZF, in which the substitution of equal terms are freely available.

The phase-valued models given in chapter 6 is our first attempt at the model-theoretic study of linear set theory. The result does not really give a model for the unrestricted comprehension but only for the axiom of separation and other standard ZF-style axioms. However, we believe that the result deserves some attention in terms of our understanding of the notion of linear sets.

The results and discussions in chapter 7 are intended to indicate the way to make linear set theory really useful, particularly in its application to the foundations of category theory. The need and plausibility of having the extensionality in linear set theory are the focal point of the whole discussion.

7.4.2 Direction of further reserach

There are three main areas in which we can expand our research on linear set theory:

- the proof-theoretic study
- the model-theoretic study
- applications

On the proof-theoretic side, the main issue seems to be the extensionality. Since we have already discussed this point extensively, we will focus on the other two areas of study.

The model-theoretic study of linear set theory

The model-theoretic study of linear set theory has been difficult for the combination of two reasons.

The first reason is that the model theory of propositional linear logic has not been very successful. In particular, the duality in classical linear logic poses a serious challenge, and it is only recently that promising lines of attack gradually emerge, for example, game semantics and Chu space model. Furthermore, the treatment of additives is still a big problem.

The second reason is that it is far from clear how we can give a model to a set theory with the unrestricted comprehension. There have been some progress in the modeling of set theory with the unrestricted comprehension over positive formulas in classical logic, and we certainly hope that this would give us at least a pointer to the modeling of linear set theory. However, the connection is not immediately clear, particularly because we do not have the restriction to positive formulas in linear set theory.

Nevertheless, we should note that the model theoretic studies of propositional linear logic and universal set theory are under way and pursued feverishly at present, and we have good reason to expect more progress in both of the fields. Along with it, we hope that we can obtain more satisfactory model theory for linear set theory than the phase-valued models.

Applications

The only possible application of linear set theory that we have discussed at some length is to the foundations of category theory. However, as we have noted already, the applications of linear set theory to various areas of computer science should be explored.

First of all, the capability of linear logic to distinguish multiple occurrences of formulas from each other seems to be particularly suitable for computer science, in which we need to distingush multiple processes of the same kind from each other.

Secondly, there is a growing interest in universal set theory in the computer science community, particularly for its ability to represent processes in a straightforward way.

In addition, the dynamic flavor of linear logic suggests that linear set theory might be useful for describing the systems which involve temporal development or change.

Theory and application are two separate matters. However, we learn from the history that the cross-fertilization between them is indeed possible and most fruitful. We strongly hope that our work on linear set theory will be the starting point of this exciting and "self-referential" back and forth process.

Bibliography

[1] S. Abramsky and R. Jagadeesan. "Games and full completeness for multiplicative linear logic." *Technical Report DoC 92/24*, Department of Computing, Imperial College, London, 1992.

[2] A. Asperti and G. Longo. *Categories, Types and Structures: An Introduction to Category Theory for the Working Computer Scientist*, The MIT Press, Cambridge, Massachusetts, 1991.

[3] P.J. Cohen. *Set Theory and the Continuum Hypothesis*, Benjamin, New York, 1966.

[4] S. Feferman. "Some formal systems for the unlimited theory of structures and categories." *unpublished*, Department of Mathematics, Stanford University, Stanford, 1974.

[5] M. Forti and F. Honsell. "Models of self-descriptive set theories." *Partial Differential Equations and the Calculus of Variations*, Vol. 1, *ed.* by F. Colombini, A. Marino, L. Modica and S. Spagnolo, Birkhaüser, Boston, 1989.

[6] M.P. Fourman and D. Scott. "Sheaves and logic." *Applications of Sheaves*, Springer Lecture Notes in Mathematics 753, Berlin, 1979, 302-401.

[7] J.Y. Girard. "Linear logic." *Theoretical computer science*, 50 (1987) 1-102.

[8] J.Y. Girard. "Geometry of interaction I : Interpretation of system F." *Logic Colloquium '88*, North-Holland, Amsterdam, 1989.

[9] J.Y. Girard, Y. Lafont and P. Taylor. *Proofs and Types*, Cambridge University Press, Cambridge, 1989.

[10] J.Y. Girard, A. Scedrov and P.J. Scott. "Bounded linear logic." *Theoretical Computer Science*, 97 (1992) 1-66.

[11] K. Gödel. "The consistency of the axiom of choice and of the generalized continuum hypothesis with the axioms of set theory." *Collected Works*, Vol. II, Clarendon Press, Oxford, 1986, 33-101.

[12] V.N. Grishin. "A nonstandard logic and its application to set theory," (Russian). *Studies in Formalized Languages and Nonclassical Logics (Russian)*, Izdat, "Nauka," Moskow, 1974, 135-171.

[13] V.N. Grishin. "Predicate and set-theoretic calculi based on logic without contraction rules," (Russian). *Izvestiya Akademii Nauk SSSR Seriya Matematicheskaya*, 45, no. 1, 1981, 47-68, 239. *Math. USSR Izv.*, 18, no. 1, 1982, 41-59 (English translation).

[14] L. Hallnäs. *On Normalization of Proofs in Set Theory*, Dissertiones Mathematicae 261. Polska Akademia Nauk, Instytut Matematyczny, Warszawa, 1988.

[15] T.J. Jech. *Set Theory.* Academic Press, New York, 1978.

[16] J. Lambek. "Deductive systems and categories." *I. J. Math. Systems Theory*, 2, 1968, 278-318.

[17] S. Mac Lane. *Categories for the Working Mathematician*, Springer, New York, 1971.

[18] S. Mac Lane and L. Moerdijk. *Sheaves in Geometry and Logic*, Springer, New York, 1992.

[19] Per Martin-Löf. *Intuitionistic Type Theory*, Bibliopolis, Napoli, 1984.

[20] G.E. Mints. "Closed categories and theory of proofs." *Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Mat. Instituta im. V.A. Steklova*, AN SSSR 68, 1977, 83-114.

[21] Y. Moschovakis. "The formal language of recursion." *The Journal of Symbolic Logic*, 54, 1989, 1216-1252.

[22] W. Pohlers. *Proof Theory*, Springer, Berlin, 1989.

[23] V. R. Pratt. "The second calculus of binary relations." *MFCS'93, Gdańsk*, Poland, 1993.

[24] D. Prawitz. "Normalizations of Proofs in Set Theory." *Atti Degli Incontri di Logica Matematica*, Vol.2. Scuola di Specializzazione in Logica Matematica, Dipartimento di Matematica, Università di Siena, 1984.

[25] P. Schroeder-Heister. "Cut-elimination in logics with definitional reflection." *Nonclassical Logic and Information Processing*, Springer, Berlin, 1992, 146-171.

[26] A. Scedrov. "A brief guide to linear logic." *Bulletin of the European Association for Theoretical Computer Science*, Vol. 41, June, 1990, 154-165.

[27] R.A.G. Seely. "Linear logic, $*$-autonomous categories and cofree coalgebras." *Categories in Computer Science and Logic*, American Mathematical Society, Providence, 1989.

[28] G. Takeuti. "Quantum set theory." *Current Issues in Quantum Logic*, Plenum, New York, 1981, 303-322.

[29] G. Takeuti and W.M. Zaring. *Axiomatic Set Theory*, Springer, New York, 1973.

[30] R.B. White. "A consistent theory of attributes in a logic without contraction." To appear in *Studia Logica*.