PUBLIC ANNOUNCEMENT LOGIC
IN CRYPTOGRAPHIC PROTOCOL

MUHAMMAD FARHAN BIN MOHD NASIR

FACULTY OF SCIENCE
UNIVERSITY OF MALAYA
KUALA LUMPUR

2019

PUBLIC ANNOUNCEMENT LOGIC IN CRYPTOGRAPHIC PROTOCOL

MUHAMMAD FARHAN BIN MOHD NASIR

DISSERTATION SUBMITTED IN FULFILMENT OF THE
REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE

INSTITUTE OF MATHEMATICAL SCIENCES
FACULTY OF SCIENCE
UNIVERSITY OF MALAYA
KUALA LUMPUR

2019

UNIVERSITY OF MALAYA

ORIGINAL LITERARY WORK DECLARATION

Name of Candidate: **MUHAMMAD FARHAN BIN MOHD NASIR**

Matric No: **SMA170032**

Name of Degree: **MASTER OF SCIENCE**

Title of Dissertation ("this Work"):

PUBLIC ANNOUNCEMENT LOGIC IN CRYPTOGRAPHIC PROTOCOL

Field of Study: **PURE MATHEMATICS**

I do solemnly and sincerely declare that:

(1) I am the sole author/writer of this Work;
(2) This work is original;
(3) Any use of any work in which copyright exists was done by way of fair dealing and for permitted purposes and any excerpt or extract from, or reference to or reproduction of any copyright work has been disclosed expressly and sufficiently and the title of the Work and its authorship have been acknowledged in this Work;
(4) I do not have any actual knowledge nor do I ought reasonably to know that the making of this work constitutes an infringement of any copyright work;
(5) I hereby assign all and every rights in the copyright to this Work to the University of Malaya ("UM"), who henceforth shall be owner of the copyright in this Work and that any reproduction or use in any form or by any means whatsoever is prohibited without the written consent of UM having been first had and obtained;
(6) I am fully aware that if in the course of making this Work I have infringed any copyright whether intentionally or otherwise, I may be subject to legal action or any other action as may be determined by UM.

Candidate's Signature Date:
18 December 2019

Subscribed and solemnly declared before,

Witness's Signature Date:

Name:
Designation:

PUBLIC ANNOUNCEMENT LOGIC IN CRYPTOGRAPHIC PROTOCOL

ABSTRACT

Public announcement logic with common knowledge (PAC) is a logic that formalizes the notion of epistemic update. The main objective of this study is to propose a labelled natural deduction proof system for PAC and to show some applications of PAC in the cryptographic protocol. We begin by modifying the Kripke model that is capable of giving semantics to formulas having announcement indexing. Then, a labelled natural deduction for PAC (**NPAC**) is proposed and its soundness and completeness are proven. Then, we proved its normalization using a proof-theoretic semantical notion of validity of a derivation. Finally, an application of PAC in cryptographic protocol is presented.

Keywords: Public announcement logic, common knowledge, labelled natural deduction, cryptographic protocol.

LOGIK PENGUMUMAN AWAM DALAM PROTOKOL KRIPTOGRAFI

ABSTRAK

Logik pengumuman awam dengan pengetahuan umum (PAC) ialah logik yang mengformalkan konsep bagi pengemaskinian pengetahuan. Matlamat utama kajian ini ialah untuk mencadangkan sistem bukti deduksi semulajadi berlabel bagi PAC dan tunjukkan beberapa kegunaan bagi PAC dalam protokol kriptografi. Kami mulakan dengan mengubah suai model Kripke yang mampu memberi makna terhadap rumus berindeks pengumuman. Seterusnya, deduksi semulajadi berlabel bagi logik pengumuman awam dengan pengetahuan umum (**NPAC**) dicadangkan dan kesempurnaan dan kelengkapannya dibuktikan. Kemudian, kami buktikan pengnormalannya dengan menggunakan konsep semantik teori bukti terhadap kesahihan suatu penerbitan. Akhir sekali, kegunaan bagi PAC dalam protokol kriptografi dibentangkan.

Kata kunci: Logik pengumuman awam, pengetahuan umum, deduksi semulajadi berlabel, protokol kriptografi.

ACKNOWLEDGEMENTS

I am to express my utmost gratitude to both of my supervisors: Associate Professor Dr. Wan Ainun binti Mior Othman and Associate Professor Dr. Wong Kok Bin. They have given me the guidance of doing a research within this past one year and a half. The training that I have received from them will definitely benefit me for my future. I appreciate every moment of encounter with them either for research purposes, administrative purposes, or even motivational purposes. All the grants that I have received to attend the international summer schools and seminars in Germany, Belgium, and Singapore will have never been realised should it not from their help and recommendation.

My gratitute goes also to both of my parents, Mohd Nasir bin Ahmad and Salasiah binti Dom Hamzah, who have been giving me ample freedom of me pursuing my journey in this very esoteric field of research whose future is still in the verge of uncertainty. Not to forget my friends, not the least of whom is Ahmad Fouad bin Abdul Mubin who has always been my closest friend and has also been aiding me financially. To all my colleagues in Persatuan Pendidikan Falsafah dan Pemikiran Malaysia, the reading groups, the seminars, the discussions, and the presentations have definitely encouraged my academic maturity.

Thank you very much everyone.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS AND ABBREVIATIONS

G	:	A finite set of agent-symbols
$C_\psi A$	:	A is a common knowledge for everyone in ψ
$\vDash \mathscr{A}$	:	$\mathscr{A}$ is true
$K_a A$	:	Agent a knows that A
$a, b, c, \ldots$	:	Agents
$\rho, \rho_1, \rho_2, \ldots$	:	Atomic formulas of the form $xR_a^{\varphi}y$, $xR_\psi^{\varphi}y$, or $xR_\psi^{\varphi*}y$
$p, q, r, \ldots$	:	Atomic propositions
$[A]B$	:	B after the announcement A
$\mathscr{A} \vdash \mathscr{B}, \mathscr{B} \dashv \mathscr{A}$	:	$\mathscr{B}$ is derivable from $\mathscr{A}$
$\mathscr{A} \dashv\vdash \mathscr{B}$	:	$\mathscr{B}$ is derivable from $\mathscr{A}$ and vice versa
$R_\psi, \mathcal{R}_\psi$	:	Binary relation of agents in ψ
$R_a, \mathcal{R}_a$	:	Binary relation of an agent a
$\wedge$	:	Conjunction
$\Pi, \Pi_1, \Pi_2, \ldots$	:	Derivations
$\vee$	:	Disjunction
$\mathcal{E}_\psi A$	:	Everyone in ψ knows that A
$\perp$	:	Falsum
$A, B, C, \ldots$	:	Formulas
$\mathscr{A} \vDash \mathscr{B}, \mathscr{B} \Dashv \mathscr{A}$	:	If $\mathscr{A}$ is true then $\mathscr{B}$ is true
$\mathscr{A} \Dashv\vDash \mathscr{B}$	:	If $\mathscr{A}$ is true then $\mathscr{B}$ is true and vice versa
$\supset$	:	Implication
$\mathcal{M}$	:	Kripke's model
$x : A$	:	Labelled formula
$\mathscr{A}, \mathscr{B}, \mathscr{C}, \ldots$	:	Labelled or relational formulas

$\varphi, \varphi_1, \varphi_2, \ldots$	:	List of labelled or relational formulas
$\neg$	:	Negation
$r(\mathscr{A})$	:	Rank of a formula $\mathscr{A}$
$xR_a y, xR_\psi y$	:	Relational formulas
$\psi, \psi_1, \psi_2, \ldots$	:	Set of agents
P	:	Set of atomic propositions
$\mathcal{R}_G$	:	Set of binary relations of agents in G
Δ	:	Set of formulas
Γ	:	Set of labelled or relational formulas
$\mathbb{R}$	:	Set of rules
$\mathcal{W}$	:	Set of worlds
$\mathcal{R}^*$	:	Transitive closure of a relation $\mathcal{R}$
$\mathcal{V}$	:	Valuation function from $\mathcal{W} \times P$ to $\{0, 1\}$
$x, y, z, \ldots$	:	Worlds
DEL	:	Dynamic Epistemic Logic
EAL	:	Epistemic Action Logic
PAC	:	Hilbert's Axiomatization for Public Announcement Logic with Common Knowledge
NPAC	:	Labelled Natural Deduction for Public Announcement Logic with Common Knowledge
ND	:	Natural Deduction
NP	:	Nondeterministic Polynomial Time
PTS	:	Proof-Theoretic Semantics
PAC	:	Public Announcement Logic with Common Knowledge
PAL	:	Public Announcement Logic

CHAPTER 1: INTRODUCTION

1.1 Literature Review

This introduction will begin very generally though briefly with the notion of logic. Since the public announcement logic that we are studying is one of the large classes of logic residing under the umbrella term of dynamic epistemic logic, we will begin also with the general notion of dynamic epistemic logic. A comprehensive introduction of public announcement logic will be presented in the next chapter. We will present here the problem statement and explicitly mention our objective and methodology.

The narrative of this literature review is historical instead of systematic. The systematic explanation (i.e. formal definitions and examples) will be given in the following chapters. We will first explain the differences between giving meaning (i.e. semantics) of a logical language by means of proof theory and by means of model theory. Then, dynamic epistemic logic is briefly introduced followed by its brief application on cryptographic protocol in current literature.

1.1.1 Proof-theoretic semantics and model-theoretic semantics

The dichotomy in studying formal logic or mathematical logic has been established since Frege's revolution on the study of logic. The dichotomy that is now called proof theory that studies the syntactical nature and provability of a logical language; and, model theory that studies the semantical nature and satisfiability of that language.

The study of semantics by means of proof theory or simply proof-theoretic semantics (PTS) is an alternative approach of semantics, in which it focuses on meaning-conferring by means of deductive systems, particularly of natural deduction (ND) system of inference. PTS focuses purely on its deductive proof of semantics which differs with the entrenched notion of model-theoretic semantics that maintains the semantics by means of its truth rather than its proof. This tradition of prescribing semantics using model-theoretic semantics has been used from Tarski's famous semantic theory of truth that lays down the foundation of almost all model theory.

By the description of proof theory stated, it is unusual, prima facie, as to how can one study meaning or semantics of a logic by its syntactical nature and provability. But this is exactly what is suggested by the proponent of inferentialist and of intuitionist. One of the main arguments conforming to this program is to argue that meaning is use, an argument being propounded by Wittgenstein (2009). The meaning of logical syntax for example is given of how the syntax is used. More particularly, the meaning of logical operator (e.g. negation $\neg$, conjunction $\wedge$, disjunction $\vee$, conditional $\supset$, existential $\exists$, and universal $\forall$) is given by how it is used by its introduction rule and elimination rule. More of the arguments can be referred to Weiss & Wanderer (2010), Brandom (2001), Peregrin (2014), Dummett (1991), and Wittgenstein (2009).

Coming back to PTS, although Gentzen (1964) has already made a short remark that his ND is capable of scrutinizing the investigation of logical operator, and although mathematical or technical ND has advanced further, thanks to Prawitz (1965); the philosophical underpinnings are to be credited to Dummett (1991) as he justifies, foundationally, the rejection of model theoretical notion of truth. Hence, PTS is inexorably propounded by Dummett as a new alternative to the inquiry of semantics and truth. Dummett, especially, rejects the principle of bivalence which has been presupposed by model theoretical study of semantics. And since principle of bivalence does not inherently conform to intuitionism, model-theoretic semantics, according to him, can no longer be appropriate in the logical study of semantics.

As have been said earlier, mathematical technicality of PTS, which is ND, had been first introduced by Gentzen (1964) and further developed by Prawitz (1965). ND is a method of proof or proof calculus/system devised by Gentzen (1964) as a mathematical or technical apparatus towards the motivation of Hilbert's philosophy of formalism. Proof theory has, at least, four proof calculus: (i) Hilbert's calculus, both of Gentzen's (ii) natural deduction and (iii) sequent calculus; and, (iv) Belnap's display calculus.

Briefly, ND, like most of the other kinds of proof calculus, consists of (i) a collection of symbols which can construct complex formula (or in colloquial sense: a(n) assertion, proposition, or statement) and (ii) rules (e.g. inference rules of both introduction and elimination) which capture the deductions that have taken place in the reasoning process. What differs ND with any other kind of proof calculus is that ND is capable of studying formal reasoning very intuitively and naturally (hence the name natural deduction) by means of its introduction rules and elimination rules. This method, as suggested by Dummett (1991), is useful to the extent that logic without principle of bivalence can be further investigated. Of course, there will be several problems that are needed to be defined and reconciled when investigating semantics and logic using ND: tonk (Prior, 1960), harmony (Dummett, 1991), validity (Schroeder-Heister, 2006), normalizability (Prawitz, 1965), and those collected and formulated by Francez (2016).

1.1.2 Dynamic epistemic logic

First order logic in a sense is extensional. This means that the semantics of its language can be given truth-functionally. We can see that Tarski's semantic theory of truth gives meaning to the logical operator truth-functionally. The semantics (truth) for the logical operator conjunction $\wedge$ in $\varphi \wedge \psi$, for example, is given uniquely (therefore a function) by the truth of its conjuncts (i.e. the formula φ and ψ). There are, however, logics that are not extensional which are called intensional. Epistemic logic is one of them which has a logical operator knowledge K that is intensional. To see this, we can say that Fermat's last theorem φ is true but it is not always the case that some person a knows that it is true (i.e. it is not the case that $K_a\varphi$ (this reads as *a knows that* φ)). This shows that the truth of $K_a\varphi$ is not uniquely determined by the truth of its subformula φ. Hence, the logical operator K is intensional.

So, Tarski's semantic theory of truth will not do and model theorist will resort to Kripke's possible world semantics when investigating intensionality. The first rigorous model theoretic investigation of epistemic logic is given by Hintikka (1962).

Modal logics with the plural 's' is a collection of many intensional logics (e.g.epistemic logic, doxastic logic, modal logic, temporal logic, etc). Examples of model theoretic study of modal logics can be seen in Renne (2008) and van Benthem et al. (2018); and, examples of proof theoretic study of modal logics in Artemov & Protopopescu (2016), Basin et al. (1998), Bierman & de Paiva (2000), Indrzejczak (2010), Martins & Martins (2006), Medeiros (2006), Payne (2015), Simpson (1994), von Plato (2005), and Williamson (1992).

Dynamic epistemic logic (DEL) studies the dynamics of epistemic logic (public announcement logic (PAL) being one of its logic). For example, the question of how can one's belief change to one's knowledge by acknowledging some facts. In other words, how can the formula $B_a\varphi$ (this reads as *a belief that* φ) change to $K_a\varphi$? The investigation of DEL is dominated mainly in model theoretic perspective. There is an abundance of literature for this investigation and Dechesne et al. (2009), Dechesne & Wang (2007), and Gattinger (2018) are just a few of them. The book by van Ditmarsch et al. (2008) is a well-known reference on this. Proof-theoretic investigation of DEL, however, has been less celebrated and to our knowledge these are some of the published works for this: Frittella et al. (2016), Greco et al. (2013), Sikimic (2013), Maffezioli & Negri (2011).

1.1.3 Dynamic epistemic logic in cryptographic protocol

We have explained a brief literature on PTS and DEL, we now will briefly present how they can be used as a tool in investigating cryptographic protocol. Cryptographic protocol is a complete description or a set of rules that ensures all the cryptographic processes are done from the beginning until the end. There are generally two methods, summarized by Boyd & Mathuria (2003), of achieving this: (i) formal methods and (ii) complexity-theoretic methods. Complexity-theoretic method models a cryptographic process and later proves that a known NP problem reduces to it. This means that it is computationally impossible for an adversary to take any action within a considerable period of time. But, considering that there are abundant of cryptographic methods, to prove that an NP problem reduces to each one of them is difficult and endless. Formal methods uses mathematical logic as a tool to axiomatize cryptographic primitives hoping that any security flaws can be deduced automatically. The main flaws of this method are usually related to the inability to provide a logical system that is sufficiently expressive enough to axiomatize all the cryptographic processes.

BAN logic in Burrows et al. (1990) is one of the pioneering formal methods that had been proposed using modal logic as its main tool but later proved to be insufficiently expressive (Lowe, 1996). As noted by Kramer (2007), various types of logic followed to compensate the inexpressiveness and to use a logic by which cryptographic primitive can be expressively complete: modal logic, doxastic logic, deontic logic, higher-order logic, epistemic logic, temporal logic and the combinations thereof. Dynamic epistemic logic (DEL) is one such combination proposed in cryptography.

Notwithstanding these various logics, as summarized by Gritzalis et al. (1999), there are at least two main approaches to how formal method can be achieved: model theoretically and proof theoretically. Although the two methods are generally intertwined even in the field of logic, what differs them in cryptographic protocol is the fact that proof-theoretic method proves the protocol to be safe by means of a proof assistant whereas model-theoretic method by model checking tool. Recent studies, for example Piecha & Schroeder-Heister (2016), have shown promising results when using PTS as a basis of logic and even as an implementation in a logic programming, which will be of use in constructing an automated theorem prover for cryptographic protocol.

Model theoretically, DEL has been investigated at a great length to study cryptographic protocol. Examples of which are in Dechesne et al. (2009), Dechesne & Wang (2007), Frydrychowicz (2010), Gattinger (2014), Gattinger (2018), Gattinger & van Eijck (2015), van Ditmarsch et al. (2012). There has yet to be any study on an application of DEL in cryptographic protocol proof theoretically.

1.2 Problem Statement

As has been explained in the foregoing discussion, formal semantics given to the logical language has been studied pervasively by means of model theory. Although proof theoretical semantics has been celebrated and discussed in philosophy, its formal counterpart has not been investigated to the extent similar to that of model theory. Particularly in the study of DEL, Kripke's possible world semantics, which is model theoretical, has been considerably studied compare to proof-theoretic semantics, which is proof theoretical. Much less is the application of PTS of DEL in the study of cryptographic protocol. In fact, we have yet to find any publication on such application.

1.3 Research Objective and Question

Our goals are of two types. Firstly, we want to have a PTS interpretation of DEL. More particularly, we want to construct an ND calculus for public announcement logic with common knowledge (PAC) which is one of the logic under DEL and prove its soundness, completeness, and normalizability. Secondly, we want to reformulate some problems involving cryptographic protocol using our ND calculus.

1.4 Research Methodology

We will first define our proposed labelled natural deduction for PAC (**NPAC**). Since our deduction system exploits formulas having the labelling upon them, we will need to define a new Kripke's semantics having labelling upon its formulas as well. The definition should preserve the usual definition of Kripke's semantics. Then we will proof the soundness of the **NPAC** directly from the Kripke's semantics and the completeness indirectly by translation into the known Hilbert axiomatic proof system **PAC** in van Ditmarsch et al. (2008). Then, we will proof normalization within the method which PTS has been proposing: by defining the notion of validity of a derivation without a notion of truth. After having the **NPAC**, we will give some examples of how our proof system can be applied and use it to solve some problems in cryptographic protocol.

1.5 Thesis Organization

Before we begin, we will present here the overall structure of this thesis. In chapter 2, we will begin defining the syntax, semantics, and proof system for public announcement logic (with common knowledge). Some preliminary results and the Hilbert axiomatisation of the logic are presented. In chapter 3, we will present our proposed labelled natural deduction for PAC and prove the soundness, completeness, and normalization of the proof system. In chapter 4, we will present some applications of dynamic epistemic logic in investigating cryptographic protocol. And finally, in chapter 5, we conclude the thesis with a comprehensive summary and some insights for further investigation.

CHAPTER 2: PUBLIC ANNOUNCEMENT LOGIC

2.1 Introduction

Public announcement logic (PAL) with common knowledge (PAC) is a logic built for the purpose of formalising the notion of epistemic update. We will present here the syntax of PAC in which there two types of formula, labelled and relational, which are built inductively. Then, the semantics of the logic is presented by first using the usual Kripke's model for modal logic and is extended using a restricted Kripke's model, a model of which is capable of giving semantics for an indexed formula. Some properties in PAC will be proven here. We will then present the Hilbert axiomatisation for PAC.

2.2 Syntax

Definition 2.2.1 (PAC language)**.** The *language* of PAC consists of a countably infinite set P of atomic propositions $p, q, r, \ldots$, brackets '(' and ')', a finite set G of agent-symbols $a, b, c, \ldots$, a corresponding finite set R_G of binary relations $R_a, R_b, R_c, \ldots$, a set $\mathcal{W}$ of worlds $x, y, z, \ldots$, set of agents $\psi, \psi_1, \psi_2 \ldots$, a transitive closure symbol $*$; and, logical *operators* $\bot$ (falsum), $\neg$ (negation), $\vee$ (disjunction), $\wedge$ (conjuction) $\supset$ (implication), K_a (modal operator 'a knows that'), $[A]$ (announcement of a formula A), $\mathcal{E}_\psi$ (modal operator 'everyone in ψ knows that'), and C_ψ (modal operator 'it is a common knowledge for everyone in ψ that').

Definition 2.2.2 (PAC formula)**.** A *formula* of PAC is defined inductively as follows:

1. $\bot$ is an *atomic formula*.
2. Every atomic proposition is an atomic formula.
3. If A and B are formulas then $(A \vee B)$, $(A \wedge B)$, and $(A \supset B)$ are formulas.

4. If A is a formula and a is an agent then $(K_a A)$ is a formula.

5. If A is a formula and ψ is a set of agent(s) then $(\mathcal{E}_\psi A)$ is a formula.

6. If A is a formula and ψ is a set of agent(s) then $(C_\psi A)$ is a formula.

7. If A and B are formulas then $([A]B)$ is a formula.

For the inductive clauses number (5) and (6), if $\psi = \{a, b, c\}$, instead of writing $(\mathcal{E}_{\{a,b,c\}} A)$ and $(C_{\{a,b,c\}} A)$ we remove the bracket and comma thus occasionally write $(\mathcal{E}_{abc} A)$ and $(C_{abc} A)$; or even $(\mathcal{E}_{bac} A)$ and $(C_{bbaaaca} A)$ as these are true in set notation.

$\neg A$ is defined as $A \supset \perp$. Hence, $\neg A$ too is a formula by 2.2.2.1 and 2.2.2.3. We let the symbols $A, B, C, \ldots$ range over formulas. The brackets will be ignored assuming the following convention from higher priority to lower over the construction of a formula: $\neg, K_a, [A], \mathcal{E}_\psi, C_\psi, \wedge, \vee, \supset$.

Definition 2.2.3 (PAC labelled formula)**.** If A is a formula, φ a list of formulas, and x a world (i.e. $x \in \mathcal{W}$) then $x :^\varphi A$ is a *labelled formula*.

Definition 2.2.4 (PAC relational formula)**.** If R_a is a binary relation over the set $\mathcal{W} \times \mathcal{W}$, $x, y \in \mathcal{W}$, φ a list of formulas, and ψ a set of agents then $xR_a^\varphi y$, $xR_\psi^\varphi y$, and $xR_\psi^{\varphi *} y$ are *relational formulas*. We let the symbols $\rho, \rho_1, \rho_2, \ldots$ range over relational formulas.

We let the symbols $\mathscr{A}, \mathscr{B}, \mathscr{C}, \ldots$ range over labelled or relational formulas and Γ (possibly empty) to be an arbitrary set of labelled or relational formulas. We sometimes just say a formula to mean either a labelled or relational formula $\mathscr{A}$; or, a formula A for brevity as which situation can be easily understood by the script font. We let also, $x :^\varphi A = x : A$ if φ is an empty list and similarly for relational formula. We say that a labelled or relational formula is unrestricted if φ is an empty list and restricted otherwise. We use similar convention as PAC formula of removing bracket and comma of ψ.

Definition 2.2.5. Suppose that $\circ$ is an operator. The *rank* of a labelled or relational formula $\mathscr{A}$ ($r(\mathscr{A})$) is defined inductively as follows.

$$\begin{cases} r(x :^{\varphi} \bot) & = \langle r'(\varphi), 0\rangle \\ r(x :^{\varphi} p) & = \langle r'(\varphi), 0\rangle \\ r(x :^{\varphi} \circ A) & = \langle r'(\varphi) + r(x : A) + 1, 0\rangle \\ r(x :^{\varphi} A \circ B) & = \langle r'(\varphi) + max(r(x : A), r(x : B)) + 1, 0\rangle \\ r(xR_a^{\varphi} y) & = \langle r'(\varphi), 0\rangle \\ r(xR_{\psi}^{\varphi} y) & = \langle r'(\varphi), 1\rangle \\ r(xR_{\psi}^{\varphi *} y) & = \langle r'(\varphi), 2\rangle \end{cases}$$

where $r'(\varphi) = r(x : A_1) + \cdots + r(x : A_n) + 1$ if $\varphi = A_1, \ldots, A_n$ and $r'(\varphi) = 0$ if φ is an empty list. We say that the formula with the rank $\langle 0, 0\rangle$ is *atomic*. The relation $<$ over the ranks is defined in lexicographical order (i.e. $\langle m, n\rangle < \langle m', n'\rangle$ iff $m < m'$; or, $m = m'$ and $n < n'$).

2.3 Semantics

Definition 2.3.1. A *Kripke model* for PAC is a structure $\mathcal{M} = \langle \mathcal{W}, \mathcal{R}_G, \mathcal{V}\rangle$ such that:

1. $\mathcal{W}$ is a non-empty set of worlds.
2. For all $a \in G$, $\mathcal{R}_a \subseteq \mathcal{W} \times \mathcal{W}$.
3. $\mathcal{V} : \mathcal{W} \times P \to \{0, 1\}$ is a valuation function such that every world x and atomic proposition p yield the truth value 0 or 1.

Definition 2.3.2 (Restricted Kripke model)**.** Let $\mathcal{M}$ be a Kripke model and A a formula. A *restricted Kripke model* for PAC is a structure $\mathcal{M}^A = \langle \mathcal{W}^A, \mathcal{R}_G^A, \mathcal{V}^A\rangle$ such that:

1. $\mathcal{W}^A = \{x \in \mathcal{W} : \models^{\mathcal{M}} x : A\}$ is a non-empty set of worlds.
2. For all $a \in G$, $\mathcal{R}^A_a = \mathcal{R}_a \cap (\mathcal{W}^A \times \mathcal{W}^A)$.
3. $\mathcal{V}^A = \mathcal{V}|_{\mathcal{M}^A \times P}$.

We write linearly $\mathcal{M}^{\varphi,A}$ instead of $(\mathcal{M}^{\varphi})^A$ to keep the symbolism readable. This convention is also applied to $\mathcal{W}^{\varphi}$, $\mathcal{R}^{\varphi}_G$, and $\mathcal{V}^{\varphi}$.

Definition 2.3.3 (Relation extension)**.** Let ψ be a subset of a set of agents G.

1. $\mathcal{R}_{\psi} = \bigcup_{a \in \psi} \mathcal{R}_a$.
2. The *transitive closure* of a relation $\mathcal{R}$ is the smallest relation $\mathcal{R}^*$ such that $\mathcal{R} \subset \mathcal{R}^*$ and for every $x, y, z \in \mathcal{W}$ if $(x, y), (y, z) \in \mathcal{R}^*$ then $(x, z) \in \mathcal{R}^*$.

Definition 2.3.4. *Truth* for a formula $\mathscr{A}$ in a model $\mathcal{M}^{\sigma}$ (i.e. $\models^{\mathcal{M}^{\sigma}} \mathscr{A}$) is defined inductively as follows:

1. $\models^{\mathcal{M}^{\sigma}} xR^{\varphi}_a y$ iff $(x, y) \in \mathcal{R}^{\sigma,\varphi}_a$.
2. $\models^{\mathcal{M}^{\sigma}} xR^{\varphi}_{\psi} y$ iff $(x, y) \in \mathcal{R}^{\sigma,\varphi}_{\psi}$.
3. $\models^{\mathcal{M}^{\sigma}} xR^{\varphi*}_{\psi} y$ iff $(x, y) \in \mathcal{R}^{\sigma,\varphi*}_{\psi}$.
4. $\not\models^{\mathcal{M}^{\sigma}} x :^{\varphi} \bot$ for every $x \in \mathcal{W}$ and every list of formulas σ and φ.
5. $\models^{\mathcal{M}^{\sigma}} x :^{\varphi} p$ iff $\mathcal{V}^{\sigma,\varphi}(x, p) = 1$.
6. $\models^{\mathcal{M}^{\sigma}} x :^{\varphi} A \vee B$ iff $\models^{\mathcal{M}^{\sigma,\varphi}} x : A$ or $\models^{\mathcal{M}^{\sigma,\varphi}} x : B$.
7. $\models^{\mathcal{M}^{\sigma}} x :^{\varphi} A \wedge B$ iff $\models^{\mathcal{M}^{\sigma,\varphi}} x : A$ and $\models^{\mathcal{M}^{\sigma,\varphi}} x : B$.
8. $\models^{\mathcal{M}^{\sigma}} x :^{\varphi} A \supset B$ iff $\models^{\mathcal{M}^{\sigma,\varphi}} x : A$ implies $\models^{\mathcal{M}^{\sigma,\varphi}} x : B$.
9. $\models^{\mathcal{M}^{\sigma}} x :^{\varphi} K_a A$ iff for all y, $\models^{\mathcal{M}^{\sigma}} xR^{\varphi}_a y$ implies $\models^{\mathcal{M}^{\sigma,\varphi}} y : A$.
10. $\models^{\mathcal{M}^{\sigma}} x :^{\varphi} \mathcal{E}_{\psi} A$ iff for all y, $\models^{\mathcal{M}^{\sigma}} xR^{\varphi}_{\psi} y$ implies $\models^{\mathcal{M}^{\sigma,\varphi}} y : A$.
11. $\models^{\mathcal{M}^{\sigma}} x :^{\varphi} \mathcal{C}_{\psi} A$ iff for all y, $\models^{\mathcal{M}^{\sigma}} xR^{\varphi*}_{\psi} y$ implies $\models^{\mathcal{M}^{\sigma,\varphi}} y : A$.
12. $\models^{\mathcal{M}^{\sigma}} x :^{\varphi} [A]B$ iff $\models^{\mathcal{M}^{\sigma,\varphi}} x : A$ implies $\models^{\mathcal{M}^{\sigma,\varphi,A}} x : B$

Definition 2.3.5. Let $\mathscr{A}$ be a labelled or relational formula and Γ be a set of formulas. The following are further notations of our truth definition:

1. $\models^{\mathcal{M}} \Gamma$ iff $\models^{\mathcal{M}} \mathscr{A}$ for all $\mathscr{A} \in \Gamma$.
2. $\models \Gamma$ iff $\models^{\mathcal{M}} \Gamma$ for all $\mathcal{M}$.
3. $\Gamma \models^{\mathcal{M}} \mathscr{A}$ iff $\models^{\mathcal{M}} \Gamma$ implies $\models^{\mathcal{M}} \mathscr{A}$.
4. $\Gamma \models \mathscr{A}$ iff $\Gamma \models^{\mathcal{M}} \mathscr{A}$ for all $\mathcal{M}$.
5. $\Gamma \Dashv^{\mathcal{M}} \mathscr{A}$ iff $\models^{\mathcal{M}} \mathscr{A}$ implies $\models^{\mathcal{M}} \mathscr{B}$ for all $\mathscr{B} \in \Gamma$.
6. $\Gamma \Dashv \mathscr{A}$ iff $\Gamma \Dashv^{\mathcal{M}} \mathscr{A}$ for all $\mathcal{M}$.

The following propositions will justify some of the rules of **NPAC**, which will be defined later, whereas the remaining rules are justified straight from the definition of their semantics.

Proposition 2.3.6. For all Kripke model $\mathcal{M}$, $\mathcal{W}^{A\wedge[A]B} = \mathcal{W}^{A,B}$.

Proof. By Definition 2.3.2 this is equivalent to proving that $x \in \mathcal{W}^{A\wedge[A]B}$ iff $x \in \mathcal{W}^{A,B}$. But $x \in \mathcal{W}^{A\wedge[A]B}$ iff $\models^{\mathcal{W}} x : A \wedge [A]B$ iff $\models^{\mathcal{W}} x : A$ and $\models^{\mathcal{W}} x : [A]B$ iff $\models^{\mathcal{W}} x : A$ and ($\models^{\mathcal{W}} x : A$ implies $\models^{\mathcal{W}} x :^{A} B$) iff $\models^{\mathcal{W}} x :^{A} B$ iff $x \in \mathcal{W}^{A,B}$. □

Proposition 2.3.7.

1. $\{xR^{\varphi}_{a}y, x :^{\varphi} A, y :^{\varphi} A\} \Dashv\models xR^{\varphi,A}_{a}y$.
2. $xR^{\varphi,A*}_{\psi}y \models xR^{\varphi*}_{\psi}y$.
3. $\models x :^{\varphi,A,B} C$ iff $\models x :^{\varphi,A\wedge[A]B} C$.
4. For all $1 \leq i \leq n$, $xR^{\varphi}_{a_i}y \models xR^{\varphi}_{a_1\ldots a_n}y$.
5. If $\models^{\mathcal{M}} xR^{\varphi}_{a_1\ldots a_n}y$ and ($\models^{\mathcal{M}} xR^{\varphi}_{a_i}y$ implies $\models^{\mathcal{M}} \mathscr{A}$ for every $1 \leq i \leq n$) then $\models^{\mathcal{M}} \mathscr{A}$.
6. $xR^{\varphi}_{\psi}y \models xR^{\varphi*}_{\psi}y$.

7. $\{xR^{\varphi}_{\psi}z_1, \ldots, z_nR^{\varphi}_{\psi}y\} \vDash xR^{\varphi*}_{\psi}y$ for all natural number n.

8. If $\vDash^{\mathcal{M}}$ $xR^{\varphi*}_{\psi}y$, ($\vDash^{\mathcal{M}}$ $xR^{\varphi}_{\psi}y$ implies $\vDash^{\mathcal{M}}$ $\mathscr{A}$), and for all natural number n ($\vDash^{\mathcal{M}}$ $xR^{\varphi}_{\psi}z_1, \cdots, \vDash^{\mathcal{M}}$ $z_nR^{\varphi}_{\psi}y$ implies $\vDash^{\mathcal{M}}$ $\mathscr{A}$); then, $\vDash^{\mathcal{M}}$ $\mathscr{A}$.

Proof. 1. For an arbitrary $\mathcal{M}$, $\vDash^{\mathcal{M}}$ $xR^{\varphi,A}_{a}y$ iff $(x,y) \in R^{\varphi,A}_{a} = R^{\varphi} \cap (\mathcal{W}^{\varphi,A} \times \mathcal{W}^{\varphi,A})$ iff $(x,y) \in R^{\varphi}_{a}$ and $(x,y) \in (\mathcal{W}^{\varphi,A} \times \mathcal{W}^{\varphi,A})$ iff $(x,y) \in R^{\varphi}_{a}$ and $x, y \in \mathcal{W}^{\varphi,A}$ iff $(x,y) \in R^{\varphi}_{a}$, $\vDash^{\mathcal{M}^{\varphi}}$ $x : A$, and $\vDash^{\mathcal{M}^{\varphi}}$ $y : A$ iff $\vDash^{\mathcal{M}}$ $xR^{\varphi}_{a}y$, $\vDash^{\mathcal{M}}$ $x :^{\varphi} A$, and $\vDash^{\mathcal{M}}$ $y :^{\varphi} A$.

2. Clearly, $R^{\varphi,A}_{\psi} \subset R^{\varphi}_{\psi}$. So, $R^{\varphi,A*}_{\psi} \subset R^{\varphi*}_{\psi}$. Therefore, for an arbitrary $\mathcal{M}$, $\vDash^{\mathcal{M}}$ $xR^{\varphi,A*}_{\psi}y$ implies $(x,y) \in R^{\varphi,A*}_{\psi} \subset R^{\varphi*}_{\psi}$ implies $\vDash^{\mathcal{M}}$ $xR^{\varphi*}_{\psi}y$.

3. Use Proposition 2.3.6.

4. If $\vDash^{\mathcal{M}}$ $xR^{\varphi}_{a_i}y$ then $(x,y) \in R^{\varphi}_{a_i} \subset \bigcup_{a_i \in \{a_1,\ldots,a_n\}} R^{\varphi}_{a_i} \subset R^{\varphi}_{a_1\ldots a_n}$. Therefore $\vDash^{\mathcal{M}}$ $xR^{\varphi}_{a_1\ldots a_n}y$.

5. Suppose that the antecedent is true. Then, $(x,y) \in R^{\varphi}_{a_1\ldots a_n} = \bigcup_{a_i \in \{a_1,\ldots,a_n\}} R^{\varphi}_{a_i}$. Then $(x,y) \in R^{\varphi}_{a_1}$ or,. . . , or $(x,y) \in R^{\varphi}_{a_n}$. Then $\vDash^{\mathcal{M}}$ $xR^{\varphi}_{a_1}y$ or,. . . , or $\vDash^{\mathcal{M}}$ $xR^{\varphi}_{a_n}y$. Therefore, since ($\vDash^{\mathcal{M}}$ $xR^{\varphi}_{a_i}y$ implies $\vDash^{\mathcal{M}}$ $\mathscr{A}$ for every $1 \leq i \leq n$), $\vDash^{\mathcal{M}}$ $\mathscr{A}$.

6. Suppose that, for an arbitrary $\mathcal{M}$, $\vDash^{\mathcal{M}}$ $xR^{\varphi}_{\psi}y$. Then $(x,y) \in R^{\varphi}_{\psi}$ but $R^{\varphi}_{\psi} \subset R^{\varphi*}_{\psi}$. So, $\vDash^{\mathcal{M}}$ $xR^{\varphi}_{\psi}y$.

7. Suppose that, for an arbitrary $\mathcal{M}$, $\vDash^{\mathcal{M}}$ $xR^{\varphi}_{\psi}z_1, \ldots, \vDash^{\mathcal{M}}$ $z_nR^{\varphi}_{\psi}y$. Then $(x, z_1), \ldots, (z_n, y) \in R^{\varphi}_{\psi}y$. Since $R^{\varphi}_{\psi} \subset R^{\varphi*}_{\psi}$ and $R^{\varphi*}_{\psi}$ is a transitive closure of R^{φ}_{ψ}, then iteratively $(x,y) \in R^{\varphi*}_{\psi}$. Therefore, $\vDash^{\mathcal{M}}$ $xR^{\varphi}_{\psi}y$.

8. Suppose that, for an arbitrary $\mathcal{M}$, $\vDash^{\mathcal{M}}$ $xR^{\varphi*}_{\psi}y$, ($\vDash^{\mathcal{M}}$ $xR^{\varphi}_{\psi}y$ implies $\vDash^{\mathcal{M}}$ $\mathscr{A}$), and for all natural number n ($\vDash^{\mathcal{M}}$ $xR^{\varphi}_{\psi}z_1, \cdots, \vDash^{\mathcal{M}}$ $z_nR^{\varphi}_{\psi}y$ implies $\vDash^{\mathcal{M}}$ $\mathscr{A}$). So $(x,y) \in R^{\varphi*}_{\psi} = R^{\varphi}_{\psi} \cup R$. If $(x,y) \in R^{\varphi}_{\psi}$ then $\vDash^{\mathcal{M}}$ $xR^{\varphi}_{\psi}y$ and, by the second supposition, $\vDash^{\mathcal{M}}$ $\mathscr{A}$. If not then $(x,y) \notin R^{\varphi}_{\psi}$ but $(x,y) \in R \subset R^{\varphi*}_{\psi}$. By contradiction, assume that for all natural

number n, $\nvDash^{\mathcal{M}} xR^{\varphi}_{\psi}z_1, \cdots, \nvDash^{\mathcal{M}} z_nR^{\varphi}_{\psi}y$. In other words, there are no $z_1, \ldots, z_n$ such that $(x, z_1), \ldots, (z_n, y) \in R^{\varphi}_{\psi}$. So, since $R^{\varphi *}_{\psi}$ is the smallest transitive closure, $(x, y) \notin R^{\varphi *}_{\psi}$ but this is a contradiction. Therefore, $\vDash^{\mathcal{M}} xR^{\varphi}_{\psi}z_1, \cdots, \vDash^{\mathcal{M}} z_nR^{\varphi}_{\psi}y$ for some natural number n, and by the third supposition, $\vDash^{\mathcal{M}} \mathscr{A}$. Hence, whichever the case, $\vDash^{\mathcal{M}} \mathscr{A}$. □

2.4 Axiomatisation

There are several proof systems proposed for PAL: display calculus in Frittella et al. (2016), sequent calculus in Maffezioli & Negri (2011) and Alberucci & Jäger (2005), algebraic semantics in Ma et al. (2014), and of course the Hilbert system which can be referred in van Ditmarsch et al. (2008). The proof system for PAC however is currently only presented with Hilbert system **PAC**. The following table consists of axioms of the Hilbert system of PAC (**PAC**) which is proven to be complete and sound (van Ditmarsch et al., 2008):

Table 2.1: Axiomatization for PAC

All instantiations of propositional tautologies	
$K_a(A \supset B) \supset (K_aA \supset K_aB)$	Distribution of K_a over $\supset$
$K_aA \supset A$	Truth axiom
$K_aA \supset K_aK_aA$	Positive introspection
$\neg K_aA \supset K_a\neg K_aA$	Negative introspection
$[A]p \supset\subset (A \supset p)$	Atomic permanence
$[A]\neg B \supset\subset (A \supset \neg[A]B)$	Announcement and negation
$[A](B \wedge C) \supset\subset ([A]B \wedge [A]C)$	Announcement and conjunction
$[A]K_aB \supset\subset A \supset K_a[A]B$	Announcement and knowledge
$[A][B]C \supset\subset [A \wedge [A]B]C$	Announcement composition
$C_\psi(A \supset B) \supset (C_\psi A \supset C_\psi B)$	Distribution of C_ψ over $\supset$
$C_\psi A \supset (A \wedge \mathcal{E}_\psi C_\psi A)$	Mix of common knowledge
From A and $A \supset B$, infer B	Modus ponens
From A, infer K_aA	Necessitation of K_a
From A, infer $C_\psi A$	Necessitation of C_ψ
From A, infer $[B]A$	Necessitation of $[B]$
From $A \supset [B]C$ and $A \wedge B \supset \mathcal{E}_\psi A$, infer $A \supset [B]C_\psi C$	Announcement and common knowledge

CHAPTER 3: LABELLED NATURAL DEDUCTION FOR PAC

3.1 Introduction

In this chapter we will present our proposed labelled natural deduction for public announcement logic with common knowledge (i.e. **NPAC**). As the logic includes a notion of epistemic update, for which a formula can be true and not true, we have to add an index for each formula in the logic. We, then, will give the inductive definition of the language or syntax for PAC including the definition of the mentioned indexed formulas. Then, the semantics of the language is given using an extended notion of Kripke's model that exploits the indexing. Next, we will formulate our proposed **NPAC** and proof some of its important properties. We then proof the extensional equivalence of our **NPAC** and PAC. Finally, we proof that the **NPAC** satisfies a strong normalization property.

3.2 Labelled Natural Deduction for PAC

Definition 3.2.1 (Propositional inference rules)**.** *Propositional inference rules* for **NPAC** are defined in Table 3.1.

Definition 3.2.2 (Other inference rules)**.** *Modal, announcement, composition*, and *atomic inference rules* for **NPAC** are defined in Table 3.2. For K_a^φ I rule, $y \neq x$ and does not occur in any undischarged topmost formula on which $y :^\varphi A$ depends other than $xR^\varphi y$. Similarly for $\mathcal{E}_\psi^\varphi$ and C_ψ^φ with the obvious condition.

Definition 3.2.3 (Relational rules)**.** The following are three *relational rules* for **NPAC**:

$$\frac{}{xR_a^\varphi x}\,\mathit{refl} \qquad \frac{xR_a^\varphi y}{yR_a^\varphi x}\,\mathit{symm} \qquad \frac{xR_a^\varphi y \qquad yR_a^\varphi z}{xR_a^\varphi z}\,\mathit{trans}$$

Definition 3.2.4 (Relational inference rules)**.** *Relational inference rules* for **NPAC** are defined in Table 3.3. For $R_\psi^{\varphi *}$ E rule, $z_1, \ldots, z_n$ does not occur in the major premis, in the conclusion, or any undischarged topmost formula ending with the premises (major or minor) other than $xR^{\varphi}_{\psi}z_1, \ldots, z_nR^{\varphi}_{\psi}y$.

Table 3.1: Propositional inference rules

Introduction Rules	Elimination Rules
$\dfrac{\begin{array}{c}[x :^{\varphi} A \supset \perp] \\ \vdots \\ y :^{\varphi} \perp\end{array}}{x :^{\varphi} A}\ \perp^{\varphi}$	
$\dfrac{x :^{\varphi} A}{x :^{\varphi} A \vee B}\ \vee^{\varphi}\mathrm{I} \quad \dfrac{x :^{\varphi} B}{x :^{\varphi} A \vee B}\ \vee^{\varphi}\mathrm{I}$	$\dfrac{x :^{\varphi} A \vee B \qquad \begin{array}{c}[x :^{\varphi} A] \\ \vdots \\ \mathscr{A}\end{array} \qquad \begin{array}{c}[x :^{\varphi} B] \\ \vdots \\ \mathscr{A}\end{array}}{\mathscr{A}}\ \vee^{\varphi}\mathrm{E}$
$\dfrac{x :^{\varphi} A \qquad x :^{\varphi} B}{x :^{\varphi} A \wedge B}\ \wedge^{\varphi}\mathrm{I}$	$\dfrac{x :^{\varphi} A \wedge B}{x :^{\varphi} A}\ \wedge^{\varphi}\mathrm{E} \quad \dfrac{x :^{\varphi} A \wedge B}{x :^{\varphi} B}\ \wedge^{\varphi}\mathrm{E}$
$\dfrac{\begin{array}{c}[x :^{\varphi} A] \\ \vdots \\ x :^{\varphi} B\end{array}}{x :^{\varphi} A \supset B}\ \supset^{\varphi}\mathrm{I}$	$\dfrac{x :^{\varphi} A \supset B \qquad x :^{\varphi} A}{x :^{\varphi} B}\ \supset^{\varphi}\mathrm{E}$

Definition 3.2.5. The labelled natural deduction system **NPAC** is a structure $\langle \mathcal{M}, \mathcal{R}_G, \mathbb{R} \rangle$ where $\mathcal{M}$ and $\mathcal{R}_G$ are similar to those in Kripke's model and $\mathbb{R}$ is a set of the rules in Definitions 3.2.1, 3.2.2, 3.2.3, and 3.2.4.

Definition 3.2.6. A *premise* of a rule is the formula appearing before the line of the rule and a *conclusion* is the formula appearing after the line. A *major premise* is a premis containing the operator that is eliminated in the rule; otherwise it is a *minor premise*.

Definition 3.2.7 (Derivation)**.** A *derivation* of a labelled or relational formula $\mathscr{A}$ from a set of labelled or relational formulas Γ is a tree of formulas satisfying the following condition:

Table 3.2: Modal, announcement, composition, and atomic inference rules

Introduction Rules	Elimination Rules
$\begin{array}{c}[xR^{\varphi}_{a}y]\\ \vdots\\ \dfrac{y :^{\varphi} A}{x :^{\varphi} K_a A}\,K^{\varphi}_{a}\,\mathrm{I}\end{array}$	$\dfrac{x :^{\varphi} K_a A \qquad xR^{\varphi}_{a}y}{y :^{\varphi} A}\,K^{\varphi}_{a}\,\mathrm{E}$
$\begin{array}{c}[xR^{\varphi}_{\psi}y]\\ \vdots\\ \dfrac{y :^{\varphi} A}{x :^{\varphi} \mathcal{E}_{\psi} A}\,\mathcal{E}^{\varphi}_{\psi}\,\mathrm{I}\end{array}$	$\dfrac{x :^{\varphi} \mathcal{E}_{\psi} A \qquad xR^{\varphi}_{\psi}y}{y :^{\varphi} A}\,\mathcal{E}^{\varphi}_{\psi}\,\mathrm{E}$
$\begin{array}{c}[xR^{\varphi *}_{\psi}y]\\ \vdots\\ \dfrac{y :^{\varphi} A}{x :^{\varphi} C_{\psi} A}\,C^{\varphi}_{\psi}\,\mathrm{I}\end{array}$	$\dfrac{x :^{\varphi} C_{\psi} A \qquad xR^{\varphi *}_{\psi}y}{y :^{\varphi} A}\,C^{\varphi}_{\psi}\,\mathrm{E}$
$\begin{array}{c}[x :^{\varphi} A]\\ \vdots\\ \dfrac{x :^{\varphi,A} B}{x :^{\varphi} [A]B}\,[A]^{\varphi}\,\mathrm{I}\end{array}$	$\dfrac{x :^{\varphi} [A]B \qquad x :^{\varphi} A}{x :^{\varphi,A} B}\,[A]^{\varphi}\,\mathrm{E}$
$\dfrac{x :^{\varphi,A,B} C}{x :^{\varphi,A\wedge[A]B} C}\,\mathrm{I}_{comp}$	$\dfrac{x :^{\varphi,A\wedge[A]B} C}{x :^{\varphi,A,B} C}\,\mathrm{E}_{comp}$
$\dfrac{x :^{\varphi} p \qquad x :^{\varphi} A}{x :^{\varphi,A} p}\,\mathrm{I}_{atom^{\varphi,A}}$	$\dfrac{x :^{\varphi,A} p}{x :^{\varphi} p}\,\mathrm{E}_{atom^{\varphi,A}} \qquad \dfrac{x :^{\varphi,A} p}{x :^{\varphi} A}\,\mathrm{E}_{atom^{\varphi,A}}$

1. The topmost formulas are either in Γ or discharged by a rule in the tree.
2. The bottommost formula is $\mathscr{A}$.
3. Every formula in the tree except $\mathscr{A}$ is a premise of a correct application of rules whose conclusion stands directly below that formula in the tree.

We say that the *conclusion* $\mathscr{A}$ is *derivable* from Γ (i.e. $\Gamma \vdash \mathscr{A}$) if such a tree exists. Let A be a formula (non-relational and non-labelled). Suppose that $\Delta \cup A$ is a set of formulas

Table 3.3: Relational inference rules

Introduction Rules	Elimination Rules
$\dfrac{xR_a^\varphi y \qquad x :^\varphi A \qquad y :^\varphi A}{xR_a^{\varphi,A} y}\, R_a^{\varphi,A}\,\mathrm{I}$	$\dfrac{xR_a^{\varphi,A} y}{xR_a^\varphi y}\, R_a^{\varphi,A}\,\mathrm{E} \quad \dfrac{xR_a^{\varphi,A} y}{x :^\varphi A}\, R_a^{\varphi,A}\,\mathrm{E}$
$\dfrac{xR^\varphi_{a_1} y}{xR^\varphi_{a_1\ldots a_n} y}\, R^\varphi_{a_1\ldots a_n}\,\mathrm{I}$ $\vdots$ $\dfrac{xR^\varphi_{a_n} y}{xR^\varphi_{a_1\ldots a_n} y}\, R^\varphi_{a_1\ldots a_n}\,\mathrm{I}$	$\dfrac{xR^\varphi_{a_1\ldots a_n} y \qquad \begin{matrix}[xR^\varphi_{a_1} y]\\ \vdots \\ \mathscr{A}\end{matrix} \qquad \cdots \qquad \begin{matrix}[xR^\varphi_{a_n} y]\\ \vdots \\ \mathscr{A}\end{matrix}}{\mathscr{A}}\, R^\varphi_{a_1\ldots a_n}\,\mathrm{E}$
$\dfrac{xR^\varphi_\psi y}{xR^{\varphi *}_\psi y}\, R^{\varphi *}_\psi\,\mathrm{I}$ $\vdots$ $\dfrac{xR^\varphi_\psi z_1 \cdots z_n R^\varphi_\psi y}{xR^{\varphi *}_\psi y}\, R^{\varphi *}_\psi\,\mathrm{I}$ $\vdots$	$\dfrac{xR^{\varphi *}_\psi y \qquad \begin{matrix}[xR^\varphi_\psi y]\\ \vdots \\ \mathscr{A}\end{matrix} \qquad \cdots \qquad \begin{matrix}[xR^\varphi_\psi z_1]\cdots[z_n R^\varphi_\psi y]\\ \vdots \\ \mathscr{A}\end{matrix} \qquad \cdots}{\mathscr{A}}\, R^{\varphi *}_\psi\,\mathrm{E}$

(non-labelled and non-relational) and $x :^\varphi \Gamma$ means putting $x :^\varphi$ on every formula in Δ. We write $\Delta \vdash A$ for $x :^\varphi \Gamma \vdash x :^\varphi A$ for every $x \in \mathcal{W}$ and every list of formulas φ. We also occasionally put a number labeling at the discharge formula and its corresponding rule application.

Proposition 3.2.8. The following are derived rules:

$$\dfrac{\begin{matrix}[x :^\varphi A]\\ \vdots \\ x :^\varphi \bot\end{matrix}}{x :^\varphi \neg A}\, \neg^\varphi\,\mathrm{I} \qquad \dfrac{x :^\varphi \neg A \qquad x :^\varphi A}{x :^\varphi \bot}\, \neg^\varphi\,\mathrm{E}$$

Proof. The introduction and elimination rules for negation are a direct substitution of $\supset^\varphi$ I and $\supset^\varphi$ E in Table 3.1 by substituting B for $\bot$. □

As noted by Viganò (2000), $\bot$ traverses between worlds. We show that $\bot$ also traverses between worlds and the index φ. This is useful later especially in showing normalizability.

Proposition 3.2.9.

1. $x :^\varphi \bot \vdash y :^\varphi \bot$

2. $x :^{\varphi,A} \bot \vdash x :^{\varphi} \bot$

3. $x :^{\varphi} \bot \vdash x :^{\varphi,A} \bot$

4. $x :^{\varphi_1} \bot \vdash x :^{\varphi_2} \bot$

5. $x :^{\varphi_1} \bot \vdash y :^{\varphi_2} \bot$

Proof. 1.

$$\dfrac{[y :^{\varphi} \bot \supset \bot] \qquad x :^{\varphi} \bot}{y :^{\varphi} \bot} \bot^{\varphi}$$

2.

$$\dfrac{x :^{\varphi,A} \bot}{x :^{\varphi} \bot} \mathrm{E}_{atom^{\varphi,A}}$$

3.

$$\dfrac{\dfrac{[x :^{\varphi} \neg A] \qquad x :^{\varphi} \bot}{x :^{\varphi} A} \bot^{\varphi} \qquad x :^{\varphi} \bot}{x :^{\varphi,A} \bot} \mathrm{E}_{atom^{\varphi,A}}$$

4. We first remove all the φ_1 by (2), then we add the formulas listed in φ_2 by (3).

5. By (1) and (4). □

The following proposition shows, as it should be expected by the definition, that R^{φ}_{ψ} is reflexive and symmetry and $R^{\varphi *}_{\psi}$ satisfies equivalence relation.

Proposition 3.2.10.

1. $\vdash x R^{\varphi}_{\psi} x$

2. $x R^{\varphi}_{\psi} y \vdash y R^{\varphi}_{\psi} x$

3. $\vdash x R^{\varphi *}_{\psi} x$

4. $\{x R^{\varphi *}_{\psi} y, y R^{\varphi *}_{\psi} z\} \vdash x R^{\varphi *}_{\psi} z$

5. $x R^{\varphi *}_{\psi} y \vdash y R^{\varphi *}_{\psi} x$

Proof. 1.

$$\dfrac{\dfrac{}{xR^{\varphi}_{a}x}\;\mathit{refl}}{xR^{\varphi}_{\psi}x}\;R^{\varphi}_{\psi}\ \mathrm{I}$$

2. Let $\psi = \{a_1, \ldots, a_n\}$.

$$\dfrac{xR^{\varphi}_{\psi}y \qquad \dfrac{\dfrac{[xR^{\varphi}_{a_1}y]}{yR^{\varphi}_{a_1}x}\;\mathit{symm}}{yR^{\varphi}_{\psi}x}\;R^{\varphi}_{\psi}\ \mathrm{I} \qquad \cdots \qquad \dfrac{\dfrac{[xR^{\varphi}_{a_n}y]}{yR^{\varphi}_{a_n}x}\;\mathit{symm}}{yR^{\varphi}_{\psi}x}\;R^{\varphi}_{\psi}\ \mathrm{I}}{yR^{\varphi}_{\psi}x}\;R^{\varphi}_{\psi}\ \mathrm{E}$$

3.

$$\dfrac{\dfrac{}{xR^{\varphi}_{\psi}x}\;1}{xR^{\varphi*}_{\psi}x}\;R^{\varphi*}_{\psi}\ \mathrm{I}$$

4.

$$\dfrac{xR^{\varphi*}_{\psi}y \qquad \begin{array}{c} yR^{\varphi*}_{\psi}z\ [xR^{\varphi}_{\psi}y]^1 \\ \vdots\,\Pi_1 \\ xR^{\varphi*}_{\psi}z \end{array} \qquad \cdots \qquad \begin{array}{c} yR^{\varphi*}_{\psi}z\ [xR^{\varphi}_{\psi}x_1]^1 \cdots [x_nR^{\varphi}_{\psi}y]^1 \\ \vdots\,\Pi_2 \\ xR^{\varphi*}_{\psi}z \end{array} \qquad \cdots}{xR^{\varphi*}_{\psi}z}\;R^{\varphi*}_{\psi}\ \mathrm{E}^1$$

where Π_1 and Π_2 are respectively

$$\dfrac{yR^{\varphi*}_{\psi}z \qquad \dfrac{[xR^{\varphi}_{\psi}y]^1[yR^{\varphi}_{\psi}z]^2}{xR^{\varphi*}_{\psi}z}\;R^{\varphi*}_{\psi}\ \mathrm{I} \qquad \cdots \qquad \dfrac{[xR^{\varphi}_{\psi}y]^1[yR^{\varphi}_{\psi}y_1]^2 \cdots [y_mR^{\varphi}_{\psi}z]^2}{xR^{\varphi*}_{\psi}z}\;R^{\varphi*}_{\psi}\ \mathrm{I} \qquad \cdots}{xR^{\varphi*}_{\psi}z}\;R^{\varphi*}_{\psi}\ \mathrm{E}^2$$

and

$$\dfrac{yR^{\varphi*}_{\psi}z \qquad \dfrac{[xR^{\varphi}_{\psi}x_1]^1 \cdots [x_nR^{\varphi}_{\psi}y]^1[yR^{\varphi}_{\psi}z]^2}{xR^{\varphi*}_{\psi}z}\;R^{\varphi*}_{\psi}\ \mathrm{I} \qquad \cdots \qquad \dfrac{[xR^{\varphi}_{\psi}x_1]^1 \cdots [x_nR^{\varphi}_{\psi}y]^1[yR^{\varphi}_{\psi}y_1]^2 \cdots [y_mR^{\varphi}_{\psi}z]^2}{xR^{\varphi*}_{\psi}z}\;R^{\varphi*}_{\psi}\ \mathrm{I} \qquad \cdots}{xR^{\varphi*}_{\psi}z}\;R^{\varphi*}_{\psi}\ \mathrm{E}^2$$

5.

$$\dfrac{xR^{\varphi*}_{\psi}y \qquad \dfrac{\dfrac{[xR^{\varphi}_{\psi}y]}{yR^{\varphi}_{\psi}x}\,2}{yR^{\varphi*}_{\psi}x}\,R^{\varphi*}_{\psi}\,\mathrm{I} \qquad \cdots \qquad \begin{array}{c}[xR^{\varphi}_{\psi}x_1]\cdots[x_nR^{\varphi}_{\psi}y]\\ \vdots\,\Pi\\ yR^{\varphi*}_{\psi}x\end{array} \qquad \cdots}{yR^{\varphi*}_{\psi}x}\,R^{\varphi*}_{\psi}\,\mathrm{E}$$

where Π is

$$\dfrac{\begin{array}{c}\dfrac{\dfrac{\dfrac{\dfrac{[x_nR^{\varphi}_{\psi}y]}{yR^{\varphi}_{\psi}x_n}\,2}{yR^{\varphi*}_{\psi}x_n}\,R^{\varphi*}_{\psi}\,\mathrm{I} \qquad \dfrac{\dfrac{[x_{n-1}R^{\varphi}_{\psi}x_n]}{x_nR^{\varphi}_{\psi}x_{n-1}}\,2}{x_nR^{\varphi*}_{\psi}x_{n-1}}\,R^{\varphi*}_{\psi}\,\mathrm{I}}{yR^{\varphi*}_{\psi}x_{n-1}}\,4 \qquad \dfrac{\dfrac{[x_{n-2}R^{\varphi}_{\psi}x_{n-1}]}{x_{n-1}R^{\varphi}_{\psi}x_{n-2}}\,2}{x_{n-1}R^{\varphi*}_{\psi}x_{n-2}}\,R^{\varphi*}_{\psi}\,\mathrm{I}}{yR^{\varphi*}_{\psi}x_{n-2}}\,4\\ \ddots\\ yR^{\varphi*}_{\psi}x_1\end{array} \qquad \dfrac{\dfrac{[xR^{\varphi}_{\psi}x_1]}{x_1R^{\varphi}_{\psi}x}\,2}{x_1R^{\varphi*}_{\psi}x}\,R^{\varphi*}_{\psi}\,\mathrm{I}}{yR^{\varphi*}_{\psi}x}\,6$$

□

3.3 Soundness and Completeness

Theorem 3.3.1 (Soundness)**.** Let $\Gamma \cup \mathscr{A}$ be a set of labelled or relational formulas. **NPAC** is *sound* with respect to the restricted Kripke model, i.e.: $\Gamma \vdash \mathscr{A}$ implies $\Gamma \vDash \mathscr{A}$.

Proof. We prove by induction over the number of rules in the derivation Π of $\mathscr{A}$. For the base case, suppose that $\mathscr{A}$ is a relational formula ρ and the number of rules used to derive it is 0. Then Π consists only ρ as its topmost and bottommost formula (i.e. $\rho \in \Gamma$). Suppose that, for an arbitrary $\mathcal{M}$, $\vDash^{\mathcal{M}} \Gamma$. Then by Definition 2.3.5.1 $\vDash^{\mathcal{M}} \rho$ since $\rho \in \Gamma$. Then by Definition 2.3.5.2, $\Gamma \vDash^{\mathcal{M}} \rho$. As the model $\mathcal{M}$ is arbitrary, $\Gamma \vDash \rho$. A similar method is applied if $\mathscr{A}$ is a labelled formula $x :^{\varphi} A$.

For the inductive step, suppose that $\Gamma \vdash \mathscr{A}$ with the derivation Π using n number of rules. Suppose now that the conclusion of Π is a relational formula. We will show only for

$R_a^{\varphi,A}$ I as others will be of similar method with the help of Proposition 2.3.7. So, suppose that the bottommost relational formula is obtained by the application of $R_a^{\varphi,A}$ I rule:

$$\dfrac{\begin{array}{c}\Gamma_1\\ \vdots\,\Pi_1\\ xR_a^{\varphi_1}y\end{array}\qquad\begin{array}{c}\Gamma_2\\ \vdots\,\Pi_2\\ x:^{\varphi_1}A\end{array}\qquad\begin{array}{c}\Gamma_3\\ \vdots\,\Pi_3\\ y:^{\varphi_1}A\end{array}}{xR_a^{\varphi_1,A}y}\,R_a^{\varphi_1,A}\text{ I}$$

where $\Gamma = \Gamma_1 \cup \Gamma_2 \cup \Gamma_3$ and $\varphi = \varphi_1, A$. By the induction hypothesis, as Π_1, Π_2, and Π_3 have fewer applications of rules than Π, $\Gamma \vDash xR_a^{\varphi_1}y$, $\Gamma \vDash x :^{\varphi_1} A$, and $\Gamma \vDash y :^{\varphi_1} A$. Suppose, for an arbitrary model $\mathcal{M}$, that $\vDash^{\mathcal{M}} \Gamma$, then $\vDash^{\mathcal{M}} xR_a^{\varphi_1}y$, $\vDash^{\mathcal{M}} x :^{\varphi_1} A$, and $\vDash^{\mathcal{M}} y :^{\varphi_1} A$. Then by Proposition 2.3.7, $\vDash^{\mathcal{M}} xR_a^{\varphi_1,A}y$. Hence, as $\mathcal{M}$ is arbitrary, $\Gamma \vDash xR_a^{\varphi_1,A}y$.

Now for the case in which the final conclusion is a labelled formula. The proof if the bottommost formula is obtained by the application of any introduction and elimination of propositional rules is obvious. As for other non-propositional rules, the proof can be obtained using Proposition 2.3.7. We will only show the case in which the bottommost formula is the application of the rules $[A]^{\varphi}$ I and $[A]^{\varphi}$ E as examples. So, as for the first case, let Π be:

$$\dfrac{\begin{array}{c}\Gamma, [x :^{\varphi} A]\\ \vdots\,\Pi_1\\ x :^{\varphi,A} B\end{array}}{x :^{\varphi} [A]B}\,[A]^{\varphi}\text{ I}$$

As Π_1 has fewer applications of rules than Π, it follows that, by the induction hypothesis, $\Gamma \cup \{x :^{\varphi} A\} \vDash x :^{\varphi,A} B$. We need to show that $\Gamma \vDash x :^{\varphi} [A]B$. By contradiction, suppose that, for some $\mathcal{M}$, $\vDash^{\mathcal{M}} \Gamma$ but $\nvDash^{\mathcal{M}} x :^{\varphi} [A]B$. Then $\vDash^{\mathcal{M}} \Gamma$, $\vDash^{\mathcal{M}} x :^{\varphi} A$, and $\nvDash^{\mathcal{M}} x :^{\varphi,A} B$. Then $\vDash^{\mathcal{M}} \Gamma \cup \{x :^{\varphi} A\}$ and $\nvDash^{\mathcal{M}} x :^{\varphi,A} B$. But this contradicts $\Gamma \cup \{x :^{\varphi} A\} \vDash x :^{\varphi,A} B$.

For the second case, let Π be:

$$\dfrac{\begin{array}{c}\Gamma_1\\ \vdots\,\Pi_1\\ x :^{\varphi_1} [A]B\end{array} \qquad \begin{array}{c}\Gamma_2\\ \vdots\,\Pi_2\\ x :^{\varphi_1} A\end{array}}{x :^{\varphi_1, A} B}\,[A]^{\varphi_1}\,\mathrm{E}$$

where $\Gamma = \Gamma_1 \cup \Gamma_2$ and $\varphi = \varphi_1, A$. By the induction hypothesis, as Π_1 and Π_2 have fewer applications of rules than Π, $\Gamma \vDash x :^{\varphi_1} [A]B$ and $\Gamma \vDash x :^{\varphi_1} A$. Suppose that, for an arbitrary $\mathcal{M}$, $\vDash^{\mathcal{M}} \Gamma$. Then $\vDash^{\mathcal{M}} x :^{\varphi_1} [A]B$ and $\vDash^{\mathcal{M}} x :^{\varphi_1} A$. Then ($\vDash^{\mathcal{M}} x :^{\varphi_1} A$ implies $\vDash^{\mathcal{M}} x :^{\varphi_1, A} B$) and $\vDash^{\mathcal{M}} x :^{\varphi_1} A$. It follows that $\vDash^{\mathcal{M}} x :^{\varphi_1, A} B$. Hence, since $\mathcal{M}$ is arbitrary, $\Gamma \vDash x :^{\varphi_1, A} B$. □

Theorem 3.3.2 (Completeness)**.** Let $\Delta \cup A$ be a set of formulas (non-relational and non labelled). **NPAC** is *complete* with respect to the unrestricted Kripke model, i.e.: $\Delta \vdash A$ implies $\Delta \vDash A$.

Proof. We will proof completeness via translation by showing that Hilbert's axiomatic system **PAC** in (van Ditmarsch et al., 2008) is a subset of **NPAC** system (i.e. $\Delta \vdash_{\mathbf{PAC}} A$ implies $\Delta \vdash_{\mathbf{NPAC}} A$). It is sufficient to show that all the axioms in **PAC** are derivable from **NPAC**. As **PAC** is complete, it follows that **NPAC** is also complete. There are 16 axioms to be shown to be derivable from **NPAC**. In the following proof we let the world x and list of formulas φ to be arbitrary. Furthermore, without lost of generality, we will ignore the φ in the proof tree to reduce notational overhead. It is important to note that, by the conventional unlabelled Kripke model, to prove $\Delta \vdash A$ is to prove $x :^{\varphi} \Gamma \vdash x :^{\varphi} A$ for all $x \in \mathcal{W}$ and for all list of formulas φ.

1. Distribution of K_a.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[x : K_a(A \supset B)]^1 \qquad [xR_a y]^3}{y : A \supset B} \qquad \dfrac{[x : K_a A]^2 \qquad [xR_a y]^3}{y : A}}{y : B}}{K_a B}\,K_a\,\mathrm{I}^3}{x : K_a A \supset K_a B}\supset \mathrm{I}^2}{x : K_a(A \supset B) \supset (K_a A \supset K_a B)}\supset \mathrm{I}^1$$

2. Truth axiom.

$$\dfrac{\dfrac{[x : K_a A] \qquad \dfrac{}{xR_a x}}{x : A}}{x : K_a A \supset A} \supset \mathrm{I}$$

3. Positive introspection.

$$\dfrac{\dfrac{\dfrac{\dfrac{[x : K_a A]^1 \qquad \dfrac{[xR_a y]^2 \qquad [yR_a z]^3}{xR_a z}}{z : A}}{y : K_a A} K_a\ \mathrm{I}^3}{x : K_a K_a A} K_a\ \mathrm{I}^2}{x : K_a A \supset K_a K_a A} \supset \mathrm{I}^1$$

4. Negative introspection.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[xR_a y]^2}{yR_a x} \qquad [y : K_a A]^3}{x : A} \qquad \dfrac{\dfrac{[xR_a z]^4 \qquad \dfrac{[xR_a y]^2}{yR_a x}}{yR_a z} \qquad [y : K_a]^3}{z : A}}{x : K_a A} K_a\ \mathrm{I} \qquad [x : \neg K_a A]^1}{x : \bot}}{y : \neg K_a A} \supset \mathrm{I}^3}{x : K_a \neg K_a A} K_a\ \mathrm{I}^2}{x : \neg K_a A \supset K_a \neg K_a A} \supset \mathrm{I}^1$$

5. Atomic permanence. For one direction,

$$\dfrac{\dfrac{\dfrac{\dfrac{[x : [A]p]^1 \qquad [x : A]^2}{x :^A p}}{x : p} E_{atom^A}}{x : A \supset p} \supset \mathrm{I}^2}{x : [A]p \supset (A \supset p)} \supset \mathrm{I}^1$$

For the other direction,

$$\dfrac{\dfrac{\dfrac{\dfrac{[x : A \supset p]^1 \qquad [x : A]^2}{x : p} \qquad [x : A]^2}{x :^A p}}{x : [A]p} [A]\ \mathrm{I}^2}{(A \supset p) \supset [A]p} \supset \mathrm{I}^1$$

6. Announcement and negation. For one direction,

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[x:[A]\neg B]^1 \qquad [x:A]^2}{x:^A \neg B} \qquad \dfrac{[x:[A]B]^3 \qquad [x:A]^2}{x^A B}}{x:^A \bot}}{x:\bot}}{x:\neg[A]B}\ \bot\,\mathrm{I}^3}{x:A\supset\neg[A]B}\ \supset\mathrm{I}^2}{x:[A]\neg B\supset(A\supset\neg[A]B)}\ \supset\mathrm{I}^1$$

For the other direction,

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[x:A\supset\neg[A]B]^1 \qquad [x:A]^2}{x:\neg[A]B} \qquad \dfrac{[x:A]^2 \qquad [x:^A B]^3}{x:[A]B}}{x:\bot} \qquad [x:A]^2}{x:^A\bot}}{x:^A\neg B}\ \bot^A\,\mathrm{I}^3}{x:[A]\neg B}\ [A]\,\mathrm{I}^2}{x:(A\supset\neg[A]B)\supset[A]\neg B}\ \supset\mathrm{I}^1$$

7. Announcement and conjunction. For one direction,

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[x:[A](B\wedge C)]^1 \qquad [x:A]^2}{x:^A B\wedge C}}{x:^A B}}{x:[A]B}\ [A]\,\mathrm{I}^2 \qquad \dfrac{\dfrac{\dfrac{[x:[A](B\wedge C)]^1 \qquad [x:A]^3}{x:^A B\wedge C}}{x:^A C}}{x:[A]C}\ [A]\,\mathrm{I}^3}{x:[A]B\wedge[A]C}\ \wedge\,\mathrm{I}}{x:[A](B\wedge C)\supset[A]B\wedge[A]C}\ \supset\mathrm{I}^1$$

For the other direction,

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[x:[A]B\wedge[A]C]^1}{x:[A]B} \qquad [x:A]^2}{x:^A B} \qquad \dfrac{\dfrac{[x:[A]B\wedge[A]C]^1}{x:[A]C} \qquad [x:A]^2}{x:^A C}}{x:^A B\wedge C}}{x:[A](B\wedge C)}\ [A]\,\mathrm{I}^2}{x:[A]B\wedge[A]C\supset[A](B\wedge C)}\ \supset\mathrm{I}^1$$

8. Announcement and kowledge. For one direction,

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[x:[A]K_aB]^1 \qquad [x:A]^2}{x:^A K_aB} \qquad \dfrac{[y:A]^4 \qquad [x:A]^2 \qquad [xR_ay]^3}{xR_ay}}{y:^A B}}{y:[A]B}\ [A]\,\mathrm{I}^4}{x:K_a[A]B}\ K_a\,\mathrm{I}^3}{x:A\supset K_a[A]B}\ \supset\mathrm{I}^2}{x:[A]K_aB\supset(A\supset K_a[A]B)}\ \supset\mathrm{I}^1$$

For the other direction,

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[x : A \supset K_a[A]B]^1 \quad [x : A]^2}{x : K_a[A]B} \quad \dfrac{[xR_a^A y]^3}{xR_a y}}{y : [A]B} \quad \dfrac{[xR_a^A y]^3}{y : A}}{y :^A B}}{x :^A K_a B}\,K_a^A\,\mathrm{I}^3}{x : [A]K_a B}\,[A]\,\mathrm{I}^2}{x : (A \supset K_a[A]B) \supset [A]K_a B}\,\supset\mathrm{I}^1$$

9. Announcement composition. For one direction,

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[x : [A][B]C]^1 \quad \dfrac{[x : A \land [A]B]^2}{x : A}}{x :^A [B]C} \quad \dfrac{\dfrac{[x : A \land [A]B]^2}{x : [A]B} \quad \dfrac{[x : A \land [A]B]^2}{x : A}}{x :^A B}}{x :^{A,B} C}}{x :^{A \land [A]B} C}\,\mathrm{I}_{comp}}{x : [A \land [A]B]C}\,[A \land [A]B]\,\mathrm{I}^2}{x : [A][B]C \supset [A \land [A]B]C}\,\supset\mathrm{I}^1$$

For the other direction,

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[x : A]^2 \quad [x :^A B]^3}{x : [A]B} \quad [x : A]^2}{x : A \land [A]B} \quad x : [[A \land [A]B]C]^1}{x :^{A \land [A]B} C}}{x :^{A,B} C}\,\mathrm{E}_{comp}}{x :^A [B]C}\,[B]\,\mathrm{I}^3}{x : [A][B]C}\,[A]\,\mathrm{I}^2}{x : [A \land [A]B]C \supset [A][B]C}\,\supset\mathrm{I}^1$$

10. Distribution of C_ψ.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[x : C_\psi(A \supset B)]^1 \quad [xR^*_\psi y]^3}{y : A \supset B} \quad \dfrac{[x : C_\psi A]^2 \quad [xR^*_\psi y]^3}{y : A}}{y : B}}{x : C_\psi B}\,C_\psi\,\mathrm{I}^3}{x : C_\psi A \supset C_\psi B}\,\supset\mathrm{I}^2}{x : C_\psi(A \supset B) \supset (C_\psi A \supset C_\psi B)}\,\supset\mathrm{I}^1$$

11. Mix of common knowledge.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{xR^*_\psi x}\,3.2.10 \quad [x : C_\psi A]^1}{x : A} \quad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[xR_\psi y]^2}{xR^*_\psi y} \quad [yR^*_\psi z]^3}{xR^*_\psi z}\,3.2.10 \quad [x : C_\psi A]^1}{z : A}}{y : C_\psi A}\,C_\psi\,\mathrm{I}^3}{x : \mathcal{E}_\psi C_\psi A}\,\mathcal{E}_\psi\,\mathrm{I}^2}{}}{x : A \land \mathcal{E}_\psi C_\psi A}}{x : C_\psi A \supset (A \land \mathcal{E}_\psi C_\psi A)}\,\supset\mathrm{I}^1$$

12. Modus ponens. Suppose that $\vdash A$ and $\vdash A \supset B$. Let Π_1 and Π_2 be the derivations of them respectively.

$$\dfrac{\begin{array}{c}\vdots\,\Pi_1\\ x : A\end{array} \qquad \begin{array}{c}\vdots\,\Pi_2\\ x : A \supset B\end{array}}{x : B} \supset \mathrm{E}$$

13. Necessitation of K_a. Suppose that $\vdash A$. Then, $\vdash y : A$ for every $y \in \mathcal{W}$. Let Π be the derivation of $y : A$ and x be an arbitrary world, then:

$$\dfrac{[xR_a y] \qquad \begin{array}{c}\vdots\,\Pi\\ y : A\end{array}}{x : K_a A} K_a\ \mathrm{I}$$

Therefore, $\vdash x : K_a A$ for every $x \in \mathcal{W}$. Hence, $\vdash K_a A$.

14. Necessitation of C_ψ. Similarly, suppose that $\vdash y : A$ for every $y \in \mathcal{W}$, then:

$$\dfrac{[xR^*_\psi y] \qquad \begin{array}{c}\vdots\,\Pi\\ y : A\end{array}}{x : C_\psi A} C_\psi\ \mathrm{I}$$

15. Necessication of $[B]$. Suppose that $\vdash y :^\varphi A$ for every $y \in \mathcal{W}$ and every list of formulas φ then:

$$\dfrac{[x : B] \qquad \begin{array}{c}\vdots\,\Pi\\ x :^B A\end{array}}{x : [B]A} [B]\ \mathrm{I}$$

16. Announcement and common knowledge. For any $x_i \in \mathcal{W}$, let Π_1 be a derivation of $x_i : A \supset [B]C$ and Π_2 be a derivation of $x_i : A \wedge B \supset \mathcal{E}_\psi A$. Then:

$$\dfrac{\dfrac{\dfrac{\dfrac{[xR^{B*}_\psi y]^3 \qquad \begin{array}{c}[xR^B_\psi y]^4\\ \vdots\,\Pi_3\\ y :^B C\end{array} \qquad \cdots \qquad \begin{array}{c}[xR^B_\psi u_1]^4 \cdots [u_n R^B_\psi y]^4\\ \vdots\,\Pi_4\\ y :^B C\end{array} \qquad \cdots}{y :^B C} R^{B*}_\psi\ \mathrm{E}^4}{x :^B C_\psi C} C_\psi\ \mathrm{I}^3 \qquad [x : B]^2}{x : [B]C_\psi C} [B]\ \mathrm{I}^2 \qquad [x : A]^1}{x : A \supset [B]C_\psi C} \supset \mathrm{I}^1$$

where Π_3 and Π_4 are as follows respectively.

$$\dfrac{\dfrac{\dfrac{\dfrac{[xR^B_\psi y]^4}{xR_\psi y} \quad \dfrac{\dfrac{[x:A]^1 \quad [x:B]^2}{x:A\wedge B} \quad \Pi_2}{x:\mathcal{E}_\psi A}}{y:A} \quad \Pi_1}{y:[B]C} \quad \dfrac{[xR^B_\psi y]^4}{y:B}}{y:^B C}$$

$$\dfrac{\begin{array}{c}\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[x:A]^1\quad[x:B]^2}{x:A\wedge B}\quad\Pi_2}{x:\mathcal{E}_\psi A}\quad\dfrac{[xR^B_\psi u_1]^4}{xR_\psi u_1}}{u_1:A}\quad\dfrac{[xR^B_\psi u_1]^4}{u_1:B}\quad\Pi_2}{u_1:\mathcal{E}_\psi A}\quad\dfrac{[u_1R^B_\psi u_2]^4}{u_1R_\psi u_2}}{u_2:A}\\ \vdots\\ y:A\end{array}\quad\begin{array}{c}\dfrac{[u_1R^B_\psi u_2]^4}{u_2:B}\\ \vdots\\ y:B\end{array}\quad\Pi_1}{y:^B C}$$

□

3.4 Normalization

We prove normalization of **NPAC** without the operator $\vee$. This operator is problematic in the sense that it seems impossible to "atomize" the application of $\perp^\varphi$ rules when its conclusion is of the form $xR^\varphi_\psi y$ or $xR^{\varphi*}_\psi y$ unless we define propositional rules to relational formulas as well. We prove the normalization of **NPAC** using an extended definition of validity of a derivation used in Stålmarck (1991) from which the validity of a rule is a spesific case. The definition of the validity of the derivation Π is defined inductively over the complexity of its conclusion $\mathscr{A}$. We will define first the notion of reduction in a derivation and the definition of normalization. Although the definition of reduction includes the definition of a conversion, we will give all the conversions after the definition of reduction as we would want to declare clearly first what normalization is about.

Definition 3.4.1.

1. A derivation Π_2 is an *immediate reduction* of Π_1 if Π_2 is obtained from Π_1 by replacing a part by one conversion.
2. A derivation Π_n is a *reduction* of Π_1 if there is a sequence $\Pi_1, \ldots, \Pi_n$ such that Π_{i+1} is an immediate reduction of Π_i where $1 \leq i \leq n - 1$.
3. A derivation is said to be *normal* if it has no immediate reduction.
4. A *reduction sequence* is a sequence $\Pi_1, \Pi_2, \ldots$ of derivations where Π_{i+1} is an immediate reduction of Π_i for $1 \leq i \leq n - 1$; and, if the sequence is finite, the last derivation in the sequence is normal. We say that the reduction sequence of Π to mean that it is a reduction sequence starting with Π.
5. From here onwards we always put our major premise of an elimination rule on the leftmost side of the derivation tree.
6. *Length* of a derivation Π is the sum of the rules in Π.

Definition 3.4.2 (Normalization theorem)**.** A natural deduction system is said to satisfy the *normalization theorem* if each derivation Π in the system has at least one finite reduction sequence starting with Π.

Definition 3.4.3 (Strong normalization theorem)**.** A natural deduction system is said to satisfy *strong normalization theorem* if each reduction sequence comes to an end.

Definition 3.4.4 (Detour conversion)**.** 1. Detour conversion for $\wedge^{\varphi}$.

$$\dfrac{\dfrac{\begin{matrix}\vdots\,\Pi_1 \\ x :^{\varphi} A_1\end{matrix} \qquad \begin{matrix}\vdots\,\Pi_2 \\ x :^{\varphi} A_2\end{matrix}}{x :^{\varphi} A_1 \wedge A_2}\,\wedge^{\varphi}\,\mathrm{I}}{x :^{\varphi} A_i}\,\wedge^{\varphi}\,\mathrm{E} \qquad \text{converts to} \qquad \begin{matrix}\vdots\,\Pi_i \\ x :^{\varphi} A_i\end{matrix}$$

2. Detour conversion for $\supset^{\varphi}$.

$$\dfrac{\dfrac{\begin{array}{c}[x :^{\varphi} A]\\ \vdots\,\Pi_1\\ x :^{\varphi} B\end{array}}{x :^{\varphi} A \supset B}\supset^{\varphi}\mathrm{I} \qquad \begin{array}{c}\vdots\,\Pi_2\\ x :^{\varphi} A\end{array}}{x :^{\varphi} B}\supset^{\varphi}\mathrm{E} \qquad \text{converts to} \qquad \begin{array}{c}\vdots\,\Pi_2\\ [x :^{\varphi} A]\\ \vdots\,\Pi_1\\ x :^{\varphi} B\end{array}$$

3. Detour conversion for K_a^{φ}.

$$\dfrac{\dfrac{\begin{array}{c}[xR_a^{\varphi}y]\\ \vdots\,\Pi_1\\ y :^{\varphi} A\end{array}}{x :^{\varphi} K_a A}K_a^{\varphi}\,\mathrm{I} \qquad \begin{array}{c}\vdots\,\Pi_2\\ xR_a^{\varphi}y\end{array}}{y :^{\varphi} A}K_a^{\varphi}\,\mathrm{E} \qquad \text{converts to} \qquad \begin{array}{c}\vdots\,\Pi_2\\ [xR_a^{\varphi}y]\\ \vdots\,\Pi_1\\ y :^{\varphi} A\end{array}$$

4. Detour conversion for $\mathcal{E}_{\psi}^{\varphi}$.

$$\dfrac{\dfrac{\begin{array}{c}[xR_{\psi}^{\varphi}y]\\ \vdots\,\Pi_1\\ y :^{\varphi} A\end{array}}{x :^{\varphi} \mathcal{E}_{\psi} A}\mathcal{E}_{\psi}^{\varphi}\,\mathrm{I} \qquad \begin{array}{c}\vdots\,\Pi_2\\ xR_{\psi}^{\varphi}y\end{array}}{y :^{\varphi} A}\mathcal{E}_{\psi}^{\varphi}\,\mathrm{E} \qquad \text{converts to} \qquad \begin{array}{c}\vdots\,\Pi_2\\ [xR_{\psi}^{\varphi}y]\\ \vdots\,\Pi_1\\ y :^{\varphi} A\end{array}$$

5. Detour conversion for C_{ψ}^{φ}.

$$\dfrac{\dfrac{\begin{array}{c}[xR_{\psi}^{\varphi *}y]\\ \vdots\,\Pi_1\\ y :^{\varphi} A\end{array}}{x :^{\varphi} C_{\psi} A}C_{\psi}^{\varphi}\,\mathrm{I} \qquad \begin{array}{c}\vdots\,\Pi_2\\ xR_{\psi}^{\varphi *}y\end{array}}{y :^{\varphi} A}C_{\psi}^{\varphi}\,\mathrm{E} \qquad \text{converts to} \qquad \begin{array}{c}\vdots\,\Pi_2\\ [xR_{\psi}^{\varphi *}y]\\ \vdots\,\Pi_1\\ y :^{\varphi} A\end{array}$$

6. Detour conversion for $[A]^{\varphi}$.

$$\dfrac{\dfrac{\begin{array}{c}[x :^{\varphi} A]\\ \vdots\,\Pi_1\\ x :^{\varphi,A} B\end{array}}{x :^{\varphi} [A]B}[A]^{\varphi}\,\mathrm{I} \qquad \begin{array}{c}\vdots\,\Pi_2\\ x :^{\varphi} A\end{array}}{x :^{\varphi,A} B}[A]^{\varphi}\,\mathrm{E} \qquad \text{converts to} \qquad \begin{array}{c}\vdots\,\Pi_2\\ [x :^{\varphi} A]\\ \vdots\,\Pi_1\\ x :^{\varphi,A} B\end{array}$$

7. Detour conversion for *comp*.

$$\dfrac{\dfrac{\overset{\vdots\,\Pi}{x :^{\varphi,A,B} C}}{x :^{\varphi,A\wedge[A]B} C}\,\mathrm{I}_{comp}}{x :^{\varphi,A,B} C}\,\mathrm{E}_{comp} \qquad \text{converts to} \qquad \overset{\vdots\,\Pi}{x :^{\varphi,A,B} C}$$

8. First detour conversion for $atom^{\varphi,A}$.

$$\dfrac{\dfrac{\overset{\vdots\,\Pi_1}{x :^{\varphi} p} \qquad \overset{\vdots\,\Pi_2}{x :^{\varphi} A}}{x :^{\varphi,A} p}\,\mathrm{I}_{atom^{\varphi,A}}}{x :^{\varphi} p}\,\mathrm{E}_{atom^{\varphi,A}} \qquad \text{converts to} \qquad \overset{\vdots\,\Pi_1}{x :^{\varphi} p}$$

9. Second detour conversion for $atom^{\varphi,A}$.

$$\dfrac{\dfrac{\overset{\vdots\,\Pi_1}{x :^{\varphi} p} \qquad \overset{\vdots\,\Pi_2}{x :^{\varphi} A}}{x :^{\varphi,A} p}\,\mathrm{I}_{atom^{\varphi,A}}}{x :^{\varphi} A}\,\mathrm{E}_{atom^{\varphi,A}} \qquad \text{converts to} \qquad \overset{\vdots\,\Pi_2}{x :^{\varphi} A}$$

10. First detour conversion for $R_a^{\varphi,A}$.

$$\dfrac{\dfrac{\overset{\vdots\,\Pi}{xR_a^{\varphi}y} \qquad \overset{\vdots\,\Pi_1}{x_1 :^{\varphi} A} \qquad \overset{\vdots\,\Pi_2}{x_2 :^{\varphi} A}}{x_1R_a^{\varphi,A}x_2}\,R_a^{\varphi,A}\,\mathrm{I}}{x_1R_a^{\varphi}x_2}\,R_a^{\varphi,A}\,\mathrm{E} \qquad \text{converts to} \qquad \overset{\vdots\,\Pi}{x_1R_a^{\varphi}x_2}$$

11. Second detour conversion for $R_a^{\varphi,A}$.

$$\dfrac{\dfrac{\overset{\vdots\,\Pi}{xR_a^{\varphi}y} \qquad \overset{\vdots\,\Pi_1}{x_1 :^{\varphi} A} \qquad \overset{\vdots\,\Pi_2}{x_2 :^{\varphi} A}}{x_1R_a^{\varphi,A}x_2}\,R_a^{\varphi,A}\,\mathrm{I}}{x_i :^{\varphi} A}\,R_a^{\varphi,A}\,\mathrm{E} \qquad \text{converts to} \qquad \overset{\vdots\,\Pi_i}{x_i :^{\varphi} A}$$

12. Detour conversion for $R^{\varphi}_{a_1\ldots a_n}$.

$$\dfrac{\dfrac{\begin{matrix}\vdots\,\Pi\\ xR^{\varphi}_{a_i}y\end{matrix}}{xR^{\varphi}_{a_1\ldots a_n}y}\,R^{\varphi}_{a_1\ldots a_n}\,\mathrm{I} \qquad \begin{matrix}[xR^{\varphi}_{a_1}y]\\ \vdots\,\Pi_1\\ \mathscr{A}\end{matrix} \qquad \cdots \qquad \begin{matrix}[xR^{\varphi}_{a_n}y]\\ \vdots\,\Pi_n\\ \mathscr{A}\end{matrix}}{\mathscr{A}}\,R^{\varphi}_{a_1\ldots a_n}\,\mathrm{E}$$

converts to

$$\begin{matrix}\vdots\,\Pi\\ [xR^{\varphi}_{a_i}y]\\ \vdots\,\Pi_i\\ \mathscr{A}\end{matrix}$$

13. Detour conversions for $R^{\varphi *}_{\psi}$.

$$\dfrac{\dfrac{\begin{matrix}\vdots\,\Pi\\ xR^{\varphi}_{\psi}y\end{matrix}}{xR^{\varphi *}_{\psi}y}\,R^{\varphi *}_{\psi}\,\mathrm{I} \qquad \begin{matrix}[xR^{\varphi}_{\psi}y]\\ \vdots\,\Pi_0\\ \mathscr{A}\end{matrix} \qquad \cdots \qquad \begin{matrix}[xR^{\varphi}_{\psi}z_1]\cdots[z_nR^{\varphi}_{\psi}y]\\ \vdots\,\Pi_n\\ \mathscr{A}\end{matrix} \qquad \cdots}{\mathscr{A}}\,R^{\varphi *}_{\psi}\,\mathrm{E}$$

converts to

$$\begin{matrix}\vdots\,\Pi\\ [xR^{\varphi}_{\psi}y]\\ \vdots\,\Pi_0\\ \mathscr{A}\end{matrix}$$

and for arbitrary n

$$\dfrac{\dfrac{\begin{matrix}\vdots\,\Pi_1\\ xR^{\varphi}_{\psi}z_1\end{matrix} \quad \cdots \quad \begin{matrix}\vdots\,\Pi_n\\ z_nR^{\varphi}_{\psi}y\end{matrix}}{xR^{\varphi *}_{\psi}y}\,R^{\varphi *}_{\psi}\,\mathrm{I} \qquad \begin{matrix}[xR^{\varphi}_{\psi}y]\\ \vdots\,\Pi'_0\\ \mathscr{A}\end{matrix} \qquad \cdots \qquad \begin{matrix}[xR^{\varphi}_{\psi}z_1]\cdots[z_nR^{\varphi}_{\psi}y]\\ \vdots\,\Pi'_n\\ \mathscr{A}\end{matrix} \qquad \cdots}{\mathscr{A}}\,R^{\varphi *}_{\psi}\,\mathrm{E}$$

converts to

$$\begin{array}{ccc} \vdots\,\Pi_1 & & \vdots\,\Pi_n \\ [xR^{\varphi}_{\psi}z_1] & \cdots & [z_nR^{\varphi}_{\psi}y] \\ & \vdots\,\Pi'_n & \\ & \mathscr{A} & \end{array}$$

Definition 3.4.5 (⊥ conversion)**.**

1. ⊥ conversion for $\wedge^{\varphi}$.

$$\dfrac{\dfrac{\begin{array}{c}[x :^{\varphi} \neg(A_1 \wedge A_2)]\\ \vdots\,\Pi\\ y :^{\varphi} \bot\end{array}}{x :^{\varphi} A_1 \wedge A_2}\;\bot^{\varphi}}{x :^{\varphi} A_i}\;\wedge^{\varphi}\text{ E} \qquad \text{converts to} \qquad \dfrac{\begin{array}{c}\dfrac{\dfrac{[x :^{\varphi} \neg A_i]^1 \qquad \dfrac{[x :^{\varphi} A_1 \wedge A_2]^2}{x :^{\varphi} A_i}\;\wedge^{\varphi}\text{ E}}{x :^{\varphi} \bot}\;\supset^{\varphi}\text{ E}}{[x :^{\varphi} \neg(A_1 \wedge A_2)]}\;\supset^{\varphi}\text{ I}^2\\ \vdots\,\Pi\\ y :^{\varphi} \bot\end{array}}{x :^{\varphi} A_i}\;\bot^{\varphi,1}$$

2. ⊥ conversion for $\supset^{\varphi}$.

$$\dfrac{\dfrac{\begin{array}{c}[x :^{\varphi} \neg(A \supset B)]\\ \vdots\,\Pi_1\\ y :^{\varphi} \bot\end{array}}{x :^{\varphi} A \supset B}\;\bot^{\varphi} \qquad \begin{array}{c}\vdots\,\Pi_2\\ x :^{\varphi} A\end{array}}{x :^{\varphi} B}\;\supset^{\varphi}\text{ E}$$

converts to

$$\dfrac{\begin{array}{c}\dfrac{\dfrac{[x :^{\varphi} \neg B]^1 \qquad \dfrac{[x :^{\varphi} A \supset B]^2 \qquad \begin{array}{c}\vdots\,\Pi_2\\ x :^{\varphi} A\end{array}}{x :^{\varphi} B}\;\supset^{\varphi}\text{ E}}{x :^{\varphi} \bot}\;\supset^{\varphi}\text{ E}}{[x :^{\varphi} \neg(A \supset B)]}\;\supset^{\varphi}\text{ I}^2\\ \vdots\,\Pi_1\\ y :^{\varphi} \bot\end{array}}{x :^{\varphi} B}\;\bot^{\varphi,1}$$

3. ⊥ conversion for K^{φ}_{a}.

$$\dfrac{\dfrac{\begin{array}{c}[x :^{\varphi} \neg K_aA]\\ \vdots\,\Pi_1\\ y :^{\varphi} \bot\end{array}}{x :^{\varphi} K_aA}\;\bot^{\varphi} \qquad \begin{array}{c}\vdots\,\Pi_2\\ xR^{\varphi}_{a}y\end{array}}{y :^{\varphi} A}\;K^{\varphi}_{a}\text{ E}$$

converts to

$$\begin{array}{c}\dfrac{\dfrac{\dfrac{[y :^{\varphi} \neg A]^1 \qquad \dfrac{[x :^{\varphi} K_a A]^2 \qquad \begin{array}{c}\vdots\,\Pi_2\\ xR^{\varphi}_a y\end{array}}{y :^{\varphi} A}\supset^{\varphi}\mathrm{E}}{y :^{\varphi} \bot}\supset^{\varphi}\mathrm{E}}{x :^{\varphi} \bot}\,3.2.9}{x :^{\varphi} \neg K_a A}\supset^{\varphi}\mathrm{I}^2\\ \vdots\,\Pi_1\\ \dfrac{y :^{\varphi} \bot}{y :^{\varphi} A}\,\bot^{\varphi,1}\end{array}$$

4. $\bot$ conversion for $\mathcal{E}^{\varphi}_{\psi}$.

$$\dfrac{\dfrac{\begin{array}{c}[x :^{\varphi} \neg \mathcal{E}_{\psi} A]\\ \vdots\,\Pi_1\\ y :^{\varphi} \bot\end{array}}{x :^{\varphi} \mathcal{E}_{\psi} A}\,\bot^{\varphi} \qquad \begin{array}{c}\vdots\,\Pi_2\\ xR^{\varphi}_{\psi} y\end{array}}{y :^{\varphi} A}\,\mathcal{E}^{\varphi}_{\psi}\,\mathrm{E}$$

converts to

$$\begin{array}{c}\dfrac{\dfrac{\dfrac{[y :^{\varphi} \neg A]^1 \qquad \dfrac{[x :^{\varphi} \mathcal{E}_{\psi} A]^2 \qquad \begin{array}{c}\vdots\,\Pi_2\\ xR^{\varphi}_{\psi} y\end{array}}{y :^{\varphi} A}\supset^{\varphi}\mathrm{E}}{y :^{\varphi} \bot}\supset^{\varphi}\mathrm{E}}{x :^{\varphi} \bot}\,3.2.9}{x :^{\varphi} \neg \mathcal{E}_{\psi} A}\supset^{\varphi}\mathrm{I}^2\\ \vdots\,\Pi_1\\ \dfrac{y :^{\varphi} \bot}{y :^{\varphi} A}\,\bot^{\varphi,1}\end{array}$$

5. $\bot$ conversion for C^{φ}_{ψ}.

$$\dfrac{\dfrac{\begin{array}{c}[x :^{\varphi} \neg C_{\psi} A]\\ \vdots\,\Pi_1\\ y :^{\varphi} \bot\end{array}}{x :^{\varphi} C_{\psi} A}\,\bot^{\varphi} \qquad \begin{array}{c}\vdots\,\Pi_2\\ xR^{\varphi *}_{\psi} y\end{array}}{y :^{\varphi} A}\,C^{\varphi}_{\psi}\,\mathrm{E}$$

converts to

$$\begin{array}{c}
\dfrac{\dfrac{\dfrac{[y :^{\varphi} \neg A]^1 \qquad \dfrac{[x :^{\varphi} C_{\psi} A]^2 \qquad \begin{array}{c}\vdots\,\Pi_2\\ xR^{\varphi *}_{\psi} y\end{array}}{y :^{\varphi} A}\supset^{\varphi} \mathrm{E}}{y :^{\varphi} \bot}\supset^{\varphi} \mathrm{E}}{x :^{\varphi} \bot}\,3.2.9}{[x :^{\varphi} \neg C_{\psi} A]}\supset^{\varphi} \mathrm{I}^2\\
\vdots\,\Pi_1\\
\dfrac{y :^{\varphi} \bot}{y :^{\varphi} A}\,\bot^{\varphi,1}
\end{array}$$

6. $\bot$ conversion for $[A]^{\varphi}$.

$$\dfrac{\dfrac{\begin{array}{c}[x :^{\varphi} \neg[A]B]\\ \vdots\,\Pi_1\\ y :^{\varphi} \bot\end{array}}{x :^{\varphi} [A]B}\,\bot^{\varphi} \qquad \begin{array}{c}\vdots\,\Pi_2\\ x :^{\varphi} A\end{array}}{x :^{\varphi,A} B}\,C^{\varphi}_{\psi}\ \mathrm{E}$$

converts to

$$\begin{array}{c}
\dfrac{\dfrac{\dfrac{[x :^{\varphi,A} \neg B]^1 \qquad \dfrac{[x :^{\varphi} [A]B]^2 \qquad \begin{array}{c}\vdots\,\Pi_2\\ x :^{\varphi} A\end{array}}{x :^{\varphi,A} B}\supset^{\varphi} \mathrm{E}}{x :^{\varphi,A} \bot}\supset^{\varphi} \mathrm{E}}{x :^{\varphi} \bot}\,3.2.9}{[x :^{\varphi} \neg[A]B]}\supset^{\varphi} \mathrm{I}^2\\
\vdots\,\Pi_1\\
\dfrac{\dfrac{y :^{\varphi} \bot}{x :^{\varphi,A} \bot}\,3.2.9}{x :^{\varphi,A} B}\,\bot^{\varphi,1}
\end{array}$$

7. First $\bot$ conversion for $atom$.

$$\dfrac{\dfrac{\begin{array}{c}[x :^{\varphi,A} \neg p]\\ \vdots\,\Pi\\ y :^{\varphi,A} \bot\end{array}}{x :^{\varphi,A} p}\,\bot^{\varphi,A}}{x :^{\varphi} p}\,\mathrm{E}_{atom}$$

converts to

$$\begin{array}{c}
\dfrac{\dfrac{\dfrac{[x^{\varphi}\neg p]^1 \qquad \dfrac{[x :^{\varphi,A} p]^2}{x :^{\varphi} p}\,\mathrm{E}_{atom}}{x :^{\varphi} \bot}}{x :^{\varphi,A} \bot}\,3.2.9}{[x :^{\varphi,A} \neg p]}\supset \mathrm{I}^2 \\
\vdots\,\Pi \\
\dfrac{\dfrac{y :^{\varphi,A} \bot}{y :^{\varphi} \bot}\,3.2.9}{x :^{\varphi} p}\,\bot^{\varphi,1}
\end{array}$$

8. Second $\bot$ conversion for *atom*.

$$\begin{array}{c}
[x :^{\varphi,A} \neg p] \\
\vdots\,\Pi \\
\dfrac{\dfrac{y :^{\varphi,A} \bot}{x :^{\varphi,A} p}\,\bot^{\varphi,A}}{x :^{\varphi} A}\,\mathrm{E}_{atom}
\end{array}$$

converts to

$$\begin{array}{c}
\dfrac{\dfrac{\dfrac{[x^{\varphi}\neg A]^1 \qquad \dfrac{[x :^{\varphi,A} p]^2}{x :^{\varphi} A}\,\mathrm{E}_{atom}}{x :^{\varphi} \bot}}{x :^{\varphi,A} \bot}\,3.2.9}{[x :^{\varphi,A} \neg p]}\supset \mathrm{I}^2 \\
\vdots\,\Pi \\
\dfrac{\dfrac{y :^{\varphi,A} \bot}{y :^{\varphi} \bot}\,3.2.9}{x :^{\varphi} A}\,\bot^{\varphi,1}
\end{array}$$

9. $\bot$ conversion for *comp*. This is done by induction on the complexity of C.

We do not have a $\bot$ conversion for the relational inference rules as $\bot$ rule is only defined for labelled formulas and not for relational formulas.

Definition 3.4.6 (Permutative conversion)**.**

1. Permutative conversion for R_{ψ}^{φ}.

$$\dfrac{\dfrac{\begin{array}{c}\vdots\,\Pi\\ xR^{\varphi}_{\psi}y\end{array}\quad\begin{array}{c}[xR^{\varphi}_{a_1}y]\\ \vdots\,\Pi'_1\\ \mathscr{A}\end{array}\quad\cdots\quad\begin{array}{c}[xR^{\varphi}_{a_n}y]\\ \vdots\,\Pi'_n\\ \mathscr{A}\end{array}}{\mathscr{A}}R^{\varphi}_{\psi}\,\mathrm{E}\qquad\begin{array}{c}\vdots\,\Pi_1\\ \mathscr{B}_1\end{array}\quad\cdots}{\mathscr{C}}R$$

converts to

$$\dfrac{\begin{array}{c}\vdots\,\Pi\\ xR^{\varphi}_{\psi}y\end{array}\quad\dfrac{\begin{array}{c}[xR^{\varphi}_{a_1}y]\\ \vdots\,\Pi'_1\\ \mathscr{A}\end{array}\quad\begin{array}{c}\vdots\,\Pi_1\\ \mathscr{B}_1\end{array}\quad\cdots}{\mathscr{C}}R\quad\cdots\quad\dfrac{\begin{array}{c}[xR^{\varphi}_{a_n}y]\\ \vdots\,\Pi'_n\\ \mathscr{A}\end{array}\quad\begin{array}{c}\vdots\,\Pi_1\\ \mathscr{B}_1\end{array}\quad\cdots}{\mathscr{C}}R}{\mathscr{C}}R^{\varphi}_{\psi}\,\mathrm{E}$$

where

$$\dfrac{\begin{array}{c}\vdots\,\Pi\\ xR^{\varphi}_{\psi}y\end{array}\quad\begin{array}{c}[xR^{\varphi}_{a_1}y]\\ \vdots\,\Pi'_1\\ \mathscr{A}\end{array}\quad\cdots\quad\begin{array}{c}[xR^{\varphi}_{a_n}y]\\ \vdots\,\Pi'_n\\ \mathscr{A}\end{array}}{\mathscr{A}}R^{\varphi}_{\psi}\,\mathrm{E}$$

is normal.

2. Permutative conversion for $R^{\varphi *}_{\psi}$.

$$\dfrac{\dfrac{\begin{array}{c}\vdots\,\Pi\\ xR^{\varphi *}_{\psi}y\end{array}\quad\begin{array}{c}[xR^{\varphi}_{\psi}y]\\ \vdots\,\Pi'_0\\ \mathscr{A}\end{array}\quad\cdots\quad\begin{array}{c}[xR^{\varphi}_{\psi}z_1]\cdots[z_nR^{\varphi}_{\psi}y]\\ \vdots\,\Pi'_n\\ \mathscr{A}\end{array}\quad\cdots}{\mathscr{A}}R^{\varphi *}_{\psi}\,\mathrm{E}\qquad\begin{array}{c}\vdots\,\Pi_1\\ \mathscr{B}_1\end{array}\quad\cdots}{\mathscr{C}}R$$

converts to

$$\dfrac{\begin{array}{c}\vdots\,\Pi\\ xR^{\varphi *}_{\psi}y\end{array}\quad\dfrac{\begin{array}{c}[xR^{\varphi}_{\psi}y]\\ \vdots\,\Pi'_0\\ \mathscr{A}\end{array}\quad\begin{array}{c}\vdots\,\Pi_1\\ \mathscr{B}_1\end{array}\quad\cdots}{\mathscr{C}}R\quad\cdots\quad\dfrac{\begin{array}{c}[xR^{\varphi}_{\psi}z_1]\cdots[z_nR^{\varphi}_{\psi}y]\\ \vdots\,\Pi'_n\\ \mathscr{A}\end{array}\quad\begin{array}{c}\vdots\,\Pi_1\\ \mathscr{B}_1\end{array}\quad\cdots}{\mathscr{C}}R\quad\cdots}{\mathscr{C}}R^{\varphi *}_{\psi}\,\mathrm{E}$$

where

$$\dfrac{\begin{array}{c}\vdots\,\Pi\\ xR^{\varphi*}_{\psi}y\end{array} \quad \begin{array}{c}[xR^{\varphi}_{\psi}y]\\ \vdots\,\Pi'_0\\ \mathscr{A}\end{array} \quad \cdots \quad \begin{array}{c}[xR^{\varphi}_{\psi}z_1]\cdots[z_nR^{\varphi}_{\psi}y]\\ \vdots\,\Pi'_n\\ \mathscr{A}\end{array} \quad \cdots}{\mathscr{A}}\, R^{\varphi*}_{\psi}\ \mathrm{E}$$

is normal.

Definition 3.4.7 (Redundant ⊥ conversion)**.**

1.

$$\dfrac{\begin{array}{c}\vdots\,\Pi\\ x :^{\varphi_1} \bot\end{array} \qquad y :^{\varphi_2} \neg\bot}{z :^{\varphi_3} \bot}\,\supset^{\varphi}\mathrm{E} \qquad \text{converts to} \qquad \begin{array}{c}\vdots\,\Pi\\ z :^{\varphi_3} \bot\end{array}$$

2.

$$\dfrac{\begin{array}{c}\vdots\,\Pi\\ x :^{\varphi_1} \bot\end{array}}{y :^{\varphi_2} \bot} \qquad \text{converts to} \qquad \begin{array}{c}\vdots\,\Pi\\ x :^{\varphi_1} \bot\end{array}$$

where no assumption is discharged by the last application of the $\bot^{\varphi_2}$ rule in the derivation

$$\dfrac{\begin{array}{c}\vdots\,\Pi\\ x :^{\varphi_1} \bot\end{array}}{y :^{\varphi_2} \bot}\,\bot^{\varphi_2}$$

Definition 3.4.8.

1. We say that $\mathscr{A}$ is a *compound formula* if $\mathscr{A}$ is of the form $xR^{\varphi}_{\psi}y$, $xR^{\varphi*}_{\psi}y$, or $x :^{\varphi} A$ where A is not an atomic formula.

2. Given a derivation

$$\Pi = \dfrac{\begin{array}{c}\vdots\,\Pi_1\\ \mathscr{A}_1\end{array} \quad \cdots \quad \begin{array}{c}\vdots\,\Pi_n\\ \mathscr{A}_n\end{array}}{\mathscr{B}}\,R$$

where R is a last rule application applied in Π, we say that Π is in *I-form* if $\mathscr{B}$ is a compound formula or is in a ρ form; and, R is either an introduction rule or the $\bot^{\varphi}$ rule. Any other rule that does not satisfy this condition is called *non I-form*.

3. From here onward we will allow the number n to be an ordinal number less than ε_0. This is necessary as the introduction and elimination rule for $R_{\psi}^{\varphi*}$ are infinite in a sense that they can have infinitely countable many premises. But we will leave the ordinal analysis.

Definition 3.4.9 (Valid derivation)**.** A derivation Π is *valid* if one of the following conditions is satisfied:

1. The derivation

$$\Pi = \quad \frac{\begin{matrix} \vdots\,\Pi_1 & & \vdots\,\Pi_n \\ \mathscr{A}_1 & \cdots & \mathscr{A}_n \end{matrix}}{\mathscr{B}}\,R$$

is in I-form, each Π_i is valid, and each derivation

$$\Pi' = \quad \frac{\begin{matrix} \vdots\,\Pi & \vdots\,\Pi'_1 & & \vdots\,\Pi'_m \\ \mathscr{B} & \mathscr{A}'_1 & \cdots & \mathscr{A}'_m \end{matrix}}{\mathscr{C}}\,R'$$

is valid given that R' is an elimination rule and each Π'_i is valid.

2. The derivation

$$\Pi = \quad \frac{\begin{matrix} \vdots\,\Pi_1 & & \vdots\,\Pi_n \\ \mathscr{A}_1 & \cdots & \mathscr{A}_n \end{matrix}}{\mathscr{B}}\,R$$

is not in I-form, each immediate reduction of Π is valid, and if the last inference rule in Π is an application of R_{ψ}^{φ} E or $R_{\psi}^{\varphi*}$ E then the derivations of minor premises of that inference are valid.

Definition 3.4.10 (Valid inference rule)**.** An inference rule R is *valid* if each derivation

$$\Pi = \quad \frac{\begin{matrix} \vdots\,\Pi_1 & & \vdots\,\Pi_n \\ \mathscr{A}_1 & \cdots & \mathscr{A}_n \end{matrix}}{\mathscr{B}}\,R$$

is valid given that each Π_i is valid.

Proposition 3.4.11. 1. A reduction of a derivation in I-form that ends with an application of a rule R ends with the same application of R.

2. Validity is closed under reduction.

3. If the derivation

$$\Pi = \dfrac{\begin{matrix}\vdots\,\Pi' \\ \mathscr{A}\end{matrix} \qquad \begin{matrix}\vdots\,\Pi_1 \\ \mathscr{A}_1\end{matrix} \qquad \cdots \qquad \begin{matrix}\vdots\,\Pi_n \\ \mathscr{A}_n\end{matrix}}{\mathscr{B}}\, R$$

is normal, where R is R^{φ}_{ψ} E or $R^{\varphi *}_{\psi}$ E, then the derivation

$$\Pi'' = \dfrac{\begin{matrix}\vdots\,\Pi' \\ \mathscr{A}\end{matrix} \qquad \begin{matrix}\vdots\,\Pi'_1 \\ \mathscr{A}'_1\end{matrix} \qquad \cdots \qquad \begin{matrix}\vdots\,\Pi'_m \\ \mathscr{A}'_m\end{matrix}}{\mathscr{B}}\, R$$

is valid, given that each Π'_i is valid.

4. If a derivation Π is valid, then the derivation

$$\Pi' = \dfrac{\begin{matrix}\vdots\,\Pi \\ \mathscr{A}\end{matrix} \qquad \begin{matrix}\vdots\,\Pi'_1 \\ \mathscr{A'}_1\end{matrix} \qquad \cdots \qquad \begin{matrix}\vdots\,\Pi'_n \\ \mathscr{A'}_n\end{matrix}}{\mathscr{B}}\, R'$$

is valid, given that each Π_i is valid and R is an elimination rule.

5. Let Π_1 be a valid derivation with a conclusion $\mathscr{A}_1$ and Π_2 be a valid derivation with a conclusion $\mathscr{A}_2$ and with the premis $\mathscr{A}_1$. Then the following derivation is valid:

$$\begin{matrix}\vdots\,\Pi_1 \\ \mathscr{A}_1 \\ \vdots\,\Pi_2 \\ \mathscr{A}_2\end{matrix}$$

Proof. 1. This is obvious by simply checking all the conversions.

2. We prove by induction on the definition of validity.

(i) If Π is a valid derivation in I-form, then

$$\Pi' = \dfrac{\begin{array}{c}\vdots\,\Pi\\ \mathscr{B}\end{array} \qquad \begin{array}{c}\vdots\,\Pi'_1\\ \mathscr{A}'_1\end{array} \qquad \cdots \qquad \begin{array}{c}\vdots\,\Pi'_n\\ \mathscr{A}'_n\end{array}}{\mathscr{C}}\, R'$$

is valid, given that R' is an elimination rule and each Π'_i is valid. Now, let Π'' be an immediate reduction of Π; then, obviously the derivation

$$\dfrac{\begin{array}{c}\vdots\,\Pi''\\ \mathscr{B}\end{array} \qquad \begin{array}{c}\vdots\,\Pi'_1\\ \mathscr{A}'_1\end{array} \qquad \cdots \qquad \begin{array}{c}\vdots\,\Pi'_n\\ \mathscr{A}'_n\end{array}}{\mathscr{C}}\, R'$$

is an immediate reduction of Π'. According to Proposition 3.4.11.1, Π'' is in I-form, and, by the definition of validity of non I-form, each immediate reduction of Π' is valid. Hence, by the definition of validity of I-form and the induction hypothesis, Π'' is valid.

(ii) Assume that Π is not in I-form. Then each immediate reduction of Π is valid by the definition of validity of non I-form.

3. We prove by the induction on the sum of lengths of the reduction sequences of the derivations $\Pi'_1, \ldots, \Pi'_m$. According to the assumption that Π is normal, there is no conversion of Π'. Hence, each immediate reduction of Π'' is the result of replacing a part of one of $\Pi'_1, \ldots, \Pi'_m$ by its conversion, and the induction value of the immediate reduction of Π'' is lower than the induction value of Π''.

4. We prove that each immediate reduction Π'' of Π' is valid, by induction on a lexicographically ordered pair $\langle m, k\rangle$ of natural numbers, where m is the sum of the lengths of the reduction sequences of $\Pi, \Pi_1, \ldots, \Pi_n$ and k is the length of Π'.

(i) If Π'' is a detour conversion of Π', then Π is in I-form. Hence, the validity of Π'' follows from the definition of validity of derivations.

(ii) If Π'' is a permutative conversion of Π', then the induction values $\langle m_i, k_i \rangle$ of the derivation of the minor premises of the last inference in Π'' are lower than $\langle m, k \rangle$, since each $m_i = m$ and each $k_i < k$. Hence the validity follows from the restrictions on the permutative conversion and Proposition 3.4.11.3.

(iii) If Π'' is a result of redundant $\perp$ conversion of Π', the validity of Π'' follows from the validity of Π'.

(iv) If Π'' is the result of replacing a proper part of Π' by its conversion, then the validity of Π'' follows from the induction hypothesis, because the induction value $\langle m', k' \rangle$ of Π'' is lower than $\langle m, k \rangle$ since $m' < m$.

(iv) Similar proof by induction. □

Theorem 3.4.12. All derivations in **NPAC** are strongly normalizable.

Proof. The theorem is proved in three steps:

I. All **NPAC** rules are valid.

II. Derivation that are built out of valid rules are valid.

III. Valid derivations are strongly normalizable.

All of which will be proven in the next three seperate lemmas. □

Lemma 3.4.13. All **NPAC** rules are valid.

Proof. 1. *All introduction rules are valid.* We need to prove that each derivation of the form

$$\Pi = \dfrac{\begin{matrix}\vdots\,\Pi_1 \\ \mathscr{A}_1\end{matrix} \qquad \cdots \qquad \begin{matrix}\vdots\,\Pi_n \\ \mathscr{A}_n\end{matrix}}{\mathscr{B}}\, R$$

where R is an introduction rule, is valid given that each Π_i is valid. So, suppose that Π is as mentioned. By Definition 3.4.9.1 we need to prove that each derivation

$$\Pi' = \dfrac{\begin{matrix}\vdots\,\Pi \\ \mathscr{B}\end{matrix} \qquad \begin{matrix}\vdots\,\Pi'_1 \\ \mathscr{A}'_1\end{matrix} \qquad \cdots \qquad \begin{matrix}\vdots\,\Pi'_m \\ \mathscr{A}'_m\end{matrix}}{\mathscr{C}}\, R'$$

is valid given that R' is an elimination rule and each Π'_i is valid. And, by Definition 3.4.9.2, to show that Π' is valid is to show that each immediate reduction Π'' of Π' is valid, and if the last inference rule in Π' is an application of R^{φ}_{ψ} E or $R^{\varphi *}_{\psi}$ E then the derivations of minor premises of that inference are valid. We prove this by induction on the sum of lengths of the reduction sequences of $\Pi_1, \ldots, \Pi_n$ and $\Pi'_1, \ldots, \Pi'_m$.

(i) Validity of $\wedge^{\varphi}$ I. If R is $\wedge^{\varphi}$ I then Π' has the form

$$\dfrac{\dfrac{\begin{matrix}\vdots\,\Pi_1 \\ x :^{\varphi} A_1\end{matrix} \qquad \begin{matrix}\vdots\,\Pi_2 \\ x :^{\varphi} A_2\end{matrix}}{x :^{\varphi} A_1 \wedge A_2}\, \wedge^{\varphi}\,\mathrm{I}}{x :^{\varphi} A_i}\, \wedge^{\varphi}\,\mathrm{E}$$

If the immediate reduction Π'' of Π' is by the detour conversion for $\wedge^{\varphi}$, then Π'' is

$$\begin{matrix}\vdots\,\Pi_i \\ x :^{\varphi} A_i\end{matrix}$$

and is valid by assumption. If not then Π'' is the result of replacing a proper part of Π' by its conversion. Since the lengths of the reduction sequences of Π'' is lower the sum of the lengths of the reduction sequences of Π_1 and Π_2, then Π'' is valid by the induction hypothesis.

If not, then Π' has the following form if $\varphi = \varphi', B \wedge [B]C$ for some formula B and C.

$$\dfrac{\dfrac{\begin{matrix}\vdots\,\Pi_1\\ x :^{\varphi',B\wedge[B]C} A_1\end{matrix}\qquad\begin{matrix}\vdots\,\Pi_2\\ x :^{\varphi',B\wedge[B]C} A_2\end{matrix}}{x :^{\varphi',B\wedge[B]C} A_1 \wedge A_2}\wedge^{\varphi',B\wedge[B]C}\text{ I}}{x :^{\varphi',B,C} A_1 \wedge A_2}\text{E}_{comp}$$

Clearly there is no detour conversion defined between $\wedge^{\varphi',B\wedge[B]C}$ I and E_{comp}. So, the immediate reduction Π'' of Π' is only by the result of replacing a proper part of Π'. Since the lengths of the reduction sequences of Π'' is lower the sum of the lengths of the reduction sequences of Π_1 and Π_2, then Π'' is valid by the induction hypothesis.

(ii) Validity of $\supset^\varphi$ I. If R is $\supset^\varphi$ I then Π' has the form

$$\dfrac{\dfrac{\begin{matrix}[x :^\varphi A]\\ \vdots\,\Pi_1\\ x :^\varphi B\end{matrix}}{x :^\varphi A \supset B}\supset^\varphi\text{ I}\qquad\begin{matrix}\vdots\,\Pi_1'\\ x :^\varphi A\end{matrix}}{x :^\varphi B}\supset^\varphi\text{ E}$$

If the immediate reduction Π'' of Π' is by the detour conversion for $\supset^\varphi$, then Π'' is

$$\begin{matrix}\vdots\,\Pi_1'\\ [x :^\varphi A]\\ \vdots\,\Pi_1\\ x :^\varphi B\end{matrix}$$

and is valid since Π_1 and Π_1' are valid by assumption and Proposition 3.4.11.5. If not then Π'' is the result of replacing a proper part of Π' by its conversion. Since the lengths of the reduction sequences of Π'' is lower the sum of the lengths of the reduction sequences of Π_1 and Π_1', then Π'' is valid by the induction hypothesis.

If not, then Π' has a form, mutatis mutandis, similar to (1) if $\varphi = \varphi', B \wedge [B]C$ for some formula B and C. The proof is similar as well.

(iii) Validity of K^{φ}_{a} I, $\mathcal{E}^{\varphi}_{\psi}$ I, C^{φ}_{ψ} I, and $[A]^{\varphi}$ I. The proofs of each rule are similar to the proof of the validity of $\supset^{\varphi}$ I since the detour conversion of all these rules are similar as can be seen in 3.4.4.

(iv) Validity of I_{comp}. If R is I_{comp} then Π' has the form

$$\dfrac{\dfrac{\begin{array}{c}\vdots\,\Pi_1\\ x :^{\varphi,A,B} C\end{array}}{x :^{\varphi,A\wedge[A]B} C}\,\mathrm{I}_{comp}}{x :^{\varphi,A,B} C}\,\mathrm{E}_{comp}$$

If the immediate reduction Π'' of Π' is by the detour conversion for *comp*, then Π'' is

$$\begin{array}{c}\vdots\,\Pi_1\\ x :^{\varphi,A,B} C\end{array}$$

and is valid since Π_1 is valid by assumption. If not then Π'' is the result of replacing a proper part of Π' by its conversion. Since the lengths of the reduction sequences of Π'' is lower the sum of the lengths of the reduction sequences of Π_1, then Π'' is valid by the induction hypothesis.

(v) Validity of $\mathrm{I}_{atom^{\varphi,A}}$. The proof is similar to the proof of the validity of $\wedge^{\varphi}$ I.

(vi) Validity of $R^{\varphi,A}_{a}$ I. The proof is similar to the proof of the validity of $\wedge^{\varphi}$ I but with three premises instead of two in Π.

(vii) Validity of R^{φ}_{ψ} I. If R is R^{φ}_{ψ} then Π' has the form

$$\dfrac{\dfrac{\begin{array}{c}\vdots\,\Pi_1\\ xR^{\varphi}_{a_i}y\end{array}}{xR^{\varphi}_{a_1\ldots a_n}y}\,R^{\varphi}_{a_1\ldots a_n}\,\mathrm{I} \qquad \begin{array}{c}[xR^{\varphi}_{a_1}y]\\ \vdots\,\Pi'_1\\ \mathscr{A}\end{array} \quad \cdots \quad \begin{array}{c}[xR^{\varphi}_{a_n}y]\\ \vdots\,\Pi'_n\\ \mathscr{A}\end{array}}{\mathscr{A}}\,R^{\varphi}_{a_1\ldots a_n}\,\mathrm{E}$$

If the immediate reduction Π'' of Π' is by the detour conversion for R^{φ}_{ψ}, then Π'' is

$$\begin{array}{c} \vdots\,\Pi_1 \\ [xR^{\varphi}_{a_i}y] \\ \vdots\,\Pi'_i \\ \mathscr{A} \end{array}$$

and is valid by assumption. If not then Π″ is the result of replacing a proper part of Π′ by its conversion. Since the lengths of the reduction sequences of Π″ is lower the sum of the lengths of the reduction sequences of Π_1 and Π'_i, then Π″ is valid by the induction hypothesis.

(viii) Validity of $R^{\varphi*}_{\psi}$ I. The proof of the detour conversions of $R^{\varphi*}_{\psi}$ I is similar to the proof of the validity of R^{φ}_{ψ} I.

Note that, for each of the previous cases, R' can also be E_{comp} or both of the E_{atom}s. But the conversion of these is clearly valid by the induction hypothesis.

2. *The $\bot^{\varphi}$ rule is valid.* Note again that a derivation ending with the application $\bot^{\varphi}$ is defined as an I-form and a conclusion of an application of the $\bot^{\varphi}$ rule is always a labelled formula as we do not define it for a relational formula. Now, suppose that a derivation Π

$$\begin{array}{c} [x :^{\varphi} \neg A] \\ \vdots\,\Pi_1 \\ \dfrac{y :^{\varphi} \bot}{x :^{\varphi} A}\,\bot^{\varphi} \end{array}$$

is a derivation whose last inference is an application of the $\bot^{\varphi}$ and Π_1 is valid. We prove by induction on the rank of $x :^{\varphi} A$ that Π is valid. Note that this induction is our main induction. We will later use another induction within this main induction.

Base case. Suppose that $x :^{\varphi} A$ is atomic (i.e. $r(x :^{\varphi} A) = \langle 0, 0 \rangle$). Since A is atomic there will be no elimination rule with $x :^{\varphi} A$ as a major premise. So, Π′ is the same as Π. We prove that each immediate reduction Π″ of Π′ is valid by induction on the length of the reduction sequence of Π_1. If Π″ is obtained by a redundant ⊥ conversion, then Π″

is Π_1 and valid by assumption. If Π'' is the result of replacing a proper part of Π' by its conversion, then Π'' is valid by the induction hypothesis.

Induction step. We prove that each immediate reduction Π'' of the derivation

$$\Pi' = \qquad \dfrac{\dfrac{\begin{matrix}[x :^{\varphi} \neg A]\\ \vdots\,\Pi_1\\ y :^{\varphi} \bot\end{matrix}}{x :^{\varphi} A}\,\bot^{\varphi} \qquad \begin{matrix}\vdots\,\Pi'_1\\ \mathscr{A}'_1\end{matrix} \qquad \cdots \qquad \begin{matrix}\vdots\,\Pi'_m\\ \mathscr{A}'_m\end{matrix}}{\mathscr{B}}\,R'$$

is valid, given that R is an elimination rule and each Π'_i is valid, by induction on the sum of the lengths of the reduction tress of Π_1 and all the Π'_is.

(i) A has the form $A_1 \wedge A_2$.

(a) If Π'' is a $\bot$ conversion of Π', then Π'' has the form

$$\dfrac{\begin{matrix}\dfrac{\dfrac{[x :^{\varphi} \neg A_i]^1 \qquad \dfrac{[x :^{\varphi} A_1 \wedge A_2]^2}{x :^{\varphi} A_i}\,\wedge^{\varphi}\mathrm{E}}{x :^{\varphi} \bot}\,\supset^{\varphi}\mathrm{E}}{[x :^{\varphi} \neg(A_1 \wedge A_2)]}\,\supset^{\varphi}\mathrm{I}^2\\ \vdots\,\Pi_1\\ y :^{\varphi} \bot\end{matrix}}{x :^{\varphi} A_i}\,\bot^{\varphi,1}$$

According to the main induction hypothesis and the validity of Π_1 it is sufficient to prove the validity of the derivation

$$\Pi''' = \qquad \begin{matrix}\dfrac{\dfrac{\begin{matrix}\vdots\,\Pi''_1\\ [x :^{\varphi} \neg A_i]^1\end{matrix} \qquad \dfrac{[x :^{\varphi} A_1 \wedge A_2]^2}{x :^{\varphi} A_i}\,\wedge^{\varphi}\mathrm{E}}{x :^{\varphi} \bot}\,\supset^{\varphi}\mathrm{E}}{[x :^{\varphi} \neg(A_1 \wedge A_2)]}\,\supset^{\varphi}\mathrm{I}^2\\ \vdots\,\Pi_1\\ y :^{\varphi} \bot\end{matrix}$$

given the validity of Π''_1. Since $\supset^{\varphi}$ is a valid rule, the validity of Π''' follows if we prove that the derivation

$$\Pi'''' = \qquad \dfrac{\begin{array}{c}\vdots\,\Pi''_1\\ [x :^{\varphi} \neg A_i]^1\end{array} \qquad \dfrac{\begin{array}{c}\vdots\,\Pi''_2\\ [x :^{\varphi} A_1 \wedge A_2]^2\end{array}}{x :^{\varphi} A_i}\,\wedge^{\varphi}\mathrm{E}}{x :^{\varphi} \bot}\,\supset^{\varphi}\mathrm{E}$$

is valid, given the validity of Π''_2. But the validity of Π'''' follows by two applications of Proposition 3.4.11.4.

(b) If Π'' is the result of replacing a proper part of Π' by its conversion, then the validity of Π'' follows from the induction hypothesis.

(ii) A has the form $A_1 \supset A_2$.

(a) If Π'' is a $\bot$ conversion of Π', then Π'' has the form

$$\dfrac{\begin{array}{c}\dfrac{\dfrac{[x :^{\varphi} \neg A_2]^1 \qquad \dfrac{[x :^{\varphi} A_1 \supset A_2]^2 \qquad \begin{array}{c}\vdots\,\Pi'_1\\ x :^{\varphi} A_1\end{array}}{x :^{\varphi} A_2}\,\supset^{\varphi}\mathrm{E}}{x :^{\varphi}\bot}\,\supset^{\varphi}\mathrm{E}}{[x :^{\varphi} \neg(A_1 \supset A_2)]}\,\supset^{\varphi}\mathrm{I}^2\\ \vdots\,\Pi_1\\ y :^{\varphi}\bot\end{array}}{x :^{\varphi} A_2}\,\bot^{\varphi,1}$$

According to the main induction hypothesis and the validity of Π_1, it is sufficient to prove the validity of the derivation

$$\Pi''' = \qquad \begin{array}{c}\dfrac{\dfrac{\begin{array}{c}\vdots\,\Pi''_1\\ [x :^{\varphi} \neg A_2]^1\end{array} \qquad \dfrac{[x :^{\varphi} A_1 \supset A_2]^2 \qquad \begin{array}{c}\vdots\,\Pi'_1\\ x :^{\varphi} A_1\end{array}}{x :^{\varphi} A_2}\,\supset^{\varphi}\mathrm{E}}{x :^{\varphi}\bot}\,\supset^{\varphi}\mathrm{E}}{[x :^{\varphi} \neg(A_1 \supset A_2)]}\,\supset^{\varphi}\mathrm{I}^2\\ \vdots\,\Pi_1\\ y :^{\varphi}\bot\end{array}$$

given the validity of Π''_1. Since $\supset^{\varphi}$ is a valid rule the validity of Π''' follows if we prove that the derivation

$$\Pi'''' = \begin{array}{c}
\dfrac{\dfrac{\begin{array}{c}\vdots\,\Pi''_1\\ {[x :^{\varphi} \neg A_2]^1}\end{array} \qquad \dfrac{\begin{array}{c}\vdots\,\Pi''_2\\ {[x :^{\varphi} A_1 \supset A_2]^2}\end{array} \qquad \begin{array}{c}\vdots\,\Pi'_1\\ x :^{\varphi} A_1\end{array}}{x :^{\varphi} A_2}\supset^{\varphi}\mathrm{E}}{x :^{\varphi}\bot}\supset^{\varphi}\mathrm{E}}{[x :^{\varphi} \neg(A_1\supset A_2)]}\supset^{\varphi}\mathrm{I}^2 \\ \vdots\,\Pi_1 \\ y :^{\varphi}\bot \end{array}$$

is valid given the validity of Π''_2. The validity of Π'''' follows by two applications of Proposition 3.4.11.4.

(iii) A has the form K_aA_1, $\mathcal{E}_\psi A_1$, $C_\psi A_1$, or $[A_1]A_2$. The proofs are similar.

(iv) A has the form $x :^{A_1\wedge[A_1]A_2} A_3$. The proof is similar.

Note that, for each of the previous cases, R' can also be E_{comp} or both of the E_{atom}s. But the conversion of these is clearly valid by the induction hypothesis.

3. *All elimination rules are valid.* We need to prove that each derivation of the form

$$\Pi = \dfrac{\begin{array}{c}\vdots\,\Pi_1\\ \mathscr{A}_1\end{array} \qquad \cdots \qquad \begin{array}{c}\vdots\,\Pi_n\\ \mathscr{A}_n\end{array}}{\mathscr{B}}\,R$$

where R is an elimination rule is valid given that each Π_i is valid. This is to show that each immediate reduction of Π is valid; and, if R is an application of R^{φ}_{ψ} E or $R^{\varphi *}_{\psi}$ E then the derivations of the minor premises of that inference are valid.

(i) Validity of $\wedge^{\varphi}$ E, $\supset^{\varphi}$ E, K^{φ}_a E, $\mathcal{E}^{\varphi}_{\psi}$ E, C^{φ}_{ψ} E, $[A]^{\varphi}$ E, E_{comp}, $\mathrm{E}_{atom^{\varphi,A}}$, and $R^{\varphi,A}_a$ E. The proofs follow immediately from Proposition 3.4.11.4.

(ii) Validity of R^{φ}_{ψ} E. If R is R^{φ}_{ψ} E then Π has the form

$$\dfrac{\begin{array}{c}\vdots\,\Pi_{n+1}\\ xR^{\varphi}_{a_1\ldots a_n}y\end{array} \qquad \begin{array}{c}[xR^{\varphi}_{a_1}y]\\ \vdots\,\Pi_1\\ \mathscr{A}\end{array} \qquad \cdots \qquad \begin{array}{c}[xR^{\varphi}_{a_n}y]\\ \vdots\,\Pi_n\\ \mathscr{A}\end{array}}{\mathscr{A}}\,R^{\varphi}_{a_1\ldots a_n}\,\mathrm{E}$$

where each Π_i is valid. We prove, by induction on a lexico-graphically ordered pair $\langle m, k\rangle$ of natural numbers, where m is the sum of the lengths of the reduction sequences of each Π_i, and k is the length of Π, that each immediate reduction Π' of Π is valid.

(a) If Π' is a detour conversion of Π, then Π' has the form

$$\begin{array}{c} \vdots\,\Pi_{n+1} \\ [xR^{\varphi}_{a_i}y] \\ \vdots\,\Pi_i \\ \mathscr{A} \end{array}$$

Then the validity of Π' follows from the validity of Π_{n+1} and Π_i; and, Proposition 3.4.11.5.

(b) if Π' is a permutative conversion of Π, then Π_{n+1} has the form

$$\dfrac{\begin{array}{c}\vdots\,\Pi''_1\\ \rho\end{array} \quad \begin{array}{c}\vdots\,\Pi'_1\\ xR^{\varphi}_{\psi}y\end{array} \quad \cdots \quad \begin{array}{c}\vdots\,\Pi'_m\\ xR^{\varphi}_{\psi}y\end{array}}{xR^{\varphi}_{\psi}y}\,R$$

where R is either R^{φ}_{ψ} E or $R^{\varphi *}_{\psi}$ E, and Π' has the form

$$\dfrac{\begin{array}{c}\vdots\,\Pi''_1\\ \rho\end{array} \quad \dfrac{\begin{array}{c}\vdots\,\Pi'_1\\ xR^{\varphi}_{\psi}y\end{array} \quad \begin{array}{c}[xR^{\varphi}_{a_1}y]\\ \vdots\,\Pi_1\\ \mathscr{A}\end{array} \quad \cdots \quad \begin{array}{c}[xR^{\varphi}_{a_n}y]\\ \vdots\,\Pi_n\\ \mathscr{A}\end{array}}{\mathscr{A}} \quad \cdots \quad \dfrac{\begin{array}{c}\vdots\,\Pi'_m\\ xR^{\varphi}_{\psi}y\end{array} \quad \begin{array}{c}[xR^{\varphi}_{a_1}y]\\ \vdots\,\Pi_1\\ \mathscr{A}\end{array} \quad \cdots \quad \begin{array}{c}[xR^{\varphi}_{a_n}y]\\ \vdots\,\Pi_n\\ \mathscr{A}\end{array}}{\mathscr{A}}}{\mathscr{A}}\,R$$

The validity of each Π'_i follows from the definition of validity and the validity of Π_{n+1}. Hence, each derivation

$$\dfrac{\begin{array}{c}\vdots\,\Pi'_i\\ xR^{\varphi}_{\psi}y\end{array} \quad \begin{array}{c}[xR^{\varphi}_{a_1}y]\\ \vdots\,\Pi_1\\ \mathscr{A}\end{array} \quad \cdots \quad \begin{array}{c}[xR^{\varphi}_{a_n}y]\\ \vdots\,\Pi_n\\ \mathscr{A}\end{array}}{\mathscr{A}}\,R^{\varphi}_{\psi}\text{ E}$$

is valid by the induction hypothesis. The validity of Π' now follows from Proposition 3.4.11.3 and the restriction on permutative conversion.

(iii) Validity $R_{\psi}^{\varphi *}$ E. The proof is similar to the proof of the validity of R_{ψ}^{φ} E. □

Lemma 3.4.14. Derivations that are built out of valid rules are valid.

Proof. By induction on the length of the derivation. □

Lemma 3.4.15. Valid derivations are strongly normalizable.

Proof. We prove by induction on the definition of validity.

(i) The derivation

$$\Pi = \quad \dfrac{\begin{array}{c} \vdots\, \Pi_1 \\ \mathscr{A}_1 \end{array} \qquad \cdots \qquad \begin{array}{c} \vdots\, \Pi_n \\ \mathscr{A}_n \end{array}}{\mathscr{B}}\, R$$

in is I-form. According to the induction hypothesis, each Π_i is strongly normalizable. Hence, by Proposition 3.4.11.1, Π is strongly normalizable.

(ii) Π is not in I-form. According to the induction hypothesis, each immediate reduction of Π is strongly normalizable. Hence Π is strongly normalizable. □

CHAPTER 4: APPLICATION IN CRYPTOGRAPHIC PROTOCOL

4.1 Reviews on DEL in Cryptographic Protocol

A logical method is used in cryptographic method mainly in the form of model checking, where certain system or algorithm is checked to be correct for all model, or in the form of a proof assistant, where certain system or algorithm is being proved to be correct. It is important to note that cryptographic protocol is not in any way the study of the cryptographic system in itself, like that of studying the complexity or the impossibility of finding a factorization of a large prime, but is the study of how the cryptographic system is implemented from the beginning to the end. Generally, both methods are being used simultaneously and their use can be seen negatively in the sense that we use the model checking to find a counter model while at the same time use the proof assistant to find a solution.

To demonstrate how PAC is applicable we take an example from (van Ditmarsch et al., 2008). Let there be three people Anne, Bill, and Cath each having one card from the stack of 0, 1, and 2 labelled cards. Suppose that Anne, Bill, and Cath has the card 0, 1, and 2 respectively. Suppose now a series of announcement/protocol:

1. Anne: I do not have card 1.
2. Bill: I still do not know Anne's card.
3. Anne: I have the card 1, Bill have the card 2, and Cath has the card 3.

From this series of announcements we can deduce a lot of information even within each step of the announcement. Now to demonstrate let N_x be the symbol for person x having the card numbered N. For example, 0_a represents the statement "Anne has the card 0". To simplify let 012 represent the world in which $0_a \wedge 1_b \wedge 2_c$ is true. The following is the diagram showing the model $\mathcal{M}$ for this situation:

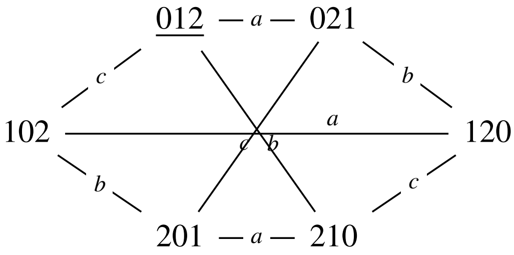

Figure 4.1: Three cards model $\mathcal{M}$

The model in this case consists of 6 worlds ($\mathcal{W} = \{012, 021, 102, 120, 201, 210\}$), $R_a = \{(012, 021), (201, 210), (102, 120)\}$, $R_b = \{(012, 210), (102, 201), (021, 120)\}$, $R_c = \{(012, 102), (021, 201), (210, 120)\}$, and the valuation function $\mathcal{V}$ in the obvious way as seen in the diagram (e.g. $\mathcal{V}(012, 0_a) = 1$ and $\mathcal{V}(012, 1_a) = 0$). Let Γ be a set including all the relations above and all atomic labelled formulas for which its valuation is 1 (e.g. $012 : 0_a$). Note that we ignore the transitive and symmetric relations to simplify. The announcement of 1, 2, and 3 can be symbolized respectively by $\neg 1_a$, $\neg K_b 0_a \wedge \neg K_b 1_a \wedge \neg K_b 2_a$, and $0_a \wedge 1_b \wedge 2_c$.

Now we know for example that Cath knows Anne's card after the first announcement by considering the following restricted model (i.e. $\models^{\mathcal{M}} 012 : [\neg 1_a](K_c 0_a \vee K_c 1_a \vee K_c 2_a)$):

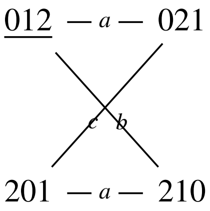

Figure 4.2: Three cards model $\mathcal{M}$ after announcing $[\neg 1_a]$

We can also show for example:

1. $\models^{\mathcal{M}} 012 : [\neg 1_a](\neg K_b 0a \wedge \neg K_b 1a \wedge \neg K_b 2_a)$; i.e. after the first announcement Bill still does not know Anne's card.

2. $\models^{\mathcal{M}} 012 : [\neg 1_a][\neg K_b 0_a \wedge \neg K_b 1_a \wedge \neg K_b 2_a][(K_a 0_b \vee K_a 1_b \vee K_a 2_b](\neg K_b 0_a \wedge \neg K_b 1_a \wedge \neg K_b 2_a)$; i.e. Bill still does not know Anne's card even after Anne's announcement that she knows Bill's card.
3. $\models^{\mathcal{M}} 012 : [\neg 1_a][\neg K_b 0_a \wedge \neg K_b 1_a \wedge \neg K_b 2_a][0_a \wedge 1_b \wedge 2_c]((\neg K_b 0_a \wedge \neg K_b 1_a \wedge \neg K_b 2_a) \wedge (\neg K_b 0_c \wedge \neg K_b 1_c \wedge \neg K_b 2_c))$; i.e. Bill knows Anne's and Cath's card after the third announcement.
4. $\models^{\mathcal{M}} 012 : [\neg 1_a][\neg K_b 0_a \wedge \neg K_b 1_a \wedge \neg K_b 2_a][0_a \wedge 1_b \wedge 2_c]C_{abc}(0_a \wedge 1_b \wedge 2_c)$; i.e. after the third announcement, it is a common knowledge for everyone that the card deal is 012.

Note that, announcing something does not imply that it is a common knowledge. This is especially true when there is a case of a formula being false after it is announced (van Ditmarsch et al., 2008). So, the following are the formal definition of this situation.

Definition 4.1.1.

1. A is a *successful formula* iff $\vdash [A]A$.
2. A is a *unsuccessful formula* iff it is not successful.

It turns out that every formula having common knowledge as its principle operator is a successful formula (van Ditmarsch et al., 2008). It can be proven semantically (van Ditmarsch et al., 2008) but we will demonstrate how it is proven using our **NPAC**. But to show this we require the following propositions.

Proposition 4.1.2. $x :^{\varphi} C_{\psi} \perp \dashv\vdash x :^{\varphi} \perp$

Proof. For one direction

$$\dfrac{x :^{\varphi} C_{\psi}\, \perp \qquad \dfrac{}{xR_{\psi}^{\varphi *}x}\,3.2.10}{x :^{\varphi} \perp}\,C_{\psi}^{\varphi}\,\mathrm{E}$$

For the other direction.

$$\dfrac{\dfrac{x :^{\varphi} \bot}{y :^{\varphi} \bot}\,3.2.9 \qquad [xR^{\varphi *}_{\psi} y]}{x :^{\varphi} C_{\psi}\ \bot}\; C^{\varphi}_{\psi}\ \mathrm{I}$$

□

Proposition 4.1.3. Suppose that $\circ$ is a propositional operator then $\vdash C_{\psi}(\neg A) \supset \neg(C_{\psi}A)$ and $\vdash C_{\psi}(A \circ B) \supset (C_{\psi}A \circ C_{\psi}B)$.

Proof. The second assertion is clearly true when $\circ$ is $\supset$ since we have proven it in Theorem 3.3.2.10. The rest of the proof can be proven using the distributivity of C_{ψ} in Theorem 3.3.2.10, Proposition 4.1.2, and the fact that two logical operators $\bot$ and $\supset$ are functionally complete for propositional operators. The following is the proof for the first assertion. For an arbitrary world x,

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[x : C_{\psi}(A \supset \bot)]^1}{x : C_{\psi}A \supset C_{\psi}\ \bot}\,3.3.2.10 \qquad [x : C_{\psi}A]^2}{x : C_{\psi}\ \bot}\,\supset \mathrm{E}}{x :\bot}\,4.1.2}{x : \neg C_{\psi}A}\,\supset \mathrm{I}^2}{x : C_{\psi}(\neg A) \supset \neg C_{\psi}A}\,\supset \mathrm{I}^1$$

□

Proposition 4.1.4.

1. $xR^{\varphi,A}_{\psi}y \vdash xR^{\varphi}_{\psi}y$
2. $xR^{\varphi,A}_{\psi}y \vdash x :^{\varphi} A$
3. $xR^{\varphi,A}_{\psi}y \vdash y :^{\varphi} A$
4. $xR^{\varphi,A*}_{\psi}y \vdash xR^{\varphi *}_{\psi}y$
5. $xR^{\varphi,A*}_{\psi}y \vdash x :^{\varphi} A$
6. $xR^{\varphi,A*}_{\psi}y \vdash y :^{\varphi} A$

Proof. 1.

$$\dfrac{xR^{\varphi,A}_{\psi}y \qquad \dfrac{\dfrac{[xR^{\varphi,A}_{a_1}y]}{xR^{\varphi}_{a_1}y}}{xR^{\varphi}_{\psi}y} \qquad \cdots \qquad \dfrac{\dfrac{[xR^{\varphi,A}_{a_n}y]}{xR^{\varphi}_{a_n}y}}{xR^{\varphi}_{\psi}y}}{xR^{\varphi}_{\psi}y}\ R^{\varphi,A}_{\psi}\,\mathrm{E}$$

2.

$$\dfrac{xR^{\varphi,A}_{\psi}y \qquad \dfrac{[xR^{\varphi,A}_{a_1}y]}{x :^{\varphi} A} \qquad \cdots \qquad \dfrac{[xR^{\varphi,A}_{a_n}y]}{x :^{\varphi} A}}{x :^{\varphi} A}\ R^{\varphi,A}_{\psi}\,\mathrm{E}$$

3. Similar to (2).

4.

$$\dfrac{xR^{\varphi,A*}_{\psi}y \qquad \dfrac{\dfrac{[xR^{\varphi,A}_{\psi}y]}{xR^{\varphi}_{\psi}y}\,1}{xR^{\varphi*}_{\psi}y} \qquad \cdots \qquad \dfrac{\dfrac{\dfrac{[xR^{\varphi,A}_{\psi}x_1]}{xR^{\varphi}_{\psi}x_1}\,1}{xR^{\varphi*}_{\psi}x_1} \qquad \cdots \qquad \dfrac{\dfrac{[x_nR^{\varphi,A}_{\psi}y]}{x_nR^{\varphi}_{\psi}y}\,1}{x_nR^{\varphi*}_{\psi}y}}{xR^{\varphi*}_{\psi}y}\,3.2.10 \qquad \cdots}{xR^{\varphi*}_{\psi}y}\ R^{\varphi,A*}_{\psi}\,\mathrm{E}$$

5.

$$\dfrac{xR^{\varphi,A*}_{\psi}y \qquad \dfrac{[xR^{\varphi,A}_{\psi}y]}{x :^{\varphi} A}\,2 \qquad \cdots \qquad \dfrac{[xR^{\varphi,A}_{\psi}x_1]}{x :^{\varphi} A}\,2 \qquad \cdots}{x :^{\varphi} A}\ R^{\varphi,A*}_{\psi}\,\mathrm{E}$$

6. Use (4) and then (5).

□

Theorem 4.1.5 (Public knowledge updates are successful)**.** $\vdash [C_\psi A]C_\psi A$.

Proof. We prove by induction over the complexity of the formula A.

Base case. If A is an atomic proposition p then for an arbitrary world x

$$\dfrac{[xR_{\psi}^{C_{\psi}p*}y]^2 \qquad \begin{matrix}[x : C_{\psi}p]^1[xR_{\psi}^{C_{\psi}p}y]^3\\ \vdots\,\Pi_1\\ y :^{C_{\psi}p} p\end{matrix} \qquad \cdots \qquad \begin{matrix}[x : C_{\psi}p]^1[xR_{\psi}^{C_{\psi}p}x_1]^3\cdots[x_nR_{\psi}^{C_{\psi}p}y]^3\\ \vdots\,\Pi_n\\ y :^{C_{\psi}p} p\end{matrix} \qquad \cdots}{\dfrac{\dfrac{y :^{C_{\psi}p} p}{x :^{C_{\psi}p} C_{\psi}p}\,C_{\psi}^{C_{\psi}p}\ \mathrm{I}^2}{x : [C_{\psi}p]C_{\psi}p}\,[C_{\psi}p]\ \mathrm{I}^1}\,R_{\psi}^{C_{\psi}p*}\ \mathrm{E}^3$$

where Π_1 is

$$\dfrac{\dfrac{\dfrac{\dfrac{[xR_{\psi}^{C_{\psi}p}y]^3}{xR_{\psi}y}\,4.1.4}{xR_{\psi}^{*}y} \qquad [x : C_{\psi}p]^1}{y : p} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[xR_{\psi}^{C_{\psi}p}y]^3}{xR_{\psi}y}}{xR_{\psi}^{*}y} \qquad [yR^{*}z]^4}{xR^{*}z} \qquad [x : C_{\psi}p]^1}{z : p}\,C_{\psi}\ \mathrm{E}}{y : C_{\psi}p}\,C_{\psi}\ \mathrm{I}^4}{y :^{C_{\psi}p} p}\,\mathrm{I}_{atom^{C_{\psi}p}}$$

and similarly for Π_n but with the use of transitivity of R_{ψ}^{*} in Proposition 3.2.10.

Induction step. We will show only for one case when A is $B \wedge C$ as the other cases can be shown with almost similar method. Recall that $\vdash A$ means that $\vdash x :^{\varphi} A$ for all world x and for all list of formulas φ. So, suppose that the formulas B and C satisfy the theorem. Let Π_1 be the derivation of $x_1 :^{\varphi_1} [C_{\psi}B]C_{\psi}B$ and Π_2 be the derivation of $x_2 :^{\varphi_2} [C_{\psi}C]C_{\psi}C$. We want to show that $x :^{\varphi} [C_{\psi}(B \wedge C)]C_{\psi}(B \wedge C)$ for all x and for all list of formulas φ. But this can be shown using Proposition 4.1.2 and 4.1.4. □

The three card game above illustrates the simple protocol of two exchanging party conveying a secret message publicly without the third person knowing the secret message. The three subjects in the example can be seen as a state machine which can be directly implemented in a computer system for cryptographic protocol purposes. A more comprehensive example can be seen in van Ditmarsch et al. (2008) in the form of Russian card problem where now there are 7 cards instead of 3. *Safe announcement* in cryptographic protocol means that two parties openly announcing between each other in order to convey a certain message without having another party learning that message. This can be formalized using the PAC as

$$K_{\psi} A \wedge [K_{\psi} A] \neg K_{eve} A.$$

In another example in Gattinger (2018), DEL is used and is extended with some additional language to formalize the protocol of Diffie-Hellman key exchange. A model checker is used to check whether there is an *eavesdropper* Eve that can eavesdrop between Alice and Bob during the key exchange. The formalization of eavesdropping is as follow:

$$(k_a = k_b) \wedge (K_{Alice} k_a \wedge K_{Bob} k_b) \wedge (\neg K_{Eve} k_a \wedge \neg K_{Eve} k_b)$$

which says informally that the key a which Alice knows is equal to the key b which Bob knows and that Eve does not know both of the keys a and b.

CHAPTER 5: CONCLUSION

5.1 Conclusion

We have given a general overview of *proof-theoretic semantics* in which we have mentioned its difference compared to *model-theoretic semantics* that gives meaning to a language by means of a model or truth. We have adopted the proof-theoretic view of the validity of an inference defined from the validity of a derivation. This differs from model-theoretic views which define the validity of an inference by the preservation of the truth from its premises to its conclusion. By using proof-theoretic views of validity we have proven the normalizability of **NPAC**. We have also briefly surveyed what dynamic epistemic logic studies, where *public announcement logic* is one of its branch, and its application in the cryptographic protocol.

We, then, comprehensively present the syntax, semantics, and the proof system of PAC. We present all the language/syntax/symbol that is comprised in PAC and from which a well formed *formula* is defined inductively to separate between meaningless concatenation of symbols in PAC and the meaningful ones. The formula in PAC has two forms, *labelled* and *relational*, which are built from a formula that is defined priorly. The *rank* of a formula in PAC is given mainly for defining the notion of validity of a derivation and for proving its normalizability in the later chapter. We then present the semantics of the well formed formulas by means of a *restricted Kripke model*, a model of which is capable of giving a meaning of an indexed labelled or relational formulas. Some properties are then proven mainly for justifying all the rules in **NPAC** or in general to prove the soundness of our **NPAC** in the later chapter. Then, we presented the known Hilbert's proof system that axiomatizes PAC (**PAC**). Although there are proof systems for PAL, Hilbert system is the only proof system of PAL with the important common knowledge operator (PAC).

We then present our proposed *labelled natural deduction for PAC* (**NPAC**). It consists of the usual *propositional inference rules* with the additional labelling and indexing, *modal, announcement, composition, and atomic inference rules*, *relational inference rules*, ;and, the three *reflexive, symmetric*, and *transitive rules*. A notion of a *derivation* is defined as a tree consisting rules consisting *premise(s)* and a *conclusion* that satisfies certain conditions. We have proven that the falsum $\perp$ traverses along worlds and also along the indexed of a list of formulas which are especially useful in proving the normalizability later. We have proven also the reflexive and symmetric properties of the R_{ψ}^{φ} operator and the equivalence relation of the $R_{\psi}^{\varphi*}$ operator which should be the case considering how they are both being defined semantically. This is especially useful in proving the completeness of **NPAC** later. Then we have proven the *soundness* of **NPAC** directly from the restricted Kripke model and have proven the completeness of **NPAC** via translation from the known Hilbert system of PAC (**PAC**). Both completeness and soundness theorem show that the **NPAC** and PAC are extensionally equivalent. We have as well proven the *strong normalizability* of the **NPAC**. This shows that every reduction of the derivation of the **NPAC** will always be reduced to a normal form. We have shown this using the proof theoretic notion of validity of a derivation from which the validity of an inference is defined.

Finally, we have presented some applications of PAC in cryptographic protocol. We have shown how the notion of *safe announcement*, where the secret can be kept although the information regarding it is announced publicly, can be formalized in PAC.

5.2 Further Work

The normalization theorem for **NPAC** is proven without the $\vee^{\varphi}$ operator mainly because it seems impossible to atomize the conclusion on an application of $\perp^{\varphi}$ rule when the conclusion is a compund relational formula. In other words, it seems impossible to atomize every relational formula ρ in the following derivation.

$$\dfrac{\dfrac{\begin{array}{c}\vdots\,\Pi\\ x :^{\varphi} A_i\end{array}}{x :^{\varphi} A_1 \vee A_2}\,\vee^{\varphi}\,\mathrm{I} \qquad \begin{array}{c}[x :^{\varphi} A_1]\\ \vdots\,\Pi_1\\ \rho\end{array} \qquad \begin{array}{c}[x :^{\varphi} A_2]\\ \vdots\,\Pi_2\\ \rho\end{array}}{\rho}\,\vee^{\varphi}\,\mathrm{E}$$

This might be circumvented if we define propositional rules to relational formulas as well. This prompts for further work to make the proof system more comprehensive by giving the relational formulas propositional rules. It is also warranting to prove the completeness directly from the restricted Kripke semantics rather than by translation into **PAC** Hilbert proof system. One can also investigate further properties of **NPAC** considering that every derivation can be normalized: consistency, sub-formula property, and other proof-theoretic principles.

Another gap that we find is that the combination of *comp* rules and other **NPAC** rules introduce an unusual detour for which we do not define a conversion in our definition. Consider the following derivation as an example:

$$\dfrac{\dfrac{\dfrac{\dfrac{\begin{array}{c}\vdots\,\Pi_1\\ x :^{\varphi',B,C} A_1\end{array}}{x :^{\varphi',B\wedge[B]C} A_1}\,\mathrm{I}_{comp} \qquad \dfrac{\begin{array}{c}\vdots\,\Pi_2\\ x :^{\varphi',B,C} A_2\end{array}}{x :^{\varphi',B\wedge[B]C} A_2}\,\mathrm{I}_{comp}}{x :^{\varphi',B\wedge[B]C} A_1 \wedge A_2}\,\wedge^{\varphi',B\wedge[B]C}\,\mathrm{I}}{x :^{\varphi',B,C} A_1 \wedge A_2}\,\mathrm{E}_{comp}}{x :^{\varphi',B,C} A_1}\,\wedge^{\varphi',B,C}\,\mathrm{E}$$

Clearly we can see that $x :^{\varphi',B,C} A_1$ appears twice in the derivation. If we are not to accept this derivation as normal then we can of course define a new conversion to circumvent this situation. In this example, the conversion would be the following

$$\begin{array}{c}\vdots\,\Pi_1\\ x :^{\varphi',B,C} A_1\end{array}$$

We can easily define all conversions of this form to avoid this kind of detour and can easily find a way to normalize all derivations in **NPAC** (i.e. weak normalization). But the challenge would be to give a new definition of valid derivation in order to achieve strong normalization.

As proof assistant is very useful as a formal method in computer science in general, it is possible to use a proof assistant to implement the **NPAC**. One possible line of research is to use *Isabella* theorem prover to implement **NPAC** like how Viganò (2000) did for non-classical modal logic.

Epistemic action logic (EAL) is another logic under the umbrella of dynamic epistemic logic. EAL is an extension of PAC which is more expressive and capable of formalizing a more complex and dynamic situation. The proof system for EAL with common knowledge operator is likewise currently only presented with the Hilbert system. Further work would be to add the **NPAC** rules towards having a new labelled natural deduction system satisfying the soundness and the completeness with respect to the EAL.

REFERENCES

Alberucci, L., & Jäger, G. (2005). About cut elimination for logics of common knowledge. *Annals of Pure and Applied Logic*, *133*(1-3), 73–99.

Artemov, S., & Protopopescu, T. (2016). Intuitionistic epistemic logic. *Review of Symbolic Logic*, *9*(2), 266–298.

Basin, D., Matthews, S., & Viganò, L. (1998). Natural deduction for non-classical logic. *Studia Logica*, *60*(1), 119–160.

Bierman, G. M., & de Paiva, V. C. V. (2000). On an intuitionistic modal logic. *Studia Logica*, *65*(3), 383–416.

Boyd, C., & Mathuria, A. (2003). *Protocols for authentication and key establishment*. Springer.

Brandom, R. B. (2001). *Articulating reasons: an introduction to inferentialism*. Harvard University Press.

Burrows, M., Abadi, M., & Needham, R. (1990). A logic of authentication. *ACM Transactions on Computer Systems*, *8*(1), 18–36.

Dechesne, F., van Eijck, J., Teepe, W., & Wang, Y. (2009). Dynamic epistemic logic for protocol analysis. In J. van Eijck & R. Verbrugge (Eds.), *Discourses on Social Software* (pp. 147–162). Amsterdam University Press.

Dechesne, F., & Wang, Y. (2007). Dynamic epistemic verification of security protocols: framework and case study. In J. van Benthem, J. Shier, & F. Veltman (Eds.), *A Meeting of the Mind: Proceeding of the Workshop on Logic, Rationality, and Interaction, Beijing* (pp. 129–146).

Dummett, M. (1991). *The logical basis of metaphysics*. Cambridge: Harvard University Press.

Francez, N. (2016). *Proof-theoretic semantics*. College Publications.

Frittella, S., Greco, G., Kurz, A., Palmigiano, A., & Sikimic, V. (2016). A proof-theoretic semantic analysis of dynamic epistemic logic. *Journal of Logic and Computation*, *26*(6), 1961–2015.

Frydrychowicz, M. Z. (2010). *An epistemic analysis of authentication* (Doctoral thesis). McGill University.

Gattinger, M. (2014). *Dynamic epistemic logic for guessing games and cryptographic protocols* (Master dissertation). Institute for Logic, Language, and Computation, University of Amsterdam.

Gattinger, M. (2018). *New directions in model checking dynamic epistemic logic* (Doctoral thesis). Institute for Logic, Language, and Computation, University of Amsterdam.

Gattinger, M., & van Eijck, J. (2015). Towards model checking cryptographic protocols with dynamic epistemic logic. In *Proceedings LAMAS* (pp. 1–14).

Gentzen, G. (1964). Investigations into logical deduction. *American Philosophical Quarterly*, *1*(4), 288–306.

Greco, G., Kurz, A., & Palmigiano, A. (2013). Dynamic epistemic logic displayed. In D. Grossi, O. Roy, & H. Huang (Eds.), *Logic, Rationality, and Interaction* (pp. 135–148). Springer, Berlin, Heidelberg.

Gritzalis, S., Spinellis, D., & Georgiadis, P. (1999). Security protocols over open networks and distributed systems: formal methods for their analysis, design, and verification. *Computer Communications*, *22*(8), 695–707.

Hintikka, J. (1962). *Knowledge and belief: an introduction to the logic of the two notions*. Cornell University Press.

Indrzejczak, A. (2010). *Natural deduction, hybrid systems and modal logics*. Springer Science & Business Media.

Kramer, S. (2007). *Logical concepts in cryptography* (Doctoral thesis). Ecole Polytechnique Federale De Lausanne.

Lowe, G. (1996). Breaking and fixing the Needham-Schroeder public-key protocol using FDR. In *International Workshop on Tools and Algorithms for the Construction and Analysis of Systems* (pp. 147–166).

Ma, M., Palmigiano, A., & Sadrzadeh, M. (2014). Algebraic semantics and model completeness for intuitionistic public announcement logic. *Annals of Pure and Applied Logic*, *165*(4), 963–995.

Maffezioli, P., & Negri, S. (2011). A proof-theoretical perspective on public announcement logic. *Logic & Philosophy of Science*, *9*(1), 49–59.

Martins, A. T., & Martins, L. R. (2006). Natural deduction for full S5 modal logic with weak normalization. *Electronic Notes in Theoretical Computer Science*, *143*, 129–140.

Medeiros, M. D. P. N. (2006). A new S4 classical modal logic in natural deduction. *The Journal of Symbolic Logic*, *71*(3), 799–809.

Payne, J. (2015). Natural deduction for modal logic with a backtracking operator. *Journal of Philosophical Logic*, *44*(3), 237–258.

Peregrin, J. (2014). *Inferentialism: why rules matter*. Palgrave Macmillan.

Piecha, T., & Schroeder-Heister, P. (2016). *Advances in proof-theoretic semantics*. Springer.

Prawitz, D. (1965). *Natural deduction: a proof-theoretical study*. Almquist and Wiksell.

Prior, A. N. (1960). The runabout inference-ticket. *Analysis*, *21*(2), 38–39.

Renne, B. (2008). *Dynamic epistemic logic with justification* (Doctoral thesis). City University of New York.

Schroeder-Heister, P. (2006). Validity concepts in proof-theoretic semantics. *Synthese*, *148*(3), 525–571.

Sikimic, V. (2013). *Towards a proof-theoretic semantics for dynamic logics* (Master dissertation). Universiteit van Amsterdam.

Simpson, A. K. (1994). *The proof theory and semantics of intuitionistic modal logic* (Doctoral thesis). University of Edinburgh.

Stålmarck, G. (1991). Normalization theorems for full first order classical natural deduction. *Journal of Symbolic Logic*, *56*(1), 129–149.

van Ditmarsch, H., van Eijck, J., Hernández-Antón, I., Sietsma, F., Simon, S., & Soler-Toscano, F. (2012). Modelling cryptographic keys in dynamic epistemic logic with DEMO. In *Highlights on Practical Applications of Agents and Multi-Agent Systems* (pp. 155–162). Springer.

van Benthem, J., van Eijck, J., Gattinger, M., & Su, K. (2018). Symbolic model checking for dynamic epistemic logic – S5 and beyond. *Journal of Logic and Computation*, *28*(2), 367–402.

van Ditmarsch, H., van der Hoek, W., & Kooi, B. (2008). *Dynamic epistemic logic*. Springer.

Viganò, L. (2000). *Labelled non-classical logics*. Springer Science & Business Media.

von Plato, J. (2005). Normal derivability in modal logic. *Mathematical Logic Quarterly*, *51*(6), 632-638.

Weiss, B., & Wanderer, J. (Eds.). (2010). *Reading Brandom: on making it explicit*. Routledge.

Williamson, T. (1992). On intuitionistic modal epistemic logic. *Journal of Philosophical Logic*, *21*(1), 63–89.

Wittgenstein, L. (2009). *Philosophical investigations*. John Wiley & Sons.