Functional Interpretation of Feasibly Constructive Arithmetic

By Naoyuki Tosa

A thesis submitted to
School of School of Information Science,
Japan Advanced Institute of Science and Technology,
in partial fulfillment of the requirements
for the degree of
Master of School of Information Science
Graduate Program in Information Science

Written under the direction of
Associate Professor Hajime Ishihara
Professor Hiroakira Ono
Professor Atsushi Ohori

March, 2001

Contents

Acknowledgment

The author is deeply grateful to Associate professor Hajime Ishihara, Professor Hiroakira Ono and Dr. Mitsuru Tada for their helpful guidance.

Special thanks to members of Ono-Ishihara laboratory and the author's friends who he has met in JAIST for their encouragement.

Finally, the author would also like to thank to my family.

Chapter 1

Introduction

In 1958, Kurt Gödel [5] suggested an interpretation of intuitionistic arithmetic in a quantifier-free theory of functionals of finite type, an interpretation which has since come to be known as *Gödel's Dialectica interpretation*.

First Gödel *Dialectica* interpretation was introduced to provide a consistency proof for intuitionistic arithmetic by elementary logic by an interpretation of an arithmetical statement by a quantifier-free formula in a theory of objects of finite type.

The *Dialectica* interpretation reduces *HA* to a theory T, where *HA* is intuitionistic first-order arithmetic "*Heyting Arithmetic*" and T is a quantifier-free theory of computable finite-type functionals, which is defined by schemata for explicit definition and a natural extension of primitive recursion to finite types, and are therefore called *primitive recursive functionals of finite type*. Atomic formulas of T are term equations : $t^\sigma =_\sigma s^\sigma$ or $t = s$, where σ is type. Axioms are initial sequents of *HA*, definition formulas of functionals and axioms of equality for each type. Inference rules are propositional logic and its induction rule.

Gödel tried to extend T to the system of intuitionistic higher type arithmetic. This higher type arithmetic is called HA^ω. We can get HA^ω from T by adding each type quantifiers and rules (or from *HA* by putting type to each function symbols and variables) .

Let A be any formula of HA^ω. We associate its *Dialectica interpretation* A^D, which is a formula of the form

$$A^D \equiv \exists \vec{Y} \forall \vec{X} \mathcal{A}(\vec{Y}, \vec{X}),$$

where $\mathcal{A}$ is a quantifier-free formula of HA^ω.

Then Gödel's main result is as follows:

> if A and A^D are provable in HA^ω, then there exists
> a primitive recursive *functional* f such that $\forall \vec{X} \mathcal{A}(f(\vec{X}), \vec{X})$ is provable in HA^ω.

Specially,

> if A is provable in *HA* and A^D is provable in HA^ω , then there exists
> a primitive recursive *function* f such that $\forall \vec{x} \mathcal{A}(f(\vec{x}), \vec{x})$ is provable in HA^ω.

This is called *functional interpretation.*

On the other hand, Troelstra[10] used an other method of realizability for same purpose in 1973.

First realizability by numbers was introduced by Kleene in 1945 as a semantics for intuitionistic arithmetic. A notion "n $\underline{\mathbf{kr}}$ P" (n realizes P) means "a number n has a property P" . In other words, "there is a number n such that P is true". This realizability is called *Kleene realizability.*

Realizability used by Troelstra for computable functionals is *modified realizability.* This was first introduced and used by Kreisel in 1959. Modified realizability in its abstract form provides interpretations the various HA^ω-versions into themselves. One of main results by Kreisel is that Markov's principle is not validated by modified realizability, where Markov's principle is the form of "$\neg\neg\exists x A \to \exists x A$". Modified realizability transform each formula A to $\vec{x}\,\underline{\mathbf{mr}}\,A$ ($\vec{x}$ modified realizes A). Then a notion $\vec{x}\,\underline{\mathbf{mr}}\,A$ means "a list of terms $\vec{x}$ makes A true in HA^ω" . In other words, "there is a list of terms $\vec{x}$ such that A is true in HA^ω".

Troelstra used the systems HA^ω same as Gödel . He proved two theorems. One is that if $\forall\vec{x}\exists y A(\vec{x}, y)$ is a theorem of HA^ω, then there exists a primitive recursive functional f and a term $\vec{t}$ such that $\forall\vec{x}(\vec{t}(\vec{x})\,\underline{\mathbf{mr}}\,A(\vec{x}, f(\vec{x})))$ is a theorem of HA^ω. Another is that if $\forall\vec{x}[\vec{t}(\vec{x})\,\underline{\mathbf{mr}}\,A(\vec{x}, f(\vec{x}))]$ is a theorem of HA^ω, then $\forall\vec{x}A(\vec{x}, f(\vec{x}))$ is a theorem of HA^ω.

Gödel and Troelstra proved the relations computable functionals and logical arithmetics HA, HA^ω. So we consider logical arithmetic which is related to polynomial time computable functionals.

Arithmetic for polynomial time computable functionals was first suggested by Stephan A. Cook[3] in 1975. This system is called PV ("Polynomially verifiable"). Cook patterned after Skolem's equational theory of primitive recursive arithmetic. Whereas Skolem's system has a function symbol for each primitive recursive function, PV has one for each polynomial time computable function. This system is logic free.

Cook's motivation for PV came from two general sources. One is the basic open problem in complexity theory of whether P equals NP, where P is a class of polynomial time computable functions (or a class based on deterministic Turing machine) and NP is a class based on nondeterministic Turing machine. His approach is to try to show they are not equal, by trying to show that the set of tautologies is not in NP (of course its complement is in NP). The second motivation comes from constructive mathematics. A constructive proof of, say, a statement $\forall x A$ must provide an effective means of finding a proof of A for each value of x, but nothing is said about how long this proof is as a function of x. If the function is exponential or super exponential, then for short values of x the length of the proof of the instance of A may exceed the number of electrons in the universe. Thus one can question the sense in which our original "constructive" provides a method of verifying $\forall x A$ for such values of x.

In 1985, Buss[1] introduced a system S^1_2 of arithmetic based on classical first order predicate calculus. One of non-logical axioms of S^1_2 is thirty-two $BASIC$ axioms. $BASIC$ axioms are axioms for function symbols and predicate symbols. Another of non-logical axioms of S^1_2 is $\Sigma^{b+}_1 - PIND$ *axiom scheme* which is the form of

$$[A(0) \wedge \forall x(A(\lfloor \tfrac{1}{2}x \rfloor))] \rightarrow A(x),$$
where A is a Σ_1^{b+}-formula.

Buss's main theorem is that

if

(1) $\forall \vec{x}(\exists y \leq t)A(\vec{x}, y)$

(2) $\forall \vec{x} \forall y \forall z[A(\vec{x}, y) \wedge A(\vec{x}, z) \rightarrow y = z]$

are provable in S_2^1 then a function f which satisfies $\forall \vec{x} A(\vec{x}, f(\vec{x}))$ is a polynomial time computable function, where $A(\vec{x}, y)$ is a Σ_1^{b+} formula.

Definition of Σ_1^{b+} formula is in Chapter 2.

In 1986 Buss[2] developed an intuitionistic version IS_2^1B of S_2^1. This is an extension of earlier work on the classical Bounded Arithmetic and was first conjectured by Stephan Cook. IS_2^1B contains polynomial hierarchy functionals of finite type. Buss proved relation for polynomial time computable functions and arithmetic same as S_2^1. But definition of IS_2^1B is complicated. One of complicated definition is a definition of axioms of IS_2^1B. Non-logical axioms of IS_2^1B are follows.

(1) If A and B are $H\Sigma_1^b$-formulas and $(A \rightarrow B)$ is theorem of S_2^1, then $(A \rightarrow B)$ is axiom of IS_2^1B.

(2) $H\Sigma_1^b$-$PIND$ *axiom scheme*

Axiom (1) is too complicated to use IS_2^1B for inference. Another of complicated definition is a definition of a class of polynomial time computable functions. Buss used a definition of a class of polynomial time computable function by p-types, $\Box_1^P$-functionals and extended $\Box_1^P$-functionals.

Therefore Cook[4] developed an another intuitionistic version IS_2^1 in 1993. Cook cleared upper two problems. Axioms and rules of inference in IS_2^1 is simple. And Cook used Cobham's function algebra as a definition of a class of polynomial time computable functions.

The system HA for computable functions and the system IS_2^1, IS_2^1B for polynomial time computable functions are based on intuitionistic logic. Especially although the class of polynomial time already has an arithmetic of classical logic version S_2^1, the intuitionistic logic version is considered. Why intuitionistic logic not classical logic? We answer by two examples of difference between classic logic and intuition principle logic. The 1st example is as follows. In classical logic, in order to prove $A \vee B$, there are two methods, where A and B are formulas. One is to prove A or B. Another is to prove that if assume $\neg A \wedge \neg B$

then arise contradiction. In intuitionistic logic, in order to prove $A \vee B$, there is only a method. It is to prove A or B. Another method which is to prove that if assume $\neg A \wedge \neg B$ then arise contradiction is not allowed. The 2st example is as follows. In classical logic, in order to prove $\exists x A(x)$, there are two methods. One is to find x such that $A(x)$ is true. Another is to prove that if assume $\forall x \neg A(x)$ then arise contradiction. In intuitionistic logic, in order to prove $\exists x A(x)$, there is only a method. It is to to find x such that $A(x)$ is true. Another method which is to prove that if assume $\forall x \neg A(x)$ then arise contradiction is not allowed. That is, it means that the proof based on intuitionistic logic had proved concrete existence in finite. Therefore it is necessary to prove on intuitionistic logic.

The aim of this thesis is the establishment of the system about "*feasibly constructive proof*". *Constructive proof* is to algorithm and *feasibly constructive proof* is to polynomial time algorithm. In Chapter 2, first we define the system S_2^1, IS_1^2 and $IS_1^2 B$. And we compare IS_1^2 with $IS_1^2 B$. Finally we prove that IS_2^1 has same properties as $IS_1^2 B$. In Chapter 3, first we define the Cook's system PV. And we prove that all of initial functions of IS_1^2 are definable in PV. But for this proof we need 206 defines, derived rules and theorems. In Chapter 4, first we introduce intuitionistic predicate logic into PV. We call this system IPV. And main theorem in this chapter is to prove that IPV is a conservative extension of IS_1^2. In Chapter 5, we introduce the typed λ-calculus. This carries out the role of T for HA. We define *types*. In Chapter 6, first we introduce higher types into PV. And adding a constant $\mathcal{R}$. We call this system PV^ω. Main theorem of this chapter is to prove that PV^ω is a conservative extension of PV. In Chapter 7, first we introduce intuitionistic many-sorted predicate logic into PV^ω. Main theorem of this chapter is to prove that IPV^ω is a conservative extension of IPV. In Chapter 8, first we define realizability for IPV^ω. Main theorem of this chapter is to prove same as Buss's main theorem for IPV^ω. In Chapter 9, first we define *Dialectica* interpretation for IPV^ω. Next, we prove (MP) and $A \leftrightarrow A^D$ are equivalent over IPV^ω. This chapter has two main theorems. One is same as realizability to prove same as Buss's main theorem for IPV^ω. Another is to prove that IS_1^2 is equivalent to $IS_1^2 B$.

Note that, in this thesis, we follow the notations and the definitions in Cook [4] .

Chapter 2

The System IS_2^1

In 1985 Buss [1] introduced a system S_2^1 of arithmetic based on classical first order predicate calculus. system S_2^1 is very closely related to the computational complexity classes of the polynomial time hierarchy and use the language $0, S, +, \cdot, \#, |x|, \lfloor \frac{1}{2}x \rfloor$ and $\leq$; where The # function is defined so that $x\#y = 2^{|x|\cdot|y|}$. The # function was first introduced Nelson, and it is evident that the # function has essentially the same growth rate as the ω_1-function. Buss proved that definable functions in his system are precisely the polynomial time computable functions.

In a later paper [2] Buss developed an intuitionistic version IS_2^1B of S_2^1. This is an extension of earlier work on the classical Bounded Arithmetic and was first conjectured by Stephan Cook. IS_2^1B contains polynomial hierarchy functionals of finite type. But definition of IS_2^1B is complicated. Therefore Cook [4] developed an another intuitionistic version IS_2^1 in 1993. We define the system IS_2^1, IS_2^1B and S_2^1 in next two sections.

2.1 Syntax and Rules of Natural Deduction

Notation 2.1.1

(1) $\equiv$ is syntactic identity.

(2) $\stackrel{d}{\equiv}$ is definitional equality.

(3) S[t/x] is the result of substituting t for free occurrences of x in S, after changing bound variables in S to avoid clashes. (S can be a term or formula.)

Definition 2.1.2 A language of IS_2^1, IS_2^1B and S_2^1 consist of the following symbols.

(1) propositional connectives ; $\vee$, $\wedge$, $\rightarrow$

(2) quantifiers ; $\forall$, $\exists$

(3) equality predicate ; $=$

(4) constant ; 0

(5) variables ; $x, y, z, \cdots$

(6) one-place function symbols ; Sx, $|x|$, $\lfloor \frac{1}{2}x \rfloor$

(7) two-place function symbols ; $x + y$, $x \cdot y$, $x \sharp y$

(8) two-place predicate ; $x \leq y$

Definition 2.1.3

$$1 \stackrel{d}{\equiv} S0 \qquad \neg A \stackrel{d}{\equiv} (A \to (0 = 1))$$
$$2 \stackrel{d}{\equiv} SS0 \qquad A \leftrightarrow B \stackrel{d}{\equiv} (A \to B) \wedge (B \to A)$$

Definition 2.1.4 *Terms* are defined inductively as follows.

(1) 0 is term,

(2) Variables are terms,

(3) If t_1 and t_2 are terms, then St_1, $|t_1|$, $\lfloor \frac{1}{2}t_1 \rfloor$, $t_1 + t_2$, $t_1 \cdot t_2$ and $t_1 \sharp t_2$ are terms,

(4) Terms are only those expressions obtained by (1)-(3).

Definition 2.1.5 *Formulas* are defined inductively as follows.

(1) If t_1 and t_2 are terms, then $t_1 = t_2$ and $t_1 \leq t_2$ are formulas. These formulas are called *atomic formula.*

(2) If A and B are formulas, then $A \vee B$, $A \wedge B$ and $A \to B$ are formulas.

(3) If A is formula and x is a variable, then $\forall x A$, $\exists x A$ are formulas.

(4) Formulas are only those expressions obtained by (1)-(3).

Definition 2.1.6 *Free occurrence* and *bounded occurrence* are defined inductively as follows.

(1) Every occurrence of a variable in an atomic formula is free.

(2) Every occurrence of a variable in $B \vee C$, in $B \wedge C$ or in $B \to C$ is free if and only if the corresponding occurrence in B or C is free.

(3) Every occurrence of a variable in $B \vee C$, $B \wedge C$ or in $B \to C$ is bounded if and only if the corresponding occurrence in B or C is bounded.

(4) Every occurrence of the variable x in $\forall x A$ and $\exists x A$ is bounded. The occurrence of the other variables in $\forall x A$ and $\exists x A$ are the same as the corresponding occurrences in A.

Definition 2.1.7 $A[t/x]$ is defined inductively as follows.

(1) If A is atomic formula (s_1=s_2, $s_1 \leq s_2$), then A[t/x] means $s_1[t/x] = s_2[t/x]$ and $s_1[t/x] \leq s_2[t/x]$.

(2) If A is $B * C$ (where $*$ is any of "$\vee$", "$\wedge$" or "$\rightarrow$"), then $A[t/x]$ is $B[t/x] * C[t/x]$.

(3) If A is $\forall z B$ or $\exists z B$,then

  (a) if x is z, $A[t/x]$ means A.

  (b) else if x is not z, then

    i. if z is not contained in t, then $A[t/z]$ means $\forall z(B[t/x])$ and $\exists z(B[t/x])$.

    ii. else $A[t/x]$ means $\forall u((B[u/z])[t/x])$ and $\exists u((B[u/z])[t/x])$ (where u is not contained in A and t).

Definition 2.1.8 *subformula* is defined inductively as follows.

(1) A is subformula of A.

(2) If A is $B * C$ (where $*$ is $\vee$, $\wedge$ or $\rightarrow$), then the subformulas of A are the subformulas of A and of B.

(3) If A is $\forall z B$ or $\exists z B$, then the subformulas of A are the subformulas of B.

Definition 2.1.9 Let A be a formula and t be a term not containing x.
We define *bounded quantifier* as follows:

$$(\exists x \leq t)A \stackrel{d}{\equiv} \exists x(x \leq t \wedge A)$$

$$(\forall x \leq t)A \stackrel{d}{\equiv} \forall x(St \leq x \vee A)$$

We define *sharply bounded quantifier* as follows:

$$(\exists x \leq |t|)A \stackrel{d}{\equiv} \exists x(x \leq |t| \wedge A)$$

$$(\forall x \leq |t|)A \stackrel{d}{\equiv} \forall x(S|t| \leq x \vee A)$$

Definition 2.1.10 *hierarchy of bounded formulas* is defined as follows.

(1) $\Pi_0^b = \Sigma_0^b$ is the set of formulas all of whose quantifiers are sharply bounded.

(2) Σ_{k+1}^b is defined inductively by ;

  (a) $\Pi_k^b \subseteq \Sigma_{k+1}^b$;

  (b) If A is in Σ_{k+1}^b then so are $(\exists x \leq t)A$, $(\forall x \leq |t|)A$;

  (c) If A and B are in Σ_{k+1}^b, so are $A \vee B$, $A \wedge B$;

  (d) If A is in Σ_{k+1}^b and B is in Π_{k+1}^b, then $\neg B$ and $B \rightarrow A$ are in Σ_{k+1}^b ;

(3) Π_{k+1}^b is defined inductively by

(a) $\Sigma^b_k \subseteq \Pi^b_{k+1}$;

(b) If A is in Π^b_{k+1} then so are $(\forall x \leq t)A$ and $(\exists x \leq |t|)A$;

(c) If A and B are in Π^b_{k+1}, so are $A \vee B$, $A \wedge B$;

(d) If A is in Π^b_{k+1} and B is in Σ^b_{k+1}, then $\neg B$ and $B \to A$ are in Π^b_{k+1} ;

(4) Σ^b_{k+1} and Π^b_{k+1} are the smallest sets which satisfy (1)-(3).

Definition 2.1.11

(1) A formula is *positive* if it contains no occurrence of $\to$.

(2) A formula is in $H\Sigma^b_1$ if all subformula of A are in Σ^b_1.

(3) A formula is in Σ^{b+}_1 if it is both positive and in Σ^b_1.

Definition 2.1.12 NJ, NK and *Identity Rules*(IR) are defined as follows.

(1) NJ is given by the following rules of inference :

$$\frac{\begin{array}{c}[A]\\ \vdots \\ B\end{array}}{A \to B}\ (\to I) \qquad \frac{A \quad A \to B}{B}\ (\to E) \qquad \frac{A \vee B \quad \begin{array}{c}[A]\\ \vdots \\ C\end{array} \quad \begin{array}{c}[B]\\ \vdots \\ C\end{array}}{C}\ (\vee E) \qquad \frac{\bot}{A}\ (\bot)$$

$$\frac{A}{A \vee B}\ (\vee I) \qquad \frac{B}{A \vee B}\ (\vee I) \qquad \frac{A \quad B}{A \wedge B}\ (\wedge I) \qquad \frac{A \wedge B}{A}\ (\wedge E) \qquad \frac{A \wedge B}{B}\ (\wedge E)$$

$$\frac{A(x)}{\forall x A(x)}\ (\forall I) \qquad \frac{\forall x A(x)}{A(t)}\ (\forall E) \qquad \frac{A(t)}{\exists x A(x)}\ (\exists I) \qquad \frac{\exists x \begin{array}{c}A(x)\\ \vdots \\ A(x)\end{array} \quad B}{B}\ (\exists E)$$

where $[A]$ and $[B]$ are hypothesis which we may cancel from proof, and in $(\forall I)$ the variable x may not occur free in any hypothesis on which $A(x)$ depends, and in $(\forall E)$ and $(\exists I)$ t is free for x, and in $(\exists E)$ x is not free in B, or in a hypothesis of the subderivation of B, other than $A(x)$.

(2) NK is given by the following rules of inference adding NJ :

$$\frac{\begin{array}{c}[\neg A]\\ \vdots \\ \bot\end{array}}{A}\ (RAA)$$

(3) IR is given by the following rules of inference :

$$\frac{}{x{=}x}\ (IR1) \qquad \frac{x{=}y}{y{=}x}\ (IR2) \qquad \frac{x{=}y \quad y{=}z}{x{=}z}\ (IR3) \qquad \frac{x{=}y \quad A}{A[y/x]}\ (IR4).$$

2.2 Definition of IS^1_2, IS^1_2B and S^1_2

Definition 2.2.1 *BASIC axioms* are defined as follows.

(1) $x = Sx \to 0 = 1$

(2) $0 \leq x$

(3) $x \leq y \to (x = y \vee Sx \leq y)$

(4) $(x \leq y \wedge y \leq z) \to x \leq z$

(5) $(x \leq y \wedge y \leq x) \to x = y$

(6) $x \leq y \vee y \leq x$

(7) $|0| = 0$

(8) $S0 \leq x \to |2 \cdot x| = S(|x|)$

(9) $|S(2 \cdot x)| = S(|x|)$

(10) $x \leq y \to |x| \leq |y|$

(11) $|x\sharp y| = S(|x| \cdot |y|)$

(12) $1\sharp 1 = 2$

(13) $x\sharp y = y\sharp x$

(14) $|x| = |u| + |v| \to x\sharp y = (u\sharp y) \cdot (v\sharp y)$

(15) $x + 0 = x$

(16) $x + Sy = S(x + y)$

(17) $(x + y) + z = x + (y + z)$

(18) $x + y \leq x + z \leftrightarrow y \leq z$

(19) $x \cdot 1 = x$

(20) $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$

(21) $x = (\lfloor \frac{1}{2}x \rfloor + \lfloor \frac{1}{2}x \rfloor) \ \vee \ x = S(\lfloor \frac{1}{2}x \rfloor + \lfloor \frac{1}{2}x \rfloor)$

Definition 2.2.2 We define some induction axioms as follows.

(1) $\mathbf{\Sigma_1^{b+}}$ **– PIND axiom scheme** :
$$[A(0) \wedge \forall x(A(\lfloor \tfrac{1}{2}x \rfloor))] \rightarrow A(x)$$
where A is a Σ_1^{b+}-formula.

(2) $\mathbf{H\Sigma_1^{b+}}$ **– PIND axiom scheme** :
$$[A(0) \wedge \forall x(A(\lfloor \tfrac{1}{2}x \rfloor))] \rightarrow A(x)$$
where A is a $H\Sigma_1^{b+}$-formula.

(3) $\mathbf{\Sigma_1^{b+}}$ **– LIND axiom scheme** :
$$[A(0) \wedge \forall x(A(x) \rightarrow A(Sx))] \rightarrow A(|x|)$$
where A is a Σ_1^{b+}-formula.

Definition 2.2.3 Let Γ be set of axiom schemes and rules of inference. If formula A is deduced from Γ, then we write $\Gamma \vdash A$

Definition 2.2.4

(1) Axioms and Rules of Inference for IS_2^1
Rules of Inference
(1) NJ
Non-Logical Axioms
(1) $BASIC\ axioms$
(2) Σ_1^{b+}–$PIND\ axiom\ scheme$

(2) Axioms and Rules of Inference for S_2^1
Rules of Inference
(1) NK
Non-Logical Axioms
(1) $BASIC\ axioms$
(2) Σ_1^{b+}–$PIND\ axiom\ scheme$

(3) Axioms and Rules of Inference for IS_2^1B
Rules of Inference
(1) NJ
Non-Logical Axioms
(1) If A and B are HΣ_1^b-formulas and (A$\rightarrow$ B) is theorem of S_2^1, then (A$\rightarrow$ B) is axiom of IS_2^1B.
(2) $H\Sigma_1^b$–$PIND\ axiom\ scheme$

2.3 Equivalence of IS_2^1 and IS_2^1B

A purpose of this section is to prove the theorem " $H\Sigma_1^b - PIND$ *scheme* is derivable in IS_2^1". This theorem is useful of proof that IS_2^1 and IS_2^1B are equivalent. This proof is in section 9.

Definition 2.3.1 We associate with each formula A of IS_2^1 two positive formula $POS(A)$ and NEG, the positive and negative transforms of A.

(1) For A atomic :
$POS(A) = A$ $\quad$ $NEG(x = y) = (Sx \leq y \vee Sy \leq x)$
$NEG(x \leq y) = (Sy \leq x)$

(2) $POS(A \to B) = NEG(A) \vee POS(B)$
$NEG(A \to B) = POS(A) \wedge NEG(B)$

(3) $POS(A \wedge B) = POS(A) \wedge POS(B)$
$NEG(A \wedge B) = NEG(A) \vee NEG(B)$

(4) $POS(\forall xA) = \forall xPOS(A)$
$NEG(\forall xA) = \exists xNEG(A)$

(5) $POS(A \vee B) = POS(A) \vee POS(B)$
$NEG(A \vee B) = NEG(A) \wedge NEG(B)$

(6) $POS(\exists xA) = \exists xPOS(A)$
$NEG(\exists xA) = \forall xNEG(A)$

This transforms take away "$\to$" from the formula A. After all $POS(A)$ and NEG don't contain "$\to$".

Lemma 2.3.2 $IS_2^1 \vdash (POS(A) \to A) \wedge (NEG(A) \to \neg A)$

(*proof*) We prove by induction on the complexity of A.

(1) A is atomic.
$POS(A) \to A$ is obvious. Therefore we need to prove $Sx \leq y \to (x = y \to (0 = 1))$ and $Sy \leq x \to (x \leq y \to (0 = 1))$, which follow easily from the $BASIC$ axioms 1, 2, 4, 5, 15, 16, 18, via the theorem $x \leq x + y$ and its corollary $x \leq Sx$.

For the remaining cases, assume that $IS_2^1 \vdash (POS(B) \to B) \wedge (NEG(B) \to \neg B)$ and $IS_2^1 \vdash (POS(C) \to C) \wedge (NEG(C) \to \neg C)$, where B and C are formulas.

(2) $A \equiv (B \to C)$, $(B \wedge C)$, $(\forall xB)$, $(B \vee C)$ and $(\exists xB)$.
For each case, we can prove by hypothesis and intuitionistic logic.

∎

Lemma 2.3.3 $IS_2^1 \vdash x = y \vee \neg(x = y)$

(*proof*) By BASIC axioms 3 and 6, $IS_2^1 \vdash x = y \vee NEG(x = y)$. The result follows by $IS_2^1 \vdash NEG(x = y) \rightarrow \neg(x = y)$(from lemma 1.3.2). ∎

Lemma 2.3.4 $IS_2^1 \vdash 2 \cdot x = x + x$

(*proof*)

By $\Sigma_1^{b+} - PIND$. The basis requires BASIC axioms 2,5,15,18,19 and 20. The induction step is based on axiom 21 and requires the theorem $1 + x = Sx$, which again uses $\Sigma_1^{b+} - PIND$ based on axiom 21. ∎

If we use BASIC axiom n (n is 1 to 21) then we abbreviate **(B.n)**.

Lemma 2.3.5 $IS_2^1 \vdash x = 0 \vee |x| = S(||\frac{1}{2}x||)$

(*proof*)
By $(B.8)$,
$IS_2^1 \vdash 2 \cdot \lfloor \frac{1}{2}x \rfloor = x \rightarrow (S0 \leq \lfloor \frac{1}{2}x \rfloor \rightarrow |x| = S(||\frac{1}{2}x||))$. $\cdots\cdots(\alpha)$.
By $(B.9), (IR4)$ and $(\rightarrow)$,
$IS_2^1 \vdash S(2 \cdot \lfloor \frac{1}{2}x \rfloor) = x \rightarrow (S0 \leq \lfloor \frac{1}{2}x \rfloor \rightarrow |x| = S(||\frac{1}{2}x||))$. $\cdots\cdots(\beta)$.
By (α),(β) and $(B.21)$
$IS_2^1 \vdash S0 \leq \lfloor \frac{1}{2}x \rfloor \rightarrow |x| = S(||\frac{1}{2}x||)$. $\cdots\cdots(\gamma)$.
Hence
$IS_2^1 \vdash S0 \leq \lfloor \frac{1}{2}x \rfloor \rightarrow (x = 0 \vee |x| = S(||\frac{1}{2}x||))$.
By $0 \leq \lfloor \frac{1}{2}x \rfloor (B.2)$ and $0 \leq \lfloor \frac{1}{2}x \rfloor \rightarrow (0 = \lfloor \frac{1}{2}x \rfloor \vee S0 \leq \lfloor \frac{1}{2}x \rfloor)(B.3)$
$IS_2^1 \vdash 0 = \lfloor \frac{1}{2}x \rfloor \vee S0 \leq \lfloor \frac{1}{2}x \rfloor$.
By $0 = \lfloor \frac{1}{2}x \rfloor \rightarrow 0 = x$
$IS_2^1 \vdash 0 = x \vee S0 \leq \lfloor \frac{1}{2}x \rfloor$. $\cdots\cdots(\delta)$
By (γ) and (δ)
$IS_2^1 \vdash x = 0 \vee |x| = S(||\frac{1}{2}x||)$. ∎

Lemma 2.3.6 The scheme of $\Sigma_1^{b+} - LIND$ is provable in IS_2^1.

(*proof*) Let formula $A(x)$ be any formula which satisfies $IS_2^1 \vdash A(0) \wedge \forall x(A(x) \rightarrow A(Sx))$ and formula $B(x)$ be $A(|x|)$. By $IS_2^1 \vdash A(0)$ and (B.7), $IS_2^1 \vdash A(|0|)$. Therefore
$IS_2^1 \vdash B(0)$. $\cdots\cdots(\alpha)$
By $\forall x(A(x) \rightarrow A(Sx))$,
$IS_2^1 \vdash A(||\frac{1}{2}y||) \rightarrow A(S(||\frac{1}{2}y||))$.
By $S(||\frac{1}{2}y||) = |y|$,
$IS_2^1 \vdash S(||\frac{1}{2}y||) = y \rightarrow (A(||\frac{1}{2}y||) \rightarrow A(|y|))$
By $y = 0, \lfloor \frac{1}{2}0 \rfloor, (IR4)$ and $(\rightarrow E)$ $\cdots\cdots(\beta)$
$IS_2^1 \vdash y = 0 \rightarrow (A(||\frac{1}{2}y||) \rightarrow A(|y|))$ $\cdots\cdots(\gamma)$.
By (β),(γ) and $(y = 0 \vee S(||\frac{1}{2}y||) = y)$ (lemma 1.3.5)

$IS_2^1 \vdash (A(||\lfloor \frac{1}{2}y \rfloor|) \to A(|y|))$.
By definition of $B(x)$
$IS_2^1 \vdash (B(\lfloor \frac{1}{2}y \rfloor) \to B(y))$. $\cdots\cdots(\delta)$
By (α),(δ) and $\Sigma_1^{b+} - PIND$
$IS_2^1 \vdash \forall y(B(y))$.
By definition of $B(x)$
$IS_2^1 \vdash \forall x(A(|x|))$.
Therefore
$IS_2^1 \vdash A(0) \wedge \forall x(A(x) \to A(Sx)) \to \forall x A(|x|)$. ∎

Lemma 2.3.7 If A is Σ_0^b formula then $IS_2^1 \vdash POS(A) \vee NEG(A)$.

(*proof*) We prove by induction on the complexity of A.

(1) $A \equiv (x = y)$
By lemma 2.3.3.

(2) $A \equiv (x \leq y)$
We need to prove $x \leq y \vee Sy \leq x$. By $(B.3)$,$y \leq x \to x \leq y \vee Sy \leq x$. By this and $x \leq y \to x \leq y \vee Sy \leq x$, $(x \leq y \vee y \leq x) \to x \leq y \vee Sy \leq x$. By this and $(B.6)$, $x \leq y \vee Sy \leq x$.

For the remaining cases, assume that $IS_2^1 \vdash POS(B) \vee NEG(B)$, $IS_2^1 \vdash POS(C) \vee NEG(C)$ and $IS_2^1 \vdash POS(E(x)) \vee NEG(E(x))$, where A, B and $E(x)$ are Σ_0^b formulas. And define formula $D(x)$ as $S|t| \leq x$, where x is a variable and t not contained x and y. Then since $D(x)$ is atomic, $IS_2^1 \vdash POS(D(x)) \vee NEG(D(x))$.

(3) $A \equiv (B \wedge C)$
We need to prove $POS(B \wedge C) \vee NEG(B \wedge C)$, *i.e.*
$(POS(B) \wedge POS(C)) \vee (NEG(B) \vee NEG(C))$.
By hypothesis,
$\vdash POP(B) \vee (NEG(B) \vee NEG(C))$ and $\vdash POS(C) \vee (NEG(B) \vee NEG(C))$.
By $POS(B) \vee (NEG(B) \vee NEG(C))$,
$\vdash POS(C) \to [(POS(B) \wedge POS(C)) \vee (NEG(B) \vee NEG(C))]$.
Hence
$\vdash (NEG(B) \vee NEG(C)) \to [(POS(B) \wedge POS(C)) \vee (NEG(B) \vee NEG(C))]$.
By $POS(C) \vee (NEG(B) \vee NEG(C))$,
$\vdash (POS(B) \wedge POS(C)) \vee (NEG(B) \vee NEG(C))$.

(4) $A \equiv (B \vee C)$
We need to prove $POS(B \vee C) \vee NEG(B \vee C)$, *i.e.*
$(POS(B) \vee POS(C)) \vee (NEG(B) \wedge NEG(C))$.
By hypothesis,
$\vdash (POP(B) \vee NEG(C)) \vee NEG(B)$ and $\vdash (POP(B) \vee NEG(C)) \vee NEG(C)$.
By $(POP(B) \vee NEG(C)) \vee NEG(B)$,

$\vdash NEG(C) \to [(POP(B) \vee NEG(C)) \vee (NEG(B) \wedge NEG(C))]$.

Hence

$\vdash (POP(B) \vee NEG(C)) \to [(POP(B) \vee NEG(C)) \vee (NEG(B) \wedge NEG(C))]$.

By $(POP(B) \vee NEG(C)) \vee NEG(C)$,

$\vdash (POP(B) \vee NEG(C)) \vee (NEG(B) \wedge NEG(C))$.

(5) $A \equiv (B \to C)$

We need to prove $POS(B \to C) \vee NEG(B \to C)$, *i.e.*
$(NEG(B) \vee POS(C)) \vee (POS(B) \wedge NEG(C))$.

By hypothesis,

$\vdash (NEG(B) \vee POS(C)) \vee POS(B)$ and $\vdash (NEG(B) \vee POS(C)) \vee NEG(C)$.

By $(NEG(B) \vee POS(C)) \vee POS(B)$,

$\vdash NEG(C) \to [(NEG(B) \vee POS(C)) \vee (POS(B) \wedge NEG(C))]$.

Hence

$\vdash (NEG(B) \vee POS(C)) \to [(NEG(B) \vee POS(C)) \vee (POS(B) \wedge NEG(C))]$.

By $(NEG(B) \vee POS(C)) \vee NEG(C)$,

$\vdash (NEG(B) \vee POS(C)) \vee (POS(B) \wedge NEG(C))$

(6) $A \equiv (\forall x \leq |t|)E(x)$

We need to prove $POS((\forall x \leq |t|)E(x)) \vee NEG((\forall x \leq |t|)E(x))$, *i.e.*
$\forall x[POS(D(x)) \vee POS(E(x))] \vee \exists x[NEG(D(x)) \wedge NEG(E(x))]$.

By hypothesis,

$\vdash [POS(D(y)) \vee POS(E(y))] \vee [NEG(D(y)) \wedge NEG(E(y))]$.

Hence

$\vdash [POS(D(y)) \vee POS(E(y))] \vee \exists x[NEG(D(x)) \wedge NEG(E(x))]$.

Therefore

$\vdash \forall x[POS(D(y)) \vee POS(E(y))] \vee \exists x[NEG(D(x)) \wedge NEG(E(x))]$.

(7) $A \equiv (\exists x \leq |t|)E(x)$

We need to prove $POS((\exists x \leq |t|)E(x)) \vee NEG((\exists x \leq |t|)E(x))$, *i.e.*
$\exists x[POS(D(x)) \wedge POS(E(x))] \vee \forall x[NEG(D(x)) \vee NEG(E(x))]$.

By hypothesis,

$\vdash [POS(D(x)) \wedge POS(E(x))] \vee [NEG(D(x)) \vee NEG(E(x))]$.

Hence

$\vdash \exists x[POS(D(x)) \wedge POS(E(x))] \vee x[NEG(D(x)) \vee NEG(E(x))]$.

Therefore

$\vdash \exists x[POS(D(x)) \wedge POS(E(x))] \vee \forall x[NEG(D(x)) \vee NEG(E(x))]$.

∎

Corollary 2.3.8 If A is Σ_0^b formula then $IS_2^1 \vdash A \vee \neg A$.

(*proof*) By $POS(A) \to A, NEG(A) \to \neg A$ (lemma 2.3.2) and $POS(A) \vee NEG(A)$ (Lemma 2.3.7). ∎

Corollary 2.3.9 If A is Σ_0^b formula then $IS_2^1 \vdash (A \leftrightarrow POS(A)) \wedge (\neg A \leftrightarrow NEG(A))$.

(*proof*) By lemma 2.3.2, $IS_2^1 \vdash (POS(A) \rightarrow A) \wedge (NEG(A) \rightarrow \neg A)$.
By $POS(A) \vee NEG(A)$, $POS(A) \rightarrow A$ and $NEG(A) \rightarrow \neg A$,
$\vdash A \vee NEG(A)$ and $\vdash POS(A) \vee \neg A$.
By $POS(A) \vee \neg A$,
$\vdash A \rightarrow POS(A)$.
By $A \vee NEG(A)$,
$\vdash \neg A \rightarrow NEG(A)$. ∎

Lemma 2.3.10 If A is $H\Sigma_1^b$ formula then $IS_2^1 \vdash A \leftrightarrow POS(A)$.

(*proof*)We prove by induction on the complexity of A.

(1) $A \in \Sigma_0^b$
By Corollary. 2.3.9.

(2) $A \in \Pi_0^b$
By $\Pi_0^b = \Sigma_0^b$, same as (1).

(3) $A \equiv (B \rightarrow C)$
Then B must be in Σ_0^b. Therefore let B be in Σ_0^b and C be in $H\Sigma_1^b$ which satisfies $IS_2^1 \vdash C \rightarrow POS(C)$. We need to prove $(B \rightarrow C) \rightarrow POS(B \rightarrow C)$, *i.e.*
$(B \rightarrow C) \rightarrow (NEG(B) \vee POS(C))$.
By $B \in \Sigma_0^b$ and cor. 2.3.9,
$IS_2^1 \vdash \neg B \rightarrow NEG(B)$ and $IS_2^1 \vdash B \vee \neg B$.
By $(B \rightarrow C)$ and $(B \vee \neg B)$,
$IS_2^1 \vdash (B \rightarrow C) \rightarrow (\neg B \vee C)$.
By $(\neg B \vee C)$, $(\neg B \rightarrow NEG(B))$ and $C \rightarrow POS(C)$,
$IS_2^1 \vdash (\neg B \vee C) \rightarrow (NEG(B) \vee POS(C))$.
By $(B \rightarrow C) \rightarrow (\neg B \vee C)$ and $(\neg B \vee C) \rightarrow (NEG(B) \vee POS(C))$,
$IS_2^1 \vdash (B \rightarrow C) \rightarrow (NEG(B) \vee POS(C))$.

For the remaining cases, assume that $IS_2^1 \vdash (B \rightarrow POS(B)) \wedge (C \rightarrow POS(C))$, where B and C are $H\Sigma_1^b$ formulas.

(4) $A \equiv (B \wedge C)$ and $A \equiv (B \vee C)$
We need to prove $(B \wedge C) \rightarrow POS(B \wedge C)$ and $(B \vee C) \rightarrow POS(B \vee C)$, *i.e.* $(B \wedge C) \rightarrow (POS(B) \wedge POS(C))$ and $(B \vee C) \rightarrow (POS(B) \vee POS(C))$. This is proved easily by hypothesis.

(5) $A \equiv (\exists x \leq t)B$
We need to prove $(\exists x \leq t)B \rightarrow POS((\exists x \leq t)B)$.
By definition of POS and Bounded quantifier,
$\vdash (\exists x \leq t)B \rightarrow \exists x(x \leq t \wedge B)$

$\rightarrow \exists x(POS(x \leq t) \wedge POS(B))$
$\rightarrow \exists x POS(x \leq t \wedge B)$
$\rightarrow POS(\exists x(x \leq t \wedge B))$
$\rightarrow POS((\exists x \leq t)B)$.

Therefore $IS_2^1 \vdash (\exists x \leq t)B \rightarrow POS((\exists x \leq t)B)$.

(6) $A \equiv (\forall x \leq |t|)B$

We need to prove $(\forall x \leq |t|)B \rightarrow POS((\forall x \leq |t|)B)$.

By definition of POS and Bounded quantifier,

$\vdash (\forall x \leq |t|)B \rightarrow \forall x(S|t| \leq x \vee B)$
$\rightarrow \forall x(POS(S|t| \leq x) \vee POS(B))$
$\rightarrow \forall x POS(S|t| \leq x \vee B)$
$\rightarrow POS(\forall x(S|t| \leq x \vee B))$
$\rightarrow POS((\forall x \leq |t|)B)$.

Therefore $IS_2^1 \vdash (\forall x \leq |t|)B \rightarrow POS((\forall x \leq |t|)B)$.

∎

Theorem 2.3.11 The $H\Sigma_1^b - PIND$ *scheme* is derivable in IS_2^1.

(*proof*)
Let $A(x)$ be any formula in $H\Sigma_1^b$. By lemma 1.3.10 2.3.10 and $A(x) \in H\Sigma_1^b$,
$IS_2^1 \vdash A(0) \leftrightarrow POS(A(0)), \vdash A(\lfloor \frac{1}{2}x \rfloor) \leftrightarrow POS(A(\lfloor \frac{1}{2}x \rfloor))$ and $\vdash A(x) \leftrightarrow POS(A(x))$.
Assume that $IS_2^1 \vdash A(0) \wedge \forall x(A(\lfloor \frac{1}{2}x \rfloor) \rightarrow A(x))$. Then
$IS_2^1 \vdash POS(A(0)) \wedge \forall x(POS(A(\lfloor \frac{1}{2}x \rfloor)) \rightarrow POS(A(x)))$.
By $POS(A(0)), POS(A(\lfloor \frac{1}{2}x \rfloor))$ and $A(x) \in \Sigma_1^{b+}$, these formulas can be apllied
$\Sigma_1^{b+} - PIND$. Therefor $IS_2^1 \vdash \forall x POS(A(x))$. Therefor $IS_2^1 \vdash \forall x A(x)$.
Therefore For any formula $A(x) \in H\Sigma_1^b$, $IS_2^1 \vdash [A(0) \wedge \forall x(A(\lfloor \frac{1}{2}x \rfloor) \rightarrow A(x))] \rightarrow \forall x A(x)$.

∎

This theorem is useful in Chapter 9 to prove that IS_2^1 and $IS_2^1 B$ are equivalent.

2.4 Bootstrapping IS_2^1

In this section, we say the relation IS_2^1 and polynomial time computable functions.

Definition 2.4.1 Let T and T' be systems.

(1) We define $L(T)$ as set of all of formulas of T.

(2) T' is *extension* of T if $\forall A \in L(T)[T \vdash A \Rightarrow T' \vdash A]$

(3) T' is *consevative extension* of T if $\forall A \in L(T)[T' \vdash A \Rightarrow T \vdash A]$

Definition 2.4.2 Let T be an extension of IS_2^1. Let A be a Σ_1^{b+} formula of T and let t be a term of T such that

$$T \vdash \forall \vec{x}(\exists y \leq t)A(\vec{x}, y)$$

$$T \vdash \forall \vec{x} \forall y \forall z[A(\vec{x}, y) \wedge A(\vec{x}, z) \rightarrow y = z]$$

Then we say that T can Σ_1^{b+}-$define$ the function f such that $\forall \vec{x} A(\vec{x}, f(\vec{x}))$. The *defining axiom* for f is:

$$f(\vec{x}) = y \leftrightarrow A(\vec{x}, y)$$

where f is a new n-ary function symbol. The *defining formula* for f is A and the *boundinig term* for f is t.

Theorem 2.4.3 Let T and f be as in the above definition, and assume that all Σ_1^{b+}-$PIND$ axioms in the language of T are theorems of T. let $T(f)$ be the extension of T obtained by adding f as a new function symbol, together with its defining axioms, and also all Σ_1^{b+}-$PIND$ axioms in the language of $T(f)$. Then $T(f)$ is a conservative extension of T.

(*proof*)

For any formula $A \in L(T)$ if A is proved in $T(f)$ without to apply Σ_1^{b+}-$PIND$ axioms in the language of $T(f)$ then A is obviously proved in T. Therefore we prove that the $\Sigma_1^{b+} - PIND$ scheme for $T(f)$ can be derived from the $\Sigma_1^{b+} - PIND$ scheme for T.

Let A be a Σ_1^{b+} formula in $T(f)$ and containing a term $f(t_1 \cdots t_n)$, where $t_1 \cdots t_n$ are terms of T. Let B be be the defining formula for f and t be the bounded term. Then A is equivalent to $\exists y \leq t(A[y/f(t_1 \cdots t_n)] \wedge B(\vec{t}, y))$, where y is a variable not occurring in A. And $\exists y \leq t(A[y/f(t_1 \cdots t_n)] \wedge B(\vec{t}, y))$ is in Σ_1^{b+} and is not containing f. Hence the $\Sigma_1^{b+} - PIND$ scheme for $T(f)$ can be derived from the $\Sigma_1^{b+} - PIND$ scheme for T. ∎

Definition 2.4.4 Let T be a theory of arithmetic containing a function $|x|$ which is a binary length function (*i.e.* $|x| = \lceil log_2(x+1) \rceil$). Then we say that T contains a set of **efficient coding functions** provided that T contains a one-place predicate **Seq**, a one-place function **Len** , two-place functions $\ast$, β, and **Bound**, for which the following are

theorems of T :

(A) $Seq(0) \wedge Len(0) = 0$;

(B) $Seq(s) \rightarrow Seq(s * u)$;

(C) $Seq(s) \rightarrow Len(s * u) = Len(s) + 1$;

(D) $Seq(s) \rightarrow Len(s) \leq |s|$;

(E) $Seq(s) \rightarrow (i < Len(s) \rightarrow \beta(i, s * u) = \beta(i, s))$;

(F) $Seq(s) \rightarrow \beta(Len(s), s * u) = u$;

(G) $(Seq(s) \wedge Seq(t)) \rightarrow [Len(s) = Len(t) \wedge (\forall i < Len(s))(\beta(i, s) = \beta(i, t)) \rightarrow s = t]$;

(H) $Seq(s) \wedge (Len(s) \leq |b| + 1) \wedge (\forall i < Len(s))(\beta(i, s) \leq a) \rightarrow s \leq Bound(a, b)$.

Definition 2.4.5 Let T be an extension of IS_2^1. We say that T is *sufficiently strong* if it satisfies the conditions :

(1) T contains a 2-place function symbols $Lmin$ for which the theorem

$$Lmin(x, y) = z \leftrightarrow (|x| \leq |y| \wedge z = x) \vee (\neg(|x| \leq |y|) \wedge z = y)$$

is provable in T ;

(2) T contains a set of efficient coding functions;

(3) T contains the Σ_1^{b+}-PIND scheme for all formulas in the language of T ;

(4) T contains a 2-place function symbols $Trunc$ for which the theorem :

$$(i) Trunc(a, |a|) = a$$

$$(ii) i \leq ||\lfloor \tfrac{1}{2} a \rfloor|| \rightarrow Trunc(\lfloor \tfrac{1}{2} a \rfloor, i) = Trunc(a, i)$$

are provable in T.

Lemma 2.4.6 There is an extension IS_2^{1*} of IS_2^1 by Σ_1^{b+} -definitions which is sufficiently strong.

(*proof*) We can Σ_1^{b+}-define under functions and predicates.

(P1) $\mathbf{a < b} \Longleftrightarrow Sa \leq b$

(F1) $\mathbf{b{=}P(a)} \Longleftrightarrow (a = 0 \wedge b = 0) \vee Sb = a$

(F2) $\mathbf{c{=}max(a,b)} \Longleftrightarrow (a \leq b \wedge b = c) \vee (b \leq a \wedge a = c)$

(F3) $\mathbf{c{=}min(a,b)} \Longleftrightarrow (a \leq b \wedge a = c) \vee (b \leq a \wedge b = c)$

(F4) $\mathbf{b{=}Mod2(a)} \Longleftrightarrow b + 2 \cdot \lfloor \frac{1}{2} a \rfloor = a$

(P2) $\mathbf{Decomp(a,b,c,d)} \Longleftrightarrow |c| \leq b \wedge d \cdot 2^{min(|a|,b)} + c = a$

(F5) $\mathbf{c{=}LSP(a,b)} \Longleftrightarrow (\exists d \leq a) Decomp(a,b,c,d)$

(F6) $\mathbf{d{=}MSP(a,b)} \Longleftrightarrow (\exists c \leq a) Decomp(a,b,c,d)$

(F7) $\mathbf{c{=}Bit(b,a)} \Longleftrightarrow c = Mod2(MSP(a,b))$

(P3) $\mathbf{QuoRem(a,b,c,d)} \Longleftrightarrow (b = 0 \wedge c = 0 \wedge d = 0) \vee (d < b \wedge a = c \cdot b + d)$

(F8) $\mathbf{c{=}\lfloor a/b \rfloor} \Longleftrightarrow (\exists d \leq b) QuoRem(a,b,c,d)$

(F9) $\mathbf{d{=}Rem(a,b)} \Longleftrightarrow (\exists c \leq a) QuoRem(a,b,c,d)$

(P4) $\mathbf{b \mid a} \Longleftrightarrow Rem(a,b) = 0 \wedge S0 \leq b$

(P5) $\mathbf{Even(a)} \Longleftrightarrow Mod2(a) = 0$

(P6) $\mathbf{Odd(a)} \Longleftrightarrow Mod2(a) = 1$

(P7) $\mathbf{Comma(b,a)} \Longleftrightarrow Even(b) \wedge Bit(b,a) = 1 \wedge Bit(Sb,a) = 0$

(F10) $\mathbf{c{=}Digit(b,a)} \Longleftrightarrow$
$[Even(b) \wedge Bit(Sb,a) = 1 \wedge Bit(b,a) = c] \vee [(Odd(b) \vee Bit(Sb,a) = 0) \wedge c = 2]$

(P8) $\mathbf{PSqSL(a,b,c)} \Longleftrightarrow |a| + 2 = 2 \cdot c \cdot Sb \wedge$
$(\forall y < |a|)((2b+2) | (y+2) \rightarrow Comma(y,a)) \wedge$
$(\forall y < |a|)(\neg((2b+2) | (y+2)) \rightarrow Digit(y,a) < 2)$

(F11) $\mathbf{b{=}ProtoSize(a)} \Longleftrightarrow$
$2 \cdot b \leq |a| \wedge (2 \cdot b = |a| \vee Comma(2 \cdot b, a)) \wedge (\forall x < b)(\neg Comma(2 \cdot x, a))$

(F12) $\mathbf{b{=}ProtoLen(a)} \Longleftrightarrow c = \lfloor (|a| + 2)/(2 \cdot ProtoSize(a) + 2) \rfloor$

(P9) $\mathbf{ProtoSeq(a)} \Longleftrightarrow PSqSL(a, ProtoSize(a), ProtoLen(a))$

(F13) $\mathbf{c{=}a \dot{-} b} \iff a = b + c \vee (c = 0 \wedge a < b)$

(F14) $\mathbf{c{=}Proto\ \beta\ (b,a)} \Longleftrightarrow (\neg ProtoSeq(a) \wedge c = 0) \vee$
$[ProtoSeq(a) \wedge |c| \leq ProtoSize(a) \wedge$
$(\forall y < ProtoSize(a))(Bit(y, c) = Digit(2 \cdot (y + (ProtoSize(a) + 1) \cdot (b \dot{-} 1)), a))]$

(F15) $\mathbf{c{=}ProtoStar(a,b)} \Longleftrightarrow (\neg ProtoSeq(a) \wedge c = 0) \vee$
$[ProtoSeq(a) \wedge ProtoSeq(c) \wedge ProtoSize(a) = ProtoSize(c) \wedge$
$ProtoLen(c) = ProtoLen(a) + 1 \wedge$
$(\forall x < ProtoLen(a))(Proto\ \beta\ (x + 1, a) = Proto\ \beta\ (x + 1, c)) \wedge$
$Proto\ \beta\ (ProtoLen(a) + 1, c) = LSP(b, ProtoSize(a))]$

(F16) Let $A(z, y, \vec{x})$ be any formula. The function $f(y, \vec{x})$ is *defined by length bounded counting from* A iff f satisfies

$$f(y, \vec{x}) = (\#z \leq |y|)A(z, y, \overrightarrow{x})$$

where $\#z \leq t)(\cdots)$ means "the number of $z \leq t$ such that $\cdots$".

(F17)

(i) $f_1(\overrightarrow{x}) = min\{t(y) : y \leq |s|\}$

(ii) $f_2(\overrightarrow{x}) = max\{t(y) : y \leq |s|\}$

(iii) $f_3(\overrightarrow{x}) = (\mu y \leq |s|)A(y)$

where s and t are terms. The free variables of s are the $\vec{x}$; The free variables of t and A may include y and $\vec{x}$.

By these functions and predicate,

(a) $\mathbf{b{=}Substring(a,i,j)} \Longleftrightarrow b = MSP(LSP(a, j), i)$

(b) $\mathbf{Seq(w)} \Longleftrightarrow (\forall x < |w|)[Even(x) \rightarrow (Comma(x, w) \vee Digit(x, w) \leq 1)] \wedge$
$(Comma(0, w) \vee w = 0)$

(c) $\mathbf{a{=}Len(w)} \Longleftrightarrow (\neg Seq(w) \wedge a = 0) \vee (Seq(w) \wedge a = (\#i < |w|)Comma(i, w))$

(d) $\mathbf{b{=}Decode(a)} \Longleftrightarrow (\neg ProtoSeq(a) \wedge b = 0) \vee (ProtoSeq(a) \wedge b = Proto\beta(1, a))$

(e) $\mathbf{b{=}Encode(a)} \Longleftrightarrow PSqSL(b, |a|, 1) \wedge a = Proto\beta(1, b)$

(f) $\mathbf{a{=}Start\ \beta\ (i,w)} \Longleftrightarrow (\neg Seq(w) \wedge a = 0) \vee$
$(Seq(w) \wedge a = (\mu x \leq |w| + 1)[Len(Substring(w, 0, x)) = i \wedge Even(x)])$

(g) $\mathbf{b=End\ \beta\ (i,w)} \Longleftrightarrow (\neg Seq(w) \wedge b = 0) \vee$
$(Seq(w) \wedge b = (\mu x \leq |w|)[S0 \leq Len(Substring(w, Start\beta(i,w), x+2)) \wedge Even(x)])$

(h) $\mathbf{a=\beta\ (i,w)} \Longleftrightarrow (i = 0 \wedge a = Len(w)) \vee$
$(S0 \leq i \wedge a = Decode(Substring(w, Start\beta(i,w), End\beta(i,w))))$

(i) $\mathbf{c=a * * b} \Longleftrightarrow c = b \cdot 2^{|a|+Mod2(|a|)} + a$

(j) $\mathbf{c=a * b} \Longleftrightarrow a * *(4 \cdot Encode(b) + 1)$

(k) $\mathbf{c=Bound(a,b)} \Longleftrightarrow (2b+1)\#(4 \cdot (2 \cdot a + 1)^2)$ ∎

Lemma 2.4.7 Let T be a sufficiently strong extension of IS_2^1, and $k(a, \vec{b})$ be an n+1-place function symbol of T. Then there is an extension T' of T by a Σ_1^{b+}-definition of a function m so that:

$$T' \vdash k(a, \vec{b}) \leq m(a, \vec{b})$$
$$T' \vdash m(\lfloor \tfrac{1}{2} a \rfloor, \vec{b}) \leq m(a, \vec{b}).$$

(*proof*)In proof we abbreviate $Trunc(a,i)$ as a_i.
It is straightforward to prove in T by $\Sigma_1^{b+} - PIND$ on a that:

$$\forall a(\exists i \leq |a|)(\forall j \leq |a|)[k(a_j, \vec{b}) \leq k(a_i, \vec{b})].$$

$$\forall a(\exists i \leq |a|)[k(a_i, \vec{b}) = c \wedge (\forall j \leq |a|)k(a_j, \vec{b}) \leq c].$$

We prove that We can thus define the function m:
$m(a, \vec{b}) = c \leftrightarrow (\exists i \leq |a|)[k(a_i, \vec{b}) = c \wedge (\forall j \leq |a|)k(a_j, \vec{b}) \leq c]$.
Let $A(a, \vec{b}, c)$ be $(\exists i \leq |a|)[k(a_i, \vec{b}) = c \wedge (\forall j \leq |a|)k(a_j, \vec{b}) \leq c]$. We need to prove
$T \vdash \forall a \forall \vec{b} \exists c \leq tA(a, \vec{b}, c)$,
$T \vdash \forall a \forall \vec{b} \forall c_1 \forall c_2 [A(a, \vec{b}, c_1) \wedge A(a, \vec{b}, c_2) \rightarrow c_1 = c_2]$.

1) $T \vdash \forall a \forall \vec{b} \exists c \leq tA(a, \vec{b}, c)$
By the function k which is Σ_1^{b+}-defined in T,
$T \vdash \exists c(c \leq t \wedge k(a_i, \vec{b}) = c)$.
By $\exists c(c \leq t \wedge k(a_i, \vec{b}) = c)$ and $(\exists i \leq |a|)[k(a_i, \vec{b}) = c \wedge (\forall j \leq |a|)k(a_j, \vec{b}) \leq c]$,
$T \vdash \exists c(c \leq t \wedge (\exists i \leq |a|)[k(a_i, \vec{b}) = c \wedge (\forall j \leq |a|)(k(a_j, \vec{b}) \leq c)])$.
Hence
$T \vdash \forall a \forall \vec{b} \exists c \leq tA(a, \vec{b}, c)$.

2) $T \vdash \forall a \forall \vec{b} \forall c_1 \forall c_2 [A(a, \vec{b}, c_1) \wedge A(a, \vec{b}, c_2) \rightarrow c_1 = c_2]$.
Let $T \vdash A(a, \vec{b}, c_1) \wedge A(a, \vec{b}, c_2)$.
By $A(a, \vec{b}, c_1)$,
$T \vdash \exists u(u \leq |a| \wedge k(a_u, \vec{b}) = c_1 \wedge (S|a| \leq v \vee k(a_v, \vec{b}) \leq c_1))$.

We number subformulas of the upper formula as follow :

$u \leq |a|$ is (1), $k(a_u, \vec{b}) = c_1$ is (2) and $(S|a| \leq v \vee k(a_v, \vec{b}) \leq c_1)$ is (3).

By $A(a, \vec{b}, c_2)$.

$T \vdash \exists v(v \leq |a| \wedge k(a_v, \vec{b}) = c_2 \wedge (S|a| \leq u \vee k(a_u, \vec{b}) \leq c_2))$.

And same as

$v \leq |a|$ is (4), $k(a_v, \vec{b}) = c_2$ is (5) and $S|a| \leq u \vee k(a_u, \vec{b}) \leq c_2$ is (6).

By (3),(4),(5),

$T \vdash c_2 \leq c_1$.

By (1),(2),(6),

$T \vdash c_1 \leq c_2$.

By (B.5),

$T \vdash c_1 = c_2$.

Therefore

$T \vdash A(a, \vec{b}, c_1) \wedge A(a, \vec{b}, c_2) \rightarrow c_1 = c_2$.

∎

Theorem 2.4.8 Let T be a sufficiently strong extension of IS_2^1, and g, h, k be n-place, n+2-place and n+1-place function symbols of T. Then there is an extension T^* of T by Σ_1^{b+}-definitions so that

$T^* \vdash f(0, \vec{b}) = g(\vec{b})$

$T^* \vdash a = 0 \vee f(a, \vec{b}) = Lmin[h(a, \vec{b}, f(\lfloor \frac{1}{2} a \rfloor, \vec{b})), k(a, \vec{b})]$.

(*proof*) First, we extend T by adding a Σ_1^{b+}-definition of a function $m(a, \vec{b})$ for which the theorems

$k(a, \vec{b}) + g(\vec{b}) + 1 \leq m(a, \vec{b})$

$m(\lfloor \frac{1}{2} a \rfloor, \vec{b}) \leq m(a, \vec{b})$

are provable. Lemma 2.4.7 guarantees the existence of such a definition. We abbreviate $Trunc(a, i)$ as a_i. Now let $B(w, a)$ be the following formula:

$\{Seq(w) \wedge Len(w) = |a| + 1 \wedge \beta(0, w) = g(\vec{b})$

$\wedge$

$(\forall i < |a|)[\beta(i+1, w) = Lmin(h(a_{i+1}, \vec{b}, \beta(i, w)), k(a_{i+1}, \vec{b}))]\}$.

The defining axiom for f is:

$$f(a, \vec{b}) = c \leftrightarrow (\exists w \leq Bound(m(a, \vec{b}), a))[B(w, a) \wedge \beta(|a|, w) = c].$$

To justify this definition, we need to prove the existence and uniqueness conditions.

EXISTENCE

Let $D'(a, \vec{b}, c)$ be $(\exists w \leq Bound(m(a, \vec{b}), a))[B(w, a) \wedge \beta(|a|, w) = c]$. We need to prove that

$$T \vdash \forall a \forall \vec{b} \exists c \leq tD'(a, \vec{b}, c).$$

By definition of $Bound$,

$w \leq Bound(m(a,\vec{b}),a) \equiv Seq(w) \wedge Len(w) \leq |a|+1 \wedge (\forall i < Len(w))(\beta(i,w) \leq m(a,\vec{b}))$.

Let $D(a,\vec{b})$ be $\exists w(B(w,a) \wedge (\forall i < Len(w))(\beta(i,w) \leq m(a,\vec{b})))$. Then we prove

$$T \vdash \forall a \forall \vec{b} D(a,\vec{b}) \rightarrow \forall a \forall \vec{b} \exists c \leq tD'(a,\vec{b},c)$$

as follows

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\forall a \forall \vec{b} D(a,\vec{b})}{D(a,\vec{b})}}{(\forall i < Len(w))(\beta(i,w) \leq m(a,\vec{b}))} \quad \dfrac{\forall a \forall \vec{b} D(a,\vec{b})}{D(a,\vec{b})}}{\beta(|a|,w) \leq m(a,\vec{b})} \quad \dfrac{}{\exists w[w \leq Bound(m(a,\vec{b}),a) \wedge B(w,a) \wedge \beta(|a|,w) = \beta(|a|,w)]}}{\beta(|a|,w) \leq m(a,\vec{b}) \wedge \exists w[w \leq Bound(m(a,\vec{b}),a) \wedge B(w,a) \wedge \beta(|a|,w) = \beta(|a|,w)]}}{\exists c(c \leq m(a,\vec{b}) \wedge \exists w[w \leq Bound(m(a,\vec{b}),a) \wedge B(w,a) \wedge \beta(|a|,w) = c])}}{(\exists c \leq m(a,\vec{b}))(\exists w \leq Bound(m(a,\vec{b}),a))[B(w,a) \wedge \beta(|a|,w) = c]}}{\forall a \forall \vec{b} \exists c \leq tD'(a,\vec{b},c).}$$

Therefore we prove $D(a,\vec{b})$ by $\Sigma_1^{b+} - PIND$ on a.

Basis Step: a=0. We wish to prove $B(w,0) \wedge (\forall i < Len(w))(\beta(i,w) \leq m(0,\vec{b}))$. By def. 2.4.4(A), $T \vdash Seq(0) \wedge Len(0) = 0$. Let w be $0 * g(\vec{b})$. By def. 2.4.4(C), $Len(w) = 1$. def. 2.4.4(F), $\beta(0,w) = \beta(Len(0),w) = g(\vec{b})$. By $\beta(0,w) \leq m(0,\vec{b})$, $(\forall i < Len(w))(\beta(i,w) \leq m(0,\vec{b}))$. Therefore $T \vdash D(0,\vec{b})$.

Induction Step: Assume $a > 0$. We prove $D(\lfloor \frac{1}{2}a \rfloor, \vec{b}) \rightarrow D(a,\vec{b})$.

$$D(\lfloor \tfrac{1}{2}a \rfloor, \vec{b}) \equiv \exists w_1[\underbrace{Seq(w_1)}_{\gamma} \wedge \underbrace{Len(w_1) = |\lfloor \tfrac{1}{2}a \rfloor| + 1}_{\delta} \wedge \underbrace{\beta(0,w_1) = g(\vec{b})}_{\theta} \wedge$$
$$\underbrace{(\forall i < |\lfloor \tfrac{1}{2}a \rfloor|)[\beta(i+1,w_1) = Lmin(h(\lfloor \tfrac{1}{2}a \rfloor_{i+1}, \vec{b}, \beta(i,w_1)), k(\lfloor \tfrac{1}{2}a \rfloor_{i+1}, \vec{b}))]}_{\phi} \wedge$$
$$\underbrace{(\forall i < Len(w_1))(\beta(i,w_1) \leq m(\lfloor \tfrac{1}{2}a \rfloor, \vec{b}))]}_{\psi}.$$

$$D(a,\vec{b}) \equiv \exists w_2[\underbrace{Seq(w_2)}_{\Gamma} \wedge \underbrace{Len(w_2) = |a|+1}_{\Delta} \wedge \underbrace{\beta(0,w_2) = g(\vec{b})}_{\Theta} \wedge$$
$$\underbrace{(\forall i < |a|)[\beta(i+1,w_2) = Lmin(h(a_{i+1}, \vec{b}, \beta(i,w_2)), k(a_{i+1}, \vec{b}))]}_{\Phi} \wedge$$
$$\underbrace{(\forall i < Len(w_2))(\beta(i,w_2) \leq m(a,\vec{b}))]}_{\Psi}.$$

Define u as $Lmin\{h(a,\vec{b},\beta(\lfloor \frac{1}{2}a \rfloor, w_1)), k(a,\vec{b})\}$ and let w_2 be $w_1 * u$. We prove that this w_2 satisfies $\Gamma, \Delta, \Theta, \Phi$ and Ψ from $\gamma, \delta, \theta, \phi$ and ψ.

(Γ) By def. 2.4.4(B) and (γ).

(Δ) By def. 2.4.4(C) and (δ), $Len(w_2) = Len(w_1) + 1 = (|\lfloor \frac{1}{2}a \rfloor| + 1) + 1 = |a| + 1$.

(Θ) By def. 2.4.4 (C) and (θ),$\beta(0,w_2) = \beta(0, w_1 * u) = \beta(0,w_1) = g(\vec{b})$.

(Φ) The case $i < ||\lfloor \frac{1}{2}a \rfloor||$.

From def. 2.4.4(E), def. 2.4.5(4) and (ϕ).

The case $i = ||\lfloor \frac{1}{2}a \rfloor||$

$$\begin{aligned}\beta(i+1, w_2) &= \beta(||\lfloor \tfrac{1}{2}a \rfloor|| + 1, w_2) \\ &= \beta(Len(w_1), w_2) \\ &= \beta(Len(w_1), w_1 * u) \\ &= u \\ &= Lmin\{h(a, \vec{b}, \beta(\lfloor \tfrac{1}{2}a \rfloor, w_1)), k(a, \vec{b})\} \\ &= Lmin\{h(a_{|a|}, \vec{b}, \beta(\lfloor \tfrac{1}{2}a \rfloor, w_1)), k(a_{|a|}, \vec{b})\} \\ &= Lmin\{h(a_{i+1}, \vec{b}, \beta(i, w_2)), k(a_{i+1}, \vec{b}))\}\end{aligned}$$

(Φ) The case $i < Len(w_1)$.

From def. 2.4.4(E), $m(\lfloor \frac{1}{2}a \rfloor, \vec{b}) \leq m(a, \vec{b})$ and (ψ).

The case $i = Len(w_1)$

$$\begin{aligned}\beta(i, w_2) &= \beta(Len(w_1, w_1 * u)) \\ &= u \\ &= Lmin\{h(a, \vec{b}, \beta(\lfloor \tfrac{1}{2}a \rfloor, w_1)), k(a, \vec{b})\} \\ &\leq k(a, \vec{b}) \\ &\leq m(a, \vec{b})\end{aligned}$$

UNIQUENESS

Let $D'(a, \vec{b}, c_1)$ be $(\exists w_1 \leq Bound(m(a, \vec{b}), a))[B(w_1, a) \wedge \beta(|a|, w_1) = c_1]$ and $D'(a, \vec{b}, c_2)$ be $(\exists w_2 \leq Bound(m(a, \vec{b}), a))[B(w_2, a) \wedge \beta(|a|, w_2) = c_2]$. We need to prove

$$T \vdash D'(a, \vec{b}, c_1) \wedge D'(a, \vec{b}, c_2) \rightarrow c_1 = c_2.$$

For this, we prove

$$T \vdash D'(a, \vec{b}, c_1) \wedge D'(a, \vec{b}, c_2) \rightarrow w_1 = w_2.$$

Assume that $T \vdash D'(a, \vec{b}, c_1) \wedge D'(a, \vec{b}, c_2)$. Then $T \vdash (Seq(w_1) \wedge Seq(w_2)) \wedge Len(w_1) = Len(w_2)$. If we prove $(\forall i < Len(w_1))(\beta(i, w_1) = \beta(i, w_2))$ then $w_1 = w_2$ by def. 2.4.4(G). Let $C(d)$ be the formula:

$$(\forall i \leq |w_1|)[(i < Len(w_1) \wedge B(w_1, a) \wedge B(w_2, a) \wedge i \leq d) \rightarrow \beta(i, w_1) = \beta(i, w_2)].$$

We prove $C(d)$ by $\Sigma_1^{b+} - LIND$ on the variable d.

base step

For $d = 0$, $\beta(i, w_1) = \beta(i, w_2) = g(\vec{b})$.

induction step

Assume $C(r)$. We prove $C(r) \rightarrow C(r+1)$

$C(r) \equiv \forall i(S|w_1| \leq i \vee [i < Len(w_1) \wedge B(w_1, a) \wedge B(w_2, a) \wedge i \leq r \rightarrow \beta(i, w_1) = \beta(i, w_2)])$,

$C(r+1) \equiv \forall i(S|w_1| \leq i \vee [i < Len(w_1) \wedge B(w_1, a) \wedge B(w_2, a) \wedge i \leq r+1 \rightarrow \beta(i, w_1) = \beta(i, w_2)])$.

The case $r < i$. Obvious.

The case $i \leq r$. By induction hypothesis.

The case $i = r+1$.

$$\begin{aligned}\beta(i, w_1) &= \beta(r+1, w_1) \\ &= Lmin\{h(a_{r+1}, \vec{b}, \beta(a, w_1)), k(a_{r+1}, \vec{b})\} \\ &= \beta(Len(w_1), w_1 * u) \\ &= \beta(r+1, w_2) \\ &= \beta(i, w_2)\end{aligned}$$

Hence $C(r) \rightarrow C(r+1)$

Therefore $\vdash \forall r C(|r|)$. Hence $\vdash C(|w_1|)$. Therefore $\vdash (\forall i < Len(w_1))(\beta(i, w_1) = \beta(i, w_2))$

Hence $w_1 = w_2$. Therefore $c_1 = c_2$. By EXISTENCE and UNIQUENESS, the function f can Σ_1^{b+}-define.

Finally, we prove that this function satisfies two conditions.

The equation

$$f(0, \vec{b}) = g(\vec{b})$$

follows immediately from the definition of $B(w, 0)$. Next, we have:

$$(\exists w_1)[B(w_1, \lfloor \tfrac{1}{2}a \rfloor) \wedge \beta(||\lfloor \tfrac{1}{2}a \rfloor|, w_1) = f(\lfloor \tfrac{1}{2}a \rfloor, \vec{b})]$$

$$(\exists w_2)[B(w_2, a) \wedge \beta(|a|, w_2) = f(a, \vec{b})].$$

Let $u = Lmin\{h(a, \vec{b}, \beta(\lfloor \tfrac{1}{2}a \rfloor, w_1)), k(a, \vec{b})\}$ and $w_3 = w_1 * u$. Then it is easy to prove that $a = 0 \vee B(w_3, a)$ so that $w_3 = w_2$. Thus:

$$\begin{aligned}&\text{Either } a = 0 \quad \text{or} \\ f(a, \vec{b}) &= \beta(|a|, w_2) \\ &= \beta(|a|, w_3) \\ &= Lmin\{h(a, \vec{b}, \beta(||\lfloor \tfrac{1}{2}a \rfloor|, w_1)), k(a, \vec{b})\} \\ &= Lmin\{h(a, \vec{b}, f(a, \vec{b})), k(a, \vec{b})\} \ \blacksquare\end{aligned}$$

Definition 2.4.9 The class of polynomial time computable functions (class **P**) is defined by Cobham as follows.

- Four initial functions are included in the class P.
- The class P is closed under composition (ordinary composition).
- The class P is closed under composition under a special recursion ("Bounded Recursion on Notation").

(1) **Initial functions**

(a) 0 (Constant)

(b) $x \sharp y = 2^{|x| \cdot |y|}$ (Smash function)

(c) $s_0 x = 2 \cdot x,\ s_1 x = 2 \cdot x + 1$ (Successor)

(d) $I_i^n(w_1, \cdots, w_n) = w_i$ (Projection)

(2) **Composition**
Let h, g be in P and f be defined as $f(x) = h(g(x))$. Then f is included in P.

(3) **Bounded Recursion on Notation (BRN)**
Let g, h and k be n-place, n+2-place and n+1-place function symbols, then the function symbol f (defined as follows) is included in P.

$$f(0, \vec{b}) = g(\vec{b})$$
$$f(a, \vec{b}) = h(a, \vec{b}, f(\lfloor \tfrac{1}{2}a \rfloor, \vec{b}))$$
$$f(a, \vec{b}) \leq k(a, \vec{b})$$

Corollary 2.4.10 If $f(\vec{x})$ is a polynomial-time computable function then f is Σ_1^{b+}-definable in IS_2^1.

(*proof*)
For initial function,
(a) and (b) are obvious.
(c) $s_0 x = y \leftrightarrow y = 2 \cdot x$ and $s_1 x = y \leftrightarrow y = 2 \cdot x + 1$.
(d) $I_i^n(\vec{x}) = y \leftrightarrow \beta(i, \vec{x}) = y$.

For composition, let defining formulas and bounding terms of g and h be $A(x, y)$, $B(u, v), s$ and t. Then $g(x) = y \leftrightarrow A(x, y), \forall x \exists y \leq sA(x, y), h(u) = v \leftrightarrow \forall u \exists v \leq tB(u, v)$. Then defining formula of $h(g(x))$ is $A(x, y) \wedge B(y, v) \wedge y \leq s$ and bounding term of $h(g(x))$ is $t[y/u]$.

For B.R.N., theorem 2.4.8. ∎

Chapter 3

The System PV

In 1975 Cook [3] introduced an equation system PV ("polynomially verifiable") of number theory. The motivation for this work comes from two general sources.

The first motivation the basic open open question in complexity theory of whether $P = NP$. His approach is to try to show they are not equal, by trying to show that the set of tautologies is not in NP (of course its complement is in NP). This is equivalent to showing that no proof system for the tautologies is "super" i the sense that there is a short proof for every tautology. Extended resolution is an example of a powerful proof system for tautologies that can simulate most standard proof system.

The second motivation comes from constructive mathematics. A constructive proof of A for each value of x, but nothing is said about how long this proof is as a function of x. If the function is exponential or super exponential, then for short values of x the length of the proof of the instance of A may exceed the number of electrons in the universe. Thus one can question the sense in which our original "constructive" provides a method of verifying $\forall x A$ for such values of x.

Cook patterned after Skolem's equational theory of primitive recursive arithmetic. Whereas Skolem's system has a function symbol for each primitive recursive function, PV has one for each polynomial time computable function. The system PV was supposed to capture an intuitive notion of "feasibly constructive proof", a form of highly constructive proof is to polynomial time algorithm.

The System PV is a logic-free equational calculus. The idea is that a proof in PV of an equation $t = u$ provides a template for verifying each instance of the equation in time polynomial in the length of the instance.

3.1 Definition of system PV

Definition 3.1.1 The *function symbols* and *terms* of PV are defined as follows:

(1) There are infinitely many numerical variables, and each such variable is a term.

(2) The constant 0 is a term.

(3) If f is an n-place function symbol and $t_1 \cdots t_n$ are terms, then $(\cdots(ft_1)\cdots t_n)$ is a term.

(4) $s_0, s_1, Parity, \lfloor \frac{1}{2} \rfloor$ are 1-place function symbols.

(5) $\dot{-}, \boxplus, \sharp$ are 2-place function symbols.

(6) $Cond$ is a 3-place function symbol.

(7) If t is a term and $x_1 \cdots x_n (n \geq 0)$ is a list of variables including all variables in t, then $[\lambda x_1 \cdots x_n.t]$ is an n-place function symbol.

(8) If g, h and k are n-place, n+2-place and n+1-place function symbols respectively, then $R[g, h, k]$ is an n+1-place function symbol.

The term notation $(\cdots(ft_1)\cdots t_n)$ in (3) is designed to fit the system PV^ω of Chapter 6. We shall depart from the formal definition above by employing the informal conventions of writing $ft_1 \cdots t_n$ or $f(t_1 \cdots t_n)$ instead of $(\cdots(ft_1)\cdots t_n)$, by employing infix notation $[x \dot{-} y$ for $((\dot{-}x)y)]$ and writing $\lfloor \frac{1}{2} x \rfloor$ for $(\lfloor \frac{1}{2} \rfloor x)$.

The axioms of PV give either explicit or recursive defining equations for each function symbol of PV except s_0 and s_1, which are considered primitive.

Definition 3.1.2 The *axioms* of PV are defined as follows:

(0) $s_0(0) = 0$

(1a) $Parity(s_0 x) = 0$

(1b) $Parity(s_1 x) = 1$

(2a) $\lfloor \frac{1}{2} s_0 x \rfloor = x$

(2b) $\lfloor \frac{1}{2} s_1 x \rfloor = x$

(3a) $Cond(0, y, z) = y$

(3b) $Cond(s_0 x, y, z) = Cond(x, y, z)$

(3c) $Cond(s_1 x, y, z) = z$

(4a) $x \boxplus s_0 y = Cond(y, x, s_0(x \boxplus y))$

(4b) $x \boxplus s_1 y = s_0(x \boxplus y)$

(5a) $x \dot{-} s_0 y = Cond(y, x, \lfloor \frac{1}{2}(x \dot{-} y) \rfloor)$

(5b) $x \dot{-} s_1 y = \lfloor \frac{1}{2}(x \dot{-} y) \rfloor$

(6a) $x \sharp s_0 y = Cond(y, 1, (x \sharp y) \boxplus x)$

(6b) $x \sharp s_1 y = (x \sharp y) \boxplus x$

(7) $[\lambda x_1 \cdots x_n . t](x_1, \cdots, x_n) = t$

(8) $R[g,h,k](x, \vec{y}) = Cond(x, g(\vec{y}), Cond(t \dot{-} k(x, \vec{y}), t, k(x, \vec{y}))), where$
$t \stackrel{d}{\equiv} h(x, \vec{y}, R[g,h,k](\lfloor \frac{1}{2} x \rfloor, \vec{y}))$

From these axioms, the intended interpretation of the function symbols $s_0, s_1, Parity, \lfloor \frac{1}{2} x \rfloor, \boxplus, \dot{-}, \sharp, Cond, R[g,h,k]$ is as follows:
Let $x \equiv (\alpha_n \cdots \alpha_0)_2$. Then
$s_0 x = (\alpha_n \cdots \alpha_0 0)_2 = 2x$,
$s_1 x = (\alpha_n \cdots \alpha_0 1)_2 = 2x + 1$,
$Parity(x) = \alpha_0$,
$\lfloor \frac{1}{2} a \rfloor = (\alpha_n \cdots \alpha_1)_2$,
$x \dot{-} y = (\alpha_n \cdots \alpha_{|y|})_2$,
$x \sharp y = 2^{|x| \cdot |y|}$,
$Cond(x, y, z) =$ (if $x = 0$ then y else z).
$R[g,h,k]$ is Bounded Recursion on Notation.

Definition 3.1.3 The *axioms* of PV are defined as follows:

R1. $t = u \vdash u = v$

R2. $t = u, u = v \vdash t = v$

R3. $t_1 = u_1, \cdots, t_n = u_n \vdash f t_1 \cdots t_n = f u_1 \cdots u_n$

R4. $t = u \vdash t[v/x] = u[v/x]$, x a variable, v any term

R5.
$$\frac{\begin{array}{c} t_1[0/x] = t_2[0/x] \\ t_1[s_0 x/x] = v_0[t_1/a] \quad t_2[s_0 x/x] = v_0[t_2/a] \\ t_1[s_1 x/x] = v_1[t_1/a] \quad t_2[s_1 x/x] = v_1[t_2/a] \end{array}}{t_1 = t_2}$$
for any terms t_1, t_2, v_0, v_1 and any variable a.

The R5 is a form of induction on binary notation. The rule may be understood as follows: if the term t_1 and t_2 satisfy the premisses of R5 for all x, then the functions defines by the two terms satisfy the same recursion equations, and hence are the same function.

3.2 Development of PV

In the formal development of PV, the abbreviations "T", "DR", "D" are used for theorems, derived rules and definitions. Most of the theorems proved below are derived using induction on notation (R5). In such a case, the proof usually breaks down into three steps, corresponding to the base of the induction, and the two induction step for the successor functions s_0 and s_1. In proving Theorem m we shall denote these three steps by $(m.\emptyset), (m.0), (m.1)$ respectively; the two equations constituting step $(m.0)$, for example, will be denoted by $(m.0a)$ and $(m.0b)$. In a case where the two steps $(m.0)$ and $(m.1)$ can be treated simultaneously, this will be written as $(m.i)$. In a statement of a derived rules, the notation "$t_1 = u_1, \cdots, t_n = u_n \vdash v = w$" should be read as an abbreviation for "If $\vdash t_1 = u_1, \cdots, \vdash t_n = u_n$ then $\vdash v = w$".

The formal development of PV is very similar to that of primitive recursive arithmetic, but is complicated by the fact that function symbols introduced by definition contain a built-in bounding term. To make use of such a symbol in the later development, it is usually necessary to show that the bound can be eliminated, so that the recursion equations hold unconditionally. If $f(x, \vec{y})$ is a function symbol introduced by definition as $R[g, h, k](x, \vec{y})$, the temporary abbreviation "$(t(f)$" will be used for the term "$h(x, \vec{y}, R[g, h, k](\lfloor \frac{1}{2}x \rfloor, \vec{y}))$" defined in Axiom 8.

We omit proof of theorems and derived rules. But we prove T4 as an example of proof.
$(proof)$

Let $t_1 \equiv Cond(x, Cond(x, c, d), Cond(x, e, f))$, $t_2 \equiv Cond(x, c, f)$. Then we define v_0 and v_1 as $v_0 \stackrel{d}{\equiv} a$ and $v_1 \stackrel{d}{\equiv} f$.

(4.$\emptyset$:) $t_1[0/x] = Cond(0, Cond(0, c, d), Cond(0, e, f)) = Cond(0, c, d) = t_2[0/x]$.

(4.0a :) $t_1[s_0x/x] = Cond(s_0x, Cond(s_0x, c, d), Cond(s_0x, e, f))$
$= Cond(x, Cond(x, c, d), Cond(x, e, f)) = t_1$
$v_0[t_1/a] = a[t_1/a] = t_1$
Therefore $t_1[s_0x/x] = v_0[t_1/a]$

(4.0b :) $t_2[s_0x/x] = Cond(s_0x, c, f) = Cond(x, c, f) = t_2$
$v_0[t_2/a] = a[t_2/a] = t_2$
Therefore $t_2[s_0x/x] = v_0[t_2/a]$

(4.1a :) $t_1[s_1x/x] = Cond(s_1x, Cond(s_1x, c, d), Cond(s_1x, e, f)) = Cond(s_1x, e, f) = f$
$v_1[t_1/a] = f[t_1/a] = f$
Therefore $t_1[s_1x/x] = v_1[t_1/a]$

(4.0b :) $t_2[s_1x/x] = Cond(s_1x, c, f) = f$
$v_1[t_1/a] = f[t_1/a] = f$
Therefore $t_2[s_1x/x] = v_1[t_2/a]$ ∎

T1: $Cond(x, y, y) = y$.

T2: $Cond(x, fy_1 \cdots y_n, fz_1 \cdots z_n) = fCond(x, y_1, z_1) \cdots Cond(x, y_n, z_n)$, f any n-place function symbol of PV.

T3: $Cond(x, fb\vec{y}, fb\vec{z}) = fbCond(x, y_1, z_1) \cdots Cond(x, y_n, z_n)$, f any (n+1)-place function symbol, a any variable distinct from x.

T4: $Cond(x, Cond(x, c, d), Cond(x, e, f)) = Cond(x, c, f)$.

T5: $Cond(x, 0, x) = x$.

T6: $Cond(x, u[0/x], u) = u$, where u is any term of PV.

T7: $Cond(x, u, y) = Cond(x, u[0/x], y)$.

T8: $Cond(x, y, u) = Cond(x, y, u[Cond(x, z, a)/a])$, for u any term of PV.

D9: "$v \neq 0 \supset t = u$" abbreviates "$Cond(v, u, t) = u$", for any terms v, t, u.

DR10: $t = u \vdash v \neq 0 \supset t = u$.

T11: $x \neq 0 \supset Cond(x, t, u) = u$.

DR12: $v \neq 0 \supset t = u \vdash v \neq 0 \supset u = t$.

DR13: $w \neq 0 \supset t = u, w \neq 0 \supset u = v \vdash w \neq 0 \supset t = v$.

DR14: $v \neq 0 \supset t_i = u_i, i = 1 \cdots n \vdash v \neq 0 \supset ft_1 \cdots t_n = fu_1 \cdots u_n$.

DR15(Conditional proof principle):
$t[0/x] = u[0/x], v \neq 0 \supset t' = u' \vdash t' = u'$, where $t' \equiv t[v/x]$ and $u' \equiv u[v/x]$.

DR16: $t[0/x] = u[0/x], x \neq 0 \supset t = u \vdash t = u$.

DR17(Conditional Induction):

$$\frac{\begin{array}{c} t_1[0/x] = t_2[0/x] \\ x \neq 0 \supset t_1[s_0x/x] = w_0[t_1/a] \qquad x \neq 0 \supset t_2[s_0x/x] = w_0[t_2/a] \\ t_1[s_1x/x] = w_1[t_1/a] \qquad t_2[s_1x/x] = w_1[t_2/a] \end{array}}{t_1 = t_2.}$$

T18: $0 \dot{-} x = 0$.

T19: $\lfloor \frac{1}{2}(s_i x \dot{-} y) \rfloor = x \dot{-} y, i = 0, 1$.

T20: For $i = 0, 1$,
$y \neq 0 \supset s_i x \dot{-} s_0 y = x \dot{-} y$
$s_i x \dot{-} s_1 y = x \dot{-} y$.

T21: $\lfloor \frac{1}{2}(x \dot{-} y) \rfloor = \lfloor \frac{1}{2} x \rfloor \dot{-} y$.

T22: $x \dot{-} x = 0$.

T23: $R[g, h, k](x, \vec{y}) \dot{-} k(x, \vec{y}) = Cond(x, g(\vec{y}) \dot{-} k(0, \vec{y}), 0)$.

D24(The successor function):
$$Sx = Cond(x, 1, Cond(t(S) \dot{-} s_1 x, t(S), s_1 x)),$$
where $t(S) \equiv Cond(Parity(x), s_1 \lfloor \frac{1}{2} x \rfloor, s_0 S \lfloor \frac{1}{2} x \rfloor)$.

T25: $Sx \dot{-} s_1 x = 0$.

T26: $Sx = Cond(Parity(x), s_1 \lfloor \frac{1}{2} x \rfloor, s_0 S \lfloor \frac{1}{2} x \rfloor)$.

T27: $x \dot{-} 1 = \lfloor \frac{1}{2} x \rfloor$.

The abbreviation "$x0$" for "$s_0 x$" and "$x1$"for"$s_1 x$" are employed below.

DR28: $t[x0/x] = u[x0/x], t[x1/x] = u[x1/x] \vdash t = u$.

T29: $x = Cond(Parity(x), \lfloor \frac{1}{2} x \rfloor 0, \lfloor \frac{1}{2} x \rfloor 1)$.

T30: $Parity(Parity(x)) = Parity(x)$.

D31: $sg(x) \stackrel{d}{\equiv} Cond(x, 0, 1)$.

D32: $\overline{sg}(x) \stackrel{d}{\equiv} Cond(x, 1, 0)$.

We shall write "$\sim x$" for "$\overline{sg}(x)$" .

D33: $(x \& y) \stackrel{d}{\equiv} Cond(x, sg(y), 1)$.

D34: $(x \vee y) \stackrel{d}{\equiv} Cond(x, 0, sg(y))$.

D35: $(x \supset y) \stackrel{d}{\equiv} Cond(x, sg(y), 0)$.

D36: $(x \Leftrightarrow y) \stackrel{d}{\equiv} Cond(x, sg(y), \overline{sg}(y))$.

Note that we are employing the convention: 0 = true, 1 = false.

We define the class of *Propositional terms* as follows:

(a) $0, 1, x, y, z, \cdots$ are propositional term;

(b) if P, Q are propositional term, so are $sg(P), \sim P, (P\&Q)$, $(P \wedge Q), (P \supset Q)$ and $(P \Leftrightarrow Q)$.

T37: $Cond(sg(x), y, z) = Cond(x, y, z)$.

T38: $Cond(\sim x, y, z) = Cond(x, z, y)$.

T39: $sg(sg(x)) = sg(x)$.

T40: $sg(Parity(x)) = Parity(x)$.

T41: If P is a propositional term which is not a variable then $P[sg(x)/x] = P$.

T42: $Cond(x, y, t[sg(x)/x]) = Cond(x, y, t[1/x])$.

T43: If P and Q are equivalent propositional terms and neither is a variable, then $P = Q$.

T44: If P is a propositional term which is not a variable then $sg(P) = P$.

T45: If P is a propositional term which is not a variable then $P \dot{-} 1 = 0$.

DR46: Let P and Q be arbitrary terms. $(P \supset Q) = 0, P = 0 \vdash Q = 0$.

D47: "$t \neq 0$" abbreviates "$\overline{sg}(t) = 0$".

D48: "$P \supset t = u$" abbreviates "$Cond(P, t, u) = u$".

DR49: $P \supset t = u, P = 0 \vdash t = u$.

DR50: $P \supset t = u, Q \supset t = u \vdash P \vee Q \supset t = u$.

DR51: $sg(t) = 0 \vdash t = 0$.

DR52: For any function symbol f,
$f(0, \vec{y}) = 0, [f(x, \vec{y}) \supset f(xi, \vec{y})] = 0, i = 0, 1 \vdash f(x, \vec{y}) = 0$.

D53: For m fixed, $I(m)$ is the term $s_1 \cdots s_1 0$ with value $2^m - 1$. $I(m)$ serves as a standard numeral of (binary) length m.

D54: $Equl(x,m) \stackrel{d}{\equiv} [(x \dot{-} I(m)) \& (I(m) \dot{-} x)]$. $Equl(x,m) = 0$ if and only if $|x|$ (the length of x in binary notation) is m.
T55: $I(m) \dot{-} x \neq 0 \supset xi \dot{-} I(m) = 0$.

D56: $$L_m(x) \stackrel{d}{\equiv} \begin{cases} If\ \ x = 0\ \ then\ \ 0 \\ else\ \ if\ \ t(L_m) \dot{-} I(m-1) = 0\ \ then\ \ t(L_m) \\ else\ \ I(m-1), \end{cases}$$
$$t(L_m) \equiv Cond(I(m-1) \dot{-} L_m(\lfloor \tfrac{1}{2}(x) \rfloor), 0, L_m(\lfloor \tfrac{1}{2}(x) \rfloor)1)$$

T57: $t(L_m) \dot{-} I(m-1) = 0$.

T58: $x \neq 0 \supset (Equl(x,k) \supset Equl(xi, k+1)) = 0$.

T59: $[Equl(L_m(x),0) \vee \cdots \vee Equl(L_m(x), m-1)] = 0$.

T60: $[Equl(L_m(x),m) \supset\sim Equl(L_m(x),n)] = 0, m \neq n$.

DR61(Bounded multi-digit recursion): For $m > 0$ and g, h, k n-place, n+2-place, n+1-place functions, there is an n+1-place function $R_m[g,h,k]$ so that:
$$R_m[g,h,k](x,\vec{y}) = \begin{cases} If\ \ x = 0\ \ then\ \ g(\vec{y}) \\ else\ \ if\ \ t(R_m) \dot{-} k(x,\vec{y}) = 0\ \ then\ \ t(R_m) \\ else\ \ k(x,\vec{y}), \end{cases}$$
where $t(R_m) \equiv h(x, \vec{y}, R_m[g,h,k](x \dot{-} I(m), \vec{y}))$.

DR62: Let $R_m[g,h,k]$ be defined as in DR61. If $h(x,\vec{y}, R_m[g,h,k](x \dot{-} I(m), \vec{y}) \dot{-} k(x,\vec{y})) = 0$ and $h(0,\vec{y}, g(\vec{y})) = g(\vec{y})$ then $R_m[g,h,k](x,\vec{y}) = R_m[g,h,k](x \dot{-} I(m), \vec{y})$.

D63: $Bit_m(x) \stackrel{d}{\equiv} Parity(x \dot{-} I(m))$. $Bit_m(x)$ is the coefficient of 2^m in x's binary representation.

D64: $Tail(x,s) \stackrel{d}{\equiv} sg^{d_0}(Bit_0(x)) \& sg^{d_1}(Bit_1(x)) \& \cdots \& sg^{d_{m-1}}(Bit_{m-1}(x))$, for fixed $s = d_{m-1}d_{m-2}\cdots d_0 \in \{1,0\}^m$, where $sg^0 \stackrel{d}{\equiv} sg$ and $sg^1 \stackrel{d}{\equiv} \overline{sg}$. $Tail(x,s) = 0$ iff the last m bits of x's binary notation (padded with leading 0's if necessary) comprise s.

T65: Let $s_1, \cdots, s_{2^m}$ be the number of $\{0,1\}^m$. Then $[Tail(x,s_1) \vee Tail(x,s_2) \vee \cdots Tail(x,s_{2^m})] = 0$.

T66: $Tail(x,s) \supset (x \dot{-} I(m))s = x$, for each $s \in \{0,1\}^m$

DR67(Proof by m-digit induction): For $m > 0$,if

$$t[0/x] = u[0/x]$$

and

$$\left.\begin{array}{l} t[xs/x] = v_s[t/a] \\ u[xs/x] = v_s[u/a] \end{array}\right\} all \;\; s \in \{0,1\}^m$$

then

$$t = u.$$

D68: $x \otimes y \stackrel{d}{\equiv} Cond(y, s_0(x), s_1(x))$.

D69(Concatenation):

$$x * y = \left\{\begin{array}{l} If \;\; y = 0 \;\; then \;\; x \\ else \;\; if \;\; t(*) \dot{-} (x1 \boxplus y) = 0 \;\; then \;\; t(*) \\ else \;\; (x1 \boxplus y), \end{array}\right.$$

where $t(*) = (x * \lfloor \frac{1}{2} y \rfloor) \otimes Parity(y)$.

T70: $y \neq 0 \supset x * y = (x * \lfloor \frac{1}{2} y \rfloor) \otimes Parity(y)$.

D71: $2^{|x|+|y|} = 1 \boxplus x \boxplus y$.

T72: $x \boxplus y1 \boxplus z = x \boxplus y \boxplus z1$.

T73: $x \boxplus y \boxplus z = x \boxplus z \boxplus y$.

T74: $2^{|x|+|y|} = 2^{|y|+|x|}$.

T75: $x \neq 0 \supset x \boxplus y \neq 0$.

T76: $2^{|x|+|y|} \neq 0$.

T77: $(x \otimes y) \dot{-} 1 = x$.

T78: $Bit_l(x \otimes y_k \otimes y_{k-1} \otimes \cdots \otimes y_0) = Parity(y_l), l \leq k$.

T79: $Bit_m((x \dot{-} 1) \otimes i) = Bit_m(x), m > 0, i = 0, 1$.

D80: For $k > 0$, we use DR61 to define

$$Puff_k(x) \stackrel{d}{\equiv} \left\{\begin{array}{l} If \;\; x = 0 \;\; then \;\; 0 \\ else \;\; if \;\; t(Puff_k) \dot{-} 2^{|x|+|y|} = 0 \;\; then \;\; t(Puff_k) \\ else \;\; 2^{|x|+|y|}, \end{array}\right.$$

$$t(Puff_k) \equiv Puff_k(x \dot{-} I(k)) \otimes Bit_{k-1}(x) \otimes \cdots \otimes Bit_0(x) \otimes 0.$$

T81: $Puff_k(x) = Puff_k(x \dot{-} I(k)) \otimes Bit_{k-1}(x) \otimes \cdots \otimes Bit_0(x) \otimes 0$.

D82: For $k > 1$,

$$Shift_k(x) \stackrel{d}{\equiv} \begin{cases} If\ \ x = 0\ \ then\ \ 0 \\ else\ \ if\ \ t(Shift_k) \dot{-} (x * I(k)) = 0\ \ then\ \ t(Shift_k) \\ else\ \ x * I(k), \end{cases}$$

where $t(Shift_k) \equiv \lfloor \frac{1}{2} Shift_k(x \dot{-} I(k)) \rfloor \otimes Bit_0(x) \otimes Bit_{k-1}(x) \otimes \cdots \otimes Bit_1(x) \otimes 0$.

T83: $Shift_k(x) \dot{-} xs = 0$.

T84: $Shift_k(x) = \lfloor \frac{1}{2} Shift_k(x \dot{-} I(k)) \rfloor \otimes Bit_0(x) \otimes Bit_{k-1}(x) \otimes \cdots \otimes Bit_1(x) \otimes 0$.

D85: For $k > 0$, $2^{k|x|} = 1 \boxplus x \boxplus \cdots \boxplus x (pad\ \ on\ \ k\ \ x's)$.

T86: $(x \dot{-} (y \dot{-} 1)) \dot{-} 1 = Cond(y, x \dot{-} 1, x \dot{-} y)$.

DR87: $t \dot{-} u = 0 \vdash (t \dot{-} x) \dot{-} (u \dot{-} x) = 0$.

T88: $y \neq 0 \supset ((x \dot{-} 1) \otimes i \dot{-} y) = x \dot{-} y, i = 0, 1$.

T89: $y \neq 0 \supset (Shift_k(x) \dot{-} y 0^k) \dot{-} (x \dot{-} y) = 0$.

D90: For $k > 1$,

$$Interleave_k(x, y) \stackrel{d}{\equiv} \begin{cases} If\ \ y = 0\ \ then\ \ Puff_{k-1}(x) \\ else\ \ if\ \ t(Interleave_k) \dot{-} Puff_{k-1}(x) * 2^{k|y|} = 0 \\ \qquad then\ \ t(Interleave_k) \\ else\ \ Puff_{k-1}(x) * 2^{k|y|}, \end{cases}$$

where $t(Interleave_k) \equiv [Shift_k(Interleave_k(x, \lfloor \frac{1}{2} y \rfloor)) \dot{-} 1] \otimes Parity(y)$.

T91: $y \neq 0 \supset t(Interleave_k) \dot{-} Puff_{k-1}(x) * 2^{k|y|} = 0$.

T92: For $k > 0$, $Shift_{k+1}(Puff_k(x)) = Puff_k(x)$.

T93: For $k > 1$, $Interleave_k(x, y) = [Shift_k(Interleave_k(x, \lfloor \frac{1}{2} y \rfloor)) \dot{-} 1] \otimes Parity(y)$.

T94: For $i, j \in \{1, 0\}, k > 1$,
$[Interleave_k(x, yi) \dot{-} 1] = Interleave_k(x, yj)$.

T95: $Bit_l(Shift_k(x)) = Bit_l(x), 0 < l < k$.

T96: $Bit_0(Interleave_k(x, y)) = Bit_0(y)$.

T97: $Shift_k(Interleave_k(xs, y)) = Interleave_k(x, y)s0, s \in \{0, 1\}^{k-1}, k > 1$.

T98: $Interleave_k(xi_1 \cdots i_{k-1}, yi_k) = Interleave_k(x, y)i_1 \cdots i_{k-1}$.

D99: $< x > \stackrel{d}{\equiv} x.$
$< x_1, \cdots, x_k > \stackrel{d}{\equiv} Interleave_k(< x_1, \cdots, x_{k-1} >, x_k), k > 1.$

T100: $< 0, \cdots, 0 >= 0.$

T101: $< x_1 i_1, \cdots, x_k i_k >=< x_1, \cdots, x_k > i_1 \cdots i_k.$

T102: For $k > 1$:

$$\Pi_L^m(x) \stackrel{d}{\equiv} \begin{cases} If\ \ x = 0\ \ then\ \ 0 \\ else\ \ if\ \ t(\Pi_L^m) \dot{-} x = 0\ \ then\ \ t(\Pi_L^m) \\ else\ \ x, \end{cases}$$

where $t(\Pi_L^m) \equiv \Pi_L^m(x \dot{-} I(m)) \otimes Bit_{m-1}(x) \otimes \cdots \otimes Bit_1(x).$

$$\Pi_R^m(x) \stackrel{d}{\equiv} \begin{cases} If\ \ x = 0\ \ then\ \ 0 \\ else\ \ if\ \ t(\Pi_R^m) \dot{-} x = 0\ \ then\ \ t(\Pi_R^m) \\ else\ \ x, \end{cases}$$

where $t(\Pi_R^m) \equiv \Pi_R^m(x \dot{-} I(m)) \otimes Bit_0(x).$

T103: $\Pi_L^m(x) = \Pi_L^m(x \dot{-} I(m)) \otimes Bit_{m-1}(x) \otimes \cdots \otimes Bit_1(x).$

T104: $\Pi_R^m(x) = \Pi_R^m(x \dot{-} I(m)) \otimes Bit_0(x).$

T105: $\Pi_L^m((x \dot{-} 1) \otimes i) = \Pi_L^m(x).$

T106: $\Pi_R^m((x \dot{-} 1) \otimes i) = (\Pi_R^m(x) \dot{-} 1) \otimes i.$

T107: $\Pi_L^m(Shift_m(x)) = \Pi_L^m(x).$

T108: $\Pi_R^m(Shift_m(x)) = \Pi_R^m(x) \otimes 0.$

T109: $\Pi_L^m(x \dot{-} I(m)) = \Pi_L^m(x) \dot{-} I(m-1).$

T110: $\Pi_R^m(x \dot{-} I(m)) = \Pi_R^m(x) \dot{-} 1.$

T111: $\Pi_L^m(Puff_{m-1}(x)) = x.$

T112: $\Pi_R^m(Puff_{m-1}(x)) = 0.$

T113: $\Pi_L^m[Interleave_m(x, y)] = x.$

T114: $\Pi_R^m[Interleave_m(x, y)] = y.$

D115: $\Pi_1^1(x) \stackrel{d}{\equiv} x$,
$\Pi_k^m(x) = \Pi_k^{m-1}(\Pi_L^m(x))$ for $0 < k < m$,
$\Pi_m^m(x) = \Pi_R^m(x)$.

T116: $\Pi_k^m(< x_1, \cdots, x_m >) = x_k, 1 \leq klem.$

T117: For $s \in \{0,1\}^n$ and $1 \leq k \leq n$,
$\Pi_k^n(xs) = \Pi_k^n(x)s_k$.

DR118(Multi-variable induction: From

$$\left.\begin{array}{l} t[0/x_1 \cdots 0/x_n] = u[0/x_1 \cdots 0/x_n] \\ t[x_1 s_1/x_1 \cdots x_n s_n/x_n] = v_s[t/a] \\ u[x_1 s_1/x_1 \cdots x_n s_n/x_n] = v_s[u/a] \end{array}\right\} \forall s \in \{0,1\}^n, s = s_1 \cdots s_n$$

infer $t = u$.

T119: $< x_1, \cdots, x_n > \dot{-} I(n) =< \lfloor \frac{1}{2} x_1 \rfloor \cdots \lfloor \frac{1}{2} x_n \rfloor >$.

DR120(Bounded multi-variable recursion):

$$R^m[g,h,k](\vec{x},\vec{y}) \stackrel{d}{\equiv} \left\{\begin{array}{l} If \;\; < x_1, \cdots, x_n >= 0 \;\; then \;\; g(\vec{y}) \\ else \;\; if \;\; t \dot{-} k(\vec{x},\vec{y}) = 0 \;\; then \;\; t \\ else \;\; k(\vec{x},\vec{y}), \end{array}\right.$$
where $t \equiv h(\vec{x},\vec{y},R^m[g,h,k](\lfloor \frac{1}{2} x_1 \rfloor \cdots \lfloor \frac{1}{2} x_n \rfloor, \vec{y}))$.

D121(Equality):

$$Equ(x,y) \stackrel{d}{\equiv} \left\{\begin{array}{l} If \;\; < x,y >= 0 \;\; then \;\; 0 \\ else \;\; if \;\; t(Equ) \dot{-} 1 = 0 \;\; then \;\; t(Equ) \\ else \;\; 1, \end{array}\right.$$
where $t(Equ) \equiv [Equ(\lfloor \frac{1}{2} x \rfloor, \lfloor \frac{1}{2} y \rfloor) \& (Parity(x) \Leftrightarrow Parity(y))]$.

T122: $Equ(x,x) = 0$.

T123: $Equ(x,y) = Equ(y,x)$.

T124: $[(Equ(x,y) \& Equ(y,z)) \supset Equ(x,z)] = 0$.

T125: $Equ(x,y) \supset x = y$.

DR126: $Equ(t,u) = 0 \vdash t = u$.

DR127: $t = u \vdash Equ(t,u) = 0$.

T128: $[Equ(x,y) \supset Equ(f(x,\vec{z}),f(y,\vec{z}))] = 0.$

DR129: From $P[0/x_1 \cdots 0/x_n] = 0$ and $[P \supset P[x_1 s_1/x_1 \cdots x_n s_n/x_n]] = 0$,
$\forall s \in \{0,1\}^n P = 0$

D130: $x \sqsubseteq y \stackrel{d}{\equiv} Equ(x \dot{-} y, 0)$. This is the characteristic function of the relation $|x| \leq |y|$.

T131: $[((x \sqsubseteq y)\&(y \sqsubseteq z)) \supset (xsqsubseteqz)] = 0.$

T132: $x \neq y \supset (S(x \dot{-} 1) \dot{-} x) = 0.$

D133:

$$|x| \stackrel{d}{\equiv} \begin{cases} If\ \ x = 0\ \ then\ \ 0 \\ else\ \ if\ \ S(|\lfloor \frac{1}{2} x \rfloor|) \dot{-} x = 0\ \ then\ \ S(|\lfloor \frac{1}{2} x \rfloor|) \\ else\ \ x. \end{cases}$$

T134: $x \neq 0 \supset S(|\lfloor \frac{1}{2} x \rfloor|) \dot{-} x = 0.$

T135: $|x| = Cond(x, 0, S(|\lfloor \frac{1}{2} x \rfloor|)).$

D136:

$$Less(x,y) \stackrel{d}{\equiv} \begin{cases} If\ \ x = y = 0\ \ then\ \ 1 \\ else\ \ Cond(t(Less) \dot{-} 1, t(Less), 1) \end{cases}$$

where $t(Less) \equiv [Equ(\lfloor \frac{1}{2} x \rfloor, \lfloor \frac{1}{2} y \rfloor) \& \sim (Parity(x) \supset Parity(y)) \vee Less(\lfloor \frac{1}{2} x \rfloor, \lfloor \frac{1}{2} y \rfloor)]$

D137: $Lesseq(x,y) \stackrel{d}{\equiv} [Less(x,y) \vee Equ(x,y)].$

T138: $[Less(x,y) \& Less(y,z) \supset Less(x,z)] = 0.$

T139: $[Lessequ(x,y) \& Lessequ(y,z) \supset Lessequ(x,z)] = 0.$

T140: $Less(x,x) = 1.$

T141: $[Lessequ(x,y) \& Lessequ(y,x) \supset Equ(x,y)] = 0.$

T142: $[Lessequ(x,y) \vee Lessequ(y,x)] = 0.$

T143: $x \neq 0 \supset Less(0,x) = 0.$

T144: $Lessequ(0,x) = 0.$

T145: $Lessequ(Sx,y) = Less(x,y).$

T146: $Less(x,Sy) = Lessequ(x,y).$

T147: $[Lessequ(x,y) \supset Equ(x,y) \vee Lessequ(Sx,y)] = 0.$

T148: $Equ(x,Sx) = 1.$

T149: $Less(Sx,Sy) = Less(x,y).$

T150: $Lessequ(x,0) = Equ(x,0).$

T151: $[Lessequ(x,y) \supset Lessequ(|x|,|y|)] = 0.$

T152: $y \neq 0 \supset (x0 \boxplus y) = x \boxplus y0.$

D153(Addition):

$$x + y \stackrel{d}{\equiv} \begin{cases} If\ \ x = y = 0\ \ then\ \ 0 \\ else\ \ if\ \ t(+) \dot{-} (1 \boxplus x \boxplus y) = 0\ \ then\ \ t(+) \\ else\ \ 1 \boxplus x \boxplus y, \end{cases}$$

$$t(+) \stackrel{d}{\equiv} \begin{cases} If\ \ Parity(x) = 0\ \ then\ \ (\lfloor \frac{1}{2}x \rfloor + \lfloor \frac{1}{2}y \rfloor) \otimes Parity(y) \\ else\ \ if\ \ Parity(y) = 0\ \ then\ \ (\lfloor \frac{1}{2}x \rfloor + \lfloor \frac{1}{2}y \rfloor)1 \\ else\ \ S(\lfloor \frac{1}{2}x \rfloor + \lfloor \frac{1}{2}y \rfloor)0. \end{cases}$$

T154: $t(+) \dot{-} (1 \boxplus x \boxplus y) = 0.$

T155: $x + 0 = x.$

T156: $Sx = x + 1.$

T157: $x + y = y + x.$

T158: $x + Sy = S(x + y).$

T159: $(x + y) + z = z + (y + z).$

T160: $[Equ(x + z, y + z) \Leftrightarrow Equ(x,y)] = 0.$

T161: $Less(x + y, y + z) = Less(x,y).$

T162: $Lessequ(x + z, y + z) = Lessequ(y,x)] = 0.$

T163: $y \neq 0 \supset x \dot{-} (y \boxplus z) = (x \dot{-} y) \dot{-} z.$

T164: $(x \sqsubseteq x) = 0.$

T165: $x \neq 0 \supset Equ(x,0) = 1.$

T166: $sg(x) = Equ(x,0).$

T167: $[x \sqsubseteq y \supset x \dot{-} z \sqsubseteq y \dot{-} z] = 0.$

T168: $[x \sqsubseteq y \supset s_i(x) \sqsubseteq s_i(y)] = 0.$

T169: $[Equ(x0,0) \supset Equ(x,0)] = 0.$

T170: $[Equ(x \boxplus y,0) \supset Equ(x,0)] = 0.$

T171: $Equ(x\#y,0) = 1.$

T172: $x \boxplus y1 = x0 \boxplus y.$

T173: $sg(Sx) = 1.$

T174: $sg(|x|) = sg(x).$

T175: $(x \sqsubseteq y) = Lessequ(|x|,|y|).$

T176: $y \neq 0 \supset x \dot{-} (y1 \boxplus z) = x \dot{-} (y \boxplus z)1.$

T177: $y \neq 0 \supset (x+y) \dot{-} (x \boxplus y) = 0.$

T178: $Equ(Sx,0) = 1.$

T179: $[Equ(x+y,0) \supset Equ(x,0)] = 0.$

T180: $x \neq 0 \supset |x \boxplus y| = |x| + |y|.$

D181(Multiplication):

$$x \cdot y \stackrel{d}{\equiv} \begin{cases} If\ \ y = 0\ \ then\ \ 0 \\ else\ \ Cond(y(\cdot) \dot{-} (x1\#y), t(\cdot), x1\#y), \end{cases}$$

where $t(\cdot) \equiv Cond(Parity(y), (x \cdot \lfloor \frac{1}{2} y \rfloor)0, (x \cdot \lfloor \frac{1}{2} y \rfloor)0 + x).$

T182: $[Equ(x \cdot y,0) \supset (Equ(x,0) \vee Equ(y,0))] = 0.$

T183: $x \cdot y = Cond(Parity(y), (x \cdot \lfloor \frac{1}{2} y \rfloor)0, (x \cdot \lfloor \frac{1}{2} y \rfloor)0 + x).$

T184: $x \cdot 1 = 0.$

T185: $s_0 x = x + x = x \cdot 2.$

T186: $x \cdot (y + 1) = (x \cdot y) + x.$

T187: $x \cdot (y + z) = (x \cdot y) + (x \cdot z).$

T188: $x0 \cdot y = (x \cdot y)0.$

T189: $x1 \cdot y = (x \cdot y)0 + y.$

T190: $0 \cdot x = 0.$

T191: $x \cdot y = y \cdot x.$

T192: $[Lessequ(1, x) \supset Equ(|2 \cdot x|, S(|x|))] = 0.$

T193: $|S(2 \cdot x)| = S(|x|).$

T194: $|x\#y| = S(|x| \cdot |y|).$

T195: $1\#1 = 2.$

T196: $0\#x = 1.$

T197: $xi \neq 0 \supset xi\#y = (x\#y) \boxplus y.$

T198: $x\#y = y\#x.$

T199: $(x \boxplus y) \cdot z = (x \cdot z) \boxplus y.$

T200: $x \neq 0 \supset (x \boxplus y)\#z = (x\#z) \cdot (y\#z).$

T201: $[Equ(|x|, |y|) \supset Equ(x\#z, y\#z)] = 0.$

T202: $[Equ(|x|, |u| + |v|) \supset Equ(x\#y, (u\#y) \cdot (v\#y))] = 0.$

T203: $[Equ(x, \lfloor \frac{1}{2}x \rfloor + \lfloor \frac{1}{2}x \rfloor) \vee Equ(x, S(\lfloor \frac{1}{2}x \rfloor + \lfloor \frac{1}{2}x \rfloor))] = 0.$

D204:

$$f^{\exists}(a,\vec{y}) \stackrel{d}{\equiv} \begin{cases} If\ \ a=0\ \ then\ \ sg(f(0,\vec{y})) \\ else\ \ if\ \ t(f^{\exists}) \dot{-} 1 = 0\ \ then\ \ t(f^{\exists}) \\ else\ \ 1, \end{cases}$$

where $t(f^{\exists}) \equiv f^{\exists}(\lfloor \frac{1}{2}a \rfloor), \vec{y}) \vee f(|a|, \vec{y})$.

$$f^{\forall}(a,\vec{y}) \stackrel{d}{\equiv} \begin{cases} If\ \ a=0\ \ then\ \ sg(f(0,\vec{y})) \\ else\ \ if\ \ t(f^{\forall}) \dot{-} 1 = 0\ \ then\ \ t(f^{\forall}) \\ else\ \ 1, \end{cases}$$

where $t(f^{\forall}) \equiv f^{\forall}(\lfloor \frac{1}{2}a \rfloor), \vec{y}) \& f(|a|, \vec{y})$.

DR205:

$(1) f^{\exists}(0,\vec{y}) = sg(f(0,\vec{y}))$,
$(2) f^{\exists}(a,\vec{y}) = f^{\exists}(\lfloor \frac{1}{2}a \rfloor), \vec{y}) \vee f(|a|, \vec{y})$,
$(3) f^{\forall}(0,\vec{y}) = sg(f(0,\vec{y}))$,
$(4) f^{\forall}(a,\vec{y}) = f^{\forall}(\lfloor \frac{1}{2}a \rfloor), \vec{y}) \& f(|a|, \vec{y})$.

T206: Let f be an n-place function symbol of PV. Then there are n+1-place function symbol f^M of PV for which the theorems are provable:

(1) $Lesseqv(f(x_1,\cdots,x_n), f^M(x_1,\cdots,x_n)) = 0$,
(2) $[(Lesswqu(x_1,y_1) \& \cdots \& Lesseqv(x_n,y_n)) \supset$
$Lesseq(f^M(x_1,\cdots,x_n), f^M(y_1,\cdots,y_n))] = 0$.

Chapter 4

The System IPV

The system IPV arises by adding intuitionistic predicate logic of PV, together with a form of induction on NP predicates. Because of availability of function symbols in PV, the form of predicates used in the induction scheme is much more restricted than IS^1_2. This restriction will simplify the realizability interpretation in Chapter 8 and 9. Main theorem of this chapter is that IPV is conservative extension of IS^1_2.

4.1 Definition of IPV

Definition 4.1.1

(1) The *predicate symbols* of IPV are $x = y$ and $x \leq y$.

(2) The *terms* and *function symbos* of IPV are those of PV.

(3) *Bounded quantifiers* and the class of formulas $\Pi^b_k, \Sigma^b_k, \Pi^{b+}_k, \Sigma^{b+}_k$ are defined in Chapter 2.

(4) *Rules of inference* of IPV are NJ and IR.

Definition 4.1.2 The *nonlogical axioms* of IPV are:

(1) All axioms of PV

(2) $x \leq y \leftrightarrow Lessequ(x, y) = 0$

(3) $x = s_0\lfloor \frac{1}{2}x \rfloor \vee x = s_1\lfloor \frac{1}{2}x \rfloor$

(4) $Cond(x, a, b) = c \leftrightarrow (x = 0 \wedge a = c) \vee (\neg(x = 0) \wedge b = c)$

(5) **NP-Induction scheme**
Any formula of the form:
$$[A(0) \wedge \forall x(A(\lfloor \tfrac{1}{2}x \rfloor) \rightarrow A(x))] \rightarrow \forall z A(z)$$
where A is of the form $(\exists y \leq t)u = v$, where t, u, v are terms of PV.

Of course, we can apply NP-Induction to the formula "$u = v$".

4.2 Conservative extension of IS_2^1

Theorem 4.2.1 Any theorem of PV is a theorem of IPV.

(*proof*) A form of theorem of PV is "$t = u$". We need to prove that axioms of PV are provable in IPV and rules of inference of PV are derived rules in IPV.

(1) **Axioms of PV**
Assume $t = u$ is an axiom of PV. Then $t = u$ is provable because axioms of PV are contained IPV.

(2) **R1**
Let $IPV \vdash t = u$. By (IR2), $IPV \vdash u = t$.

(3) **R2**
Let $IPV \vdash t = u$ and $u = v$. By (IR3), $IPV \vdash t = v$.

(4) **R3**
Let $IPV \vdash t_1 = u_1, \cdots, t_n = u_n$. By (IR4), $IPV \vdash f t_1 \cdots t_n = f u_1 \cdots u_n$.

(5) **R4**
Let $IPV \vdash t = u$. By $(\forall I)$ and $(\forall E)$, $IPV \vdash t[v/x] = u[v/x]$.

(6) **R5**
Let $IPV \vdash t_1[0/x] = t_2[0/x], t_1[s_0 x/x] = v_0[t_1/a], t_2[s_0 x/x] = v_0[t_2/a]$,
$t_1[s_1 x/x] = v_1[t_1/a]$ and $t_2[s_1 x/x] = v_0[t_2/a]$. Define $A(x)$ as $t_1(x) = t_2(x)$. Then we prove $IPV \vdash A(x)$ by NP-Induction.
By $t_1[0/x] = t_2[0/x]$,
$IPV \vdash A(0)$.
By $A(\lfloor \frac{1}{2} x \rfloor), x = s_0 \lfloor \frac{1}{2} x \rfloor$, $t_1[s_0 x/x] = v_0[t_1/a]$ and $t_2[s_0 x/x] = v_0[t_2/a]$,
$IPV \vdash x = s_0 \lfloor \frac{1}{2} x \rfloor \rightarrow (A(\lfloor \frac{1}{2} x \rfloor) \rightarrow A(x))$.
Similarly by $t_1[s_1 x/x] = v_1[t_1/a]$ and $t_2[s_1 x/x] = v_0[t_2/a]$,
$IPV \vdash x = s_1 \lfloor \frac{1}{2} x \rfloor \rightarrow (A(\lfloor \frac{1}{2} x \rfloor) \rightarrow A(x))$.
By above and $(x = s_0 \lfloor \frac{1}{2} x \rfloor \vee x = s_1 \lfloor \frac{1}{2} x \rfloor)$(Def. 4.1.2(3)),
$IPV \vdash A(\lfloor \frac{1}{2} x \rfloor) \rightarrow A(x)$.
By NP-Induction,
$IPV \vdash A(x)$.
Therefore R5 is derived rule.

∎

Theorem 4.2.2 The following are theorems of IPV:

(1) $Equ(x, y) = 0 \leftrightarrow (x = y)$.

(2) $\sim x = 0 \leftrightarrow \neg(x = 0)$

(3) $x\&y = 0 \leftrightarrow (x = 0 \wedge y = 0)$

(4) $x \vee y = 0 \leftrightarrow (x = 0 \vee y = 0)$

(5) $x \supset y \leftrightarrow (x = 0 \rightarrow y = 0)$

(6) $x \Leftrightarrow y = 0 \leftrightarrow (x = 0 \leftrightarrow y = 0)$

(7) $f^{\exists}(a, \vec{y}) = 0 \leftrightarrow (\exists x \leq |a|) f(x, \vec{y}) = 0$

(8) $f^{\forall}(a, \vec{y}) = 0 \leftrightarrow (\forall x \leq |a|) f(x, \vec{y}) = 0$

(*proof*)

(1) $Equ(x, y)$ is defined in D121.
By $(T125)$,
$$IPV \vdash Equ(x, y) = 0 \rightarrow x = y.$$
By $(T122)$,
$$IPV \vdash x = y \rightarrow Equ(x, y) = 0.$$

(2) $\sim x$ is defined in D32.
By definition,
$$IPV \vdash \sim x = 0 \rightarrow \neg(x = 0).$$
By Def. 4.1.2(4),
$$IPV \vdash \neg(x = 0) \rightarrow \sim x = 0.$$

(3) $x\&y$ is defined in D33.
Next two are obvious,
$$\vdash (x = 0 \wedge sg(y) = 0) \rightarrow (x = 0 \wedge y = 0)$$
and
$$\vdash (\neg(x = 0) \wedge 1 = 0) \rightarrow (x = 0 \wedge y = 0).$$
By $(x\&y = 0) \equiv (x = 0 \wedge sg(y) = 0) \vee (\neg(x = 0) \wedge 1 = 0)$,
$$IPV \vdash (x\&y = 0) \rightarrow (x = 0 \wedge y = 0).$$
By definition,
$$IPV \vdash (x = 0 \wedge y = 0) \rightarrow x\&y = 0.$$

(4) $x \vee y$ is defined in D34.
By $(x = 0 \wedge 0 = 0) \rightarrow x = 0, (\neg(x = 0) \wedge sg(y) = 0) \rightarrow y = 0$ and
$(x \vee y = 0) \equiv (x = 0 \wedge 0 = 0) \vee (\neg(x = 0) \wedge sg(y) = 0)$,
$$IPV \vdash x \vee y = 0 \rightarrow (x = 0 \vee y = 0).$$
By $\vdash x = 0 \rightarrow (x \vee y = 0), \vdash y = 0 \rightarrow (x \vee y = 0)$,
$$IPV \vdash (x = 0 \vee y = 0) \rightarrow x \vee y = 0.$$

(5) $x \supset y$ is defined in D35.
By $x = 0 \wedge sg(y) = 0$,
$$\vdash (x = 0 \wedge sg(y) = 0) \rightarrow (x = 0 \rightarrow y = 0).$$
Next is obvious,

$$\vdash (\neg(x=0) \wedge 0=0) \to (x=0 \to y=0).$$

By $(x \supset y=0) \equiv (x=0 \wedge sg(y)=0) \vee (\neg(x=0) \wedge 0=0)$,

$$IPV \vdash (x \supset y=0) \to (x=0 \to y=0).$$

By $\neg(x=0)$,

$$\vdash \neg(x=0) \to [(x=0 \to y=0) \to (x \supset y=0)].$$

By Def. 4.1.2(4),

$$\vdash x=0 \to [(x=0 \to y=0) \to (x \supset y=0)].$$

By $x=0 \vee \neg(x=0)$,

$$IPV \vdash (x=0 \to y=0) \to (x \supset y=0).$$

(6) $x \Leftrightarrow y$ is defined in D36.

Next is obvious,

$$\vdash (x=0 \wedge sg(y)=0) \to (x=0 \leftrightarrow y=0).$$

Next two are obvious,

$$\vdash (\neg(x=0) \wedge \overline{sg}(y)=0) \to (y=0 \to x=0).$$

and

$$\vdash (\neg(x=0) \wedge \overline{sg}(y)=0) \to (x=0 \to y=0).$$

Hence

$$\vdash (\neg(x=0) \wedge \overline{sg}(y)=0) \to (x=0 \leftrightarrow y=0).$$

By $x \Leftrightarrow y \equiv (x=0 \wedge sg(y)=0) \vee (\neg(x=0) \wedge \overline{sg}(y)=0$,

$$IPV \vdash (x \Leftrightarrow y) \to (x=0 \leftrightarrow y=0).$$

Next two are obvious,

$$\vdash y=0 \to [(x=0 \leftrightarrow y=0) \to (x \Leftrightarrow y)].$$

and

$$\vdash \neg(y=0) \to [(x=0 \leftrightarrow y=0) \to (x \Leftrightarrow y)].$$

By $y=0 \vee \neg(y=0)$

$$IPV \vdash (x=0 \leftrightarrow y=0) \to (x \Leftrightarrow y).$$

(7) $f^{\exists}(a,\vec{y})$ is defined in D204.

i) $(\exists \mathbf{x} \leq |\mathbf{a}|)\mathbf{f}(\mathbf{x},\vec{\mathbf{y}})=\mathbf{0} \to \mathbf{f}^{\exists}(\mathbf{a},\vec{\mathbf{y}})=\mathbf{0}$

Let $B(a)$ be $(x \leq |a| \wedge f(x,\vec{y})=0) \to f^{\exists}(a,\vec{y})=0$. By Def. 4.1.2(2)and this theorem(3), $(x \leq |a| \wedge f(x,\vec{y})=0) \equiv [Lesseq(x,|a|)\&f(x,\vec{y})]=0$. Therefore we can apply NP-Induction to $B(a)$. Hence we prove $B(a)$ by NP-Induction on the variable a.

Basis step Assume $x \leq |0| \wedge f(x,\vec{y})=0$. Then $x=0 \wedge f(x,\vec{y})=0$. Therefore $f(0,\vec{y})=0$. By D204, $f^{\exists}(0,\vec{y})=0$. Therefore

$$\vdash B(0).$$

Induction step Assume $\vdash B(\lfloor \frac{1}{2}a \rfloor)$ and $\vdash x \leq |a| \wedge f(x,\vec{y})=0$.

By $x \leq |a| \to (x \leq ||\lfloor \frac{1}{2}a \rfloor|| \vee x=|a|)$,

$$\vdash [x \leq |a| \wedge f(x,\vec{y})=0] \to [(x \leq ||\lfloor \tfrac{1}{2}a \rfloor|| \vee x=|a|) \wedge f(x,\vec{y})=0].$$

By $(x \leq ||\lfloor \frac{1}{2}a \rfloor|| \wedge f(x,\vec{y})=0)$ and $B(\lfloor \frac{1}{2}a \rfloor)$,

$$\vdash f^{\exists}(\lfloor \tfrac{1}{2}a \rfloor,\vec{y})=0.$$

Therefore $f^{\exists}(a,\vec{y})=[f^{\exists}(\lfloor \frac{1}{2}a \rfloor,\vec{y}) \vee f(|a|,\vec{y})]=[0 \vee f(|a|,\vec{y})]=0$.

By $x = |a| \wedge f(x, \vec{y}) = 0$,
$\vdash f(|a|, \vec{y}) = 0$.
Therefore $f^{\exists}(a, \vec{y}) = [f^{\exists}(\lfloor \frac{1}{2}a \rfloor, \vec{y}) \vee f(|a|, \vec{y})] = [f^{\exists}(\lfloor \frac{1}{2}a \rfloor, \vec{y}) \vee 0] = 0$.
By hypothesis, $\vdash f^{\exists}(a, \vec{y}) = 0$.
Therefore
$\vdash B(\lfloor \frac{1}{2}a \rfloor) \to B(a)$.
By NP-Induction,
$\vdash B(a)$.
Therefore
$$IPV \vdash (\exists x \leq |a|) f(x, \vec{y}) = 0 \to f^{\exists}(a, \vec{y}) = 0$$

ii) $\mathbf{f^{\exists}(a, \vec{y}) = 0 \to (\exists x \leq |a|) f(x, \vec{y}) = 0}$
Let $D(a)$ be $(\exists x \leq |a|)(f(x, \vec{y}) = 0 \vee f^{\exists}(a, \vec{y}) = 1)$. We prove $D(a)$ by NP-Induction on the variable a.
Basis step By $f^{\exists}(0, \vec{y}) = Cond(f(0, \vec{y}), 0, 1)$ and Def. 4.1.2(4),
$\vdash (f(0, \vec{y}) = 0 \wedge f^{\exists}(0, \vec{y}) = 0) \vee (\neg(f(0, \vec{y}) = 0) \wedge f^{\exists}(0, \vec{y}) = 1)$
By this and $0 \leq |0|$,
$\vdash 0 \leq |0| \wedge [f(0, \vec{y}) = 0 \vee f^{\exists}(0, \vec{y}) = 1]$.
Hence
$\vdash \exists x(x \leq |0| \wedge [f(x, \vec{y}) = 0 \vee f^{\exists}(0, \vec{y}) = 1])$.
Therefore
$\vdash D(0)$.
Induction step Let $\vdash D(\lfloor \frac{1}{2}a \rfloor) (\equiv \exists x(x \leq |\lfloor \frac{1}{2}a \rfloor| \wedge [f(x, \vec{y}) = 0 \vee f^{\exists}(\lfloor \frac{1}{2}a \rfloor, \vec{y}) = 1]))$.
By $x \leq |\lfloor \frac{1}{2}a \rfloor|, f(x, \vec{y}) = 0$,
$\vdash (x \leq |\lfloor \frac{1}{2}a \rfloor| \wedge f(x, \vec{y}) = 0) \to x \leq |a|$
$\vdash (x \leq |\lfloor \frac{1}{2}a \rfloor| \wedge f(x, \vec{y}) = 0) \to (f(x, \vec{y}) = 0 \vee f^{\exists}(a, \vec{y}) = 1)$.
Hence
$$\vdash \underline{(x \leq |\lfloor \frac{1}{2}a \rfloor| \wedge f(x, \vec{y}) = 0) \to (x \leq |a| \wedge [f(x, \vec{y}) = 0 \vee f^{\exists}(a, \vec{y}) = 1])}_{\alpha}.$$
By $f^{\exists}(\lfloor \frac{1}{2}a \rfloor, \vec{y}) = 1$ and $f^{\exists}(a, \vec{y}) = Cond(f^{\exists}(\lfloor \frac{1}{2}a \rfloor, \vec{y}), 0, sg(f(|a|, \vec{y})))$,
$\vdash f^{\exists}(\lfloor \frac{1}{2}a \rfloor, \vec{y}) = 1 \to [(f(|a|, \vec{y}) = 0 \wedge f^{\exists}(a, \vec{y}) = 0) \vee (\neg(f(|a|, \vec{y}) = 0) \wedge f^{\exists}(a, \vec{y}) = 1)]$.
By $(f(|a|, \vec{y}) = 0 \wedge f^{\exists}(a, \vec{y}) = 0)$,
$\vdash (f(|a|, \vec{y}) = 0 \wedge f^{\exists}(a, \vec{y}) = 0) \to \exists x(x \leq |a| \wedge (f(|a|, \vec{y}) = 0 \vee f^{\exists}(a, \vec{y}) = 1))$.
By $(\neg(f(|a|, \vec{y}) = 0) \wedge f^{\exists}(a, \vec{y}) = 1)$,
$\vdash (\neg(f(|a|, \vec{y}) = 0) \wedge f^{\exists}(a, \vec{y}) = 1) \to \exists x(x \leq |a| \wedge (f(|a|, \vec{y}) = 0 \vee f^{\exists}(a, \vec{y}) = 1))$.
Hence
$$\vdash \underline{(x \leq |\lfloor \frac{1}{2}a \rfloor| \wedge f^{\exists}(\lfloor \frac{1}{2}a \rfloor, \vec{y}) = 1) \to \exists x(x \leq |a| \wedge (f(|a|, \vec{y}) = 0 \vee f^{\exists}(a, \vec{y}) = 1))}_{\beta}.$$
By $(\alpha), (\beta)$, and $D(\lfloor \frac{1}{2}a \rfloor)$,
$\vdash D(\lfloor \frac{1}{2}a \rfloor) \exists x(x \leq |a| \wedge (f(|a|, \vec{y}) = 0 \vee f^{\exists}(a, \vec{y}) = 1))$.
Therefore
$\vdash D(\lfloor \frac{1}{2}a \rfloor) \to D(a)$
By NP-Induction ,

$\vdash D(a)$

By $x \leq |a| \wedge f(|a|, \vec{y}) = 0$,

$\vdash (x \leq |a| \wedge f(|a|, \vec{y}) = 0) \rightarrow [f^{\exists}(a, \vec{y}) = 0 \rightarrow \exists x(x \leq |a| \wedge f(|a|, \vec{y}) = 0)]$.

By $x \leq |a| \wedge f^{\exists}(a, \vec{y}) = 1$,

$\vdash (x \leq |a| \wedge f^{\exists}(a, \vec{y}) = 1) \rightarrow [f^{\exists}(a, \vec{y}) = 0 \rightarrow \exists x(x \leq |a| \wedge f(|a|, \vec{y}) = 0)]$.

By these and $D(a)$,

$$IPV \vdash f^{\exists}(a, \vec{y}) = 0 \rightarrow (\exists x \leq |a|) f(|a|, \vec{y}) = 0.$$

(8) $f^{\forall}(a, \vec{y})$ is defined in D204.

Let $E(a)$ be $f^{\forall}(a, \vec{y}) = 0 \leftrightarrow (\forall x \leq |a|) f(x, \vec{y}) = 0$. We prove $E(a)$ by NP-Induction on the variable a.

Basis step

By $(f^{\forall}(0, \vec{y}) = 0) \leftrightarrow f(0, \vec{y}) = 0$ and $(\forall x \leq |a|) f(x, \vec{y}) = 0 \leftrightarrow f(0, \vec{y}) = 0$,

$\vdash f^{\forall}(0, \vec{y}) = 0 \leftrightarrow f(0, \vec{y}) = 0$

Therefore

$\vdash E(0)$

Induction step Let $IPV \vdash E(\lfloor \frac{1}{2} a \rfloor)$.

Assume $\vdash f^{\forall}(a, \vec{y}) = 0$. By T205,

$\vdash f^{\forall}(\lfloor \frac{1}{2} a \rfloor, \vec{y}) \& f(|a|, \vec{y}) = 0$.

By this theorem (3),

$\vdash f^{\forall}(\lfloor \frac{1}{2} a \rfloor, \vec{y}) = 0 \wedge f(|a|, \vec{y}) = 0$.

By $E(\lfloor \frac{1}{2} a \rfloor)$,

$\vdash (\forall x \leq |\lfloor \frac{1}{2} a \rfloor|) f(x, \vec{y}) = 0 \wedge f(|a|, \vec{y}) = 0$.

In a word,

$\vdash (\forall x \leq |a|) f(x, \vec{y}) = 0$.

Therefore

$\vdash f^{\forall}(a, \vec{y}) = 0 \rightarrow (\forall x \leq |a|) f(x, \vec{y}) = 0$.

Assume $(\forall x \leq |a|) f(x, \vec{y}) = 0$. Then

$\vdash f(|a|, \vec{y}) = 0 \wedge (\forall x \leq |\lfloor \frac{1}{2} a \rfloor|) f(x, \vec{y}) = 0$.

By $E(\lfloor \frac{1}{2} a \rfloor)$,

$\vdash f(|a|, \vec{y}) = 0 \wedge f^{\forall}(\lfloor \frac{1}{2} a \rfloor, \vec{y}) = 0$.

By T205,

$\vdash f^{\forall}(a, \vec{y}) = 0$.

Therefore

$\vdash (\forall x \leq |a|) f(x, \vec{y}) = 0 \rightarrow f^{\forall}(a, \vec{y}) = 0$.

Therefore

$\vdash E(\lfloor \frac{1}{2} a \rfloor) \rightarrow E(a)$.

By NP-Induction,

$$IPV \vdash f^{\forall}(a, \vec{y}) = 0 \leftrightarrow (\forall x \leq |a|) f(x, \vec{y}) = 0$$

∎

Theorem 4.2.3 If A is a Σ_0^bformula of IPV then there is a term t^A of PV so that

$$IPV \vdash A \leftrightarrow t^A = 0$$

(*proof*) We prove by induction on the logical structure of A
Let t_1 and t_2 be terms.

1) If A is $t_1 = t_2$, then $t_1 = t_2 \leftrightarrow Equ(t_1, t_2) = 0$ by Th. 4.2.2(1).

2) If A is $t_1 \leq t_2$, then $t_1 \leq t_2 \leftrightarrow Lesseq u(t_1, t_2) = 0$ by Def. 4.1.2(2).

For the remaining cases,assume that $\vdash B \leftrightarrow t^B = 0$ and $\vdash C \leftrightarrow t^C = 0$, where B and C are Σ_0^b formula and $t^B = 0$ and $t^C = 0$ are terms of PV.

3) If A is $B \wedge C$, then $B \wedge C \leftrightarrow (t^B = 0) \wedge (t^C = 0) \leftrightarrow (t^B \& t^C = 0)$ by Th. 4.2.2(3).

4) If A is $B \vee C$, then $B \vee C \leftrightarrow (t^B = 0) \vee (t^C = 0) \leftrightarrow (t^B \vee t^C = 0)$ by Theorem 4.2.2(4).

5) If A is $B \rightarrow C$, then $B \rightarrow C \leftrightarrow (t^B = 0) \rightarrow (t^C = 0) \leftrightarrow (t^B \supset t^C = 0)$ by Theorem 4.2.2(5).

For the remaining cases,assume that $\vdash D(x, \vec{y}) \leftrightarrow t^B(x, \vec{y}) = 0$, where $D(x, \vec{y})$ is Σ_0^b formula and $t^B(x, \vec{y})$ is term of PV.

6) If A is $(\exists x \leq |a|)B(x, \vec{y})$, then $(\exists x \leq |a|)B(x, \vec{y}) \leftrightarrow (\exists x \leq |a|)t^B(x, \vec{y}) = 0 \leftrightarrow (t^B)^{\exists}(x, \vec{y}) = 0$ by Theorem 4.2.2(7).

7) If A is $(\forall x \leq |a|)B(x, \vec{y})$, then $(\forall x \leq |a|)B(x, \vec{y}) \leftrightarrow (\forall x \leq |a|)t^B(x, \vec{y}) = 0 \leftrightarrow (t^B)^{\forall}(x, \vec{y}) = 0$ by Theorem 4.2.2(8). ∎

Theorem 4.2.4 If A is a Σ_0^bformula of IPV then $IPV \vdash A \vee \neg A$.

(*proof*) By theorem 4.2.2(2),(4),T1,T4,D31,D34,T38 and theorem 4.2.3. ∎

Lemma 4.2.5 The $\Sigma_1^b - PIND$ and $\Sigma_1^b - LIND$ are derivable in IPV, provided that the formula $A(x)$ is of the form $(\exists y \leq t)B$, where B is Σ_0^b.

(*proof*) By theorem 4.2.3, $A \equiv (\exists y \leq t)t^B = 0$. So The $\Sigma_1^b - PIND$ scheme for $A(x)$ is equivalent to NP-Induction. Therefore the $\Sigma_1^b - PIND$ scheme is a theorem of IPV. The $\Sigma_1^b - LIND$ scheme for $A(x)$ is provided exactly as in lemma 2.3.6. ∎

Theorem 4.2.6 There are functions $Sx, |x|, \lfloor \frac{1}{2}x \rfloor, x + y, x \cdot y$ and $x \sharp y$ definable in PV so that all the *BASIC axioms* of IS_2^1 are provable in IPV.

(*proof*) $Sx, |x|, x + y$ and $x \cdot y$ are defined in each D24,D133,D153 and D181.

B.1 is by T122 and T148 .
B.2 is by T122 and T148 .
B.3 is by D137 and T144 .
B.4 is by T139 .
B.5 is by T141 .
B.6 is by T142 .
B.7 is by D133 .
B.8 is by T192 .
B.9 is by T193 .
B.10 is by T151 .
B.11 is by T194 .
B.12 is by T195 .
B.13 is by T198 .
B.14 is by T202 .
B.15 is by T155 .
B.16 is by T158 .

B.17 is by T159 . **B.18** is by T162 .
B.19 is by T184 . **B.20** is by T187 .
B.21 is by T203 . ∎

Theorem 4.2.7 IPV contains a set of efficient coding functions.

(*proof*) A sequence $s_0, \cdots, s_k$ can be encoded by replacing each digit in an entry in the sequence by a two-digit sequence, then concatenating all the encoded entries with a two-digit code as a separator. The result coding functions are fairly easy to define in PV, and the theorems required by def. 2.4.4 may be established by using multi-variable induction (DR118). ∎

Definition 4.2.8 The Σ_0^b-*replacement scheme* is the family of formulas of the form:

$$(\forall x \leq |t|)(\exists y \leq s)A(x,y) \leftrightarrow (\exists w \leq Bound(s^*,t))(\forall x \leq |t|)[A(x,\beta(x,w)) \wedge \beta(x,w) \leq s].$$

where $A(x,y)$is a Σ_0^b formula of IPV and $s^* = s^M[|t|/x]$, where now s^M is the monotone upper bound on s obtained from T206.

Theorem 4.2.9 All instances of the Σ_0^b-*replacement scheme* are provable in IPV.

(*proof*) Let
$L \stackrel{d}{\equiv} (\forall x \leq |t|)(\exists y \leq s)A(x,y)$,
$M \stackrel{d}{\equiv} (\exists w \leq Bound(s^*,t))(\forall x \leq |t|)[A(x,\beta(x,w)) \wedge \beta(x,w) \leq s]$,
$N(u) \stackrel{d}{\equiv} (\exists w \leq Bound(s^*,t))(\forall x \leq |t|)[x \leq u \rightarrow A(x,\beta(x,w)) \wedge \beta(x,w) \leq s]$.
1)M $\rightarrow$ L

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{w \leq Bound(s^*,t) \wedge (\forall x \leq |t|)[A(x,\beta(x,w)) \wedge \beta(x,w) \leq s]}{\forall x(S|t| \leq x \vee [A(x,\beta(x,w)) \wedge \beta(x,w) \leq s])}}{S|t| \leq x \vee [A(x,\beta(x,w)) \wedge \beta(x,w) \leq s]}}{S|t| \leq x \quad \exists y[A(x,y) \wedge y \leq s]}}{S|t| \leq x \quad (\exists y \leq s)A(x,y)}}{S|t| \leq x \vee (\exists y \leq s)A(x,y) \quad S|t| \leq x \vee (\exists y \leq s)A(x,y)}}{S|t| \leq x \vee (\exists y \leq s)A(x,y)}}{\forall x(S|t| \leq x \vee (\exists y \leq s)A(x,y))}}{M \qquad\qquad L}}{L \quad \text{(by } (\exists E) \text{ for } w)}$$

2)L $\rightarrow$ M
For $L \rightarrow M$, we prove $L \rightarrow N(u)$ by $\Sigma_1^b - LIND$.
We first show $A \rightarrow N(0)$, that is ,

$$A \rightarrow (\exists w \leq Bound(s^*,t))(\forall x \leq |t|)[x \leq u \rightarrow A(0,\beta(0,w)) \wedge \beta(0,w) \leq s].$$

Assuming L, we have $A(0,b)$ for some $b \le s[0/x]$. Let w be $0 * b$.
By def. 2.4.4(A,B,C),
$\vdash Seq(w) \wedge Len(w) = 1$.
By def. 2.4.4(F),
$\vdash \beta(0,w) = b$.
By $\beta(0,w) = b \le s[0/x] \le s^M[0/x] \le s^M[|t|/x] = s^*$,
$\vdash (\forall i < Len(w))(\beta(i,w) \le s^*)$.
By def. 2.4.4(H),
$\vdash w \le Bound(s^*, t)$.
By $A(0,b)$ and $\beta(0,w) = b$,
$\vdash A(0, \beta(0,w))$.
By $A(0,\beta(0,w))$,
$\vdash x \le 0 \to A(0,\beta(0,w))$.
By $x \le 0 \to x = 0$ and $\beta(0,w) \le s[0/x]$,
$\vdash x \le 0 \to \beta(x,w) \le s[x/x]$.
So the proof of $L \to N(0)$ is complete.

Secondly, for to prove $L \to (N(u) \to N(Su))$ we prove $L \wedge N(u) \wedge |t| \le u \to N(Su)$ and $L \wedge N(u) \wedge u < |t| \to N(Su)$. $L \wedge N(u) \wedge |t| \le u \to N(Su)$ is easy because of $x \le |t| \to x \le u$ and $N(u)$. Therefore we prove $L \wedge N(u) \wedge u < |t| \to N(Su)$. Assuming the antecedent, we have :

$N(u) \equiv (\exists w_1 \le Bound(s^*,t))(\forall x \le |t|)[x \le u \to A(x, \beta(x,w_1)) \wedge \beta(x,w_1) \le s]$.
$N(Su) \equiv (\exists w_2 \le Bound(s^*,t))(\forall x \le |t|)[x \le Su \to A(x, \beta(x,w_2)) \wedge \beta(x,w_2) \le s]$.

By L and $u < |t| (\equiv Su \le |t|)$, we have $A(Su, b)$ for some $b \le s[Su/x]$ (take Su as x). We define w_2 to be $w_1 * b$. By def. 2.4.4(B), $Seq(w_2)$. By $Len(w_1) \le |t|+1$, $Len(w_2) \le S|t|+1$. By $b \le s[Su/x] \le s[|t|/x] = s^*, N(u)$,and def. 2.4.4(E), $(\forall i < Len(w_2))\beta(i,w_2) \le s^*$. By def. 2.4.4(H), $w_2 \le Bound(s^*,t)$. By def. 2.4.4(E) and $N(u)$,

$\vdash x \le u \to A(x,\beta(x,w_2)) \wedge \beta(i,w) \le s^* \cdots\cdots (\alpha)$.

By $A(Su,b)$ and $b = \beta(Su,w_2)$
$\vdash x = Su \to A(Su, \beta(Su,w_2))$.
By $\beta(Su,w_2)(= b) \le s^*$,
$\vdash x = Su \to \beta(x,w_2) \le s^*$.
By $(\wedge I)$,

$\vdash x = Su \to A(Su,\beta(Su,w_2)) \wedge \beta(x,w_2) \le s^*. \cdots\cdots (\beta)$

By (α),(β) and $x \le Su \to x \le u \vee x = Su$,

$\vdash x \le Su \to A(x,\beta(x,w_2)) \wedge \beta(i,w) \le s^*$.

By these, we prove $L \wedge N(u) \wedge u < |t| \to N(Su)$. By $\Sigma_1^b - LIND$, $L \to N(|u|)$.

Therefore $L \to M$ is proved. ∎

Lemma 4.2.10 $IPV \vdash (\exists y_1 \le t_1)(\exists y_2 \le t_2)u = v \leftrightarrow (\exists z \le s)u' = v'$

(proof)
(1) $(\exists z \le s)u' = v' \to (\exists y_1 \le t_1)(\exists y_2 \le t_2)u = v$
$(\exists z \le s)u' = v' \to (0 \le 0 \wedge (\exists z \le s)u' = v')$
$\to \exists x(x \le 0 \wedge (\exists z \le s)u' = v')$

$$\to (\exists x \le 0)(\exists z \le s)u' = v'.$$

(2) $(\exists y_1 \le t_1)(\exists y_2 \le t_2)u = v \to (\exists z \le s)$
Let A be $(\exists y_1 \le t_1)(\exists y_2 \le t_2)u = v$. By definition of bounded quantifiers (def. 2.1.9), y_i does not occur in t_i, i=1,2. If y_2 occurs in t_1 then we may avoid this occurrence by renaming the variable in the second quantifier. However, y_1 may occur in t_1. To eliminate this occurrence, we appeal to T206 and th. 4.2.2 to find a term s_2 whose variables are among those of t_2 such that $\vdash t_2 \le s_2$ and $\vdash (y_1 \le t_1 \to s_2 \le s_2[t_1/y_1])$. Then

$$IPV \vdash A \leftrightarrow (\exists y_1 \le t_1)(\exists y_2 \le s_2[t_1/y_1])(y_2 \le t_2 \wedge u = v)$$
$$\leftrightarrow (\exists y_1 \le t_1)(\exists y_2 \le s_2[t_1/y_1])Lessequ(y_2, t_2) \wedge Equ(u, v) = 0.$$

Thus we may assume that in the formula A neither y_1 or y_2 occur in t_1 or t_2.

We use the pairing function $< x, y >$ (D99) and projection function Π^2_1, Π^2_2 (D115) which have the which has the properties of $\Pi^2_1(y_1, y_2) = y_1$,$\Pi^2_2(y_1, y_2) = y_2$ and $(y_1 \le t_1 \wedge y_2 \le t_2) \to < y_1, y_2 > \le < t_1, t_2 >$.
By use of these functions,

$$\begin{aligned}
&(\exists y_1 \le t_1)(\exists y_2 \le t_2)u = v \\
&\quad \to \exists y_1(\exists y_2((y_1 \le t_1 \wedge y_2 \le t_2) \wedge y_1 \le t_1 \wedge y_2 \le t_2 \wedge u = v)) \\
&\quad \to \exists y_1(\exists y_2((< y_1, y_2 > \le < t_1, t_2 >) \wedge \Pi^2_1(< y_1, y_2 >) \le t_1 \wedge \\
&\qquad\qquad \Pi^2_2(< y_1, y_2 >) \le t_2 \wedge u[\Pi^2_i(< y_1, y_2 >)/y_i] = v[\Pi^2_i(< y_1, y_2 >)/y_i])) \\
&\quad \to \exists z(z \le < t_1, t_2 > \wedge \Pi^2_1(z) \le t_1 \wedge \Pi^2_2(z) \le t_2 \wedge u[\Pi^2_i(z)/y_i] = v[\Pi^2_i(z)/y_i])) \\
&\quad \to (\exists z \le < t_1, t_2 >)(\Pi^2_1(z) \le t_1 \wedge \Pi^2_2(z) \le t_2 \wedge u' = v') \\
&\quad \to (\exists z \le < t_1, t_2 >)([Lessequ(\Pi^2_1(z), t_1) \& Lessequ(\Pi^2_2(z), t_2) \& Equ(u'v')] = 0), \\
&\quad \text{where } u' \text{ and } v' \text{ are } u[\Pi^2_i(z)/y_i] \text{ and } v[\Pi^2_i(z)/y_i]. \ \blacksquare
\end{aligned}$$

Lemma 4.2.11 Every Σ^{b+}_1 formula of IPV is equivalent in IPV to a formula of the form $(\exists y \le t)(u = v)$.

(*proof*) We prove by induction on the complexity of Σ^{b+}_1 formula A.
1) $A \equiv u = v$
Assume $u = v$. Then by $\vdash 0 \le t \wedge u = v$, $\vdash \exists y(y \le t \wedge u = v)$. Therefore
$$IPV \vdash A \to (\exists y \le t)(u = v).$$
Assume $(\exists y \le t)(u = v)$. Then by $\vdash \neg(u = v) \to ((\exists y \le t)(u = v) \to \bot)$,
$\vdash \neg(u = v) \to ((\exists y \le t)(u = v) \to u = v)$. By $(u = v) \vee \neg(u = v)$, $\vdash u = v$. Therefore
$$IPV \vdash (\exists y \le t)(u = v) \to A.$$

2) $A \equiv u \le v$
Assume $u \le v$. By $0 \le t, \vdash 0 \le t \wedge u \le v$. By def. 4.1.2(2), $\vdash \exists y(y \le t \wedge Lessequ(u, v) = 0)$. Therefore
$$IPV \vdash A \to (\exists v \le t)(Lessequ(u, v) = 0).$$
Assume $(\exists y \le t)(u \le v)$. Then $\vdash \neg(u \le v) \to ((\exists y \le t)(u = v) \to u \le v)$. By $(u \le v \to u \le v)$ and $(u \le v) \vee \neg(u = v)$, $\vdash u \le v$. Therefore
$$IPV \vdash (\exists y \le t)(u = v) \to A.$$

For the remaining cases, assume that Σ_1^{b+} formulas B and C are $B \leftrightarrow (\exists y_1 \le t_1)(u_1 = v_1)$ and $C \leftrightarrow (\exists y_2 \le t_2)(u_2 = v_2)$.

3) $A \equiv (\exists y \le t)B$
Assume $(\exists y \le t)B$. By definition of B, $\vdash (\exists y \le t)(\exists y_1 \le t_1)(u_1 = v_1)$. By lemma 4.2.10, $\vdash \exists z(z \le s)u' = v'$. Therefore

$$IPV \vdash A \rightarrow (z \le s)u' = v'.$$

By to reverse the method, we can prove $(\exists y \le t)(u = v) \rightarrow A$.

4) $A \equiv (\forall y \le |t|)B$
Assume $(\forall y \le |t|)B$. By definition of B, $\vdash (\forall y \le |t|)(\exists y_1 \le t_1)(u_1 = v_1)$. By th. 4.2.9,

$$\vdash (\exists w \le Bound(t_1^*, t))(\forall y \le |t|)(u_1[\beta(y,w)/y_1] = v_1[\beta(y,w)/y_1] \wedge \beta(y,w) \le t_1) \ .$$

By th. 4.2.2(1),(3),(8) and def. 4.1.2,

$$\vdash (\exists w \le Bound(t_1^*, t))[(Equ(u_1', v_1')\&Lessequ(\beta(t,w), s))^{\forall} = 0],$$

where u_1' and v_1' are $u_1[\beta(y,w)/y_1]$ and $v_1[\beta(y,w)/y_1]$.
Hence

$$IPV \vdash A \rightarrow (\exists w \le Bound(t_1^*, t))[(Equ(u_1', v_1')\&Lessequ(\beta(t,w), s))^{\forall} = 0].$$

By to reverse the method, we can prove
$IPV \vdash \exists w \le Bound(t_1^*, t))[(Equ(u_1', v_1')\&Lessequ(\beta(t,w), s))^{\forall} = 0] \rightarrow A$.

5) $A \equiv B \wedge C$
Assume $B \wedge C$. Then $\vdash (\exists y_1 \le t_1)(\exists y_2 \le t_2)(u_1 = v_1 \wedge u_2 = v_2)$.
By th. 4.2.2(1),(3),

$$\vdash (\exists y_1 \le t_1)(\exists y_2 \le t_2)(Equ(u_1, v_1)\&Equ(u_2, v_2) = 0).$$

By lemma 4.2.10,

$$\vdash (z \le s)u' = v'.$$

Hence

$$IPV \vdash A \rightarrow (z \le s)u' = v'.$$

By to reverse the method, we can prove $(z \le s)u' = v' \rightarrow A$.

6) $A \equiv B \vee C$
Assume $B \vee C$. Then $\vdash (\exists y_1 \le t_1)(\exists y_2 \le t_2)(u_1 = v_1 \vee u_2 = v_2)$. By th. 4.2.2(1),(4), $\vdash (\exists y_1 \le t_1)(\exists y_2 \le t_2)(Equ(u_1, v_1) \vee Equ(u_2, v_2) = 0)$. By lemma 4.2.10, $\vdash (z \le s)u' = v'$.
Hence

$$IPV \vdash A \rightarrow (z \le s)u' = v'.$$

By to reverse the method, we can prove $(z \le s)u' = v' \rightarrow A$. ∎

Theorem 4.2.12 *IPV* is a conservative extension of IS_2^1.

(*proof*) We need to prove $\forall A \in L(IS_2^1)[IPV \vdash A \Rightarrow IS_2^1 \vdash A]$. We define the system T which is extension of IS_2^1 by 1) Σ_1^{b+} definition which is sufficiently strong and 2) function symbol f by th. 2.4.8. To prove this theorem, we prove $\forall A \in L(IS_2^1)[IS_2^1 \vdash A \Rightarrow IPV \vdash A]$ and $\forall A \in L(IPV)[IPV \vdash A \Rightarrow T \vdash A]$.

1) $\forall A \in L(IS_2^1)[IS_2^1 \vdash A \Rightarrow IPV \vdash A]$
By th. 4.2.6,

$IPV \vdash$BASIC axioms .

Let $A(x)$ be $IPV \vdash A(0) \wedge \forall x(A(\lfloor \frac{1}{2}x \rfloor) \rightarrow A(x))$, where $A(x)$ is any Σ_1^{b+}-formula. By lemma 4.2.11, $IPV \vdash A \leftrightarrow (\exists y \leq t)(u = v)$. Let $B(x)$ be $(\exists y \leq t)(u = v)$. Then $IPV \vdash B(0) \wedge \forall x(B(\lfloor \frac{1}{2}x \rfloor) \rightarrow B(x))$. By NP-Induction for $B(x)$, $IPV \vdash \forall x B(x)$. By definition of $B(x)$, $IPV \vdash \forall x A(x)$.
Therefore $IPV \vdash A(0) \wedge \forall x(A(\lfloor \frac{1}{2}x \rfloor) \rightarrow A(x)) \rightarrow xA(x)$.
Therefore

$IPV \vdash \Sigma_1^{b+} - PIND.$

2) $\forall A \in L(IPV)[IPV \vdash A \Rightarrow T \vdash A]$
Each basic function symbol of PV is either a function symbol of IS_2^1, or has a simple defining formula in IS_2^1. Thus

$s_0(x) = 2 \cdot x$
$s_1(x) = 2 \cdot x + 1$
$y = Parity(x) \leftrightarrow x = y + 2 \cdot \lfloor \frac{1}{2}x \rfloor$
$w = Cond(x, y, z) \leftrightarrow (x = 0 \wedge y = w) \vee (\neg(x = 0) \wedge z = w)$
$x \boxplus y = x \cdot (y \sharp 1)$
$z = x \dot{-} y \leftrightarrow (\exists w \leq x)(|w| \leq |y| \wedge x = z \boxplus y + w)$
$[\lambda x_1 \cdots x_n.t](y_1 \cdots y_n) = t[y_1/x_1 \cdots y_n/x_n]$
$Lessequ(x, y) = z \leftrightarrow ((x \leq y \wedge z = 0) \vee (\neg(x \leq y) \wedge z = 1)).$

We prove $T \vdash$ PV axioms (0)-(7) (def. 3.1.2).

PV Axiom (0) $s_0(0) = 2 \cdot 0 = 0.$

PV Axiom (1a)
By (B.21),

$\vdash s_0(x) = 2 \cdot \lfloor \frac{1}{2}s_0x \rfloor \vee 2 \cdot \lfloor \frac{1}{2}s_0x \rfloor + 1.$

Hence

$\vdash 2 \cdot x = 2 \cdot \lfloor \frac{1}{2}s_0x \rfloor.$

Therefore

$\vdash s_0(x) = 2 \cdot \lfloor \frac{1}{2}s_0x \rfloor + 0.$

By definition of $Parity$,

$\vdash Parity(s_0x) = 0.$

PV Axiom (1b)
By (B.21),

$\vdash s_1(x) = 2 \cdot \lfloor \frac{1}{2}s_1x \rfloor \vee 2 \cdot \lfloor \frac{1}{2}s_1x \rfloor + 1.$

Hence

$\vdash 2 \cdot x + 1 = 2 \cdot \lfloor \frac{1}{2}s_0x \rfloor + 1.$

Therefore

$\vdash s_1(x) = 2 \cdot \lfloor \frac{1}{2}s_1x \rfloor + 1.$

By definition of $Parity$,
$\vdash Parity(s_1x) = 1$.

PV Axiom (2a) By 1a, $\vdash 2 \cdot x = 2 \cdot \lfloor \frac{1}{2} s_0 x \rfloor$. Therefore $\vdash x = \lfloor \frac{1}{2} s_0 x \rfloor$.

APV xiom (2b) By 1b, $\vdash 2 \cdot x + 1 = 2 \cdot \lfloor \frac{1}{2} s_0 x \rfloor + 1$. Therefore $\vdash x = \lfloor \frac{1}{2} s_0 x \rfloor$.

PV Axiom (3a)
By $(0 = 0) \to [(0 = 0 \wedge y = y) \vee (\neg(0 = 0) \wedge z = y)]$,
$\neg(0 = 0) \to [(0 = 0 \wedge y = y) \vee (\neg(0 = 0) \wedge z = y)]$ and $(0 = 0) \vee \neg(0 = 0)$,
$\vdash (0 = 0 \wedge y = y) \vee (\neg(0 = 0) \wedge z = y)$.
Therefore
$\vdash Cond(0, y, z) = y$.

PV Axiom (3b)
By $x = 0 \leftrightarrow s_0x = 0$ and $\neg(x = 0) \leftrightarrow \neg(s_0x = 0)$,

$$\begin{aligned} Cond(x, y, z) = w &\leftrightarrow [(x = 0 \wedge y = w) \vee (\neg(x = 0) \wedge z = w)] \\ &\leftrightarrow [(s_0x = 0 \wedge y = w) \vee (\neg(s_0x = 0) \wedge z = w)] \\ &\leftrightarrow Cond(s_0x, y, z) = w \end{aligned}$$

PV Axiom (3c) By $IPV \vdash \neg(s_1x = 0)$, $\vdash (s_1x = 0 \wedge y = z) \vee (\neg(s_1x = 0) \wedge z = z)$.

PV Axiom (4a)
By $(y = 0) \to [(y = 0 \wedge x = x \boxplus s_0y) \vee (\neg(y = 0) \wedge s_0(x \boxplus y) = x \boxplus s_0y)]$,
$\neg(y = 0) \to [(y = 0 \wedge x = x \boxplus s_0y) \vee (\neg(y = 0) \wedge s_0(x \boxplus y) = x \boxplus s_0y)]$
and $(y = 0) \vee \neg(y = 0)$,
$\vdash Cond(y, x, s_0(x \boxplus y)) = x \boxplus s_0y$.

PV Axiom (4b)

$$x \boxplus s_1y = x \cdot (s_1y\#1) = x \cdot 2^{|s_1y| \cdot |1|} = x \cdot 2^{|y| \cdot |1|} \cdot 2 = s_0(x \cdot (y\#1)) = s_0(x \boxplus y)$$

PV Axiom (5a)
By $\neg(y = 0) \to [\neg(y = 0) \wedge \lfloor \frac{1}{2}(x \dot{-} y) \rfloor = x \dot{-} s_0y]$,
$\vdash \neg(y = 0) \to ([y = 0 \wedge x = x \dot{-} s_0y] \vee [\neg(y = 0) \wedge \lfloor \frac{1}{2}(x \dot{-} y) \rfloor = x \dot{-} s_0y])$
By $(y = 0) \to [y = 0 \wedge x = x \dot{-} s_0y]$,
$\vdash (y = 0) \to ([y = 0 \wedge x = x \dot{-} s_0y] \vee [\neg(y = 0) \wedge \lfloor \frac{1}{2}(x \dot{-} y) \rfloor = x \dot{-} s_0y])$
By $(y = 0) \vee \neg(y = 0)$,
$\vdash [y = 0 \wedge x = x \dot{-} s_0y] \vee [\neg(y = 0) \wedge \lfloor \frac{1}{2}(x \dot{-} y) \rfloor = x \dot{-} s_0y])$

PV Axiom (5b)

$$\begin{aligned} z = x \dot{-} s_1y &\leftrightarrow x = z \boxplus s_1y + w \\ &\leftrightarrow x = z \cdot 2^{|s_1y| \cdot |1|} + w \\ &\leftrightarrow x = s_0z \cdot 2^{|y| \cdot |1|} + w \\ &\leftrightarrow x = (s_0z \boxplus y) + w \end{aligned}$$

$\leftrightarrow s_0 z = x \dot{-} y$
$\leftrightarrow z = \lfloor \frac{1}{2}(x \dot{-} y) \rfloor$

PV Axiom (6a)
By $(y = 0) \rightarrow [(y = 0 \wedge 1 = (x \# s_0 y)) \vee (\neg(y = 0) \wedge (x \# y) \boxplus x = (x \# s_0 y))]$,
$\neg(y = 0) \rightarrow [(y = 0 \wedge 1 = (x \# s_0 y)) \vee (\neg(y = 0) \wedge (x \# y) \boxplus x = (x \# s_0 y))]$
and $(y = 0) \vee \neg(y = 0)$,
$\vdash [(y = 0 \wedge 1 = (x \# s_0 y)) \vee (\neg(y = 0) \wedge (x \# y) \boxplus x = (x \# s_0 y))]$.

PV Axiom (6b) $x \# s_1 y = 2^{|x| \cdot (|y|+1)} = 2^{|x| \cdot |y|} \cdot 2^{|x|} \cdot 1 = (x \# y) \boxplus x$.

PV Axiom (7) $[\lambda x_1 \cdots x_n . t](x_1 \cdots x_n) = t[x_1/x_1] \cdots [x_n/x_n] = t$.

We prove $T \vdash$ IPV axioms (2)-(5) (def. 4.1.2).

IPV axiom (2)
By definition,
$\vdash (x \leq y) \rightarrow (x \leq y \wedge 0 = 0)$
$\rightarrow ([x \leq y \wedge 0 = 0] \vee [\neg(x \leq y) \wedge 0 = 1])$
$\rightarrow Lessequ(x, y) = 0$.
By $(x \leq y \wedge 0 = 0) \rightarrow x \leq y, (neg(x \leq y) \wedge 0 = 1) \rightarrow x \leq y$ and
$Lessequ(x, y) = 0 \rightarrow (x \leq y \wedge 0 = 0) \vee (neg(x \leq y) \wedge 0 = 1)$,
$\vdash Lessequ(x, y) = 0 \rightarrow x \leq y$.

IPV axiom (3) By (B.21).

IPV axiom (4) By definition of $Cond$.

IPV axiom (5) Let $A(x)$ be any formula of the form $(\exists y \leq t)u = v$. Then $A(x)$ is Σ_1^{b+} formula. By $\Sigma_1^{b+} - PIND, \vdash A(0) \wedge \forall x(A(\lfloor \frac{1}{2}x \rfloor) \rightarrow A(x)) \rightarrow \forall x A(x)$. Therefore $T \vdash$ NP-Induction .

We prove $T \vdash$ PV Axiom (8).

PV Axiom (8) By definition of $Lmin$, $\vdash Lmin(x, y) = z \rightarrow Cond(x \dot{-} y, x, y) = z$. By th. 2.4.8, there is an n+1-place function f which satisfies
$f(0, \vec{b}) = g(\vec{b})$
$a = 0 \vee f(a, \vec{b}) = Lmin[h(a, \vec{b}, f(\lfloor \frac{1}{2}a \rfloor), \vec{b}), k(a, \vec{b})]$.
By f and $Lmin$,
$\vdash (a = 0 \wedge g(\vec{b}) = f(a, \vec{b})) \vee (\neg(a = 0) \wedge Cond(t \dot{-} k(a, \vec{b}), t, k(a, \vec{b})))$,
where $t \stackrel{d}{\equiv} h(a, \vec{b}, f(\lfloor \frac{1}{2}a \rfloor), \vec{b})$.
Therefore
$T \vdash f(a, \vec{b}) = Cond(a, g(\vec{b}), Cond(t \dot{-} k(a, \vec{b}), t, k(a, \vec{b})))$.

Therefore $T \vdash$ PV axioms (8).
Therefore

$$\forall A \in L(IPV)[IPV \vdash A \Rightarrow T \vdash A].$$

By T which is conservative extension of IS_2^1,

3) $\forall A \in L(IS_2^1)[T \vdash A \Rightarrow IS_2^1 \vdash A]$.

By **1)** and **2)** ,

4) $\forall A \in L(IS_2^1)[IPV \vdash A \Rightarrow T \vdash A]$.

By **3)** and **4)** ,

$$\forall A \in L(IS_2^1)[IPV \vdash A \Rightarrow IS_2^1 \vdash A].$$

Therefore IPV is a conservative extension of IS_2^1. ∎

Chapter 5

The Typed λ Calculus

5.1 Definition

In this section we introduce the basic concepts of the typed λ-calculus which will be used in later section.

Definition 5.1.1 The *class* of type is defined as follows:

(1) 0 is type.

(2) $(\sigma \to \tau)$ is a type is σ and τ are types.

Definition 5.1.2 If $\tau = 0 \to 0 \to \cdots \to 0$, with at least one "$\to$",
then τ is a type **1 type**.

Definition 5.1.3 Let $\mathcal{F}$ be a collection of function symbols (of any types). The collection of λ-term generated from $\mathcal{F}$, denoted $\Lambda(\mathcal{F})$, is defined as follows :

(1) There are infinitely many variables $X^\sigma, Y^\sigma, Z^\sigma, \cdots$ for each type σ , and each such variable is a term of type σ ;

(2) Every function symbol in $\mathcal{F}$ of type σ is a term of type σ ;

(3) If T is a term of type τ and X is a variable of type σ , then $(\lambda X.T)$ is a term of type $(\sigma \to \tau)$ (**abstraction**);

(4) If S is a term of type $(\sigma \to \tau)$ and T is a term of type σ , then (ST) is a term of type τ (**application**).

Definition 5.1.4 *Subterm* is defined as follows :

(1) P is a subterm of P.

(2) If P is a subterm of M or N,then P is a subterm of (MN).

(3) If P is a subterm of M or $P \equiv x$,then P is a subterm of $(\lambda x.M)$.

Definition 5.1.5 The *free occurrence* and *bounded occurrence* of a variable x in a term t are defined inductively as follows :

(1) if t is the variable x, then the occurrence of x in t is free ;

(2) if $t = MN$, then the free occurrences of x in t are those of x in M and N ;

(3) if $t = \lambda y.M$, then the free occurrences of x in t are those of x in M, except if $x = y$; in that case, occurrence of x in t is bounded.

Definition 5.1.6
A *free variable* in t is a variable which has at least one free occurrence in t.
A *bounded variable* in t is a variable which occurs in t just after the symbol λ.
Let M be a term. Then $FV(M)$ is set of free variables in M. $BV(M)$ is set of bounded variables in M. A term which has no free variable is called a *closed term*.

Definition 5.1.7 If S and T are terms of types σ and τ, and X is a variable of type τ , then $S[T/X]$ is defined to be the terms of type τ which results from S by substituting T for all free occurrences of X in S. The rules of substitution are defined as follows ;

(1) $x[N/x] \equiv N$

(2) $y[N/x] \equiv y \quad if \;\; x \neq y$

(3) $(PQ)[N/x] \equiv (P[N/x])(Q[N/x])$

(4) $(\lambda x.P)[N/x] \equiv \lambda x.P$

(5) $(\lambda y.P)[N/x] \equiv \lambda y.(P[N/x]) \quad if \;\; y \not\equiv x \text{ , } and \;\; y \notin FV(N) \;\; or \;\; x \notin FV(P)$

(6) $(\lambda y.P)[N/x] \equiv \lambda z.(P[z/y][N/x]) \quad if \;\; y \not\equiv x, and \;\; y \in FV(N) \;\; and \;\; x \in FV(P)$

Definition 5.1.8 A term of the from $(\lambda X.S)T$ is said to be a **β redex**, and the term $S[T/X]$ is its **contractum**. A term of the form $(\lambda X.TX)$ such that X has no free occurrence in T is said to be an **η redex** and the term T is its **contractum**. A term S contracts to a term T if T is obtained from S by replacing a β or η redex in S by its contractum. A *term S reduces to a term T* if T is obtained from S by a finite sequence of contractions and changes of bound variable. The rules of *$\beta\eta$-contraction*($1\beta\eta$-*reduction*) and *$\beta\eta$-reduction* are defined as follows ;

(1) $(\lambda X.M)N \overset{1\beta\eta}{\to} M[N/X]$

(2) $(\lambda X.TX) \overset{1\beta\eta}{\to} T$

(3) If $M \overset{1\beta\eta}{\to} N$, then $ZM \overset{1\beta\eta}{\to} ZN, MZ \overset{1\beta\eta}{\to} NZ \;\; and \;\; \lambda X.M \overset{1\beta\eta}{\to} \lambda X.N$

(4) $M \overset{\beta\eta}{\to} M$

(5) If $M \overset{1\beta\eta}{\to} N$, then $M \overset{\beta\eta}{\to} N$

(6) $M \overset{\beta\eta}{\to} L, L \overset{\beta\eta}{\to} N \Rightarrow M \overset{\beta\eta}{\to} N$

$P \overset{1\beta\eta}{\to} Q : P$ *$\beta\eta$- contracts to* Q (P *$\beta\eta$-reduces to* Q *in one step*)
$P \overset{\beta\eta}{\to} Q : P$ *$\beta\eta$-reduces to* Q

Definition 5.1.9

(1) A term T is in *normal form* if T has no redex.

(2) $NF(T)$ denotes a particular term in normal form such that T reduces to $NF(T)$. (The choice of $NF(T)$ is unique up to changes in bound variables).

Definition 5.1.10 Rules of *parallel $\beta\eta$-reduction* are defined as follows ;

(1) $x \overset{\beta\eta}{\Rightarrow} x$

(2) If $P \overset{\beta\eta}{\Rightarrow} Q$, then $\lambda x.P \overset{\beta\eta}{\Rightarrow} \lambda x.Q$

(3) If $P_i \overset{\beta\eta}{\Rightarrow} Q_i$ $(i = 1, 2)$, then $P_1P_2 \overset{\beta\eta}{\Rightarrow} Q_1Q_2$

(4) If $P_i \overset{\beta\eta}{\Rightarrow} Q_i$ $(i = 1, 2)$, then $(\lambda x.P_1)P_2 \overset{\beta\eta}{\Rightarrow} Q_1[Q_2/x]$

(5) If $P \overset{\beta\eta}{\Rightarrow} Q$ and $x \notin FV(P)$, then $\lambda x.Px \overset{\beta\eta}{\Rightarrow} Q$.

Definition 5.1.11 Rules of *length of term* are defined as follows.

(1) If x is a variable or constant 0, then $lgh(x) = 1$

(2) $lgh(MN) = lgh(M) + lgh(N)$

(3) $lgh(\lambda x.M) = 1 + lgh(M)$

5.2 Some theorems

Next two theorems are used to prove *Church-Rosser Theorem*.

Theorem 5.2.1 If $P_i \stackrel{\beta\eta}{\Rightarrow} Q_i$ $(i = 1, 2)$, then $P_1[P_2/y] \stackrel{\beta\eta}{\Rightarrow} Q_1[Q_2/y]$.

(*proof*) Assume $P_i \stackrel{\beta\eta}{\Rightarrow} Q_i$ $(i = 1, 2)$. Then we prove by induction on length of term.

(1) $lgh(P_1) = 1$ (base step).
Then P_1 is constant 0 or variable x. $P_1 \equiv 0$ is obvious. Therefore We assume $P_1 \equiv x$. Then $Q_1 \equiv x$, too.

(a) $x \equiv y$
Then $P_1[P_2/y] \equiv P_2$ and $Q_1[Q_2/y] \equiv Q_2$. By $P_2 \stackrel{\beta\eta}{\Rightarrow} Q_2$, $P_1[P_2/y] \stackrel{\beta\eta}{\Rightarrow} Q_1[Q_2/y]$.

(b) $x \not\equiv y$
Then $P_1[P_2/y] \equiv x$ and $Q_1[Q_2/y] \equiv x$.
By definition of $\stackrel{\beta\eta}{\Rightarrow}$, $P_1[P_2/y] \stackrel{\beta\eta}{\Rightarrow} Q_1[Q_2/y]$.

(2) Let if $lgh(P_1'') = n$ and $P_i'' \stackrel{\beta\eta}{\Rightarrow} Q_i''$ $(i = 1, 2)$, then $P_1''[P_2''/y] \stackrel{\beta\eta}{\Rightarrow} Q_1''[Q_2''/y]$ (induction step).

Assume $lgh(P_1) = n + 1$ and $P_i \stackrel{\beta\eta}{\Rightarrow} Q_i$ $(i = 1, 2)$.

(a) $P_1 \equiv \lambda x.P_1'$
Then Q_1 which satisfies $P_1 \stackrel{\beta\eta}{\Rightarrow} Q_1$ is $Q_1 \equiv \lambda x.Q_1'$, where $P_1' \stackrel{\beta\eta}{\Rightarrow} Q_1'$.

i. $x \equiv y$
Then $P_1[P_2/y] \equiv (\lambda x.P_1')[P_2/y] \equiv (\lambda x.P_1') \equiv P_1$ and
$Q_1[Q_2/y] \equiv (\lambda x.Q_1')[Q_2/y] \equiv (\lambda x.Q_1') \equiv Q_1$.
By induction hypothesis, $P_1[P_2/y] \stackrel{\beta\eta}{\Rightarrow} Q_1[Q_2/y]$.

ii. $x \not\equiv y$, *and* $y \notin FV(P_2)$ *or* $x \notin FV(P_1)$
By $lgh(P_1') = n$ and $P_2 \stackrel{\beta\eta}{\Rightarrow} Q_2$, we can use induction hypothesis.
Therefore $P_1'[P_2/y] \stackrel{\beta\eta}{\Rightarrow} Q_1'[Q_2/y]$.
By definition of $\stackrel{\beta\eta}{\Rightarrow}$, $\lambda x(P_1'[P_2/y]) \stackrel{\beta\eta}{\Rightarrow} \lambda x(Q_1'[Q_2/y])$.
Therefore $(\lambda x.P_1')[P_2/y] \stackrel{\beta\eta}{\Rightarrow} (\lambda x.Q_1')[Q_2/y]$.

iii. $y \not\equiv x$, *and* $y \in FV(P_2)$ *and* $x \in FV(P_1)$
Then $P_1[P_2/y] \equiv (\lambda x.P_1')[P_2/y] \equiv (\lambda z.(P_1'[z/x])[P_2/y])$.
By $lgh(P_1') = n$ and $z \stackrel{\beta\eta}{\Rightarrow} z$, $P_1'[z/x] \stackrel{\beta\eta}{\Rightarrow} Q_1'[z/x]$.
By $lgh(P_1'[z/x]) = n$ and $P_2 \stackrel{\beta\eta}{\Rightarrow} Q_2$, we can use induction hypothesis.
Therefore $P_1'[z/x][P_2/y] \stackrel{\beta\eta}{\Rightarrow} Q_1'[z/x][Q_2/y]$.
Hence $\lambda z.(P_1'[z/x][P_2/y]) \stackrel{\beta\eta}{\Rightarrow} \lambda z.(Q_1'[z/x][Q_2/y])$.
Therefore $P_1[P_2/y] \stackrel{\beta\eta}{\Rightarrow} Q_1[Q_2/y]$.

(b) $P_1 \equiv P_1' P_1''$

Then $Q_1 \equiv Q_1' Q_1''$, where $P_1' \overset{\beta\eta}{\Rightarrow} Q_1'$, $P_1'' \overset{\beta\eta}{\Rightarrow} Q_1''$, $lgh(P_1') \leq n$ and $lgh(P_1'') \leq n$.
Then $P_1[P_2/y] \equiv (P_1' P_1'')[P_2/y] \equiv (P_1'[P_2/y])(P_1''[P_2/y])$.
By these and $P_2 \overset{\beta\eta}{\Rightarrow} Q_2$, $P_1'[P_2/y] \overset{\beta\eta}{\Rightarrow} Q_1'[Q_2/y]$ and $P_1''[P_2/y] \overset{\beta\eta}{\Rightarrow} Q_1''[Q_2/y]$.
By definition of $\overset{\beta\eta}{\Rightarrow}$, $(P_1'[P_2/y])(P_1''[P_2/y]) \overset{\beta\eta}{\Rightarrow} (Q_1'[P_2/y])(Q_1''[P_2/y])$.
By $(Q_1'[P_2/y])(Q_1''[P_2/y]) \equiv (Q_1' Q_1'')[P_2/y] \equiv Q_1[P_2/y]$, $P_1[P_2/y] \overset{\beta\eta}{\Rightarrow} Q_1[Q_2/y]$.

∎

Theorem 5.2.2 $M \overset{\beta\eta}{\rightarrow} N$ and $M \overset{\beta\eta}{\Rightarrow} N$ are equivalent.

(*proof*)

(1) First we prove if $M \overset{\beta\eta}{\rightarrow} N$ then $M \overset{\beta\eta}{\Rightarrow} N$
We prove by induction on length of term M.

(a) $lgh(M) = 1$ (base step).

Then M is a variable. Let $M \equiv x$. Then by definition of $\overset{\beta\eta}{\rightarrow}$, $N \equiv x$.
By $x \overset{\beta\eta}{\Rightarrow} x$, $M \overset{\beta\eta}{\Rightarrow} N$.

(b) Let if $lgh(M') = n$ and $M' \overset{\beta\eta}{\rightarrow} N'$, then $M' \overset{\beta\eta}{\Rightarrow} N'$.

Assume $lgh(M) = n + 1$ and $M \overset{\beta\eta}{\rightarrow} N$.

i. $M \equiv \lambda x.M_1$.

$n + 1 = lgh(M) = lgh(\lambda x.M_1) = lgh(M_1) + 1$. Hence $lgh(M_1) = n$. And N which satisfies $M \overset{\beta\eta}{\rightarrow} N$ is $\lambda x.N_1$, where $M_1 \overset{\beta\eta}{\rightarrow} N_1$. By $lgh(M_1) = n$ and induction hypothesis, $M_1 \overset{\beta\eta}{\Rightarrow} N_1$. By definition of $\overset{\beta\eta}{\Rightarrow}$, $\lambda x.M_1 \overset{\beta\eta}{\Rightarrow} \lambda x.N_1$.
Therefore $M \overset{\beta\eta}{\Rightarrow} N$.

ii. $M \equiv (\lambda x.M_1)M_2$.

Then N which satisfies $M \overset{\beta\eta}{\rightarrow} N$ is under three patterns.

($\spadesuit$) $N \equiv (\lambda x.N_1)M_2$, where $M_1 \overset{\beta\eta}{\rightarrow} N_1$
($\blacklozenge$) $N \equiv (\lambda x.M_1)N_2$, where $M_2 \overset{\beta\eta}{\rightarrow} N_2$
($\clubsuit$) $N \equiv M_1[M_2/x]$.

CASE ($\spadesuit$)

By $lgh(M) = lgh(M_1) + lgh(M_2) + 1 = n + 1$, $lgh(M_1) \leq n$.
Hence by $lgh(M_1) \leq n$, $M_1 \overset{\beta\eta}{\rightarrow} N_1$ and induction hypothesis, $M_1 \overset{\beta\eta}{\Rightarrow} N_1$.
By definition of $\overset{\beta\eta}{\Rightarrow}$, $(\lambda x.M_1)M_2 \overset{\beta\eta}{\Rightarrow} (\lambda x.N_1)M_2$.
Therefore $M \overset{\beta\eta}{\Rightarrow} N$.

CASE ($\blacklozenge$)

Same as ($\spadesuit$).

CASE (♣)

By $lgh(M_1) \leq n$, $lgh(M_2) \leq n$, $M_1 \stackrel{\beta\eta}{\rightarrow} M_1$ and $M_2 \stackrel{\beta\eta}{\rightarrow} M_2$, we can use induction hypothesis. Therefore $M_1 \stackrel{\beta\eta}{\Rightarrow} M_1$ and $M_2 \stackrel{\beta\eta}{\Rightarrow} M_2$. By these and definition of $\stackrel{\beta\eta}{\Rightarrow}$, $(\lambda x.M_1)M_2 \stackrel{\beta\eta}{\Rightarrow} M_1[M_2/x]$.

Therefore $M \stackrel{\beta\eta}{\Rightarrow} N$.

iii. $M \equiv M_1M_2$, where $M_1 \not\equiv \lambda x.M'$.

Then N which satisfies $M \stackrel{\beta\eta}{\rightarrow} N$ is under two patterns.

(♠) $N \equiv N_1M_2$,where $M_1 \stackrel{\beta\eta}{\rightarrow} N_1$

(♣) $N \equiv M_1N_2$,where $M_2 \stackrel{\beta\eta}{\rightarrow} N_2$

CASE (♠)

By $n+1 = lgh(M) = lgh(M_1) + lgh(M_2)$ and $0 < lgh(M_i)$, $lgh(M_i) \leq n$. By $lgh(M_1) \leq n$ and $M_1 \stackrel{\beta\eta}{\rightarrow} N_1$, we can use induction hypothesis. Therefore $M_1 \stackrel{\beta\eta}{\Rightarrow} N_1$. By these and definition of $\stackrel{\beta\eta}{\Rightarrow}$, $M_1M_2 \stackrel{\beta\eta}{\Rightarrow} N_1M_2$.

Therefore $M \stackrel{\beta\eta}{\Rightarrow} N$.

CASE (♣)

Same as (♠).

(2) We prove if $M \stackrel{\beta\eta}{\Rightarrow} N$ then $M \stackrel{\beta\eta}{\rightarrow} N$.

(a) $lgh(M) = 1$ (base step).

Then M is a variable. Let $M \equiv x$. Then by definition of $\stackrel{\beta\eta}{\Rightarrow}$, $N \equiv x$.

By $x \stackrel{\beta\eta}{\rightarrow} x$, $M \stackrel{\beta\eta}{\rightarrow} N$.

(b) Let if $lgh(M') = n$ and $M' \stackrel{\beta\eta}{\Rightarrow} N'$, then $M' \stackrel{\beta\eta}{\rightarrow} N'$.

Assume $lgh(M) = n+1$ and $M \stackrel{\beta\eta}{\Rightarrow} N$.

i. $M \equiv \lambda x.M_1$.

$n+1 = lgh(M) = lgh(\lambda x.M_1) = lgh(M_1) + 1$. Hence $lgh(M_1) = n$. And N which satisfies $M \stackrel{\beta\eta}{\Rightarrow} N$ is $\lambda x.N_1$, where $M_1 \stackrel{\beta\eta}{\Rightarrow} N_1$. By $lgh(M_1) = n$ and induction hypothesis, $M_1 \stackrel{\beta\eta}{\rightarrow} N_1$. By definition of $\stackrel{\beta\eta}{\rightarrow}$, $\lambda x.M_1 \stackrel{\beta\eta}{\rightarrow} \lambda x.N_1$.

Therefore $M \stackrel{\beta\eta}{\rightarrow} N$.

ii. $M \equiv (\lambda x.M_1)M_2$.

Then N which satisfies $M \stackrel{\beta\eta}{\Rightarrow} N$ is under two patterns.

(♠) $N \equiv (\lambda x.N_1)N_2$, where $M_i \stackrel{\beta\eta}{\Rightarrow} N_i$.

(♣) $N \equiv N_1[N_2/x]$, where $M_i \stackrel{\beta\eta}{\Rightarrow} N_i$.

CASE (♠)

By $lgh(M) = lgh(M_1) + lgh(M_2) + 1 = n+1$, $lgh(M_i) \leq n$.

Hence by $lgh(M_i) \leq n$, $M_i \stackrel{\beta\eta}{\Rightarrow} N_i$ and induction hypothesis, $M_i \stackrel{\beta\eta}{\rightarrow} N_i$.

By $M_1 \overset{\beta\eta}{\to} N_1$, $(\lambda x.M_1)M_2 \overset{\beta\eta}{\to} (\lambda x.N_1)M_2$.
By $M_2 \overset{\beta\eta}{\to} N_2$, $(\lambda x.N_1)M_2 \overset{\beta\eta}{\to} (\lambda x.N_1)N_2$.
By $(\lambda x.M_1)M_2 \overset{\beta\eta}{\to} (\lambda x.N_1)M_2$ and $(\lambda x.N_1)M_2 \overset{\beta\eta}{\to} (\lambda x.N_1)N_2$,
$(\lambda x.M_1)M_2 \overset{\beta\eta}{\to} (\lambda x.N_1)N_2$.
Therefore $M \overset{\beta\eta}{\to} N$.

CASE (♣)
By same method as (♠), $(\lambda x.M_1)M_2 \overset{\beta\eta}{\to} (\lambda x.N_1)N_2$.
By this and $(\lambda x.N_1)N_2 \overset{\beta\eta}{\to} N_1[N_2/x]$, $(\lambda x.M_1)M_2 \overset{\beta\eta}{\to} N_1[N_2/x]$.
Therefore $M \overset{\beta\eta}{\to} N$.

iii. $M \equiv M_1M_2$, where $M_1 \not\equiv \lambda x.M'$.
Then N which satisfies $M \overset{\beta\eta}{\Rightarrow} N$ is N_1N_2, where $M_i \overset{\beta\eta}{\Rightarrow} N_i$.
By $n+1 = lgh(M) = lgh(M_1) + lgh(M_2)$ and $0 < lgh(M_i)$, $lgh(M_i) \leq n$.
By $lgh(M_i) \leq n$ and $M_i \overset{\beta\eta}{\to} N_i$, we can use induction hypothesis.
Therefore $M_i \overset{\beta\eta}{\to} N_i$.
By these and definition of $\overset{\beta\eta}{\to}$, $M_1M_2 \overset{\beta\eta}{\to} N_1M_2$ and $N_1M_2 \overset{\beta\eta}{\to} N_1N_2$.
Hence $M_1M_2 \overset{\beta\eta}{\to} N_1N_2$.
Therefore $M \overset{\beta\eta}{\to} N$.

∎

Theorem 5.2.3 (**Church-Rosser Theorem**)
If S reduces to T and S reduces to T' then there is a term T'' such that both T and T' reduce to T''.

(*proof*) First we prove that
for any term M there exists term M'' such that

$$\forall M'(\text{if } M \overset{\beta\eta}{\Rightarrow} M', \text{ then } M' \overset{\beta\eta}{\Rightarrow} M''). \cdots\cdots(\alpha)$$

We define M^* as follows.

(1) If $M \equiv x$, then $M^* \equiv x$,

(2) if $M \equiv \lambda x.M_1$, then $M^* \equiv \lambda x.M_1^*$,

(3) if $M \equiv M_1M_2$ and $M_1 \not\equiv \lambda x.M_3$, then $M^* \equiv M_1^*M_2^*$,

(4) if $M \equiv (\lambda x.M_1)M_2$, then $M^* \equiv M_1^*[M_2^*/x]$.

Then we prove that M^* satisfies conditions of M'' by induction on complexity of M.

(1) $M \equiv x$.
Then by $M' \equiv x \equiv M^*$, $M' \overset{\beta\eta}{\Rightarrow} M^*$ is obvious.

(2) $M \equiv \lambda x.M_1$.

Then there exists M_1' such that $M' \equiv \lambda x.M_1'$, where $M_1 \overset{\beta\eta}{\Rightarrow} M_1'$. Then by induction hypothesis $M_1' \overset{\beta\eta}{\Rightarrow} M_1^*$, $\lambda x.M_1' \overset{\beta\eta}{\Rightarrow} \lambda x.M_1^*$.

Therefore $M' \overset{\beta\eta}{\Rightarrow} M^*$.

(3) $M \equiv M_1 M_2$, where $M_1 \not\equiv \lambda x.M_3$.

Then there exist M_i' $(i = 1, 2)$ such that $M' \equiv M_1' M_2'$ and $M_i \overset{\beta\eta}{\Rightarrow} M_i'$. Then by induction hypothesis $M_i' \overset{\beta\eta}{\Rightarrow} M_i^*$, $M_1' M_2' \overset{\beta\eta}{\Rightarrow} M_1^* M_2^*$.

Therefore $M' \overset{\beta\eta}{\Rightarrow} M^*$.

(4) $M \equiv (\lambda x.M_1)M_2$.

By definition of $\overset{\beta\eta}{\Rightarrow}$, there exist M_i' $(i = 1, 2)$ which satisfy $M_i \overset{\beta\eta}{\Rightarrow} M_i'$ such that

($\spadesuit$) $M' \equiv (\lambda x.M_1')M_2'$

or

($\clubsuit$) $M' \equiv M_1'[M_2'/x]$.

CASE ($\spadesuit$)

By induction hypothesis $M_i' \overset{\beta\eta}{\Rightarrow} M_i^*$ and definition of $\overset{\beta\eta}{\Rightarrow}$(4), $M' \overset{\beta\eta}{\Rightarrow} M_1'[M_2'/x]$.

Therefore $M' \overset{\beta\eta}{\Rightarrow} M^*$.

CASE ($\clubsuit$)

By induction hypothesis and theorem 5.2.1, $M' \overset{\beta\eta}{\Rightarrow} M_1'[M_2'/x]$.

Therefore $M' \overset{\beta\eta}{\Rightarrow} M^*$.

Hence we proved (α). By (α) and theorem 5.2.2, *Church-Rosser Theorem* is obvious. ∎

Next two definition, five notes and three theorems are used to prove *Strong Normalization Theorem.*

Definition 5.2.4 strongly normalizable (SN) terms
A term M is *strongly normalizable* iff all reductions starting at M are finite. It is *normalizable* iff reduces to a normal form.

Definition 5.2.5 strongly computable (SC) terms
For term, *strongly computable* is defined by induction on the number of occurrence of $\rightarrow$ in the term's type :

(1) A term of type 0 is *SC* iff it is SN.

(2) A term $M^{\alpha\rightarrow\beta}$ is *SC* iff, for all SC term N^{α}, the term $(MN)^{\beta}$ is SC.

Note 5.2.6 Each type α can be written in a unique way in the form $\alpha_1 \rightarrow \cdots \rightarrow \alpha_n \rightarrow 0$.

Note 5.2.7 Let $\alpha \equiv \alpha_1 \to \cdots \to \alpha_n \to 0$. Then M^α is SC iff, for all SC terms $M_1^{\alpha_1}, \cdots, M_n^{\alpha_n}$, $(MM_1 \cdots M_n)^0$ is SC iff it is SN. And $(MM_1 \cdots M_n)^0$ is SC iff it is SN.

Note 5.2.8 If M^α is SC, then every term which differs from M^α only by changes of bound variables is SC. And the same holds for SN.

Note 5.2.9 If $M^{\alpha\to\beta}$ is SC and N^α is SC, then $(MN)^\beta$ is SC.

Note 5.2.10 If M^α is SN, then every subterm of M^α is SN, because any infinite reduction from a subterm from a of M gives rise to an infinite reduction M.

Theorem 5.2.11 Let α be any type.

(1) Every term $(aM_1 \cdots M_n)^\alpha$, where a is type 0 and $M_1, \cdots, M_n$ are all SN, is SC.

(2) Every SC term of type α is SN.

(*proof*) We prove by induction on the number of occurrence of $\to$ in α. And we define $|\alpha|$ as the number of occurrence of $\to$ in α.
base step α is 0.

(1) Then $(aM_1 \cdots M_n)^0$ is SN because a is type 0 and $M_1, \cdots, M_n$ are SN. Therefore $(aM_1 \cdots M_n)^0$ is SC because α is type 0 and definition 5.2.5 (1).

By a : type 0 and $M_1, \cdots, M_n$: SN, $(aM_1 \cdots M_n)^0$ is SN. By α : type 0 and definition 5.2.5 (1), $(aM_1 \cdots M_n)^0$ is SC.

(2) Let M be type 0 SC term. Then by definition 5.2.5 (1), M is SN term.

(induction step) Assume that if $|\alpha'| \leq m$ then (1) and (2) are true. And $|\alpha| = m + 1$ and α is $\beta \to \gamma$.

(1) Let N^β be any SC term. By induction hypothesis of (2), N^β is SN and so $(aM_1 \cdots M_n N)^\gamma$ is SN. By $|\gamma| \leq m$ and induction hypothesis of (2), $(aM_1 \cdots M_n N)^\gamma$ is SC.
Therefore by definition 5.2.5 (2), $(aM_1 \cdots M_n)$ is SC.

(2) Let term M^α be SC and a variable m^β which is not contained in M^α. By induction hypothesis of (1), m is SC. By this and Note 5.2.9, $(Mm)^\gamma$ is SC. By induction hypothesis of (2), $(Mm)^\gamma$ is SN. Therefore by Note 5.2.10, M^α is SN.

∎

Theorem 5.2.12 If $M^\beta[N^\alpha/x^\alpha]$ is SC, then $(\lambda x^\alpha.M^\beta)N^\alpha$ is SC; provided that N^α is SC if x^α is not free in M^β.

(*proof*) Let β be $\beta_1 \to \cdots \to \beta_n \to 0$ and $M_1^{\beta_1}, \cdots, M_n^{\beta_n}$ be SC terms.
$([N/x]M)M_1 \cdots M_n)^0$ is SN because $M^\beta[N^\alpha/x^\alpha]$ is SC and by Note 5.2.7.

(1) x is not contained in M.
By induction, N is SC. By theorem 5.2.11, N is SN. And subterms of $(([N/x]M)M_1 \cdots M_n)^0$ are SN. Hence $M, M_1, \cdots, M_n$ and N do not have infinite reduction.
Therefore $((\lambda x.M)NM_1 \cdots M_n)$ do not have infinite reduction.

(2) x is contained in M.
Assume $((\lambda x.M)NM_1 \cdots M_n)$ has an infinite reduction.

(a) $M \overset{\beta\eta}{\to} M'$ or $N \overset{\beta\eta}{\to} N'$ or $M_i \overset{\beta\eta}{\to} M_i'$ is infinite reduction.
Then we can construct an infinite reduction from $(([N/x]M)M_1 \cdots M_n)$:

$$\begin{aligned}(([N/x]M)M_1 \cdots M_n) &\overset{\beta\eta}{\to} (([N'/x]M')M_1' \cdots M_n') \\ &\overset{\beta\eta}{\to} \cdots \quad .\end{aligned}$$

This contradicts that $(([N/x]M)M_1 \cdots M_n)$ is SN.

(b) $M \overset{\beta\eta}{\to} M'$ and $N \overset{\beta\eta}{\to} N'$ and $M_i \overset{\beta\eta}{\to} M_i'$ are finite reductions. And $x \in FV(M)$.
Then by induction, there is an infinite reduction such that

$$\begin{aligned}((\lambda x.M)NM_1 \cdots M_n) &\overset{\beta\eta}{\to} ((\lambda x.M')N'M_1' \cdots M_n') \\ &\overset{1\beta\eta}{\to} (([N'/x]M')M_1' \cdots M_n') \\ &\overset{\beta\eta}{\to} \cdots \quad .\end{aligned}$$

Then there exists an infinite reduction such that

$$\begin{aligned}(([N/x]M)M_1 \cdots M_n) &\overset{\beta\eta}{\to} (([N'/x]M')M_1' \cdots M_n') \\ &\overset{\beta\eta}{\to} \cdots \quad .\end{aligned}$$

This contradicts that $(([N/x]M)M_1 \cdots M_n)$ is SN.

(c) $M \overset{\beta\eta}{\to} M'$ and $N \overset{\beta\eta}{\to} N'$ and $M_i \overset{\beta\eta}{\to} M_i'$ are finite reductions. And $x \notin FV(M)$.

$$\begin{aligned}((\lambda x.M)NM_1 \cdots M_n) &\overset{\beta\eta}{\to} ((\lambda x.M')N'M_1' \cdots M_n') \\ &\equiv ((\lambda x.M'x)N'M_1' \cdots M_n') \\ &\overset{1\beta\eta}{\to} M'N'M_1' \cdots M_n' \\ &\overset{\beta\eta}{\to} \cdots \quad .\end{aligned}$$

Then there exists an infinite reduction such that

$$\begin{aligned}(([N/x]M)M_1 \cdots M_n) &\overset{\beta\eta}{\to} (([N'/x]M')M_1' \cdots M_n') \\ &\overset{\beta\eta}{\to} \cdots \quad .\end{aligned}$$

This contradicts that $(([N/x]M)M_1 \cdots M_n)$ is SN.

Hence an assumption which $((\lambda x.M)NM_1 \cdots M_n)$ has an infinite reduction, contradicts. Therefore $((\lambda x.M)NM_1 \cdots M_n)$ has no infinite reduction.

∎

Theorem 5.2.13 For every term M^β:

(1) For all $x_1^{\alpha_1}, \cdots, xn^{\alpha_n}$ and for all SC terms $N_1^{\alpha_1}, \cdots, Nn^{\alpha_n}$, the term $M^{*\beta} \equiv M[N_1/x_1] \cdots [N_n/x_n]$ is SC.

(2) M^β is SC.

(*proof*)

(1) We prove by induction on the construction of M.

(a) $M \equiv x_i$
Then $M^* \equiv N_i$. By N_i : SC, M^* is SC.

(b) M is a variable distinct from $x_1, \cdots, x_n$.
Then $M^* \equiv M$. By theorem 5.2.11, M^* is SC.

(c) $M \equiv M_1 M_2$, where M_1^* and M_2^* are SC.
Then $M^* \equiv (M_1 M_2)[N_1/x_1] \cdots [N_n/x_n]$
$\equiv (M_1[N_1/x_1] \cdots [N_n/x_n])(M_2[N_1/x_1] \cdots [N_n/x_n])$
$\equiv M_1^* M_2^*$. By Note 5.2.9, $M_1^* M_2^*$ is SC. Therefore M^* is SC.

(d) $M^\beta \equiv \lambda x^\gamma . M_1^\delta$, where M_1^* is SC. Then
$$M^* \equiv \lambda x . M_1^*$$
if we neglect changes in bound variables.
Let N^γ be any SC term. Then $M^* N \equiv (\lambda x . M_1^*) N \overset{1\beta\eta}{\to} M_1^*[N/x]$. By M_1^* and N be SC, $M_1^*[N/x]$ is SC. By theorem 5.2.12, $\lambda x . M_1^*$ is SC.

(2) By (1), (2) is obvious.

∎

Theorem 5.2.14 (**Strong Normalization Theorem**)
Every sequence of contractions of a term T terminates with a term in normal form.

(*proof*) By theorem 5.2.13 (2), all terms are SC. By theorem 5.2.11 (2), all terms are SN. Therefore we can prove Strong Normalization Theorem. ∎

Theorem 5.2.15 Let $\mathcal{F}$ be a collection of function symbols of types 0 and 1. Let t be a term of type 0 in $Lambda(\mathcal{F})$ in which all free variables have type 0. Then $NF(t)$ has no occurrence of λ, and hence all subterms have type 0 or type 1.

(*proof*) Assume that $NF(t)$ has a left-most subterm of the form $\lambda X.S$.

(1) $NF(t) \equiv \lambda X.S$
Then type of $NF(t)$ is $\alpha \to \beta$. This contradicts that $NF(t)$ is type 0. There cannot be this.

(2) $NF(t) \equiv (\lambda X.S)U$
$NF(t)$ is normal form. Hence $NF(t)$ should be the form of $S[U/X]$. Therefore there cannot be this.

(3) $NF(t) \equiv \lambda Y.(\lambda X.S)$
his contradicts that $NF(t)$ has a left-most subterm of the form $\lambda X.S$. Therefore there cannot be this.

(4) $NF(t) \equiv U(\lambda X^{\alpha}.S^{\beta})$, where U does not contain λ.
Then type of U is $(\alpha \to \beta) \to 0$. Hence U cannot be only variable. If U contains function symbols, one of function symbols has a type of $\cdots \to (\alpha \to \beta) \to 0$. This type is distinct 0 and 1. Therefore there cannot be this.

Therefore $NF(t)$ has no λ.

∎

Chapter 6

The System PV^ω

We now extend the system PV to a system PV^ω by adding variables of all finite types. We need only one constant in addition to these in PV, namely the *recursor* $\mathcal{R}$. This is used to introduce higher type functions by limited recursion on notation. Main theorem of this chapter is to prove that PV^ω is conservative extension of PV.

6.1 Definition

Definition 6.1.1 The *function symbols* of PV^ω are defined as follows:

(1) For each $n \geq 0$ each n-place function symbol of PV is a function symbol of PV^ω of type $0 \to 0 \cdots \to 0$ (n+1 zeros).

(2) The Constant $\mathcal{R}$ is a function symbol of PV^ω of type
$0 \to (0 \to 0 \to 0) \to (0 \to 0) \to 0 \to 0$.

Definition 6.1.2 The *terms* of PV^ω comprise the set $\Lambda(\mathcal{F})$ (see Definition 5.1.3), where $\mathcal{F}$ is the set of function symbols given in definition 6.1.1 .

Notation 6.1.3 $S\{T\}$ refers to a term with a distinguished occurrence of a subterm T. Then $S\{U\}$ means $S\{T\}$ with the indicated occurrence of T replaced by U. In general T and U may have free variables which become bound in $S\{T\}$ and $S\{U\}$.

Definition 6.1.4 The *formulas* of PV^ω are all equations $s = t$, where s, t are type 0 terms of PV^ω.

Definition 6.1.5 The *axioms* of PV^ω are defined as follows :

(1) All axioms of PV

(2) (**HTLRN**)

$$\mathcal{R}(y, Z, W, x) = \begin{cases} if \;\; x = 0 \;\; then \;\; y \\ \quad else \\ Cond(t \dot{-} W(x), t, W(x)) \end{cases}$$

where

$$t \stackrel{d}{\equiv} Z(x, \mathcal{R}(y, Z, W, \lfloor \tfrac{1}{2}x \rfloor))$$

and the variables

$$x, y : type\ 0$$
$$Z : type\ 0 \to 0 \to 0$$
$$W : type\ 0 \to 0$$

(3) **(α)** $s\{\lambda X.T\} = s\{\lambda Y.T[Y/X]\}$, provided Y does not occur free in T.

(4) **(β)** $s\{(\lambda X.T)U\} = s\{T[U/X]\}$.

(5) **(η)** $s\{(\lambda X.TX)\} = s\{T\}$, provided X does not occur free in T.

Definition 6.1.6 The *rules of infernce* of PV^ω are defined as follows :

$(R1^\omega) s = t \vdash t = s$

$(R2^\omega) s = t, t = u \vdash s = u$

$(R3^\omega) s = t \vdash u\{s\} = u\{t\}$

$(R4^\omega) s = t \vdash s[T/X] = t[T/X]$

$(R5^\omega)$
$$\frac{t_1[0/x] = t_2[0/x] \quad t_1[s_0x/x] = v_0[t_1/a] \quad t_2[s_0x/x] = v_0[t_2/a] \quad t_1[s_1x/x] = v_1[t_1/a] \quad t_2[s_1x/x] = v_1[t_2/a]}{t_1 = t_2}$$

where t_1, t_2, v_0 and v_1 are terms of type 0.

6.2 Conservative extension of PV

Proposition 6.2.1

$PV^\omega \vdash s\{T\} = s\{NF(T)\}$
$PV^\omega \vdash s = NF(s)$

(*proof*) We prove by induction on the complexity of the term T.

(1) $PV^\omega \vdash s\{T\} = s\{NF(T)\}$

a) $T \equiv X$

By $NF(T) \equiv X$.

b) $T \equiv \lambda X.AX$

By $NF(T) \equiv A$ and (η), $s\{T\} = s\{\lambda X.AX\} = s\{A\} = s\{NF(T)\}$.

c) $T \equiv \lambda X.A$

By $NF(T) \equiv \lambda X.A \equiv T$ and (β), $s\{T\} = s\{\lambda X.A\} = s\{NF(T)\}$.

d) $T \equiv (\lambda X.A)U$

By $NF(T) \equiv A[U/X]$, $s\{T\} = s\{(\lambda X.A)U\} = s\{A[U/X]\} = s\{NF(T)\}$.

e) $T \equiv AB$, where A don't contain λ and $s\{B\} = s\{NF(B)\}$

By $NF(T) \equiv A(NF(B)) \equiv NF(AB)$,

$s\{T\} = s\{AB\} = s\{A(NF(B))\} = s\{NF(AB)\} = s\{NF(T)\}$.

(2) $PV^\omega \vdash s = NF(s)$

$s = x$ or $s = (\lambda X.A)U$ because the type of s is 0.

a) $s = x$

By $NF(s) \equiv x$, $s = NF(s)$.

b) $s = (\lambda X.A)U$

By $(\alpha), (\beta), (\eta)$ and th. 5.2.14, $s = (\lambda X.A)U = A[U/X] = NF(A)[NF(U)/X]$.

By definition of NF, $NF(s) = NF(A)[NF(U)/X]$. Therefore $s = NF(s)$. ∎

Theorem 6.2.2 (Conditional Proof Principle)

If $PV^\omega \vdash t[0/x] = u[0/x]$ and $PV^\omega \vdash x \neq 0 \supset t = u$ then $PV^\omega \vdash t = u$.

(*proof*) By DR16. ∎

Definition 6.2.3 Let $\tau = \tau_1 \to \cdots \to \tau_n \to 0$ $(n \geq 0)$ and $\vec{W} = (W_1, \cdots, W_n)$, where W_i is a variable of type τ_i, $1 \leq i \leq n$. Then

$$Cond_\tau(x, Y, Z) \stackrel{d}{\equiv} \lambda \vec{W}.Cond(x, Y(\vec{W}), Z(\vec{W})).$$

In particular,

$$Cond_0(x, y, z) \stackrel{d}{\equiv} Cond(x, y, z).$$

Lemma 6.2.4 $PV^\omega \vdash Cond_0(x, t\{S\}, t\{T\}) = t\{Cond_\tau(x, S, T)\}$

(*proof*) By th. 6.2.2, if we prove $A[0/x] = B[0/x]$ and $x \neq 0 \supset A = B$, then $PV^\omega \vdash A = B$. Let x' be a variable not contained in $Cond_0(x, t\{S\}, t\{T\})$ and $t\{Cond_\tau(x, S, T)\}$. Let $W_1, \cdots, W_n$ be variables where each W_i has type τ_i. Define $A(x')$ and $B(x')$ as $Cond_0(x', t\{S\}, t\{T\})$ and $t\{Cond_\tau(x', S, T)\}$.

(1) $x' = 0$

By (η),def. 3.1.2(3a) and def. 6.2.3,

$$\begin{aligned} A(0) &= Cond_0(0, t\{S\}, t\{T\}) \\ &= t\{S\} \\ &= t\{\lambda W_1.SW_1\} \\ &= t\{\lambda W_1.(\lambda W_2.(SW_1)W_2)\} \\ &\vdots \\ &= t\{\lambda W_1.(\lambda W_2.(\cdots(\lambda W_n.(SW_1)W_2)\cdots)W_n)\} \end{aligned}$$

$$
\begin{aligned}
&= t\{\lambda\vec{W}.S(\vec{W})\}\\
&= t\{\lambda\vec{W}.Cond(0, S(\vec{W}), T(\vec{W}))\}\\
&= t\{Cond_\tau(0, S, T)\}\\
&= B(0)
\end{aligned}
$$

2) $x' \neq 0$

By T11,

$$
\begin{aligned}
A(x') &= t\{T\}\\
&= t\{\lambda W_1.TW_1\}\\
&\vdots\\
&= t\{\lambda\vec{W}.T(\vec{W})\}\\
&= t\{\lambda\vec{W}.Cond(x', S(\vec{W}), T(\vec{W}))\}\\
&= t\{Cond_\tau(x', S, T)\}
\end{aligned}
$$

By (1), (2) and th. 6.2.2, $\vdash A(x') = B(x')$. By $(R4^\omega)$, $PV^\omega \vdash A(x) = B(x)$.

∎

Theorem 6.2.5 *a)* $PV^\omega \vdash t\{Cond_\tau(0, S, T)\} = t\{S\}$
b) $PV^\omega \vdash x \neq 0 \supset t\{Cond_\tau(x, S, T)\} = t\{T\}$

(*proof*)
a) By lemma 6.2.4
b) By lemma 6.2.4

$$PV^\omega \vdash t\{Cond_\tau(x, S, T)\} = Cond_0(x, t\{S\}, t\{T\}).$$

By $x \neq 0$,

$$PV^\omega \vdash Cond_0(x, t\{S\}, t\{T\}) = t\{T\}.$$

Hence

$$PV^\omega \vdash t\{Cond_\tau(x, S, T)\} = t\{T\}.$$ ∎

Theorem 6.2.6 (Simultaneous Recursion)
For each $n \geq 2$ there are closed terms $\rho_1, \cdots, \rho_n$ such that for $1 \leq i \leq n$

$$PV^\omega \vdash \rho_i(\vec{y}, \vec{Z}, \vec{W}, x) = \begin{cases} if\ \ x = 0\ \ then\ \ y_i \\ \quad else \\ Cond(< \vec{t} > \dot{-} < \vec{W}_i(x) >, t_i, W_i(x)) \end{cases}$$

where

$$t_i \stackrel{d}{\equiv} Z_i(x, \vec{\rho}(\vec{y}, \vec{Z}, \vec{W}, \lfloor \tfrac{1}{2}x \rfloor))$$

and the variables

$$x_i, y_i : type\ \ 0$$
$$Z_i : type\ \ 0 \to 0 \to \cdots \to 0 \quad (n+2 \text{ zeroes})$$
$$W_i : type\ \ 0 \to 0.$$

(*proof*) For $1 \leq i \leq n$, let

$$\rho_i \stackrel{d}{\equiv} \lambda\vec{y}\vec{Z}\vec{W}x.\pi_i^n(\mathcal{R}(s, T, U, x))$$

where ,

$s \stackrel{d}{\equiv} < \vec{y} >$,

$T \stackrel{d}{\equiv} < \vec{Z}(x', \pi_1^n(z), \cdots, \pi_n^n(z)) >$,

and

$U \stackrel{d}{\equiv} \lambda x'. < \vec{W}(x') >$.

Then form the axioms (β) and (HTLRN) and equality reasoning we have in PV^ω

$$\mathcal{R}(s,T,U,x) = \begin{cases} if\ \ x = 0\ \ then\ \ < \vec{y} > \\ \quad else \\ Cond(< \vec{t} > \dot{-} < \vec{W}(x) >, < \vec{t} >, < \vec{W}(x) >) \end{cases}$$

where

$$< \vec{t} > \stackrel{d}{\equiv} < \vec{Z}(x, \vec{\rho}(\vec{y}, \vec{Z}, \vec{W}, \lfloor \tfrac{1}{2} x \rfloor)) >.$$

Then

$$\rho_i(\vec{y}, \vec{Z}, \vec{W}, x) = \pi_i^n(\mathcal{R}(s,T,U,x))$$

$$= \begin{cases} if\ \ x = 0\ \ then\ \ \pi_i^n < \vec{y} > \\ \quad else \\ Cond(< \vec{t} > \dot{-} < \vec{W}(x) >, \pi_i^n < \vec{t} >, \pi_i^n < \vec{W}(x) >) \end{cases}$$

$$= \begin{cases} if\ \ x = 0\ \ then\ \ y_i \\ \quad else \\ Cond(< \vec{t} > \dot{-} < \vec{W}_i(x) >, t_i, W_i(x)) \end{cases}$$ ∎

Definition 6.2.7 A term T is *zero-order open* if all free variables of T have type 0. A subterm U of a term T is $free$ in T if no variable has an occurrence which is free in U and bound in T.

Definition 6.2.8 The transformation $t \rightsquigarrow \{t\}^{PV}$ takes a zero-order open type 0 term t of PV^ω to an equivalent term $\{t\}^{PV}$ of PV. The following three cases partition the set of such terms t (we sometimes write t^{PV} for $\{t\}^{PV}$, and $\vec{u}^{PV}$ for $u_1^{PV}, \cdots, u_n^{PV}$).

Case 1. $NF(t)$ is a term of PV. Then

$$\{t\}^{PV} \stackrel{d}{\equiv} NF(t).$$

Case 2. $NF(t) \equiv f(t_1, \cdots, t_n)$, where f is PV function symbol but not all of $t_1, \cdots, t_n$ are PV terms. Then

$$\{t\}^{PV} \stackrel{d}{\equiv} f(t_1^{PV}, \cdots, t_n^{PV}) \ .$$

Case 3. $NF(t) \equiv \mathcal{R}(s,T,U,v)$. Then

$$\{t\}^{PV} \stackrel{d}{\equiv} R[g,h,k](v^{PV}, \vec{u}^{PV})$$

where $u_1 \stackrel{d}{\equiv} s$, and $u_2, \cdots, u_n$ are the maximal type 0 subterms, listed in order and not necessarily distinct, occurring free in T, U, and g, h, k are PV function symbols defined as follows. Let $y_1, \cdots, y_n$ be distinct new variables, and let

T', U' be terms whose only type 0 subterms occurring free are the $y_i's$ such that

$$T \equiv T'[u_2/y_2, \cdots, u_n/y_n]$$

and

$$U \equiv U'[u_2/y_2, \cdots, u_n/y_n]$$

then

$$g \equiv [\lambda \vec{y}.y_1]$$
$$h \equiv [\lambda x \vec{y} z.T'(x,z)^{PV}]$$
$$k \equiv [\lambda x \vec{y}.U'(x)^{PV}]$$

where x and z are new variables.

Lemma 6.2.9 $\{t[u/x]\}^{PV} \equiv t^{PV}[u^{PV}/x]$, for all terms t, u in the domain of $\{\cdot\}^{PV}$, and all type 0 variables x.

(*proof*) By Church-Rosser theorem 5.2.3, $NF(t[u/x]) \equiv NF(t)[NF(u)/x]$. We prove by induction on the length of $NF(t[u/x])$.

(1) $NF(t[u/x])$ is a term of PV.
$NF(t) \equiv t^{PV}$ and $NF(u) \equiv u^{PV}$ because $NF(t)$ and $NF(u)$ are terms of PV.
By hypothesis,
$\{t[u/x]\}^{PV} \equiv NF(t[u/x]) \equiv NF(t)[NF(u)/x] \equiv t^{PV}[u^{PV}/x]$.

(2) $NF(t[u/x]) \equiv f(t_1, \cdots, t_n)$,
where $NF(t) \equiv f(t_1', \cdots, t_n'), t_i \equiv t_i'[NF(u)/x]$ and $t_i^{PV} \equiv t_i'^{PV}[u^{PV}/x]$.
$$\begin{aligned}\{t[u/x]\}^{PV} &\equiv f(t_1^{PV}, \cdots, t_n^{PV}) \\ &\equiv f(t_1'^{PV}[u^{PV}/x], \cdots, t_n'^{PV}[u^{PV}/x]) \\ &\equiv (f(t_1'^{PV}, \cdots, t_n'^{PV}))[u^{PV}/x] \\ &\equiv t^{PV}[u^{PV}/x].\end{aligned}$$

(3) $NF(t[u/x]) \equiv \mathcal{R}(\hat{s}, \hat{T}, \hat{U}, \hat{v})$,
where $NF(t) \equiv \mathcal{R}(s, T, U, v), \hat{s} \equiv s[NF(u)/x], \hat{T} \equiv T[NF(u)/x]$,
$\hat{U} \equiv U[NF(u)/x], \hat{v} \equiv v[NF(u)/x]$ and $\{t\}^{PV} \equiv R[g,h,k](v'^{PV}, u'^{\vec{P}V})$,
where $g \equiv [\lambda \vec{y}.y_1], h \equiv [\lambda x_1 \vec{y} z.\{T'(x_1,z)\}^{PV}]$ and $k \equiv [\lambda x_1 \vec{y}.\{U'(x_1)\}^{PV}]$,
where x_1 and z are new variables.
Then $\{t[u/x]\}^{PV} \equiv R[g', h', k'](v''^{PV}, u''^{\vec{P}V})$, where $g' \stackrel{d}{\equiv} [\lambda \vec{y}.y_1]$,
$h' \stackrel{d}{\equiv} [\lambda x_1 \vec{y} z.\{T''(x_1,z)\}^{PV}], k' \stackrel{d}{\equiv} [\lambda x_1 \vec{y}.\{U''(x_1)\}^{PV}]$,
$v''^{PV} \stackrel{d}{\equiv} \{v'[u/x]\}^{PV} \equiv v'^{PV}[u^{PV}/x]$ and $u_i''^{PV} \stackrel{d}{\equiv} \{u_i'[u/x]\}^{PV} \equiv u_i'^{PV}[u^{PV}/x]$.
By free variables of $T'(x_1,z)$ and $U''(x_1)$ be only $y_2, \cdots, y_n$,
$T''(x_1,z) \equiv T'(x_1,z)[u/x] \equiv T'(x_1,z)$ and $U''(x_1) \equiv U'(x_1)[u/x] \equiv U'(x_1)$.
Hence $g \equiv g', h \equiv h'$ and $k \equiv k'$.
Therefore
$$\begin{aligned}\{t[u/x]\}^{PV} &\equiv R[g', h', k'](v''^{PV}, u''^{\vec{P}V}) \\ &\equiv R[g,h,k](v'^{PV}[u^{PV}/x], u'^{\vec{P}V}[u^{PV}/x])\end{aligned}$$

$$\equiv (R[g,h,k](v'^{PV}, u'^{\vec{PV}}))[u^{PV}/x]$$
$$\equiv t^{PV}[u^{PV}/x]. \blacksquare$$

Theorem 6.2.10 $PV^\omega \vdash t = t^{PV}$, for each type 0 term t in the domain of $\{\cdot\}^{PV}$.

(*proof*) We prove by induction on the length of $NF(t)$.

(1) $NF(t)$ is a term of PV.
By prop. 5.2.14, $t = NF(t)$. Therefore $t^{PV} = NF(t) = t$.

(2) $NF(t) \equiv f(t_1, \cdots, t_n)$, where $t_i^{PV} \equiv t_i$.
$t^{PV} \equiv f(t_1^{PV}, \cdots, t_n^{PV}) \equiv f(t_1, \cdots, t_n) \equiv NF(t)$. By prop. 5.2.14, $t = NF(t) \equiv t^{PV}$.
Therefore $t = t^{PV}$.

Assume $v = v^{PV}$ and $u_i = u_i^{PV}$.

(3) $NF(t[u/x]) \equiv \mathcal{R}(\hat{s}, \hat{T}, \hat{U}, \hat{v})$.
$t^{PV} \equiv R[g,h,k](v^{PV}, \vec{u^{PV}})$.

$$\mathcal{R}(s,T,U,v) = \begin{cases} if\ \ v = 0\ \ then\ \ s \\ \quad else \\ Cond(t_1 \dot{-} U(v), t_1, U(v)), \end{cases}$$

where

$$t_1 \stackrel{d}{\equiv} T(v, \mathcal{R}(s,T,U,\lfloor \tfrac{1}{2} v \rfloor)).$$

$$R[g,h,k](v^{PV}, \vec{u^{PV}}) = \begin{cases} if\ \ v^{PV} = 0\ \ then\ \ g(\vec{u}^{PV}) \\ \quad else \\ Cond(t_2 \dot{-} k(v^{PV}, \vec{u}^{PV}), t_2, k(v^{PV}, \vec{u}^{PV})), \end{cases}$$

where

$$t_2 \stackrel{d}{\equiv} h(v^{PV}, \vec{u}^{PV}, R[g,h,k](\lfloor \tfrac{1}{2} v^{PV} \rfloor, \vec{u}^{PV})).$$

(a) $v = 0$
$v^{PV} = v = 0$. Therefore $g(\vec{u}^{PV}) = g(\vec{u}) = u_1 \equiv s$.
Therefore $v = 0 \supset \mathcal{R}(s,T,U,v) = R[g,h,k](v^{PV}, \vec{u^{PV}})$.

(b) $v \neq 0$
Assume $\mathcal{R}(s,T,U,\lfloor \frac{1}{2} v \rfloor) = R[g,h,k](\lfloor \frac{1}{2} v^{PV} \rfloor, \vec{u}^{PV})$. By ($\beta$) and lemma 6.2.9,

$$\begin{aligned} t_2 &= h(v^{PV}, \vec{u}^{PV}, R[g,h,k](\lfloor \tfrac{1}{2} v^{PV} \rfloor, \vec{u}^{PV})) \\ &= [\lambda x \vec{y} z.\{T'(x,z)\}^{PV}](v^{PV}, \vec{u}^{PV}, R[g,h,k](\lfloor \tfrac{1}{2} v^{PV} \rfloor, \vec{u}^{PV})) \\ &= \{T(v^{PV}, R[g,h,k](\lfloor \tfrac{1}{2} v^{PV} \rfloor, \vec{u}^{PV}))\}^{PV} \\ &= T(v^{PV}, R[g,h,k](\lfloor \tfrac{1}{2} v^{PV} \rfloor, \vec{u}^{PV})) \\ &= t_1 \end{aligned}$$

$$\begin{aligned} k(v^{PV}, \vec{u}^{PV}) &= [\lambda x \vec{y}.\{U'(x)\}^{PV}](v^{PV}, \vec{u}^{PV}) \\ &= \{U(v)\}^{PV} \end{aligned}$$

$= U(v)$

Therefore $Cond(t_1 \dot{-} U(v), t_1, U(v)) = Cond(t_2 \dot{-} k(v^{PV}, \vec{u}^{PV}), t_2, k(v^{PV}, \vec{u}^{PV}))$.

Therefore $v \neq 0 \supset \mathcal{R}(s,T,U,v) = R[g,h,k](v^{PV}, u^{\vec{P}V})$.

By (a),(b) and th. 6.2.2, $\mathcal{R}(s,T,U,v) = R[g,h,k](v^{PV}, u^{\vec{P}V})$.

Therefore $t = NF(t) = \mathcal{R}(s,T,U,v) = R[g,h,k](v^{PV}, u^{\vec{P}V}) = t^{PV}$.

∎

Definition 6.2.11 Let S,T be terms of PV^ω. We say that (S',T') is an *instance* of (S,T) iff there is a common substitution of terms of free variables which yields S' from S and T' from T, and (S',T') is a *zero-order open instance* of (S,T) if in addition S' and T' are zero-order open.

Definition 6.2.12 Suppose S,T are terms of type $\sigma_1 \to \sigma_2 \to \cdots \to \sigma_n \to 0$. We write $S \overset{PV}{\sim} T$ iff $PV \vdash \{S'(\vec{\phi})\}^{PV} = \{T'(\vec{\phi})\}^{PV}$ for all zero-order open instances (S',T') of (S,T), and all $\vec{\phi} \equiv \phi_1, \cdots, \phi_n$ such that ϕ_i is zero-order open of type σ_i, $1 \leq i \leq n$.

Definition 6.2.13 Let S,T be zero-order open terms of PV^ω of type $\sigma_1 \to \sigma_2 \to \cdots \to \sigma_n \to 0$. Then $S \approx T$ iff $PV \vdash \{S(\vec{\phi})\}^{PV} = \{T(\vec{\phi})\}^{PV}$ for all $\vec{\phi} \equiv \phi_1, \cdots, \phi_n$ such that ϕ_i is zero-order open of type σ_i, $1 \leq i \leq n$.

Thus for S,T any terms of PV^ω, $S \overset{PV}{\sim} T$ iff $T\ S' \approx T'$ for all zero-order open instances (S',T') of (S,T).

Definition 6.2.14 The properties $G_\sigma(T)$ are defined by induction on the type σ.

(1) $G_0(t)$ iff t is zero-order open of type 0.

(2) If $\sigma \equiv \sigma_1 \to \cdots \to \sigma_n \to 0$, then $G_\sigma(T)$ iff T is zero-order open of type σ and $T(\vec{\phi}) \approx T(\vec{\psi})$ for all $\vec{\phi} \equiv \phi_1, \cdots, \phi_n$, and $\vec{\psi} \equiv \psi_1, \cdots, \psi_n$ such that $G_{\sigma_i}(\phi_i), G_{\sigma_i}(\psi_i)$, and $\sigma_i \approx \psi_i$, $(1 \leq i \leq n)$.

Definition 6.2.15 For any term T of PV^ω, $G^*(T)$ iff $G(T[\vec{\phi}/\vec{X}])$ and $T[\vec{\phi}/\vec{X}] \approx T[\vec{\psi}/\vec{X}]$ for all $\vec{\phi} \equiv \phi_1, \cdots, \phi_n$, and $\vec{\psi} \equiv \psi_1, \cdots, \psi_n$ such that

(1) $G(\phi_i), G(\psi_i), \sigma_i \approx \psi_i$

(2) $T[\vec{\phi}/\vec{X}]$ is zero-order open.

Lemma 6.2.16 $G^*(T)$ for all terms T of PV^ω.

(*proof*) We prove by induction on the definition 6.1.2 of term T. Assume that $\vec{\phi} \equiv \phi_1, \cdots, \phi_n$, and $\vec{\psi} \equiv \psi_1, \cdots, \psi_n$ are (1) $G(\phi_i), G(\psi_i), \phi_i \approx \psi_i$, (2) $T[\vec{\phi}/\vec{X}]$ be zero-order open.

(1) T is a type 0 variable X.

(a) $X = X_i\ (1 \leq i \leq n)$
By $T[\vec{\phi}/\vec{X}] = \phi_i$ and definition of $\vec{\phi}$, $G(T[\vec{\phi}/\vec{X}])$.
By $T[\vec{\phi}/\vec{X}] = \phi_i, T[\vec{\psi}/\vec{X}] = \psi_i$ and $\phi_i \approx \psi_i$, $T[\vec{\phi}/\vec{X}] \approx T[\vec{\psi}/\vec{X}]$.

(b) X is not in the list $\vec{X}$.
By $T[\vec{\phi}/\vec{X}] = X$ and def. 6.1.2, $G(T[\vec{\phi}/\vec{X}])$.
By $T[\vec{\phi}/\vec{X}] = X, T[\vec{\psi}/\vec{X}] = X$ and $X \approx X$, $T[\vec{\phi}/\vec{X}] \approx T[\vec{\psi}/\vec{X}]$.

Therefore $G^*(T)$.

(2) T is a variable X not type 0.

(a) $X \equiv X_i\ (1 \leq i \leq n)$
By $T[\vec{\phi}/\vec{X}] \equiv \phi_i$ and definition of $\vec{\phi}$, $G(T[\vec{\phi}/\vec{X}])$.
By $T[\vec{\phi}/\vec{X}] \equiv \phi_i, T[\vec{\psi}/\vec{X}] = \equiv \psi_i$ and $\phi_i \approx \psi_i$, $T[\vec{\phi}/\vec{X}] \approx T[\vec{\psi}/\vec{X}]$.

(b) X is not in the list $\vec{X}$.
We don't need to think this case. $\forall i(X \not\equiv X_i)$ is impossible. $T[\vec{\phi}/\vec{X}] \equiv T \equiv X$.
But this condition is contradiction to def. 6.2.15 (2).

Therefore $G^*(T)$.

(3) $T \equiv f$, where f is a function symbol of PV.
By $\phi_i \approx \psi_i$, $PV \vdash \phi_i^{PV} = \psi_i^{PV}$. By this and $NF(T(\vec{\phi})) = f(\phi_1, \cdots, \phi_n)$,
$\{T(\vec{\phi})\}^{PV} = f(\phi_1^{PV}, \cdots, \phi_n^{PV}) = f(\psi_1^{PV}, \cdots, \psi_n^{PV}) = \{T(\vec{\psi})\}^{PV}$.
Therefore $G(f)$.
By f be not contained free variable, $T[\vec{\phi}/\vec{X}] \equiv T$.
Therefore $G(T[\vec{\phi}/\vec{X}])$.
By $T[\vec{\phi}/\vec{X}] \equiv T, T[\vec{\psi}/\vec{X}] \equiv T$ and $T \approx T$, $T[\vec{\phi}/\vec{X}] \approx T[\vec{\psi}/\vec{X}]$.

Therefore $G^*(T)$.

(4) $T \equiv \mathcal{R}$

(a) We prove $G(T[\vec{\phi}/\vec{X}])$.
By $\mathcal{R}$ has no free variable, $T[\vec{\phi}/\vec{X}] \equiv T$. Hence we prove $G(T)$ for $G(T[\vec{\phi}/\vec{X}])$.
Assume $s \approx \hat{s}, T \approx \hat{T}, U \approx \hat{U}$ and $v \approx \hat{v}$. Then we prove $\mathcal{R}(s,T,U,v) \approx \mathcal{R}(\hat{s},\hat{T},\hat{U},\hat{v})$ for to prove $G(T)$. We prove
$PV \vdash \{\mathcal{R}(s,T,U,v)\}^{PV} = \{\mathcal{R}(\hat{s},\hat{T},\hat{U},\hat{v})\}^{PV}$ for $\mathcal{R}(s,T,U,v) \approx \mathcal{R}(\hat{s},\hat{T},\hat{U},\hat{v})$.
By hypothesis, $PV \vdash s^{PV} = \hat{s}^{PV}, v^{PV} = \hat{v}^{PV}$.

i. $g(\vec{u}^{PV}) = u_1^{PV} = s^{PV} = \hat{s}^{PV} = \hat{u_1}^{PV} = \hat{g}(\vec{\hat{u}}^{PV})$.

ii. $k(v^{PV}, \vec{u}^{PV}) = [\lambda x\vec{y}.\{U'(x)\}^{PV}](v^{PV}, \vec{u}^{PV})$
$= \{U'(x)\}^{PV}[v^{PV}/x][\vec{u}^{PV}/\vec{y}]$
$= \{U'[v/x][\vec{u}/\vec{y}]((x)[v/x][\vec{u}/\vec{y}])\}^{PV}$
$= \{U'[\vec{u}/\vec{y}]((x)[v/x])\}^{PV}$
$= \{U(v)\}^{PV}$
$= \{\hat{U}(\hat{v})\}^{PV}$
$= \{\hat{U}'[\vec{\hat{u}}/\vec{\hat{y}}]((\hat{x})[\hat{v}/\hat{x}])\}^{PV}$
$= [\lambda\hat{x}\vec{\hat{y}}.\{\hat{U}'(\hat{x})\}^{PV}](\hat{v}^{PV}, \vec{\hat{u}}^{PV})$
$= \hat{k}(\hat{v}^{PV}, \vec{\hat{u}}^{PV})$.

iii. Same as $h(v^{PV}, \vec{u}^{PV}, R[g,h,k](\lfloor\frac{1}{2}v^{PV}\rfloor, \vec{u}^{PV})) =$
$\hat{h}(\hat{v}^{PV}, \vec{\hat{u}}^{PV}, R[\hat{g},\hat{h},\hat{k}](\lfloor\frac{1}{2}\hat{v}^{PV}\rfloor, \vec{\hat{u}}^{PV}))$.

By (i)-(iii),

$$\{\mathcal{R}(s,T,U,v)\}^{PV} = R[g,h,k](v^{PV}, \vec{u}^{PV})$$
$$= \begin{cases} if\ \ v^{PV} = 0\ \ then\ \ g(\vec{u}^{PV}) \\ \quad else \\ Cond(t \dot{-} k(v^{PV}, \vec{u}^{PV}), t, k(v^{PV}, \vec{u}^{PV})) \end{cases}$$
$$= \begin{cases} if\ \ \hat{v}^{PV} = 0\ \ then\ \ \hat{g}(\vec{\hat{u}}^{PV}) \\ \quad else \\ Cond(\hat{t} \dot{-} \hat{k}(\hat{v}^{PV}, \vec{\hat{u}}^{PV}), \hat{t}, \hat{k}(\hat{v}^{PV}, \vec{\hat{u}}^{PV})) \end{cases}$$
$$= \{\mathcal{R}(\hat{s}, \hat{T}, \hat{U}, \hat{v})\}^{PV},$$

where $t \stackrel{d}{\equiv} h(v^{PV}, \vec{u}^{PV}, R[g,h,k](\lfloor\frac{1}{2}v^{PV}\rfloor, \vec{u}^{PV}))$ and
$\hat{t} \stackrel{d}{\equiv} \hat{h}(\hat{v}^{PV}, \vec{\hat{u}}^{PV}, R[\hat{g},\hat{h},\hat{k}](\lfloor\frac{1}{2}\hat{v}^{PV}\rfloor, \vec{\hat{u}}^{PV}))$.

(b) We prove $T[\vec{\phi}/\vec{X}] \approx T[\vec{\psi}/\vec{X}]$.
By $\mathcal{R}$ has no free variable.

By (a) and (b), $G^*(T)$.

(5) $G^*(TU)$, where $G^*(T)$ and $G^*(U)$.
Define T', T'', U' and U'' as $T[\vec{\phi}/\vec{X}], T[\vec{\psi}/\vec{X}], U[\vec{\phi}/\vec{X}]$ and $U[\vec{\psi}/\vec{X}]$. Then by $G^*(T)$ and $G^*(U)$, $T' \approx T'', U' \approx U'', G(T'), G(T''), G(U')$ and $G(U'')$.

(a) We prove $G(TU[\vec{\phi}/\vec{X}])$.
By $G(T')$, $T'(U', \vec{\eta}) \approx T'(U', \vec{\mu})$, where $\vec{\eta}$ and $\vec{\mu}$ are any suitable sequences of zero-order open. Then $T'U'(\vec{\eta}) \approx T'U'(\vec{\mu})$. Hence $G(T'U')$. Therefore $G(TU[\vec{\phi}/\vec{X}])$.

(b) We prove $TU[\vec{\phi}/\vec{X}] \approx TU[\vec{\psi}/\vec{X}]$.
By $T' \approx T''$, $PV \vdash \{T'(U', \vec{\eta})\}^{PV} = \{T''(U', \vec{\eta})\}^{PV}$, where $\vec{\eta}$ is any suitable sequences of zero-order open. By def. 6.2.13, $T'(U', \vec{\eta}) \approx T''(U', \vec{\eta})$. By def. 6.2.14, $T''(U', \vec{\eta}) \approx T''(U'', \vec{\eta})$. By $T'(U', \vec{\eta}) \approx T''(U', \vec{\eta})$ and $T''(U', \vec{\eta}) \approx T''(U'', \vec{\eta})$, $T'(U', \vec{\eta}) \approx T''(U'', \vec{\eta})$. Then for any suitable sequences $\vec{\eta}$,

$PV \vdash \{T'U'(\vec{\eta})\}^{PV} = \{T''U''(\vec{\eta})\}^{PV}$. Hence $T'U' \approx T''U''$.
Therefore $TU[\vec{\phi}/\vec{X}] \approx TU[\vec{\psi}/\vec{X}]$.

By (a) and (b), $G^*(TU)$.

(6) $G^*(\lambda X.T)$, where $G^*(T)$
Let $\phi_i \approx \psi_i, G(\phi_i), G(\psi_i)$ and $T' \equiv T[\vec{\phi}/\vec{Y}]$ and $T'' \equiv T[\vec{\psi}/\vec{Y}]$, where X is not among the components of $\vec{Y}$. Let any $\vec{\eta}$ and $\vec{\mu}$ such that $G(\eta_i), G(\mu_i), \eta_i \approx \mu_i$. Assume any U and V such that zero-order open, $U \approx V$ and same type as X.

(a) We prove $G((\lambda X.T)[\vec{\phi}/\vec{x}])$.
By $G(T)$, $T[\vec{\phi}/\vec{Y}, U/X] \approx T[\vec{\phi}/\vec{Y}, V/X]$. Hence $T'[U/X] = T'[V/X]$.
Therefore $\forall\vec{\eta}(PV \vdash \{T'[U/X](\vec{\eta})\}^{PV} = \{T'[V/X](\vec{\eta})\}^{PV})$.
By type of $T'[U/X](\vec{\eta})$ be 0, $T'[U/X](\vec{\eta}) \approx T'[V/X](\vec{\eta})$.
By $G^*(T)$, $G(T[\vec{\phi}/\vec{Y}, V/X])$. Therefore $G(T'[V/X])$.
By $G(T'[V/X]), G(\eta_i), G(\mu_i)$ and $\eta_i \approx \mu_i$, $T'[V/X](\vec{\eta}) \approx T'[V/X](\vec{\mu})$.
By $T'[U/X](\vec{\eta}) \approx T'[V/X](\vec{\eta})$ and $T'[V/X](\vec{\eta}) \approx T'[V/X](\vec{\mu})$,
$T'[U/X](\vec{\eta}) \approx T'[V/X](\vec{\mu})$.
Therefore $PV \vdash \{T'[U/X](\vec{\eta})\}^{PV} = \{T'[V/X](\vec{\mu})\}^{PV}$.
By $NF(T'[U/X](\vec{\eta})) = NF((\lambda X.T')(U, \vec{\eta}))$ and
$NF(T'[V/X](\vec{\mu})) = NF((\lambda X.T')(V, \vec{\mu}))$,
$PV \vdash \{(\lambda X.T')(U, \vec{\eta})\}^{PV} = \{(\lambda X.T')(V, \vec{\mu})\}^{PV}$.
Hence $G(\lambda X.T')$.
Therefore $G((\lambda X.T)[\vec{\phi}/\vec{Y}])$.

(b) We prove $(\lambda X.T)[\vec{\phi}/\vec{Y}] \approx (\lambda X.T)[\vec{\psi}/\vec{Y}]$.
By $G^*(T)$, $T[\vec{\phi}/\vec{Y}, U/X] \approx T[\vec{\psi}/\vec{Y}, U/X]$. Hence $T'[U/X] \approx T''[U/X]$.
Therefore $\forall\vec{\eta}(PV \vdash \{T'[U/X](\vec{\eta})\}^{PV} = \{T''[U/X](\vec{\eta})\}^{PV})$.
By $NF(T'[U/X](\vec{\mu})) = NF((\lambda X.T')(U, \vec{\mu}))$ and
$NF(T''[U/X](\vec{\mu})) = NF((\lambda X.T'')(U, \vec{\mu}))$,
$\forall(U, \vec{\eta})(PV \vdash \{(\lambda X.T')(U, \vec{\mu})\}^{PV} = \{(\lambda X.T'')(U, \vec{\mu})\}^{PV})$.
Hence $(\lambda X.T') \approx (\lambda X.T'')$.
Therefore $(\lambda X.T)[\vec{\phi}/\vec{Y}] \approx (\lambda X.T)[\vec{\psi}/\vec{Y}]$.

By (a) and (b), $G^*(\lambda X.T)$.

∎

Lemma 6.2.17 If $S \overset{PV}{\sim} T$ then $(\lambda X.S) \overset{PV}{\sim} (\lambda X.T)$.

(*proof*) Let (S', T') be zero-order open instance of (S, T) and X be free variable of (S', T') and (S, T). Assume $S \overset{PV}{\sim} T$. We need to prove that for any suitable zero-order open terms ψ and $\vec{\phi}$, $PV \vdash \{(\lambda X.S')(\psi, \vec{\phi})\}^{PV} = \{(\lambda X.T')(\psi, \vec{\phi})\}^{PV}$

Define A, A', B, B' as $(\lambda X.S')(\psi, \vec{\phi}), S'[\psi/X](\vec{\phi}), (\lambda X.T')(\psi, \vec{\phi})$ and $T'[\psi/X](\vec{\phi})$.
By $NF(A) = NF(A')$ and $NF(B) = NF(B')$, $A^{PV} = A'^{PV}$ and $B^{PV} = B'^{PV}$.

By S' and T' be zero-order open, $S'[\psi/X]$ and $T'[\psi/X]$ are zero-order open. By (S', T') be instance of (S, T), $S' \equiv S[\vec{v}/\vec{x}]$ and $T' \equiv T[\vec{v}/\vec{x}]$. By $S'[\psi/X] \equiv S[\vec{v}/\vec{x}, \psi/X]$ and $T'[\psi/X] \equiv T[\vec{v}/\vec{x}, \psi/X]$, $(S'[\psi/X], T'[\psi/X])$ is zero-order open instance of (S, T).
By $S \overset{PV}{\sim} T$,
$PV \vdash \{S'[\psi/X](\vec{\phi})\}^{PV} = \{T'[\psi/X](\vec{\phi})\}^{PV}$
Therefore $PV \vdash A'^{PV} = B'^{PV}$.
Therefore $PV \vdash A^{PV} = B^{PV}$. ∎

Lemma 6.2.18 If $S \overset{PV}{\sim} T$ then $(SU) \overset{PV}{\sim} (TU)$.

(*proof*) Let types of T, S be $\sigma_1 \to \cdots \sigma_n \to 0$ and U be σ_1. Assume $(S'U', T'U')$ be any zero-order open instance of (SU, TU), where S', T' and U' are $S[\vec{v}/\vec{v}], T[\vec{v}/\vec{v}]$ and $U[\vec{v}/\vec{v}]$. Then S', T' and U' are zero-order open because $S'U'$ and $T'U'$ are zero-order open instance. Define a set Φ as

$\Phi \overset{d}{\equiv} \{\vec{\phi} \mid [\vec{\phi} \equiv \phi_1, \cdots, \phi_n]$, each ϕ_i is zero-order open of type $\sigma_i, 1 \leq i \leq n\}$.

By $S \overset{PV}{\sim} T$, $\forall (S', T') \forall \vec{\phi} \in \Phi (PV \vdash \{S'(\vec{\phi})\}^{PV} = \{T'(\vec{\phi})\}^{PV})$. Define a set Φ'' as

$\Phi'' \overset{d}{\equiv} \{\vec{\phi''} \mid [\vec{\phi''} \equiv \phi''_1, \cdots, \phi''_{n-1}]$, each ϕ''_i is zero-order open of type $\sigma_{i+1}, 1 \leq i \leq n\}$.

For any $\vec{\phi''} \in \Phi''$, define a sequence $\vec{\phi'}$ as

$\phi'_1 \overset{d}{\equiv} U'$ and Then $\vec{\phi'} \in \Phi$. By $\vec{\phi'} \in \Phi$ and $S \overset{PV}{\sim} T$, $PV \vdash \{S'(\vec{\phi'})\}^{PV} = \{T'(\vec{\phi'})\}^{PV}$.
Therefore

$$\begin{aligned} PV \vdash \{S'(\vec{\phi'})\}^{PV} &= \{(\cdots (S'\phi'_1)\phi'_2 \cdots \phi'_n)\}^{PV} \\ &= \{(\cdots (S'U')\phi'_2 \cdots \phi'_n)\}^{PV} \\ &= \{(\cdots (S'U')\phi''_1 \cdots \phi''_{n-1})\}^{PV} \\ &= \{(S'U')(\vec{\phi''})\}^{PV}. \end{aligned}$$

Same as $PV \vdash \{T'(\vec{\phi'})\}^{PV} = \{(T'U')(\vec{\phi''})\}^{PV}$.
Therefore $PV \vdash \{(S'U')(\vec{\phi''})\}^{PV} = \{(T'U')(\vec{\phi''})\}^{PV}$.
Therefore $\forall (S'U', T'U') \forall \vec{\phi''} \in \Phi'' (PV \vdash \{(S'U')(\vec{\phi''})\}^{PV} = \{(T'U')(\vec{\phi''})\}^{PV})$.
Therefore $(SU) \overset{PV}{\sim} (TU)$. ∎

Lemma 6.2.19 If $S \overset{PV}{\sim} T$ then $(US) \overset{PV}{\sim} (UT)$.

(*proof*) By lemma 6.2.16, $G^*(U)$.
Hence $\forall \vec{\phi'}, \vec{\psi'}, \vec{\eta} (PV \vdash \{U[\vec{\eta}/\vec{X}](\vec{\phi'})\}^{PV} = \{U[\vec{\eta}/\vec{X}](\vec{\psi'})\}^{PV})$.
By $S \overset{PV}{\sim} T$, $\forall \vec{\phi}, \vec{\psi}, \vec{\eta} (PV \vdash \{S[\vec{\eta}/\vec{X}](\vec{\phi})\}^{PV} = \{T[\vec{\eta}/\vec{X}](\vec{\psi})\}^{PV})$.
Therefore we take $S[\vec{\eta}/\vec{X}](\vec{\phi})$ and $T[\vec{\eta}/\vec{X}](\vec{\psi})$ as $\vec{\phi'}$ and $\vec{\psi'}$.
Then $\forall \vec{\phi}, \vec{\psi}, \vec{\eta} (PV \vdash \{U[\vec{\eta}/\vec{X}](S[\vec{\eta}/\vec{X}](\vec{\phi}))\}^{PV} = \{U[\vec{\eta}/\vec{X}](T[\vec{\eta}/\vec{X}](\vec{\psi}))\}^{PV})$.
Therefore $\forall \vec{\phi}, \vec{\psi}, \vec{\eta} (PV \vdash \{U[\vec{\eta}/\vec{X}]S[\vec{\eta}/\vec{X}](\vec{\phi})\}^{PV} = \{U[\vec{\eta}/\vec{X}]T[\vec{\eta}/\vec{X}](\vec{\psi})\}^{PV})$.
Therefore $(US) \overset{PV}{\sim} (UT)$. ∎

Lemma 6.2.20 If $S \overset{PV}{\sim} T$ then $U\{S\} \overset{PV}{\sim} U\{T\}$.

(*proof*) By lemma 6.2.17, 6.2.18 and 6.2.19. ∎

Theorem 6.2.21 If $PV^\omega \vdash t = u$, then $PV \vdash t_1^{PV} = u_1^{PV}$, where $t_1 = u_1$ is any zero-order open substitution instance of $t = u$.

(proof)

We prove induction on the PV^ω proof of PV.

(1) $t = u$ is an axiom of PV.
By lemma 6.2.9 and $(R4)$, $PV \vdash t_1^{PV} = u_1^{PV}$.

(2) $t = u$ is an instance of $(\alpha), (\beta)$ or (γ).
Let $t \equiv s\{\lambda X.T\}$ and $u \equiv s\{\lambda Y.T[Y/X]\}$. Then $t^{PV} \equiv \{s\{\lambda X.T\}\}^{PV}$ and $u^{PV} \equiv \{s\{\lambda Y.T[Y/X]\}\}^{PV}$. By th. 5.2.3, $NF(t_1^{PV}) \equiv NF(u_1^{PV})$. Hence $t_1^{PV} = u_1^{PV}$ is instance of $x = x$.

(3) $t = u$ is an instance of $(HTLRN)$.
Let $t = \mathcal{R}(s, T, U, v)$ and $u = \begin{cases} if\ \ v = 0\ \ then\ \ s \\ \quad else \\ Cond(w \dot{-} U(v), w, U(v)), \end{cases}$
where
$$w \stackrel{d}{\equiv} T(v, \mathcal{R}(s, T, U, \lfloor \tfrac{1}{2} v \rfloor)).$$
Then $t^{PV} = R[g, h, k](v^{PV}, \vec{r}^{PV})$
$$= \begin{cases} if\ \ v^{PV} = 0\ \ then\ \ g(\vec{r}^{PV}) \\ \quad else \\ Cond(w' \dot{-} k(v^{PV}, \vec{r}^{PV}), w', k(v^{PV}, \vec{r}^{PV})), \end{cases}$$
where
$r_1^{PV} \stackrel{d}{\equiv} s^{PV}, T \equiv T'[r_2/y_2, \cdots, r_n/y_n], U \equiv U'[r_2/y_2, \cdots, r_n/y_n], g \equiv [\lambda \vec{y}.y_1]$,
$h \equiv [\lambda x \vec{y} z.T'(x, z)^{PV}], k \equiv [\lambda x \vec{y}.\{U'(x)\}^{PV}]$ and
$w' \stackrel{d}{\equiv} h(v^{PV}, \vec{r}^{PV}, R[g, h, k](\lfloor \frac{1}{2} v^{PV} \rfloor, \vec{r}^{PV}))$.
And $u^{PV} = \begin{cases} if\ \ v^{PV} = 0\ \ then\ \ s^{PV} \\ \quad else \\ Cond(w'' \dot{-} \{U(v^{PV})\}^{PV}, w'', \{U(v^{PV})\}^{PV}), \end{cases}$
where
$$w'' \stackrel{d}{\equiv} \{T(v^{PV}, \{\mathcal{R}(s, T, U, \lfloor \tfrac{1}{2} v \rfloor)\}^{PV})\}^{PV}.$$
By $PV \vdash g(\vec{r}^{PV}) = r_1^{PV} = s^{PV}$,
$$\begin{aligned} PV \vdash w' &= h(v^{PV}, \vec{r}^{PV}, R[g, h, k](\lfloor \tfrac{1}{2} v^{PV} \rfloor, \vec{r}^{PV})) \\ &= \{T(v^{PV}, R[g, h, k](\lfloor \tfrac{1}{2} v^{PV} \rfloor, \vec{r}^{PV}))\}^{PV} \\ &= \{T(v^{PV}, \{\mathcal{R}(s, T, U, \lfloor \tfrac{1}{2} v \rfloor)\}^{PV})\}^{PV} \\ &= w''. \end{aligned}$$
and
$$\begin{aligned} PV \vdash k(v^{PV}, \vec{r}^{PV}) &= [\lambda x \vec{y}.\{U'(x)\}^{PV}](v^{PV}, \vec{r}^{PV}) \\ &= \{U(v^{PV})\}^{PV}. \end{aligned}$$

Therefore $PV \vdash t^{PV} = u^{PV}$.

(4) $t = u$ is an instance of $(R1^\omega)$.
Assume $PV^\omega \vdash t = u \Rightarrow PV \vdash t^{PV} = u^{PV}$.
Then we need to prove that $PV^\omega \vdash u = t \Rightarrow PV \vdash u^{PV} = t^{PV}$.
This proof follows from $(R1^\omega)$, hypothesis and $(R1)$.

(5) $t = u$ is an instance of $(R2^\omega)$.
Assume $PV^\omega \vdash t = s \Rightarrow PV \vdash t^{PV} = s^{PV}$ and $PV^\omega \vdash s = u \Rightarrow PV \vdash s^{PV} = u^{PV}$.
Then we need to prove $PV^\omega \vdash t = s, s = u \Rightarrow PV \vdash t^{PV} = u^{PV}$.
This proof follows from $(R2^\omega)$,hypothesis and $(R2)$.

(6) $t = u$ is an instance of $(R3^\omega)$.
Assume $PV^\omega \vdash t = u \Rightarrow PV \vdash t^{PV} = u^{PV}$.
Then we need to prove $PV^\omega \vdash s\{t\} = s\{u\} \Rightarrow PV \vdash \{s\{t\}\}^{PV} = \{s\{u\}\}^{PV}$.
By lemma 6.2.20, $s\{t\} \overset{PV}{\sim} s\{u\}$.
Hence by definition of $\overset{PV}{\sim}$, $PV \vdash \{s\{t\}\}^{PV} = \{s\{u\}\}^{PV}$.

(7) $t = u$ is an instance of $(R5^\omega)$.
Assume $PV^\omega \vdash t = u \Rightarrow PV \vdash t^{PV} = u^{PV}$.
Then we need to prove $PV^\omega \vdash u = t \Rightarrow PV \vdash \{su[\phi/x]\}^{PV} = \{st[\phi/x]\}^{PV}$.
This proof follows from lemma 6.2.9, th. 6.2.10 and hypothesis.

(8) $t = u$ is an instance of $(R5^\omega)$.
Assume

$$PV^\omega \vdash t[0/x] = u[0/x], t[s_0x/x] = v_0[t/a], u[s_0x/x] = v_0[u/a],$$
$$t[s_1x/x] = v_1[t/a], u[s_1x/x] = v_1[u/a]$$
$$\Rightarrow$$
$$PV \vdash \{t[0/x]\}^{PV} = \{u[0/x]\}^{PV},$$
$$\{t[s_0x/x]\}^{PV} = \{v_0[t/a]\}^{PV}, \{u[s_0x/x]\}^{PV} = \{v_0[u/a]\}^{PV},$$
$$\{t[s_1x/x]\}^{PV} = \{v_1[t/a]\}^{PV}, \{u[s_1x/x]\}^{PV} = \{v_1[u/a]\}^{PV}.$$

Then we need to prove $PV^\omega \vdash t[0/x] = u[0/x], t[s_0x/x] = v_0[t/a]$,
$u[s_0x/x] = v_0[u/a], t[s_1x/x] = v_1[t/a], u[s_1x/x] = v_1[u/a] \Rightarrow PV \vdash t^{PV} = u^{PV}$.
This proof follows from lemma 6.2.9, th. 6.2.10,$(R4)$, $(R5)$ and hypothesis.

∎

Theorem 6.2.22 PV^ω is a conservative extension of PV.

(*proof*)
By th. 6.2.21,
$\forall(t = u) \in L(PV)[PV^\omega \vdash t = u \Rightarrow PV \vdash t^{PV} = u^{PV}]$.
By $t = u \in L(PV)$, $t^{PV} = t$ and $u^{PV} = u$. Hence
$\forall(t = u) \in L(PV)[PV^\omega \vdash t = u \Rightarrow PV \vdash t = u]$.
Therefore PV^ω is a conservative extension of PV. ∎

Chapter 7

The System IPV^ω

The system IPV^ω is a quantified version of PV^ω, employing intuitionistic predicate logic. Main theorem of this chapter is to prove that IPV^ω is a conservative extension of IPV.

7.1 Definition

Definition 7.1.1

(1) The *function symbols* and *terms* of IPV^ω are same as PV^ω.

(2) The *predicate symbols* of IPV^ω are $=$ and $\leq$.

(3) *Bounded quantifiers* are same as defined in Chapter 2.

Definition 7.1.2 The *formulas* of IPV^ω are defined as follows:

(1) The *atomic formulas* are all formulas of the form $t = u$ or $t \leq u$, where t and u are any type 0 term.

(2) If A and B are formulas , then $A \vee B$, $A \wedge B$ and $A \to B$ are formulas.

(3) If A is a formula and x is a variable with type 0, then $\forall x A$ and $\exists x A$ are formulas .

Definition 7.1.3 The *rules of inference* of IPV^ω are defined as follows:

(1) NJ and IR which understood to apply to the many-sorted predicate calculus.

(2) $A \to s = t \vdash A \to u\{s\} = u\{t\}$, where every free variable of s or t which becomes bound in $u\{s\}$ or $u\{t\}$ has no free occurrence in A.

Notice that we have placed all theorems of PV^ω as axioms of IPV^ω, rather than just the axioms of PV^ω (just the axioms of PV are needed as axioms for IPV). The difficulty lies with the powerful PV^ω rule $R3^\omega$. The analogous rule $R3$ of PV is a derived rule in IPV because of the identity axioms, but $R3^\omega$ does not follow from the identity axioms

because s and t may have free variables which are bounding $u\{s\}$ and $u\{t\}$. We cannot translate the rule as an axiom scheme, say $s = t \to u\{s\} = u\{t\}$, because this is not sound. We could incorporate the rule $R3^\omega$ as a rule of IPV^ω, but then the deduction theorem would not hold in IPV^ω. To preserve the deduction theorem, we could add the more general rule

$$A \to s = t \vdash A \to u\{s\} = u\{t\},$$

subject to the restriction that every free variables of s or t which become bound in $u\{s\}$ or $u\{t\}$ has no free occurrence in A. This rule is sound, but (because of $HTLRN$) it would considerably complicate our proof that IPV^ω is a conservative extension of IPV.

Definition 7.1.4 The *axioms* of IPV^ω are defined as follows:

(1) The theorems of PV^ω.

(2) The non-logical axioms of IPV.

(3) $PIND^\omega$ *axiom* :

$$(A[0/x] \wedge \forall x(A[\lfloor \tfrac{1}{2}x \rfloor/x] \to A)) \to \forall x A \ ,$$

where A has the form

$$(\exists y \leq t)u = v$$

with t zero-order open.

Notice that in the formula A of the $PIND^\omega$ scheme the term u and v may have free higher variables, but free variables of t must have type 0. The reason for the latter restriction is that we will require that each bounding term t is bounded by a monotone term. On the other hand, to prove the results on realizability the terms u and v must have free occurrences of higher type variables.

7.2 Conservative extension of IPV

Notation 7.2.1 $A\{S\}$ refers to a formula with a distinguished occurrence of a term S. Then $A\{T\}$ means $A\{S\}$ with the indicated occurrence of S replaced by T. In general S and T may have free variables which become bound in $A\{S\}$ and $A\{T\}$.

Theorem 7.2.2

$a) IPV^\omega \vdash x = 0 \to (A\{Cond_\tau(x, S, T)\} \leftrightarrow A\{S\})$

$b) IPV^\omega \vdash x \neq 0 \to (A\{Cond_\tau(x, S, T)\} \leftrightarrow A\{T\})$,

provided the indicated occurrence of x on the right are free (not bound by quantifiers or λ-terms in $A\{\}$).

(*proof*) We prove by induction on the logical structure of $A\{\}$.

a)

(1) $A\{\}$ is $u = v$.

Then $A\{S\} \equiv u\{S\} = v\{S\}$.

By th. 6.2.5, $u\{S\} = u\{Cond_\tau(0,S,T)\}$ and $v\{S\} = v\{Cond_\tau(0,S,T)\}$.
Hence $u\{S\} = v\{S\} \leftrightarrow u\{Cond_\tau(0,S,T)\} = v\{Cond_\tau(0,S,T)\}$.
Therefore $x = 0 \rightarrow (u\{S\} = v\{S\} \leftrightarrow u\{Cond_\tau(x,S,T)\} = v\{Cond_\tau(x,S,T)\})$.

(2) $A\{\}$ is $u \leq v$.
Same as (1).

For the remaining cases, assume that
$IPV^\omega \vdash x = 0 \rightarrow (B\{S\} \leftrightarrow B\{Cond_\tau(x,S,T)\})$ and
$IPV^\omega \vdash x = 0 \rightarrow (C\{S\} \leftrightarrow C\{Cond_\tau(x,S,T)\})$, where B and C are formulas.

(3) $A\{\}$ is $B\{\} \vee C\{\}$.
Then $A\{S\} \equiv B\{S\} \vee C\{S\}$.
By hypothesis, $B\{S\} \vee C\{S\} \leftrightarrow B\{Cond_\tau(0,S,T)\} \vee C\{Cond_\tau(0,S,T)\}$.
Therefore $x = 0 \rightarrow (B\{S\} \vee C\{S\} \leftrightarrow B\{Cond_\tau(x,S,T)\} \vee C\{Cond_\tau(x,S,T)\})$.

(4) $A\{\}$ is $B\{\} \wedge C\{\}$.
Same as (3).

(5) $A\{\}$ is $\forall z B\{\}$.
By $(\forall I), (\forall E)$ and hypothesis,
$\forall z B\{S\} \leftrightarrow \forall z B\{Cond_\tau(0,S,T)\}$.
Therefore $x = 0 \rightarrow (\forall z B\{S\} \leftrightarrow \forall z B\{Cond_\tau(x,S,T)\})$.

(6) $A\{\}$ is $\exists z B\{\}$.
Same as (5).

B)
Same as A). ∎

Theorem 7.2.3
If A is a Σ_0^b formula of IPV^ω, then there is a term t^A of PV^ω so that

$$IPV^\omega \vdash A \leftrightarrow t^A = 0.$$

(*proof*) We prove by induction on the logical structure of A.
a)

(1) A is $u = v$.
By $u = v \leftrightarrow Equ(u,v) = 0$, and $Equ(u,v) = 0$ is a term of PV^ω.

(2) A is $u \leq v$.
By $u \leq v \leftrightarrow Lessequ(u,v) = 0$, and $Lessequ(u,v) = 0$ is a term of PV^ω.

For the remaining cases, assume that $B \leftrightarrow t^B = 0$, $C \leftrightarrow t^C = 0$ and $D(x,\vec{y}) \leftrightarrow t^D(x,\vec{y}) = 0$.

(3) A is $B \vee C$.
By $B \vee C \leftrightarrow (t^B = 0 \vee t^C = 0) \leftrightarrow (t^B \vee t^C = 0)$.

(4) A is $B \wedge C$.
By $B \wedge C \leftrightarrow (t^B = 0 \wedge t^C = 0) \leftrightarrow (t^B \& t^C = 0)$.

(5) A is $(\forall x \leq |a|)D(x, \vec{y})$.
By $(\forall x \leq |a|)D(x, \vec{y}) \leftrightarrow t^{D^{\forall}}(a, \vec{y}) = 0$.

(6) A is $(\exists x \leq |a|)D(x, \vec{y})$.
By $(\exists x \leq |a|)D(x, \vec{y}) \leftrightarrow t^{D^{\exists}}(a, \vec{y}) = 0$.

∎

Theorem 7.2.4 If A is a Σ_0^b formula of IPV^ω then $IPV^\omega \vdash A \vee \neg A$.

(*proof*) For any Σ_0^b formula A, $PV^\omega \vdash A \rightarrow t^A = 0$ by th. 7.2.3. Then
$PV^\omega \vdash Cond(t^A, 0, 0) = 0$, by T1
$PV^\omega \vdash Cond(t^A, Cond(t^A, 0, 0), Cond(t^A, 1, 0)) = 0$, by T4
$PV^\omega \vdash Cond(t^A, 0, Cond(\sim t^A, 0, 1)) = 0$, by T38
$PV^\omega \vdash Cond(t^A, 0, sg(\sim t^A)) = 0$, by D31
$PV^\omega \vdash t^A \vee \sim t^A = 0$, by D31.
Therefore
$IPV^\omega \vdash t^A \vee \sim t^A = 0$,
$IPV^\omega \vdash t^A = 0 \vee \sim t^A = 0$, by th. 4.2.2(4)
$IPV^\omega \vdash t^A = 0 \vee \neg(t^A = 0)$, by th. 4.2.2(2)
$IPV^\omega \vdash A \vee \neg A$, by th. 7.2.3. ∎

Proposition 7.2.5 For each type 0 zero-order open term s and all type 0 variables x, y there is a term t of PV whose free variables are among those in a such that
(a) $IPV^\omega \vdash s \leq t$
and
(b) $IPV^\omega \vdash x \leq y \rightarrow t \leq t[y/x]$.

(*proof*) Assume that s is an any zero-order open type 0 term.
By th. 6.2.10, $IPV^\omega \vdash s = s^{PV}$.
By T206 and s be a term of PV, there is a term s^{PVM} in PV such that
(1)$Lessequ(s^{PV}(x), s^{PVM}(x)) = 0$
(2)$[Lessequ(x, y) \Rightarrow Lessequ(s^{PVM}(x), s^{PVM}(y))] = 0$
Then
$IPV \vdash Lessequ(s^{PV}(x), s^{PVM}(x)) = 0$ and
$\vdash [Lessequ(x, y) \Rightarrow Lessequ(s^{PVM}(x), s^{PVM}(y))] = 0$ by th. 4.2.1.
$IPV \vdash s^{PV}(x) \leq s^{PVM}(x) = 0$ and $x \leq y \rightarrow s^{PVM}(x) \leq s^{PVM}(y)$ by th. 4.2.2.
Therefore
$IPV^\omega \vdash s^{PV}(x) \leq s^{PVM}(x) = 0$ and $x \leq y \rightarrow s^{PVM}(x) \leq s^{PVM}(y)$.

$IPV^\omega \vdash s(x) \leq s^{PV^M}(x)) = 0$ and $x \leq y \rightarrow s^{PV^M}(x) \leq s^{PV^M}(y)$ by $s = s^{PV}$.
Therefore if we take s^{PV^M} as t, then satisfies (a) and (b). ∎

Recall that $(\exists \vec{y} \leq \vec{t})$ stands for $(\exists y_1 \leq t_1) \cdots (\exists y_n \leq t_n)$.

Theorem 7.2.6 Each instance of the $PIND^\omega$ axiom scheme is a theorem of IPV^ω when A has the more general form

$$(\exists \vec{y} \leq \vec{t})u = v$$

with each t_i zero-order open.

(*proof*) By prop. 7.2.5 and T206, we can prove
$IPV^\omega \vdash (\exists y_1 \leq t_1)(\exists y_2 \leq t_2)u = v \leftrightarrow (\exists z \leq s)u' = v' \cdots\cdots (a)$
by a method same as lemma 4.2.11. By (a), we can prove
$IPV^\omega \vdash (\exists \vec{y} \leq \vec{t})u = v \leftrightarrow (\exists z \leq s)u' = v'$.
Therefore We can apply $PIND^\omega$ to a formula which has a form $(\exists \vec{y} \leq \vec{t})u = v$. ∎

To apply cut elimination, the system IPV and IPV^ω are reformulated in terms of Gentzen's sequent system LJ. In LJ, each node in a proof tree is a sequent of the form $A_1, \cdots, A_n \rightarrow B$, where possibly n=0 or B is missing. The logical rules are those described later. In particular we divide cut rule into *high cut* and *normal cut*. If cut formula A has *higher type quantifiers* then the cut rule is called *high cut* , where *higher type quantifier* is one of the form $\forall X$ or $\exists X$, where X is a variable not of type 0. The logical axioms are all those of the form $A \rightarrow A$, where we require that A be atomic. The set of axioms must be closed under substitution in order for cut elimination to work, so we take as a nonlogical axiom in the old formulation. It is important that no axiom involve higher type quantifiers, so we take as identity axioms every instance of any sequent $x = y \rightarrow (A \leftrightarrow A[y/x])$, where A is atomic.

Since LJ is equivalent to the logical system NJ which is given in Chapter 2, it is not hard to see that the resulting sequent systems for IPV and IPV^ω are equivalent to the original systems, in the sense that $\rightarrow A$ is a theorem of the sequent system iff A is a theorem of the original system.

For the rest of this section we assume that IPV and IPV^ω have their sequent formulations.

Definition 7.2.7 LJ is given by the following rules of inference:

1) Structural rules:

$\dfrac{\Gamma \rightarrow \Delta}{A,\Gamma \rightarrow \Delta}$ (weakening left) $\qquad \dfrac{\Gamma \rightarrow}{\Gamma \rightarrow A}$ (weakening right)

$\dfrac{A,A,\Gamma \rightarrow \Delta}{A,\Gamma \rightarrow \Delta}$ (contraction left) $\qquad \dfrac{\Gamma,A,B,\Pi \rightarrow \Delta}{\Gamma,B,A,\Pi \rightarrow \Delta}$ (exchange left)

$\dfrac{\Gamma \rightarrow A \quad A,\Pi \rightarrow \Delta}{\Gamma,\Pi \rightarrow \Delta}$(normal cut), where A has no higher type quantifier.

$\dfrac{\Gamma \rightarrow A \quad A,\Pi \rightarrow \Delta}{\Gamma,\Pi \rightarrow \Delta}$(high cut), where A has higher type quantifiers.

2) Logical rules:

$$\frac{A,\Gamma\to\Delta}{A\wedge B,\Gamma\to\Delta}\ (\wedge \text{ left1}) \qquad \frac{B,\Gamma\to\Delta}{A\wedge B,\Gamma\to\Delta}\ (\wedge \text{ left2})$$

$$\frac{\Gamma\to A \quad \Gamma\to B}{\Gamma\to A\wedge B}(\wedge \text{ right}) \qquad \frac{A,\Gamma\to\Delta \quad B,\Gamma\to\Delta}{A\vee B,\Gamma\to\Delta}(\vee \text{ left})$$

$$\frac{\Gamma\to A}{\Gamma\to A\vee B}\ (\vee \text{ right1}) \qquad \frac{\Gamma\to B}{\Gamma\to A\vee B}(\vee \text{ right2})$$

$$\frac{\Gamma\to A \quad B,\Pi\to C}{A\supset B,\Gamma,\Pi\to C}(\supset \text{ left}) \qquad \frac{A,\Gamma\to B}{\Gamma\to A\supset B}(\supset \text{ right})$$

$$\frac{\Gamma\to A}{\neg A,\Gamma\to}(\neg \text{ left}) \qquad \frac{A,\Gamma\to}{\Gamma\to\neg A}(\neg \text{ right})$$

3) Quantifier rules

$$\frac{A[T/X],\Gamma\to\Delta}{\forall X A,\Gamma\to\Delta}(\forall \text{ left}) \qquad \frac{\Gamma\to A[Z/X]}{\Gamma\to\forall X A}\ (\forall \text{ right})$$

$$\frac{A[Z/X],\Gamma\to\Delta}{\exists X A,\Gamma\to\Delta}(\exists \text{ left}) \qquad \frac{\Gamma\to A[T/X]}{\Gamma\to\exists X A}\ (\exists \text{ right})$$

where Z does not occur in the lower sequent, and T is an arbitrary term.The variable Z is called *eigenvariable*.

Definition 7.2.8
Mixture rule

$$\frac{\Gamma\to A \quad \Pi_1\to\Delta}{\Gamma,\Pi_2\to\Delta}(\text{A}),$$

where Π_1 contain the formula A, and Π_2 is obtained from Π_1 by deleting all the occurrence of A.

We call A the *mixing formula*. If A has higher type quantifiers then mixture rule is called *higher mixture*, else mixture rule is called *normal mixture*.

Mixture rule is equivalent to cut rule.

Lemma 7.2.9 If $\Gamma\to A$ has a proof in IPV^ω which has no high cut, then every substitution instance of $\Gamma\to A$ has such a proof.

(*proof*) We prove $[\Gamma(x)\to A(x)]\Rightarrow[\Gamma(t)\to A(t)]$ (where t is a term) by induction on a proof P .

(a-1) P is an only logical axiom $A(x)\to A(x)$.
By $A(t)\to A(t)$ be a logical axiom, too.

(a-2) P is an only nonlogical axiom $\to A(x)$.
By only nonlogical axioms be closed under substitution.

For the remaining cases, assume that every substitution instance before last inference has such a proof.

(b) The last inference rule of P is structural rule or logical rule. We prove the rule (normal cut) as an example.

Let P be

$$\dfrac{\begin{array}{cc} M(x) \to M(x) & N(x) \to N(x) \\ \vdots & \vdots \\ \Gamma(x) \to A(x) & A(x), \Pi(x) \to B(x) \end{array}}{\Gamma(x), \Pi(x) \to B(x)}$$

By hypothesis,

$$\begin{array}{ccc} M(t) \to M(t) & & N(t) \to N(t) \\ \vdots & \text{and} & \vdots \\ \Gamma(t) \to A(t) & & A(t), \Pi(t) \to B(t) \end{array}$$

are provable. Hence by (cut),

$$\dfrac{\begin{array}{cc} M(t) \to M(t) & N(t) \to N(t) \\ \vdots & \vdots \\ \Gamma(t) \to A(t) & A(t), \Pi(t) \to B(t) \end{array}}{\Gamma(t), \Pi(t) \to B(t)}$$

(c) The last inference rule of P is a quantifier rule.

Assume that a variable z is the eigenvariable. We prove the rule ($\forall$ right) as an example.

(1) a term t is a variable b and x is the eigenvariable.

Let P be

$$\dfrac{\begin{array}{c} M(x) \to M(x) \\ \vdots \\ \Gamma \to A(x) \end{array}}{\Gamma \to \forall y A(y)}$$

By hypothesis and ($\forall$ right),

$$\dfrac{\begin{array}{c} M(b) \to M(b) \\ \vdots \\ \Gamma \to A(b) \end{array}}{\Gamma \to \forall y A(y)}$$

By $t = b$,

$$\dfrac{\begin{array}{c} M(t) \to M(t) \\ \vdots \\ \Gamma \to A(t) \end{array}}{\Gamma \to \forall y A(y)}$$

(2) a term t is a variable b and x is not the eigenvariable.

Let P be

$$\dfrac{\begin{array}{c} M(x) \to M(x) \\ \vdots \\ \Gamma(x) \to A(x,z) \end{array}}{\Gamma(x) \to \forall y A(x,y)}$$

By hypothesis and ($\forall$ right),

$$\dfrac{\begin{array}{c} M(b) \to M(b) \\ \vdots \\ \Gamma(b) \to A(b,z) \end{array}}{\Gamma(b) \to \forall y A(b,y)}$$

By $t = b$,

$$\dfrac{\begin{array}{c} M(t) \to M(t) \\ \vdots \\ \Gamma(t) \to A(t,z) \end{array}}{\Gamma(t) \to \forall y A(t,y)}$$

By (1) and (2), if P is a proof which contains a variable x, then P' which obtains from replacement x in P a variable b is a proof, too.
($IPV^\omega \vdash \Gamma(x) \to A(x) \Rightarrow IPV^\omega \vdash \Gamma(b) \to A(b)$, where x and b are variables).
We call this property (♣).

(3) $x \neq z$ and z is not free variable in t.
Let P be

$$\dfrac{\begin{array}{c} M(x) \to M(x) \\ \vdots \\ \Gamma(x) \to A(x,z) \end{array}}{\Gamma(x) \to \forall y A(x,y)}$$

By hypothesis and ($\forall$ right),

$$\dfrac{\begin{array}{c} M(t) \to M(t) \\ \vdots \\ \Gamma(t) \to A(t,z) \end{array}}{\Gamma(t) \to \forall y A(t,y)}$$

(4) $x \neq z$ and z is free variable in t.
Let P be

$$\dfrac{\begin{array}{c} M(x,z) \to M(x,z) \\ \vdots \\ \Gamma(x) \to A(x,z) \end{array}}{\Gamma(x) \to \forall y A(x,y)}$$

By (♣),

$$\dfrac{\begin{array}{c} M(x,b) \to M(x,b) \\ \vdots \\ \Gamma(x) \to A(x,b) \end{array}}{}$$

$\Gamma(x) \to \forall y A(x,y)$

where the variable b is not contained in P and t.

By hypothesis and ($\forall$ right),

$$\dfrac{\begin{array}{c} M(t,b) \to M(t,b) \\ \vdots \\ \Gamma(t) \to A(t,b) \end{array}}{\Gamma(t) \to \forall y A(t,y)}$$

By ($\clubsuit$),

$$\dfrac{\begin{array}{c} M(t,z) \to M(t,z) \\ \vdots \\ \Gamma(t) \to A(t,z) \end{array}}{\Gamma(t) \to \forall y A(t,y)}$$

(5) $x = y$ (*i.e.* x is the eigenvariable).

Let P be

$$\dfrac{\begin{array}{c} M(x) \to M(x) \\ \vdots \\ \Gamma \to A(x) \end{array}}{\Gamma \to \forall x A(x)}$$

Then x is not free variable in Γ because of condition of ($\forall$ right). Therefore by hypothesis,

$$\dfrac{\begin{array}{c} M(t) \to M(t) \\ \vdots \\ \Gamma \to A(t) \end{array}}{\Gamma \to \forall x A(t)}$$

∎

Definition 7.2.10 We define *grade*, *thread* and *rank* for next theorem "high mix elimination".

Let P be a proof which contains a mix only as the last inference:

$$J : \dfrac{\Gamma \to A \quad \Pi_1 \to \Delta}{\Gamma, \Pi_2 \to \Delta}\ (\mathrm{A}),$$

The *grade* of a formula A (denoted by $g(A)$) is the number of logical symbols contained in A. The grade of a mix is the grade of the mix formula. When a proof P has a mix as the last inference, we define the grade of P (denoted by $g(P)$) to be the grade of this mix. We refer to the left and right upper sequents as S_1 and S_2, respectively, and to the lower sequent as S. We call a thread in P a $left(right)$ *thread* if it contains the left(right) upper sequent of the mix. J. The *rank* of a thread $\mathbf{T}$ in P is defined as follows : if $\mathbf{T}$ is a left(right) thread, then the rank of $\mathbf{T}$ is the number of consecutive sequents, counting upward from the left(right) upper sequent of J, that contains the mix formula, the rank

of a thread in P is at least 1. The rank of thread $\mathbf{T}$ in P is denoted by $\mathrm{rank}(\mathbf{T};P)$. We define

$$\mathrm{rank}_l(P) = \max(\mathrm{rank}(\mathbf{T};P)),$$

where $\mathbf{T}$ ranges over all the left threads in P, and

$$\mathrm{rank}_r(P) = \max(\mathrm{rank}(\mathbf{T};P)),$$

where $\mathbf{T}$ ranges over all the right threads in P. The rank of (P) , $\mathrm{rank}(P)$, is defined as

$$\mathrm{rank}(P) = \mathrm{rank}_l(P) + \mathrm{rank}_r(P).$$

Notice that $\mathrm{rank}(P)$ is always ≥ 2.

Lemma 7.2.11 If $\Gamma \to A$ is a sequent of IPV and a theorem of IPV^ω, then $\Gamma \to A$ has a proof in IPV^ω which does not involve higher type quantifiers.

(*proof*) Since $\Gamma \to A$ has no higher type quantifier, it suffices to find a proof of $\Gamma \to A$ which has no high mix. Therefore we need to prove high mix elimination.

proof of high mix elimination

Let P be a proof which contains a mix only as the last inference. We prove by double induction on the grade d and rank r.

(1) r=2 *i.e.* $\mathrm{rank}_l(P) = \mathrm{rank}_r(P) = 1$

(a) The left upper sequent S_1 is an initial sequent.
In this case assume P is of the form

$$J : \frac{A \to A \quad \Pi_1 \to \Delta}{A, \Pi_2 \to \Delta}\ (A).$$

We prove $A, \Pi_2 \to \Delta$ without a mix.

$$\cfrac{\cfrac{\cfrac{\Pi_1 \to \Delta}{\text{some exchanges}}\ A, \cdots, A, \Pi_2 \to \Delta}{\text{some contractions}}}{A, \Pi_2 \to \Delta}$$

(b) The left upper sequent S_2 is an initial sequent.
Same as (a).

(c) Neither S_1 nor S_2 is an initial sequent, and S_1 is the lower sequent of a structural inference J_1. Since $\mathrm{rank}_l(P) = 1$, the formula A cannot appear in

the upper sequent of J_1, *i.e.*, J_1 must be a weakening : right, whose weakening formula is A :

$$\dfrac{\dfrac{\Gamma \to}{\Gamma \to A}\ J_1 \quad \Pi_1 \to \Delta}{\Gamma, \Pi_2 \to \Delta}\ (A)$$

We prove $\Gamma, \Pi_2 \to \Delta$ without a mix.

$$\dfrac{\dfrac{\dfrac{\dfrac{\Gamma \to}{some\ \ weakenings}}{\Pi_2, \Gamma \to}}{some\ \ exchanges}}{\Gamma, \Pi_2 \to \Delta}\ (weakening\ \ right)$$

(d) Neither S_1 nor S_2 is an initial sequent, and S_2 is the lower sequent of a structural inference J_2. Same as (c).

(e) Both S_1 and S_2 are lower sequents of logical inferences.
In this case, mixing formula has the form $B \wedge C, B \vee C, B \supset C$ and $\neg B$, where bounded quantifiers are contained in B or C always. We prove $B \wedge C$ as an example. Since $\mathrm{rank}_l(P) = \mathrm{rank}_r(P) = 1$, assume P is of the form

$$\dfrac{\dfrac{\Gamma \to B \quad \Gamma \to C}{\Gamma \to B \wedge C} \quad \dfrac{\Pi_2 \to \Delta}{B \wedge C, \Pi_2 \to \Delta}}{\Gamma, \Pi_2 \to \Delta}\ (B \wedge C)$$

We prove $\Gamma, \Pi_2 \to \Delta$ without a mix.

$$\dfrac{\dfrac{\Pi_2 \to \Delta}{some\ \ weakenings}}{\Gamma, \Pi_2 \to \Delta}$$

(f) Both S_1 and S_2 are lower sequents of quantifier inferences.
In this case, mixing formula has the form $\forall X B(X)$ or $\exists X B(X)$. We prove $\forall X B(X)$ as an example. Since $\mathrm{rank}_l(P) = \mathrm{rank}_r(P) = 1$, assume P is of the form

$$\dfrac{\dfrac{\Gamma \to B(Z)}{\Gamma \to \forall X B(X)} \quad \dfrac{B(T), \Pi_2 \to \Delta}{\forall X B(X), \Pi_2 \to \Delta}}{\Gamma, \Pi_2 \to \Delta}\ (\forall X B(X))$$

By eigenvariable condition, Z does not occur in Γ and $B(X)$. By lemma 7.2.9, we can prove $\Gamma \to B(T)$ from $\Gamma \to B(Z)$ without high mix. Using this, We prove $\Gamma, \Pi_2 \to \Delta$ without a mix.

$$\dfrac{\dfrac{\Gamma \to B(Z)}{\Gamma \to B(T)} \quad B(T), \Pi_2 \to \Delta}{\Gamma, \Pi_2 \to \Delta}\ (normal\ \ cut)$$

(2) $\mathrm{rank}_r(P) > 1$

(a) Γ (in S_1) contains A.
We prove $\Gamma, \Pi_2 \to \Delta$ without a mix as follows.

$$\dfrac{\dfrac{\dfrac{\Pi_1 \to \Delta}{\textit{some exchanges and contractions}}}{A, \Pi_2 \to \Delta}}{\dfrac{\textit{some weakenings and exchanges}}{\Gamma, \Pi_2 \to \Delta}}$$

(b) S_1 is the lower sequent of an inference J_2, where J_2 is not a logical inference whose principal formula is A. The last part of P looks like this:

$$\dfrac{\Gamma \to A \quad \dfrac{\Phi \to \Psi}{\Pi_1 \to \Delta}\, J_2}{\Gamma, \Pi_2 \to \Delta}\, (A),$$

where the proofs of $\Gamma \to \Delta$ and $\Phi \to \Psi$ contain no mixes and Φ contains at least one A. Consider the following proof P':

$$\textit{high mix} \quad \dfrac{\Gamma \to A \quad \Phi \to \Psi}{\Gamma, \Phi^* \to \Psi}\, (A).$$

Then $\mathrm{rank}_l(P') = \mathrm{rank}_l(P)$ and $\mathrm{rank}_r(P')$ =$\mathrm{rank}_r(P)$ - 1. Thus by the induction hypothesis, $\Gamma, \Phi^* \to \Psi$ is provable without a mix. Therefore

$$\dfrac{\dfrac{\dfrac{\dfrac{\Gamma, \Phi^* \to \Psi}{\textit{some exchanges}}}{\Phi^*, \Gamma \to \Psi}}{\Pi_2, \Gamma \to \Delta}\, J_2}{\textit{some exchanges}}}{\Gamma, \Pi_2 \to \Delta}$$

(c) Γ contains no A's, and S_2 is the lower sequent of a logical rule or quantifier rule whose principal formula is A. Although there are several cases according to the outermost logical symbol of A, we prove two examples.

i. A is $B \supset C$, where bounded quantifiers are contained in B or C always. The last part of P is of the form:

$$J \quad \dfrac{\Gamma \to B \supset C \quad \dfrac{\Phi_1 \to B \quad C, \Phi_2 \to \Delta}{B \supset C, \Phi_1, \Phi_2 \to \Delta}\, J_2}{\Gamma, \Phi_1^*, \Phi_2^* \to \Delta}\, (B \supset C).$$

If $B \supset C$ is in Φ_1 and Φ_2, then we consider the following proofs P_1 and P_2:

$$P_1 \quad \dfrac{\Gamma \to B \supset C \quad \Phi_1 \overset{\vdots}{\to} B}{\Gamma, \Phi_1^* \to B}\, (B \supset C),$$

$$P_2 \qquad \frac{\begin{array}{cc}\vdots & \vdots \\ \Gamma \to B \supset C & C, \Phi_2 \to \Delta\end{array}}{\Gamma, C, \Phi_2^* \to \Delta}\,(B \supset C),$$

else if $B \supset C$ is not in Φ_1 or Φ_2, then Φ_1 and Φ_2 are defined as follows :

$$P_1 \qquad \frac{\begin{array}{c}\vdots \\ \Phi_1 \to B\end{array}}{\dfrac{weakenings\ and\ exchanges}{\Gamma, \Phi_1^* \to B}}$$

$$P_2 \qquad \frac{\begin{array}{c}\vdots \\ C, \Phi_2 \to \Delta\end{array}}{\dfrac{weakenings\ and\ exchanges}{\Gamma, C, \Phi_2^* \to \Delta}}$$

Note that $g(P_1) = g(P_2) = g(P)$, $\mathrm{rank}_l(P_1) = \mathrm{rank}_l(P_2) = \mathrm{rank}_l(P)$ and $\mathrm{rank}_l(P_1) = \mathrm{rank}_l(P_2) = \mathrm{rank}_l(P)$ - 1. Hence by induction hypothesis, the end sequents of P_1 and P_2 are provable without a high mix (say by P_1' and P_2'). Consider the following proof P' :

$$J \qquad \frac{\Gamma \to B \supset C \quad \dfrac{\begin{array}{c}P_1' \\ \vdots \\ \Gamma, \Phi_1^* \to B\end{array} \quad \dfrac{\begin{array}{c}P_2' \\ \vdots \\ C, \Gamma, \Phi_2^* \to \Delta\end{array}}{B \supset C, \Gamma, \Phi_1^*, \Gamma, \Phi_2^* \to \Delta}}{\Gamma, \Gamma, \Phi_1^*, \Gamma, \Phi_2^* \to \Delta}\ (B \supset C).$$

Then $g(P') = g(P)$, $\mathrm{rank}_l(P') = \mathrm{rank}_l(P)$, $\mathrm{rank}_r(P') = 1$, for Γ contains no occurrences of $B \supset C$ and $\mathrm{rank}(P') < \mathrm{rank}(P)$. Thus the end-sequent of P' is provable without a mix by the induction hypothesis, and hence so is the end-sequent of P.

ii. A is $\exists X F(X)$.
The last part of P is of the form:

$$J \quad \frac{\Gamma \to \exists X F(X) \quad \dfrac{F(T), \Phi_1 \to \Delta}{\exists X F(X), \Phi_1 \to \Delta}}{\Gamma, \Phi_1^* \to \Delta}\ (\exists X F(X)).$$

Let Y be a free variable not occurring in P. Then the result of replacing T by Y throughout the proof ending with $F(T), \Phi_1 \to \Delta$ is a proof, without a mix, ending with $F(Y), \Phi_1 \to \Delta$, since by the eigenvariable condition, Y does not occur in Φ_1 or Δ.
Consider the following proof :

$$J \qquad \frac{\begin{array}{cc}\vdots & \vdots \\ \Gamma \to \exists X F(X) & F(Y), \Phi_1 \to \Delta\end{array}}{\Gamma, F(Y), \Phi_1^* \to \Delta}\ (\exists X F(X)).$$

By the induction hypothesis, the end-sequent of this proof can be proved without a mix (say by P'). Now consider the proof

$$J\dfrac{\begin{array}{c}\vdots\\ \Gamma \to \exists X F(X)\end{array} \quad \dfrac{\dfrac{\begin{array}{c}P'\\ \vdots\\ \Gamma, F(Y), \Phi_1 \to \Delta\end{array}}{some\ \ exchange}}{F(Y), \Gamma, \Phi_1 \to \Delta}}{\exists X F(X), \Gamma, \Phi_1^* \to \Delta}\ (\exists X F(X)),$$

$$\Gamma, \Gamma, \Phi_1^* \to \Delta$$

where Y occurs in none of $\exists X F(X), \Gamma, \Phi_1, \Delta$ This mix can then also be eliminated by the induction hypothesis.

(3) $\mathrm{rank}_r(P) = 1$ and $\mathrm{rank}_l(P) > 1$
Same as (2).

∎

Definition 7.2.12 The transformation $t \rightsquigarrow \{t\}^{PV}$ takes a zero-order open formula A of IPV^ω with no higher type quantifiers to an equivalent formula $\{A\}^{IPV}$ of IPV, and is defined inductively as follows:

$$\begin{array}{l}
\{t = u\}^{IPV} \stackrel{d}{\equiv} t^{PV} = u^{PV}\\
\{t \le u\}^{IPV} \stackrel{d}{\equiv} t^{PV} \le u^{PV}\\
\{AcB\}^{IPV} \stackrel{d}{\equiv} A^{IPV} c B^{IPV}, \text{ where } c \text{ is } \to, \vee \text{ or } \wedge\\
\{\forall x A\}^{IPV} \stackrel{d}{\equiv} \forall x A^{IPV}\\
\{\exists x A\}^{IPV} \stackrel{d}{\equiv} \exists x A^{IPV}\\
\{A_1, \cdots, A_n\}^{IPV} \stackrel{d}{\equiv} A_1^{IPV}, \cdots, A_n^{IPV}
\end{array}$$

For every zero-order open type zero term t of PV^ω
$\{S[t/x]\} \equiv S^{IPV}[t^{PV}/x]$,
where S is a sequent or formula of IPV^ω.

Lemma 7.2.13 If a proof P of IPV^ω does not involve higher type quantifiers, then $IPV \vdash \{S'\}^{IPV}$ for every zero-order open instance S' of any sequent S in P.

(*proof*) We prove by induction on the length of the longest path S to a leaf in P.

base step S is an axiom.

(1) S is an axiom of IPV.
By $IPV \vdash S$ and $\{S\}^{IPV} \equiv S$, $IPV \vdash \{S\}^{IPV}$.

(2) S is a theorem of PV^ω.
Let $S \equiv (u = v)$. By th. 6.2.21, $PV^\omega \vdash t = u \Rightarrow PV \vdash t_1^{PV} = u_1^{PV}$.
By $t_1^{PV} = u_1^{PV} \equiv \{t_1 = u_1\}^{IPV}$, $IPV \vdash \{t_1 = u_1\}^{IPV}$.
Therefore $IPV \vdash \{S'\}^{IPV}$.

(3) S is $PIND^\omega$.
By $S \equiv A(0) \wedge \forall x(A(\lfloor \frac{1}{2}x \rfloor) \rightarrow A(x)) \rightarrow \forall x A(x)$,
$\{S\}^{IPV} \equiv \{A(0)\}^{IPV} \wedge \forall x(\{A(\lfloor \frac{1}{2}x \rfloor)\}^{IPV} \rightarrow \{A(x)\}^{IPV}) \rightarrow \forall x\{A(x)\}^{IPV}$.
This is NP-Induction of IPV. Hence $IPV \vdash \{S\}^{IPV}$.

induction step S is the consequence in P of appling a rule of LJ. Then we define S' as upper sequent of S. We need to prove for each rule. In here, We prove the rule ($\wedge$ left) as an example. Define $S \equiv A \wedge B, \Gamma \rightarrow \Delta$ and $S' \equiv A, \Gamma \rightarrow \Delta$. Then we need to prove that $[IPV \vdash \{A\}^{IPV}, \{\Gamma\}^{IPV} \rightarrow \{\Delta\}^{IPV}] \Rightarrow [IPV \vdash \{A \wedge B\}^{IPV}, \{\Gamma\}^{IPV} \rightarrow \{\Delta\}^{IPV}]$.
Assume $IPV \vdash \{A\}^{IPV}, \{\Gamma\}^{IPV} \rightarrow \{\Delta\}^{IPV}$.
By ($\wedge$ left), $IPV \vdash \{A\}^{IPV} \wedge \{B\}^{IPV}, \{\Gamma\}^{IPV} \rightarrow \{\Delta\}^{IPV}$.
By definition of $\{\}^{IPV}$, $IPV \vdash \{A \wedge B\}^{IPV}, \{\Gamma\}^{IPV} \rightarrow \{\Delta\}^{IPV}$. ∎

Theorem 7.2.14 IPV^ω is a conservative extension of IPV.

(*proof*)
By lemma 7.2.13,
$\forall(\Gamma \rightarrow \Delta) \in L(IPV)[IPV^\omega \vdash \Gamma \rightarrow \Delta \Rightarrow IPV \vdash \{\Gamma\}^{IPV} \rightarrow \{\Delta\}^{IPV}]$.
By $(\Gamma \rightarrow \Delta) \in L(IPV)$, $(\{\Gamma\}^{IPV} \rightarrow \{\Delta\}^{IPV}) \equiv \Gamma \rightarrow \Delta$. Hence
$\forall(\Gamma \rightarrow \Delta) \in L(IPV)[IPV^\omega \vdash \Gamma \rightarrow \Delta \Rightarrow IPV \vdash \Gamma \rightarrow \Delta]$.
Therefore IPV^ω is a conservative extension of IPV. ∎

Chapter 8

Realizability

Realizability by numbers was first introduced by S.C.Kleene in 1945 [7], and was intended as a kind of reinterpretation of intuitionistic arithmetic, so as to bring out more explicitly the intended constructive interpretation of the logical operators. As such, it may be viewed as a variant of the abstract interpretation scheme first introduced by Heyting. As we shall see from the definition and results in the sequel, Kleene's notion is not just a variant of , but essentially differs from the interpretation intended by Heyting. Hence, it cannot be said to make the intended meaning of the logical operators more precise. As a "philosophical reduction" of the interpretation of the logical operators it is also only moderately successful ; *i.e.* negative formulae are essentially interpreted by themselves.

On the other hand, realizability possesses some nice formal properties, which provide it with some mathematical interest of its own ; but more important, realizability and he many variants deriving from it turn out to be very convenient tools in the development intuitionistic proof theory.

Modified realizability was first introduced and used in Kreisel. Modified realizability in its abstract form provides interpretation s of the various HA^ω-versions into themselves ; the interpretation may be specialized (to an interpretation in (a subsystem of) a version of another system) by specifying a model for the objects of finite type.

One of its most distinctive properties is that Markov's principle is no validated by modified realizability ; this was already noted and used by Kreisel to show underivability of Markov's principle in systems of intuitionistic analysis.

On the other hand, modified realizability validates

$(\neg A \to \exists y B) \to \exists y(\neg A \to B)$, where y is not free in A.

This fact is connected with its invalidating Markov's principle.

This property was used for proof-theoretic applications("derived rules").

In this section we present a form of Kreisel's modified realizability for the system IPV^ω. As applications, we show that decidable formula represent polynomial time predicates, prove a version of Buss's main theorem for IS^2_1 relating existence proofs and polynomial time functions, and prove two of Buss's conjectures concerning IS^2_1.

Our version of realizability is a translation of IPV^ω a formula $\vec{X}\circledR A$ (read $\vec{X}$ realizes A) of IPV^ω, where $\vec{X}$ is a sequence of zero or more variables of types determined by the variables $\vec{X}$ help to explain why A is true. Our definition follows that presented in

[10]. The main difference is the conjunct $A \to B$ in clause (iv) below, which assures that provably realizable formulas are provable, and allows us to prove theorem 8.1.6 and Buss's conjectures. In standard realizability, a suitable version of the axiom of choice is provably realizable but not provable [10].

Main theorem of this chapter is to prove that if $IPV \vdash \forall \vec{x} \exists y A(\vec{x}, y)$ then there is a PV function symbol f such that $IPV \vdash \forall \vec{x} A(\vec{x}, f(\vec{x}))$.

8.1 Definition

To apply realizability, the system IPV and IPV^ω are reformulated in terms of *Hilbert Style* system. *Hilbert Style* is very similar to NJ. NJ has some rules which of hypothesis are struck out, $(\to I), (\vee E)$ and $(\exists E)$. But *Hilbert Style* has no such a rule. This property is very useful of realizability. And *Hilbert Style* is equivalent to the logical system NJ. Therefore in this chapter and next chapter we assume that logical rules and axioms of IPV and IPV^ω are *Hilbert Style*.

Definition 8.1.1 *Hilbert Style of intuitionistic predicate logic* is given by the following axioms and rules of inference:

Axiom Schemes

1. $A \to (A \wedge A)$
2. $(A \vee A) \to A$
3. $(A \wedge B) \to B$
4. $B \to (A \vee B)$
5. $(A \wedge B) \to (B \wedge A)$
6. $(A \vee B) \to (B \vee A)$
7. $\forall x A \to A[t/x]$
8. $A[t/x] \to \exists x A$
9. $(0 = 1) \to A$

Rules of Inference

10. $\dfrac{A, A \to B}{B}$
11. $\dfrac{A \to B, B \to C}{A \to C}$
12. $\dfrac{(A \wedge B) \to C}{A \to (B \to C)}$
13. $\dfrac{A \to (B \to C)}{(A \wedge B) \to C}$
14. $\dfrac{A \to B}{C \vee A \to C \vee B}$
15. $\dfrac{A \to B}{A \to \forall x B}$
16. $\dfrac{B \to A}{\exists x B \to A}$

Identity axioms

17. $x = x$
18. $x = y \to (A \leftrightarrow A[y/x])$

In axiom schemes 7 and 8, $A[t/x]$ stands for the result of substituting the term t for all free occurrences of x in A; t must not contain an occurrence of a free variable which becomes bound in $A[t/x]$. In rules 15 and 16, x must not occur free in A.

Notation 8.1.2 We use the notation $\vec{X}$ for $X_1, \cdots, X_n$ and $\vec{Y}$ for $Y_1, \cdots, Y_k$, $n, k \geq 0$, and $\vec{Y}(\vec{X})$ for $Y_1(\vec{X}), \cdots, Y_k(\vec{X})$, etc. Also Λ stands for the empty sequence of variables, and $Y(\Lambda) \stackrel{d}{\equiv} Y$.

Definition 8.1.3 (Kreisel's modified realizability)
$\vec{X} \circledR A$ is defined by induction on the logical structure of A. We assume that no variable in

the list $\vec{X}$ occurs free in A. $\vec{T}\circledR A \stackrel{d}{\equiv} (\vec{X}\circledR A)[\vec{T}/\vec{X}]$; that is $\vec{X}\circledR A$ with the simultaneous substitution of T_i for X_i $(1 \leq i \leq n)$.

(i) $\Lambda\circledR A \stackrel{d}{\equiv} A$, if A is atomic.

(ii) $\vec{X},\vec{Y}\circledR(A \wedge B) \stackrel{d}{\equiv} \vec{X}\circledR A \wedge \vec{Y}\circledR B$.

(iii) $z,\vec{X},\vec{Y}\circledR(A \vee B) \stackrel{d}{\equiv} (z = 0 \wedge \vec{X}\circledR A) \vee (z \neq 0 \wedge \vec{Y}\circledR B)$.

(iv) $\vec{Y}\circledR(A \to B) \stackrel{d}{\equiv} \forall\vec{X}(\vec{X}\circledR A \to \vec{Y}(\vec{X})\circledR B) \wedge (A \to B)$.

(v) $\vec{X}\circledR\forall Y A \stackrel{d}{\equiv} \forall Y(\vec{X}(Y)\circledR A)$.

(vi) $Z,\vec{X}\circledR\exists Y A \stackrel{d}{\equiv} \vec{X}\circledR A[Z/Y]$.

Proposition 8.1.4 $\Lambda\circledR\neg A \equiv \forall\vec{Y}(\neg(\vec{Y}\circledR A)) \wedge \neg A$

(*proof*)
$\Lambda\circledR\neg A \equiv \Lambda\circledR(A \to (0 = 1))$, by def. 8.1.3 (iv)
$\equiv \forall\vec{Y}(\vec{Y}\circledR A \to A(\vec{Y})\circledR(0 = 1)) \wedge (A \to (0 = 1))$, by def. 8.1.3 (i)
$\equiv \forall\vec{Y}(\vec{Y}\circledR A \to (0 = 1)) \wedge \neg A$,
$\equiv \forall\vec{Y}(\neg(\vec{Y}\circledR A)) \wedge \neg A$. ∎

Proposition 8.1.5

a)Each free variables of $\vec{X}\circledR A$ is either free in A or in the list $\vec{X}$.

b)If Y is not in the list $\vec{X}$, then $\vec{X}\circledR A[T/Y] \equiv (\vec{X}\circledR A)[T/Y]$.

(*proof*)
a)We prove by induction on the logical structure of A.

(1) A is atomic.
There are only free variables in A. Therefore variables in $\vec{X}\circledR A$ are only free variables in A or in the list $\vec{X}$.

For the remaining cases, we assume that free variables of $\vec{X}\circledR B$ are either free in B or in the list $\vec{X}$ and free variables of $\vec{Y}\circledR C$ are either free in C or in the list $\vec{Y}$.

(2) A is $B \wedge C$.
By def. 8.1.3 (ii), $\vec{X},\vec{Y}\circledR(B \wedge C) \equiv (\vec{X}\circledR B) \wedge (\vec{Y}\circledR C)$.
Hence each free variables of $\vec{X},\vec{Y}\circledR(B \wedge C)$ is a free variable of $\vec{X}\circledR B$ or $\vec{Y}\circledR C$.
Therefore each free variables of $\vec{X},\vec{Y}\circledR(B \wedge C)$ is in the list $\vec{X},\vec{Y}$ or in $B \wedge C$.

(3) A is $B \vee C$.
By def. 8.1.3 (iii), $z, \vec{X}, \vec{Y}®(B \vee C) \equiv (z = 0 \wedge \vec{X}®B) \vee (z \neq 0 \wedge \vec{Y}®C)$.
By hypothesis,
each free variables of $z, \vec{X}, \vec{Y}®(B \vee C)$ is z or free variable of $\vec{X}®B$ or $\vec{Y}®C$.
Therefore each free variables of $z, \vec{X}, \vec{Y}®(B \vee C)$ is in the list $z, \vec{X}, \vec{Y}$ or in $B \vee C$.

(4) A is $B \to C$.
By def. 8.1.3 (iv), $\vec{Y}®(B \to C) \equiv \forall \vec{X}(\vec{X}®B \to \vec{Y}(\vec{X})®C) \wedge (B \to C)$. Hence free variables of $\vec{Y}®(B \to C)$ are free variables of $(B \to C)$ or B or $\vec{Y}(\vec{X})®C$ without $\vec{X}$. Therefore each free variables of $\vec{Y}®(B \to C)$ is in $(B \to C)$ or in the list $\vec{Y}$.

(5) A is $\forall ZB$.
By def. 8.1.3 (v), $\vec{X}®\forall ZB \equiv \forall Z(\vec{X}(Z)®B)$.
Hence free variables of $\vec{X}®\forall ZB$ are free variables of $\vec{X}(Z)®B$ without Z.
Therefore each free variables of $\vec{X}®\forall ZB$ is in the list $\vec{X}$ or in B.

(6) A is $\exists ZB$.
By def. 8.1.3 (vi), $W, \vec{X}®\exists ZB \equiv \vec{X}®B[W/Z]$.
Hence free variables of $W, \vec{X}®\exists ZB$ are free variables of $\vec{X}®B[W/Z]$.
Therefore each free variables of $W, \vec{X}®\exists ZB$ is in the list $W, \vec{X}$ or in $\exists ZB$.

b) By Y be not in the list $\vec{X}$, $\vec{X} \equiv \vec{X}[T/Y]$.
Therefore $\vec{X}®(A[T/Y]) \equiv \vec{X}[T/Y]®A[T/Y] \equiv (\vec{X}®A)[T/Y]$. ∎

Theorem 8.1.6 For every formula A of IPV^ω

$$IPV^\omega \vdash \exists \vec{X}(\vec{X}®A) \to A.$$

(*proof*) We prove by induction on the logical structure of A.

(1) A is atomic.
By $A \to A$, $\Lambda®A \to A$. By $\Lambda®A \to A$, $\exists \vec{X}(\vec{X}®A) \to A$.

For the remaining cases, we assume that $\exists \vec{Y}(\vec{Y}®B) \to B$ and $\exists \vec{Z}(\vec{Z}®D) \to D$.
Let variables $a, \vec{U}, \vec{V}, W, W'$ and W'' are not contained in B, D and in the list $\vec{Y}, \vec{Z}$.

(2) A is $B \wedge D$.
By $\vec{U}®B \to \vec{U}®B$, $\vec{U}®B \to \exists \vec{Y}(\vec{Y}®B)$.
By this and $\exists \vec{Y}(\vec{Y}®B) \to B$, $\vec{U}®B \to B$. Hence $\vec{U}®B \wedge \vec{V}®D \to B$.
Same as $\vec{U}®B \wedge \vec{V}®D \to D$. Hence $\vec{U}®B \wedge \vec{V}®D \to B \wedge D$.
Therefore $\exists \vec{Y} \exists \vec{Z}(\vec{Y}, \vec{Z}®(B \wedge D)) \to (B \wedge D)$.

(3) A is $B \vee D$.
By same method as (2), $\vec{U}®B \to B$. Hence $a = 0 \wedge \vec{U}®B \to B \vee D$.
By same method as upper, $a \neq 0 \wedge \vec{U}®D \to B \vee D$.

Hence $(a = 0 \wedge \vec{U}\circledR B) \vee (a \neq 0 \wedge \vec{U}\circledR D) \rightarrow B \vee D$.
Therefore $\exists z \exists \vec{Y} \exists \vec{Z}(z, \vec{Y}, \vec{Z}\circledR(B \vee D)) \rightarrow B \vee D$.

(4) A is $B \rightarrow D$.
By $(B \rightarrow D) \rightarrow (B \rightarrow D)$, $\forall \vec{V}(\vec{V}\circledR B \rightarrow \vec{U}(\vec{V})\circledR D) \wedge (B \rightarrow D) \rightarrow (B \rightarrow D)$.
Hence $\vec{U}\circledR(B \rightarrow D) \rightarrow (B \rightarrow D)$.
Therefore $\exists \vec{X}(\vec{X}\circledR(B \rightarrow D)) \rightarrow (B \rightarrow D)$.

(5) A is $\forall W D$.
By same method as (2), $\vec{U}(W')\circledR D \rightarrow D$. Hence $\forall W(\vec{U}(W)\circledR D) \rightarrow D$.
By this, $\forall W(\vec{U}(W)\circledR D) \rightarrow \forall W D$. Hence $\vec{U}\circledR \forall W D \rightarrow \forall W D$.
Therefore $\exists \vec{Z}(\vec{Z}\circledR \forall W D) \rightarrow \forall W D$.

(6) A is $\exists W D$.
By same method as (2), $\vec{U}\circledR A[W'/W] \rightarrow A[W'/W]$.
Hence $\vec{U}\circledR A[W'/W] \rightarrow \exists W D$.
By def. 8.1.3 (vi), $W', \vec{U}\circledR \exists W D \rightarrow \exists W D$.
Therefore $\exists W'' \exists \vec{Z}(W'', \vec{Z}\circledR \exists W D) \rightarrow \exists W D$.

∎

Corollary 8.1.7 $IPV^\omega \vdash (\Lambda\circledR\neg A) \leftrightarrow \neg A$.

(*proof*)

(1) $\Lambda\circledR\neg A \rightarrow \neg A$.
By th. 8.1.6, $\vec{X}(\vec{X}\circledR\neg A) \rightarrow \neg A$.
By $\Lambda\circledR\neg A \rightarrow \Lambda\circledR\neg A$. By this and $\vec{X}(\vec{X}\circledR\neg A) \rightarrow \neg A$, $\Lambda\circledR\neg A \rightarrow \neg A$.

(2) $\neg A \rightarrow \Lambda\circledR\neg A$.
By $\neg A \rightarrow \neg A$, $\neg A \rightarrow (\Lambda\circledR A \rightarrow \Lambda(\Lambda)\circledR(0 = 1))$.
Hence $\neg A \rightarrow \forall \vec{Y}(\vec{Y}\circledR\vec{Y} \rightarrow \Lambda(\vec{Y})\circledR(0 = 1))$.
By this and $\neg A \rightarrow \neg A$, $\neg A \rightarrow \forall \vec{Y}(\vec{Y}\circledR\vec{Y} \rightarrow \Lambda(\vec{Y})\circledR(0 = 1)) \wedge (A \rightarrow (0 = 1))$.
Hence $\neg A \rightarrow \Lambda\circledR(A \rightarrow (0 = 1))$. Therefore $\neg A \rightarrow \Lambda\circledR\neg A$.

∎

8.2 Soundness of Realizability

Theorem 8.2.1 (**Soundness Theorem**)
If $IPV^\omega \vdash A$ then $IPV^\omega \vdash \vec{T}\circledR A$ for some sequence $\vec{T}$ of terms whose free variables are among the free variables of A.

(*proof*) We prove by induction on the IPV^ω proof of A. We first consider the logical axiom and rules.

(1) **Axiom scheme 1**

Define as $R \stackrel{d}{\equiv} \lambda\vec{Y}.0$ and $\vec{S} \equiv \vec{T} \stackrel{d}{\equiv} \lambda\vec{Y}.\vec{Y}$. Then by $\vec{U}\circledR A \to \vec{U}\circledR A$,
$\vec{U}\circledR A \to (R(\vec{U}) = 0 \wedge \vec{S}(\vec{U})\circledR A) \vee (R(\vec{U}) \neq 0 \wedge \vec{T}(\vec{U})\circledR A)$.
By def. 8.1.3(iii), $\vec{U}\circledR A \to (R(\vec{U}), \vec{S}(\vec{U}), \vec{T}(\vec{U}))\circledR A \vee A$.
Hence $\forall\vec{X}[\vec{X}\circledR A \to (R, \vec{S}, \vec{T})(\vec{X})\circledR A \vee A] \wedge (A \to A \vee A)$.
Therefore $(R, \vec{S}, \vec{T})\circledR(A \to A \vee A)$.

(2) **Axiom scheme 2**

By $(z = 0 \wedge \vec{X}\circledR A) \vee (z \neq 0 \wedge \vec{Y}\circledR A) \to (z = 0 \wedge \vec{X}\circledR A) \vee (z \neq 0 \wedge \vec{Y}\circledR A)$
and th. 7.2.2,
$(z = 0 \wedge \vec{X}\circledR A) \vee (z \neq 0 \wedge \vec{Y}\circledR A) \to [(\vec{X}\circledR A \wedge (\vec{X}\circledR A \to Cond_\tau(z, \vec{X}, \vec{Y})\circledR A)) \vee$
$(\vec{Y}\circledR A \wedge (\vec{Y}\circledR A \to Cond_\tau(z, \vec{X}, \vec{Y})\circledR A))]$.
Hence $(z = 0 \wedge \vec{X}\circledR A) \vee (z \neq 0 \wedge \vec{Y}\circledR A) \to Cond_\tau(z, \vec{X}, \vec{Y})\circledR A \vee Cond_\tau(z, \vec{X}, \vec{Y})\circledR A$.
By def. 8.1.3 (iii), $(z, \vec{X}, \vec{Y})\circledR(A \vee A) \to Cond_\tau(z, \vec{X}, \vec{Y})\circledR A$. Hence
$\forall z\vec{X}\vec{Y}[(z, \vec{X}, \vec{Y})\circledR(A \vee A) \to (\lambda u\vec{S}\vec{T}.Cond(u, \vec{S}, \vec{T}))(z, \vec{X}, \vec{Y})\circledR A] \wedge (A \vee A \to A)$.
By def. 8.1.3 (iv), $(\lambda u\vec{S}\vec{T}.Cond(u, \vec{S}, \vec{T}))\circledR(A \vee A \to A)$.

(3) **Axiom scheme 3**

By $\vec{X}\circledR A \wedge \vec{Y}\circledR B \to \vec{Y}\circledR B$,
$\forall\vec{X}\vec{Y}[\vec{X}, \vec{Y}\circledR A \wedge B \to (\lambda\vec{S}\vec{T}.\vec{T})(\vec{X}, \vec{Y})\circledR B] \wedge (A \wedge B \to B)$.
Therefore by def. 8.1.3 (iv), $(\lambda\vec{S}\vec{T}.\vec{T})\circledR(A \wedge B \to B)$.

(4) **Axiom scheme 4**

Define as $R \stackrel{d}{\equiv} \lambda\vec{Y}.1$ and $\vec{S} \equiv \vec{T} \stackrel{d}{\equiv} \lambda\vec{Y}.\vec{Y}$. Then by $\vec{X}\circledR B \to \vec{X}\circledR B$,
$\vec{X}\circledR B \to [(R(\vec{X}) = 0 \wedge \vec{S}(\vec{X})\circledR A) \vee (R(\vec{X}) \neq 0 \wedge \vec{T}(\vec{X})\circledR B)]$.
By def. 8.1.3 (iii), $\vec{X}\circledR B \to (R(\vec{X}), \vec{S}(\vec{X}), \vec{T}(\vec{X}))\circledR A \vee B$.
Hence $\forall\vec{X}[\vec{X}\circledR B \to (R, \vec{S}, \vec{T})(\vec{X})\circledR A \vee B] \wedge (B \to A \vee B)$.
By def. 8.1.3 (iv), $(R, \vec{S}, \vec{T})\circledR(B \to A \vee B)$.

(5) **Axiom scheme 5**

By $\vec{X}\circledR A \wedge \vec{Y}\circledR B \to \vec{Y}\circledR B \wedge \vec{X}\circledR A$ and def. 8.1.3 (ii),
$\vec{X}, \vec{Y}\circledR A \wedge B \to \vec{Y}, \vec{X}\circledR B \wedge A$. Hence $\vec{X}, \vec{Y}\circledR A \wedge B \to (\lambda\vec{S}\vec{T}.(\vec{T}, \vec{S}))(\vec{X}, \vec{Y})\circledR B \wedge A$.
Therefore $\forall\vec{X}\vec{Y}[\vec{X}, \vec{Y}\circledR A \wedge B \to (\lambda\vec{S}\vec{T}.(\vec{T}, \vec{S}))(\vec{X}, \vec{Y})\circledR B \wedge A] \wedge (A \wedge B \to B \wedge A)$.
By def. 8.1.3 (iv), $(\lambda\vec{S}\vec{T}.(\vec{T}, \vec{S}))\circledR(A \wedge B \to B \wedge A)$.

(6) **Axiom scheme 6**

Define as $R \stackrel{d}{\equiv} \lambda u\vec{V}\vec{W}.sg(u)$, $\vec{S} \stackrel{d}{\equiv} \lambda u\vec{V}\vec{W}.\vec{W}$ and $\vec{T} \stackrel{d}{\equiv} \lambda u\vec{V}\vec{W}.\vec{V}$.
By D47, $z = 0 \leftrightarrow \overline{sg}(z) \neq 0$ and $z \neq 0 \leftrightarrow \overline{sg}(z) = 0$.
By $(z = 0 \wedge \vec{X}\circledR A) \vee (z \neq \vec{Y}\circledR B) \to (z \neq \vec{Y}\circledR B) \vee (z = 0 \wedge \vec{X}\circledR A)$,
$(z = 0 \wedge \vec{X}\circledR A) \vee (z \neq \vec{Y}\circledR B) \to (\overline{sg}(z) \neq \vec{Y}\circledR B) \vee (\overline{sg}(z) = 0 \wedge \vec{X}\circledR A)$.
By def. 8.1.3 (iii), $(z, \vec{X}, \vec{Y}\circledR A \vee B) \to ((R, \vec{S}, \vec{T})(z, \vec{X}, \vec{Y})\circledR B \vee A)$.
Hence $\forall z\vec{X}\vec{Y}[z, \vec{X}, \vec{Y}\circledR A \vee B) \to ((R, \vec{S}, \vec{T})(z, \vec{X}, \vec{Y})\circledR B \vee A)] \wedge (A \vee B \to B \vee A)$.
By def. 8.1.3 (iv), $(R, \vec{S}, \vec{T})\circledR(A \vee B \to B \vee A)$.

(7) **Axiom scheme 7**

By $\forall Y(\vec{X}(Y)\circledR A) \to (\vec{X}(Y)\circledR A)[T/Y]$, $\forall Y(\vec{X}(Y)\circledR A) \to (\vec{X}(T)\circledR A[T/Y]$.
Hence $\forall \vec{X}(\forall Y(\vec{X}(Y)\circledR A) \to (\lambda \vec{V}.\vec{V}(T))\vec{X}\circledR A[T/Y]) \wedge (\forall Y A \to A[T/Y]$.
By def. 8.1.3 (iv), $(\lambda \vec{V}.\vec{V}(T))\circledR \forall Y A \to A[T/Y]$.

(8) **Axiom scheme 8**

Define as $R \stackrel{d}{\equiv} \lambda \vec{V}.T$ and $\vec{S} \stackrel{d}{\equiv} \lambda \vec{V}.\vec{V}$.
By $\vec{X}\circledR A[T/Y] \to \vec{X}\circledR A[T/Y]$ and def. 8.1.3 (vi), $\vec{X}\circledR A[T/Y] \to T, \vec{X}\circledR \exists Y A$.
Hence $\forall \vec{X}[\vec{X}\circledR A[T/Y] \to (R, \vec{S})(\vec{X})\circledR \exists Y A] \wedge (A[T/Y] \to \exists Y A)$.
By def. 8.1.3 (iv), $(R, \vec{S})\circledR(A[T/Y] \to \exists Y A)$.

(9) **Axiom scheme 9**

By $(0 = 1) \to \vec{R}\circledR A$ and def. 8.1.3 (i), $\Lambda\circledR(0 = 1) \to \vec{R}(\Lambda)\circledR A$.
Hence $\forall \vec{X}(\vec{X}\circledR(0 = 1) \to \vec{R}(\vec{X})\circledR A) \wedge (0 = 1) \to A$.
By def. 8.1.3 (iv),$\vec{R}\circledR(0 = 1) \to A$.

(10) **Axiom scheme 17**

By def. 8.1.3 (i), $\Lambda\circledR x = x$.

(11) **Axiom scheme 18**

Define as $S \equiv T \stackrel{d}{\equiv} \lambda \vec{W}.\vec{W}$. And assume that variables x and y are not contained in the list $\vec{Y}$.
By $x = y \to (\vec{Y}\circledR A \to (\vec{Y}\circledR A)[y/x])$,
$x = y \to (\vec{Y}\circledR A \to (\lambda \vec{W}.\vec{W})(\vec{Y})\circledR A[y/x])$.
By Rule 15 and Axiom 18,
$x = y \to \forall \vec{Y}(\vec{Y}\circledR A \to (\lambda \vec{W}.\vec{W})(\vec{Y})\circledR A[y/x]) \wedge (A \to A[y/x])$.
By def. 8.1.3 (iv), $x = y \to (\lambda \vec{W}.\vec{W})\circledR(A \to A[y/x])$.
Therefore $x = y \to S\circledR(A \to A[y/x])$.
Therefore $x = y \to S(\Lambda)\circledR(A \to A[y/x]) \cdots\cdots (\alpha)$.
Same as $x = y \to T(\Lambda)\circledR(A[y/x] \to A) \cdots\cdots (\beta)$.
By $x = y \to x = y \wedge x = y, (\alpha), (\beta)$ and def. 8.1.3 (i),
$\Lambda\circledR x = y \to (S(\Lambda)\circledR(A \to A[y/x]) \wedge T(\Lambda)\circledR(A[y/x] \to A))$.
By 8.1.3 (ii), $\Lambda\circledR x = y \to S(\Lambda), T(\Lambda)\circledR(A \to A[y/x] \wedge A[y/x] \to A)$.
Hence $0 = 0 \to (\Lambda\circledR x = y \to (S, T)(\Lambda)\circledR A \leftrightarrow A[y/x])$.
By Rule 15, $0 = 0 \to \forall \vec{X}(\vec{X}\circledR x = y \to (S, T)(\vec{X})\circledR A \leftrightarrow A[y/x])$.
By 0=0 and def. 8.1.3 (iv), $(S, T)\circledR(x = y \to (A \leftrightarrow A[y/x]))$.

(12) **Rule of inference 10**

We need to prove that if $\vec{S}\circledR A$ and $\vec{T}\circledR A \to B$ then there exists $\vec{W}$ which satisfy $\vec{W}\circledR B$. Assume $\vec{S}\circledR A$ and $\vec{T}\circledR(A \to B)$.
By $\vec{T}\circledR A \to B \equiv \forall \vec{X}(\vec{X}\circledR A \to \vec{T}(\vec{X})\circledR B) \wedge (A \to B)$, $\vec{S}\circledR A \to \vec{T}(\vec{S})\circledR B$.
By this and $\vec{S}\circledR A$, $\vec{T}(\vec{S})\circledR B$. Therefore we take $\vec{S}(\vec{X})$ as $\vec{W}$.

(13) **Rule of inference 11**

We need to prove that if $\vec{S}®(A \to B)$ and $\vec{T}®(B \to C)$ then there exists $\vec{W}$ such that $\vec{W}®(A \to C)$. Assume $\vec{S}®(A \to B)$ and $\vec{T}®(B \to C)$. By hypothesis, $\vec{U}®A \to \vec{S}(\vec{U})®B$ and $\vec{S}(\vec{U})®B \to \vec{T}(\vec{S}(\vec{U}))®C$. Hence $\vec{U}®A \to \vec{T}(\vec{S}(\vec{U}))®C$. By this, $A \to B$ and $B \to C$, $\forall\vec{U}(\vec{U}®A \to (\lambda\vec{W}.\vec{T}(\vec{S}(\vec{W})))(\vec{U})®C) \wedge (A \to C)$. Therefore $(\lambda\vec{W}.\vec{T}(\vec{S}(\vec{W})))®(A \to C)$. Therefore we take $\lambda\vec{W}.\vec{T}(\vec{S}(\vec{W}))$ as $\vec{W}$.

(14) **Rule of inference 12**

We need to prove that if $\vec{S}®(A \wedge B \to C)$ then there exists $\vec{T}$ which satisfy $\vec{T}®(A \to (B \to C))$. Assume $\vec{S}®(A \wedge B \to C)$.

$\vec{S}®(A \wedge B \to C) \equiv \forall\vec{X}\vec{Y}(\vec{X},\vec{Y}®A \wedge B \to \vec{S}(\vec{X},\vec{Y})®C) \wedge (A \wedge B \to C)$

$\equiv \forall\vec{X}\vec{Y}(\vec{X}®A \wedge \vec{Y}®B \to \vec{S}(\vec{X},\vec{Y})®C) \wedge (A \wedge B \to C)$.

Hence $\vec{X}®A \wedge \vec{Y}®B \to \vec{S}(\vec{X},\vec{Y})®C$.

By Rule 12, $\vec{X}®A \to (\vec{Y}®B \to \vec{S}(\vec{X},\vec{Y})®C))$

By Rule 15, $\vec{X}®A \to \forall\vec{Y}(\vec{Y}®B \to (\lambda\vec{W}.\vec{S}(\vec{X},\vec{W}))(\vec{Y})®C)$.

By def. 8.1.3 (iv), $\vec{X}®A \to (\lambda\vec{W}.\vec{S}(\vec{X},\vec{W}))®(B \to C)$.

By Axiom 7, Rule 11 and $(A \wedge B \to C)$,

$\forall\vec{X}(\vec{X}®A \to (\lambda\vec{V}\vec{W}.\vec{S}(\vec{V},\vec{W}))(\vec{X})®(B \to C)) \wedge (A \to (B \to C))$.

By def. 8.1.3 (iv), $(\lambda\vec{V}\vec{W}.\vec{S}(\vec{V},\vec{W}))®(A \to (B \to C))$.

Therefore we take $(\lambda\vec{V}\vec{W}.\vec{S}(\vec{V},\vec{W}))$ as $\vec{T}$.

(15) **Rule of inference 13**

We need to prove that if $\vec{S}®(A \to (B \to C))$ then there exists $\vec{T}$ such that $\vec{T}®(A \wedge B \to C)$. Assume $\vec{S}®(A \to (B \to C))$.

$\vec{S}®(A \to (B \to C)) \equiv \forall\vec{X}(\vec{X}®A \to \vec{S}(\vec{X})®(B \to C)) \wedge (A \to (B \to C))$

$\equiv \forall\vec{X}(\vec{X}®A \to \forall\vec{Y}(\vec{Y}®B \to \vec{S}(\vec{X}(\vec{Y})))) \wedge (A \to (B \to C))$.

Hence $\vec{V}®A \to (\vec{W}®B \to \vec{S}(\vec{V}(\vec{W}))®C)$.

By Rule 13, $(\vec{V}®A \wedge \vec{W}®B) \to (\lambda\vec{M}\vec{N}.\vec{S}(\vec{M}(\vec{N})))(\vec{V},\vec{W})®C$.

By Axiom 7, Rule 11 and $A \to (B \to C)$,

$\forall\vec{X}\vec{Y}(\vec{X},\vec{Y}®A \wedge B \to (\lambda\vec{M}\vec{N}.\vec{S}(\vec{M}(\vec{N})))(\vec{X},\vec{Y})®C) \wedge (A \wedge B \to C)$.

By def. 8.1.3 (iv), $(\lambda\vec{M}\vec{N}.\vec{S}(\vec{M}(\vec{N})))®(A \wedge B \to C)$.

Therefore we take $(\lambda\vec{M}\vec{N}.\vec{S}(\vec{M}(\vec{N})))$ as $\vec{T}$.

(16) **Rule of inference 14**

We need to prove that if $\vec{T}®(A \to (B \to C))$ then there exists $\vec{W}$ such that $\vec{W}®(C \vee A \to C \vee B)$. Assume $\vec{T}®(A \to (B \to C))$. We define $P, \vec{R}$ and $\vec{S}$ as $P \stackrel{d}{\equiv} \lambda u\vec{V}\vec{W}.u$, $\vec{R} \stackrel{d}{\equiv} \lambda u\vec{V}\vec{W}.\vec{V}$ and $\vec{S} \stackrel{d}{\equiv} \lambda u\vec{V}\vec{W}.\vec{T}(\vec{W})$. By hypothesis, $\vec{Y}®A \to \vec{T}(\vec{Y})®B$. Hence $z \neq 0 \wedge \vec{Y}®A \to z \neq 0 \wedge \vec{T}(\vec{Y})®B$. By Rule 14, $(z = 0 \wedge \vec{X}®C) \vee (z \neq 0 \wedge \vec{Y}®A) \to (z = 0 \wedge \vec{X}®C) \vee (z \neq 0 \wedge \vec{T}(\vec{Y})®B)$.

By def. 8.1.3 (iii), $z, \vec{X}, \vec{Y}®C \vee A \to z, \vec{X}, \vec{T}(\vec{Y})®C \vee B$.

Hence $z, \vec{X}, \vec{Y}®C \vee A \to (P, \vec{R}, \vec{S})(z, \vec{X}, \vec{Y})®C \vee B$. By this and $A \to B$, $\forall z\vec{X}\vec{Y}[z, \vec{X}, \vec{Y}®C \vee A \to (P, \vec{R}, \vec{S})(z, \vec{X}, \vec{Y})®C \vee B] \wedge (C \vee A \to C \vee B)$.

By def. 8.1.3 (iv), $(P, \vec{R}, \vec{S})\circledR(C \vee A \to C \vee B)$. Therefore we take $(P, \vec{R}, \vec{S})$ as $\vec{W}$.

(17) **Rule of inference 15**
We need to prove that if $\vec{T}\circledR(A \to B)$ then there exists $\vec{R}$ such that $\vec{R}\circledR(A \to \forall Y B)$, where Y is not contained in A. Assume $\vec{T}\circledR(A \to B)$.
By hypothesis, $\vec{S}\circledR A \to \vec{T}(\vec{S})\circledR B$, where $\vec{S}$ not contain Y. By Rule 15,
$\vec{S}\circledR A \to \forall Y((\lambda V.\vec{T}(\vec{S}))(Y)\circledR\forall Y B)$, where V is not free variable in $\vec{T}(\vec{S})$.
By def. 8.1.3 (v), $\vec{S}\circledR A \to (\lambda V.\vec{T}(\vec{S}))\circledR\forall Y B$.
Hence $\vec{S}\circledR A \to (\lambda\vec{W}V.\vec{T}(\vec{W}))(\vec{S})\circledR\forall Y B$.
By Axiom 7, Rule 11 and $A \to B$,
$\forall\vec{X}(\vec{X}\circledR A \to (\lambda\vec{W}V.\vec{T}(\vec{W}))(\vec{X})\circledR\forall Y B) \wedge (A \to \forall Y B)$.
By def. 8.1.3 (iv), $(\lambda\vec{W}V.\vec{T}(\vec{W}))\circledR(A \to \forall Y B)$.
Therefore we take $\lambda\vec{W}V.\vec{T}(\vec{W})$ as $\vec{R}$.

(18) **Rule of inference 16**
We need to prove that if $\vec{T}\circledR(B[Z/Y] \to A)$ then there exists $\vec{R}$ such that $\vec{R}\circledR(\exists Y B \to A)$. where Y is not free variable in A. Assume $\vec{T}\circledR(B[Z/Y] \to A)$.
By hypothesis, $\vec{X}\circledR B[Z/Y] \to \vec{T}(\vec{X})\circledR A$. By def. 8.1.3 (vi),
$Z, \vec{X}\circledR\exists Y B \to (\lambda V\vec{W}.\vec{T}(\vec{W}))(z, \vec{X})\circledR A$, where V is not free variable in $\vec{T}(\vec{X})$.
By $B[Z/X] \to A$, $\forall Z, \vec{X}(Z, \vec{X}\circledR\exists Y B \to (\lambda V\vec{W}.\vec{T}(\vec{W}))(z, \vec{X})\circledR A) \wedge \exists Y B \to A$.
By def. 8.1.3 (iv), $(\lambda V\vec{W}.\vec{T}(\vec{W}))\circledR(\exists Y B \to A)$.
Therefore we take $(\lambda V\vec{W}.\vec{T}(\vec{W}))$ as $\vec{R}$.

(19) **Theorems of** PV^ω (def. 4.1.2(1))
Theorems of PV^ω are form of $u = v$. Therefore $\Lambda\circledR u = v$.

(20) $\mathbf{x \le y \leftrightarrow Lessequ(x, y) = 0}$ (def. 4.1.2(2))
$x \le y$ and $Lessequ(x, y) = 0$ are atomic formulas. Therefore
$$\begin{aligned}(x \le y \leftrightarrow Lessequ(x, y) = 0) &\leftrightarrow (\Lambda\circledR x \le y \leftrightarrow \Lambda(\Lambda)\circledR Lessequ(x, y) = 0)\\ &\leftrightarrow (\forall\vec{X}(\vec{X}\circledR x \le y \leftrightarrow \vec{X}(\Lambda)\circledR Lessequ(x, y) = 0))\\ &\leftrightarrow (\Lambda\circledR(x \le y \leftrightarrow Lessequ(x, y) = 0)).\end{aligned}$$

(21) $\mathbf{x = s_0\lfloor\frac{1}{2}x\rfloor \vee x = s_1\lfloor\frac{1}{2}x\rfloor}$ (def. 4.1.2(3))
By $x = s_0\lfloor\frac{1}{2}x\rfloor \vee x = s_1\lfloor\frac{1}{2}x\rfloor$,
$(Parity(x) = 0 \wedge (\Lambda\circledR x = s_0\lfloor\frac{1}{2}x\rfloor)) \vee (Parity(x) \neq 0 \wedge (\Lambda\circledR x = s_1\lfloor\frac{1}{2}x\rfloor))$.
By def. 8.1.3 (iii), $(Parity(x), \Lambda, \Lambda)\circledR(x = s_0\lfloor\frac{1}{2}x\rfloor \vee x = s_1\lfloor\frac{1}{2}x\rfloor)$.

(22) $\mathbf{Cond(x, a, b) = c \leftrightarrow (x = 0 \wedge a = c) \vee (\neg(x = 0) \wedge b = c)}$ (def. 4.1.2(4))
By same method of (21),
$(x, \Lambda, \Lambda)\circledR(Cond(x, a, b) = c \to (x = 0 \wedge a = c) \vee (\neg(x = 0) \wedge b = c))$ and
$(\lambda u\vec{S}\vec{T}.\Lambda)\circledR((x = 0 \wedge a = c) \vee (\neg(x = 0) \wedge b = c) \to Cond(x, a, b) = c)$. Therefore
$(x, \Lambda, \Lambda), (\lambda u\vec{S}\vec{T}.\Lambda)\circledR Cond(x, a, b) = c \leftrightarrow (x = 0 \wedge a = c) \vee (\neg(x = 0) \wedge b = c)$.

(23) $\mathbf{PIND}^\omega$ (def. 4.1.2(5))
We use the notation $B(x, y)$ for the equation $u = v$ of PV^ω, where x, y are type 0

variables, and $B(s,t)$ denotes $u = v$ with the simultaneous substitution of s,t for x,y. Then a $PIND^\omega$ axiom has the form

$$I \stackrel{d}{\equiv} ((\exists y \le t'')B(0,y) \wedge \forall x J) \to \forall x(\exists y \le t)B(x,y)$$

where

$$J \stackrel{d}{\equiv} ((\exists y \le t')B(\lfloor \tfrac{1}{2}x \rfloor, y) \to (\exists y \le t)B(x,y)),$$
$$t'' \equiv t[0/x] \text{ and } t' \equiv t[\lfloor \tfrac{1}{2}x \rfloor / x],$$

and t is zero-order open with no free occurrence of y.

We need to find a term $\mathcal{S}$ of PV^ω for proof such that $IPV^\omega \vdash \mathcal{S}\circledR I$.

$$\mathcal{S}\circledR I \equiv \forall y Y[(y \le t'' \wedge B(0,y) \wedge \forall x(Y(x)\circledR J)) \to \forall x(\mathcal{S}(y,Y,x) \le t \wedge B(x,\mathcal{S}(y,Y,x)))] \wedge I$$

and

$$Y(x)\circledR J \equiv \forall y[y \le t' \wedge B(\lfloor \tfrac{1}{2}x \rfloor, y) \to Y(x,y) \le t \wedge B(x, Y(x,y))] \wedge J.$$

We hope that $\mathcal{S}$ satisfies under conditions.

1) $\mathcal{S}(y,Y,0) = y$

If $x = 0$, then $B(x,\mathcal{S}(y,Y,x)) \equiv B(0,\mathcal{S}(y,Y,0))$. And the hypothesis of $\mathcal{S}\circledR I$ contain the condition "$B(0,y)$".

2) $\mathcal{S}(y,Y,x) = Y(x,\mathcal{S}(y,Y,\lfloor \tfrac{1}{2}x \rfloor))$

Assume $x \neq 0$. Then $B(\lfloor \tfrac{1}{2}x \rfloor, \mathcal{S}(y,Y,\lfloor \tfrac{1}{2}x \rfloor)) \to B(x, Y(x,\mathcal{S}(y,Y,\lfloor \tfrac{1}{2}x \rfloor)))$ by $Y(x)\circledR J$. And one of result of $\mathcal{S}\circledR I$ is $B(x,\mathcal{S}(y,Y,x))$.

3) $\mathcal{S}(y,Y,x) \le t$

This is obvious.

Therefore we define $\mathcal{S}$ by $HTLRN$ as follows

$$\mathcal{S} \stackrel{d}{\equiv} \lambda y Y x.\mathcal{R}(y, \lambda x' z.Y(x',z), \lambda x'.2 \cdot t[x'/x], x).$$

Then

$$IPV^\omega \vdash \mathcal{S}(y,Y,x) = Cond(x,y,Cond(u \dot{-} 2 \cdot t, u, 2 \cdot t)) \cdot \cdots \cdot \textcircled{2},$$

where $u \stackrel{d}{\equiv} Y(x,\mathcal{S}(y,Y,\lfloor \tfrac{1}{2}x \rfloor))$.

We would like to prove $\mathcal{S}\circledR I$ in IPV^ω by induction on x. In order to apply a suitable $PIND^\omega$ axiom, we must transform $\mathcal{S}\circledR I$ to be of the form $\exists y \le t(u = v)$. First we drop the conjunct I from $\mathcal{S}\circledR I$, since I is already an axiom of IPV^ω, and we strengthen the assertion $\mathcal{S}\circledR I$ by dropping the conjunct J from $Y(x)\circledR J$. The result has the form

$$\forall y Y[(C \wedge \forall x y D) \to \forall x E] \cdot \cdots \cdot \textcircled{1},$$

where

$$C \stackrel{d}{\equiv} y \le t'' \wedge B(0,y)$$
$$D \stackrel{d}{\equiv} y \le t' \wedge B(\lfloor \tfrac{1}{2}x \rfloor, y) \to Y(x,y) \le t \wedge B(x, Y(x,y))$$
$$E \stackrel{d}{\equiv} \mathcal{S}(y,Y,x) \le t \wedge B(x,\mathcal{S}(y,Y,x)).$$

Note that C, D and E are quantifier-free.

Let

$$A(x) \stackrel{d}{\equiv} \exists x' \le x \exists y' \le u(C \wedge D' \to E)$$

where

$$u \stackrel{d}{\equiv} t[\lfloor \tfrac{1}{2}x' \rfloor / x] \text{ and } D' \stackrel{d}{\equiv} D[x'y'/xy].$$

This is a suitable formula for a $PIND^{\omega}$ axiom by theorem 7.2.3 and theorem 7.2.6. We use this fact to prove below that $IPV^{\omega} \vdash A(x)$. First note that using Theorem 4.2.2, the truth-functional connectives in $A(x)$ can be re-interpreted as the usual connective $\wedge, \vee\neg, \rightarrow$ in IPV^{ω}. Next, the bounds on the existential quantifiers in A can be dropped (they only strengthen the assertion) and standard intuitionistic reasoning then yield ①, and hence $IPV^{\omega} \vdash \mathcal{S}\circledR I$.

It remains to prove A by $PIND^{\omega}$ induction.

1) base step

By $C \rightarrow y \leq t[0/x] \wedge B(0,y)$ and $y = \mathcal{S}(y,Y,0)$,
$C \rightarrow \mathcal{S}(y,Y,0) \leq t[0/x] \wedge B(0,\mathcal{S}(y,Y,0))$. Hence $C \rightarrow E[0/x]$.
By this and $C \wedge D[00/xy] \rightarrow C$, $C \wedge D[00/xy] \rightarrow E[0/x]$.
Therefore $0 \leq 0 \wedge (0 \leq t[\lfloor \frac{1}{2}0 \rfloor/x] \wedge (C \wedge D[00/xy] \rightarrow E[0/x]))$.
Hence $\exists x'(x' \leq 0 \wedge \exists y' \leq t[\lfloor \frac{1}{2}x' \rfloor/x](C \wedge D[x'y'/xy] \rightarrow E[0/x]))$.
Therefore $\exists x' \leq 0 \exists y' \leq u(C \wedge D' \rightarrow E[0/x])$.
Therefore We can prove $A(0)$ in IPV^{ω}.

2) induction step

Assume $A(\lfloor \frac{1}{2}x \rfloor)$. For any x' and y' $IPV^{\omega} \vdash (C \wedge D') \vee \neg(C \wedge D')$ because $C \wedge D'$ is Σ_0^b-formula.

i) The case "$\neg(C \wedge D')$".
$A(x)$ is obvious.

ii) The case "$C \wedge D'$".
By $A(\lfloor \frac{1}{2}x \rfloor)$, $E[\lfloor \frac{1}{2}x \rfloor/x]$ is provable. $E[\lfloor \frac{1}{2}x \rfloor/x] \equiv \mathcal{S}(y,Y,\lfloor \frac{1}{2}x \rfloor) \leq t[\lfloor \frac{1}{2}x \rfloor/x] \wedge B(\lfloor \frac{1}{2}x \rfloor, \mathcal{S}(y,Y,\lfloor \frac{1}{2}x \rfloor))$. We define x' and y' as $x' \stackrel{d}{\equiv} x$ and $y' \stackrel{d}{\equiv} \mathcal{S}(y,Y,\lfloor \frac{1}{2}x \rfloor)$.
Then $y' \leq t[\lfloor \frac{1}{2}x' \rfloor/x] \wedge B(\lfloor \frac{1}{2}x' \rfloor, y')(\equiv y' \leq u \wedge B(\lfloor \frac{1}{2}x' \rfloor, y'))$ is provable, too.
And $IPV^{\omega} \vdash (C \wedge D') \vee \neg(C \wedge D')$ for these x' and y'.

i') The case "$\neg(C \wedge D')$".
$C \wedge D' \rightarrow E$ is obvious.

ii') The case "$C \wedge D'$".
By C, D' and $E[\lfloor \frac{1}{2}x' \rfloor/x]$, $Y(x',y') \leq t \wedge B(x', Y(x',y'))$. Therefore $Y(x, \mathcal{S}(y,Y,\lfloor \frac{1}{2}x \rfloor)) \leq t \wedge B(x, Y(x, \mathcal{S}(y,Y,\lfloor \frac{1}{2}x \rfloor)))$. By this and ②, $u \leq t \wedge B(x,u)$. Hence $(u \leq t \wedge B(x,u)) \wedge u \dot{-} 2 \cdot t = 0 \wedge x \neq 0$.
By ②, $(u \leq t \wedge B(x,u)) \wedge u = \mathcal{S}(y,Y,x)$.
Therefore E.

By i' and ii', if $C \wedge D'$ then E.
By i and ii, if $A(\lfloor \frac{1}{2}x \rfloor)$, then $A(x)$.

By 1 and 2, A is provable.

By (1)-(23), Realizability is soundness.

∎

8.3 Main theorem

Proposition 8.3.1 If $IPV^\omega \vdash A(x) \vee \neg A(x)$, where $A(x)$ has only the type 0 variable x occurring free, then there is a PV function symbol f such that

$$IPV^\omega \vdash f(x) = 0 \leftrightarrow A(x).$$

The same holds with IPV^ω replaced (twice) by IPV.

(*proof*)Assume $IPV^\omega \vdash A(x) \vee \neg A(x)$. By soundness theorem, There exist $T, \vec{U}$ and Λ such that $T, \vec{U}, \Lambda ® \forall x(A(x) \vee \neg A(x))$, where $T, \vec{U}, \Lambda ® \forall x(A(x) \vee \neg A(x)) \equiv$
$T, \vec{U}, \Lambda ® \forall x[(T(x) = 0 \wedge \vec{U} ® A(x)) \vee (T(x) \neq 0 \wedge \Lambda ® \neg A(x))]$, where T is closed and has type $0 \to 0$. Then $\{T(x)\}^{PV}$ is term of PV because a term of IPV^ω is a term of PV^ω and $T(x)$ is zero-order open. We define f as $f \stackrel{d}{\equiv} [\lambda x.\{T(x)\}^{PV}]$. Then f is a function symbol of IPV^ω because f is a function symbol of PV by definition 3.1.2(7). Therefore

$$\begin{aligned} IPV^\omega \vdash f(x) &= [\lambda x.\{T(x)\}^{PV}](x) \\ &= \{T(x)\}^{PV} \\ &= T(x), \text{ by theorem } 6.2.10. \end{aligned}$$

(1) $A(x) \to f(x) = 0$

(i) $(T(x) = 0 \wedge \vec{U} ® A(x)) \to T(x) = 0$
$\to f(x) = 0.$

(ii) $(T(x) \neq 0 \wedge \Lambda ® \neg A(x)) \to \neg A(x)$
$\to (A(x) \to 0 = 1)$
$\to (A(x) \to f(x) = 0).$

By (i),(ii), $(T(x) = 0 \wedge \vec{U} ® A(x)) \vee (T(x) \neq 0 \wedge \Lambda ® \neg A(x))$ and $(\vee E)$,
$IPV^\omega \vdash A(x) \to f(x) = 0.$

(2) $f(x) = 0 \to A(x)$

(i) $(T(x) = 0 \wedge \vec{U} ® A(x)) \to (f(x) = 0 \to A(x))$.
Assume $T(x) = 0 \wedge \vec{U} ® A(x)$. By theorem 8.1.6, $\exists \vec{X}(\vec{X} ® A(x)) \to A(x)$.
By this and $\vec{U} ® A(x) \to \exists \vec{X}(\vec{X} ® A(x))$, $\vec{U} ® A(x) \to A(x)$.
By $(T(x) = 0 \wedge \vec{U} ® A(x))$, $\vec{U} ® A(x)$. By this and $\vec{U} ® A(x) \to A(x)$, $A(x)$.
Hence $f(x) = 0 \to A(x)$.
Therefore $(T(x) = 0 \wedge \vec{U} ® A(x)) \to (f(x) = 0 \to A(x))$.

(ii) $(T(x) \neq 0 \wedge \Lambda ® \neg A(x)) \to (f(x) = 0 \to A(x))$.
Assume $T(x) \neq 0 \wedge \Lambda ® \neg A(x)$. Then $T(x) \neq 0$. Hence $f(x) \neq 0$.
If we assume $f(x) = 0$ then this contradict to $f(x) \neq 0$.
Therefore $f(x) = 0 \to 0 = 1$.
Hence $f(x) = 0 \to A(x)$.

Therefore $(T(x) \neq 0 \wedge \Lambda \circledR \neg A(x)) \rightarrow (f(x) = 0 \rightarrow A(x))$.

By (i) and (ii), $IPV^\omega \vdash f(x) = 0 \rightarrow A(x)$.

By (1) and (2), if $IPV^\omega \vdash A(x) \vee \neg A(x)$ then $IPV^\omega \vdash f(x) = 0 \leftrightarrow A(x)$. ∎

Theorem 8.3.2 Let $\forall \vec{X} \exists Y A(\vec{X}, Y)$ be a closed Theorem of IPV^ω. Then there is a closed term S of IPV^ω such that

$$IPV^\omega \vdash \forall \vec{X} A(\vec{X}, S(\vec{X})).$$

The same is true with IPV^ω replaced (twice) by IPV.

(*proof*)

(1) $IPV^\omega \vdash \forall \vec{X} A(\vec{X}, S(\vec{X}))$.
Assume $IPV^\omega \vdash \forall \vec{X} \exists Y A(\vec{X}, Y)$. By theorem 8.2.1,
there exist closed terms $S, \vec{T}$ such that $IPV^\omega \vdash S, \vec{T} \circledR \forall \vec{X} \exists Y A(\vec{X}, Y)$.
This means $IPV^\omega \vdash \forall \vec{X} (\vec{T}(\vec{X}) \circledR A(\vec{X}, S(\vec{X})))$.
By theorem 8.1.6, $IPV^\omega \vdash \forall \vec{X} A(\vec{X}, S(\vec{X}))$.

(2) $IPV \vdash \forall \vec{X} A(\vec{X}, S(\vec{X}))$.
Same as IPV^ω.

∎

Theorem 8.3.3 Let $\forall \vec{x} \exists y A(\vec{x}, y)$ be a closed theorem of IPV^ω such that the variables $\vec{x}, y$ have type 0. Then there is a PV function symbol f such that

$$IPV^\omega \vdash \forall \vec{x} A(\vec{x}, f(\vec{x})).$$

The same is true with IPV^ω replaced (twice) by IPV.

(*proof*)

(1) $IPV^\omega \vdash \forall \vec{x} A(\vec{x}, f(\vec{x}))$.
Assume $IPV^\omega \vdash \forall \vec{x} \exists y A(\vec{x}, y)$. Then by theorem 8.3.2, then there is a type 1 closed term S of IPV^ω such that $IPV^\omega \vdash \forall \vec{x} A(\vec{x}, S(\vec{x}))$. Then $\{S(\vec{x})\}^{PV}$ is a term of PV because $S(\vec{x})$ is a term of PV^ω and zero-order open. We define f as
$f \stackrel{d}{\equiv} [\lambda \vec{x}.\{S(\vec{x})\}^{PV}]$. Then f is a function symbol of PV. Therefore

$$\begin{aligned} PV \vdash f(\vec{x}) &= [\lambda \vec{x}.\{S(\vec{x})\}^{PV}](x) \\ &= \{S(\vec{x})\} \\ &= \{f(\vec{x})\}. \end{aligned}$$

Therefore $f(\vec{x}) \stackrel{PV}{\sim} S(\vec{x})$. By lemma 6.2.20, $A(\vec{x}, f(\vec{x})) \stackrel{PV}{\sim} A(\vec{x}, S(\vec{x}))$.
Therefore $PV \vdash \{A(\vec{x}, f(\vec{x}))\}^{PV} = \{A(\vec{x}, S(\vec{x}))\}^{PV}$.
By theorem 6.2.10, $IPV^\omega \vdash A(\vec{x}, f(\vec{x})) = A(\vec{x}, S(\vec{x}))$.
By $IPV^\omega \vdash \forall \vec{x} A(\vec{x}, S(\vec{x}))$, $IPV^\omega \vdash \forall \vec{x} A(\vec{x}, f(\vec{x}))$.

(2) $IPV \vdash \forall \vec{x} A(\vec{x}, f(\vec{x}))$.
Assume $IPV \vdash \forall \vec{x} \exists y A(\vec{x}, y)$. Then $IPV^{\omega} \vdash \forall \vec{x} \exists y A(\vec{x}, y)$.
By same method as (1), $IPV^{\omega} \vdash \forall \vec{x} A(\vec{x}, f(\vec{x}))$. Then $A(\vec{x}, f(\vec{x}))$ is a IPV formula because $A(x, y)$ is a IPV formula and f is a function symbol of PV.
Therefore by theorem 7.2.14, $IPV \vdash \forall \vec{x} A(\vec{x}, f(\vec{x}))$.

∎

The next result proves Conjecture 1 of Buss [2].

Theorem 8.3.4 If $IS^1_2 \vdash \exists y A(\vec{x}, y)$, then there is a Σ^{b+}_1 formula $B(\vec{x}, y)$ such that IS^1_2 proves the following formulas:

(1) $\forall \vec{x} \forall y (B(\vec{x}, y) \rightarrow A(\vec{x}, y))$

(2) $\forall \vec{x} \forall y \forall z (B(\vec{x}, y) \wedge B(\vec{x}, z) \rightarrow y = z)$

(3) $\forall \vec{x} \exists y B(\vec{x}, y)$

(*proof*)

(1) Assume $IS^1_2 \vdash \exists y A(\vec{x}, y)$. Then $IPV \vdash \exists y A(\vec{x}, y)$. Hence $IPV \vdash \forall \vec{x} \exists y A(\vec{x}, y)$.
By theorem 8.3.3, $IPV \vdash \forall \vec{x} A(\vec{x}, f(\vec{x}))$. By theorem 7.2.14 and theorem 4.2.12, $IS^1_2 \vdash \forall \vec{x} A(\vec{x}, f(\vec{x}))$. Then there is a IS^1_2 formula $B(\vec{x}, y)$ such that $IS^1_2 \vdash f(\vec{x}) = y \leftrightarrow B(\vec{x}, y)$ because f is a PV function symbol and corollary 2.4.10.
By this and $IS^1_2 \vdash \forall \vec{x} A(\vec{x}, f(\vec{x}))$, $IS^1_2 \vdash B(\vec{x}, y) \rightarrow A(\vec{x}, y)$.
Therefore $IS^1_2 \vdash \forall \vec{x} \forall y (B(\vec{x}, y) \rightarrow A(\vec{x}, y))$.

(2) By definition of Σ^{b+}_1-definition for f.

(3) By $IS^1_2 \vdash A(\vec{x}, y) \leftrightarrow A(\vec{x}, f(\vec{x}))$ and (2), $IS^1_2 \vdash f(\vec{x}) = y$.
By this and $IS^1_2 \vdash f(\vec{x}) = y \leftrightarrow B(\vec{x}, y)$, $IS^1_2 \vdash B(\vec{x}, y)$.
Therefore $IS^1_2 \vdash \forall \vec{x} \exists y B(\vec{x}, y)$.

∎

We think about *Felmat's "Little Theorem* as an example of use of realizability. *Felmat's "Little Theorem*" is that if $0 < a < n$ and n is prime, then $a^{n-1} \bmod n = 1$. Since $a^{n-1} \bmod n$ is a polynomial time computable function of a and n, the conclusion is an atomic formula of IPV which has the form $a^{n-1} \bmod n = 1$.

We let the formula B be the following form of the contrapositive:

$\forall a \forall n [(0 < a \wedge a < n \wedge a^{n-1} \bmod n \neq 1) \rightarrow \exists d (d | n \wedge d \neq 1 \wedge d \neq n)]$

where $d|n$ is the polynomial time predicate "d divides n". Then if B is provable in IPV^{ω}, by the soundness theorem there is a term D such that $\vdash D \textcircled{R} B$. That is , the formula

$\forall a \forall n [(0 < a \wedge a < n \wedge a^{n-1} \bmod n \neq 1) \rightarrow (D(a, n) | n \wedge D(a, n) \neq 1 \wedge D(a, n) \neq n)]$

would be a theorem of IPV^{ω}. For "most" composite numbers n a random number a such

that $0 < a < n$ will satisfy the antecedent. Hence such a realizing function D might well provide a practical method for factoring large numbers. In any case the existence of such a polynomial time function D would represent a surprising and major result in complexity theory. B is conjectured not a theorem of IPV^{ω}.

Chapter 9

The *Dialectica* Interpretation

The *Dialectica* interpretation and translation were first introduced in 1958 Gödel, for intuitionistic arithmetic. The purpose was to provide a consistency proof for intuitionistic arithmetic (and hence for classical arithmetic) by elementary "logic" (*i.e.* quantifiers especially) by an interpretation of an arithmetical statement by a quantifier-free formula in a theory of objects of finite type, where the concept of a constructive object of finite type was to be regarded as primitive and intuitively evident.

Hence logic was to be eliminated in favor of a suitable basic concept of object of finite type. It seems that a concept with decidable equality at all types as a primitive was intended.

In 1959 Kreisel applies the interpretation to intuitionistic analysis, only equality between objects of type 0 is taken as a primitive ; equality between higher type objects is interpreted as extensional equality.

A characterization of *Dialectica* interpretable formula of $WE\text{-}HA^\omega$ was first given explicitly by Yasugi in 1963, after Kreisel already noted that (weakenings of) AC, IP, M implied the equivalence of a formula with its interpretation and showed the interpretability of M, where $AC \equiv \forall x_\sigma \exists y_\tau A(x_\sigma, y_\tau) \to \exists z_{\sigma\to\tau} \forall x_\sigma A(x_\sigma, z_{\sigma\to\tau} x_\sigma)$, $IP \equiv \forall x(A \vee \neg A) \wedge (\forall x A \to \exists y B) \to \exists y(\forall x A \to B)$ and $M \equiv \forall x(A \vee \neg A) \wedge \neg\neg \exists x A \to \exists x A$.

We define a second translation from IPV^ω into itself which follows the functional interpretation of Heyting arithmetic in Gödel [5]. The translation differs from that of the previous chapter in the treatment of implication. The more radical translation of implications in Gödel's interpretation allows elimination of logical operators.

The translation associates with each formula A of IPV^ω a formula $\exists \vec{x} \forall \vec{y} t_A = 0$, where $\vec{x}$ and $\vec{y}$ are finite sequences of variables of finite type and t_A is a term of PV^ω. The types of $\vec{x}$ and $\vec{y}$ depend only on the logical structure of A; the free variables of A are included in the free variables of t_A.

First we prove that "over IPV^ω, (MP) and $A \leftrightarrow A^D$ are equivalent", MP is defined in next section. This chapter has two main theorems. One is to prove same as realizability by *Dialectica* interpretation that if $IPV \vdash \forall \vec{x} \exists y A(\vec{x}, y)$ then there is a PV function symbol f such that $IPV \vdash \forall \vec{x} A(\vec{x}, f(\vec{x}))$. Another is to prove that IS_1^2 is equivalent to $IS_1^2 B$.

9.1 Definition

Notation 9.1.1 In definition 1.1.2, the following notational conventions are used:

1. If $s = 0$ and $t = 0$ are equation of PV^ω, we write:

$$\begin{array}{lll} (s = 0 \& t = 0) & \text{for} & (s \& t = 0); \\ (s = 0 \vee t = 0) & \text{for} & (s \vee t = 0); \\ (s = 0 \supset t = 0) & \text{for} & (s \supset t = 0); \\ s \neq 0 & \text{for} & \sim s = 0. \end{array}$$

2. $\vec{x}, \vec{y}, \vec{u}, \vec{v}$ are finite sequences of distinct variables of finite type, while z is a numerical variable.

3. $\vec{U}$ is a sequence of variables whose number and types are determined by the fact that each of them can be applied to $\vec{x}$ as an argument sequence and that the sequence $\vec{U}(\vec{x})$ so obtained agrees with the sequence $\vec{u}$ with respect to the number and type of its numbers. If $\vec{u}$ is the empty sequence then $\vec{U}$ is empty; if $\vec{x}$ is empty then $\vec{U} = \vec{u}$.

4. One-element sequences are identified with their only elements.

Definition 9.1.2 If A is a formula of IPV^ω, the *Dialectica translation* of A, A^D, is defined by induction on the logical complexity of A:

(1) If A is an equation $u = v$, then A^D is $Equ(u, v) = 0$;

(2) If A is an inequality $u \leq v$, then A^D is $Lessequ(u, v) = 0$;

For the remaining cases, assume that

$$A^D \stackrel{d}{\equiv} \exists \vec{x} \forall \vec{y} t_A(\vec{x}, \vec{y}) = 0,$$
$$B^D \stackrel{d}{\equiv} \exists \vec{u} \forall \vec{v} t_B(\vec{u}, \vec{v}) = 0.$$

(3) $(A \wedge B)^D \stackrel{d}{\equiv} \exists \vec{x}\vec{u} \forall \vec{y}\vec{v} [t_A(\vec{x}, \vec{y}) = 0 \ \& \ t_B(\vec{u}, \vec{v}) = 0]$;

(4) $(A \vee B)^D \stackrel{d}{\equiv} \exists z \vec{x}\vec{u} \forall \vec{y}\vec{v} [(z = 0 \ \& \ t_A(\vec{x}, \vec{y}) = 0) \vee (z \neq 0 \ \& \ t_B(\vec{u}, \vec{v}) = 0)]$;

(5) $(\exists w A)^D \stackrel{d}{\equiv} \exists w \vec{x} \forall \vec{y} t_A(\vec{x}, \vec{y}) = 0$;

(6) $(\forall w A)^D \stackrel{d}{\equiv} \exists \vec{X} \forall w \vec{y} t_A(\vec{X}(w), \vec{y}) = 0$;

(7) $(A \to B)^D \stackrel{d}{\equiv} \exists \vec{U}\vec{Y} \forall \vec{x}\vec{v} [t_A(\vec{x}, \vec{Y}(\vec{x}\vec{v})) = 0 \supset t_B(\vec{U}(\vec{x}), \vec{v}) = 0]$;

(8) $(\neg A)^D \stackrel{d}{\equiv} \exists \vec{Y} \forall \vec{x} t_A(\vec{x}, \vec{Y}(\vec{x})) \neq 0$.

9.2 Soundness of *Dialectica* Interpretation

Definition 9.2.1 We denote by $MP(Markov's\ Principle)$ the scheme $\neg\neg\exists\vec{x}A \to \exists\vec{x}A$, where A is an atomic formula.

Theorem 9.2.2 (Soundness of *Dialectica* interpretation)
If $A(\vec{z})$ is a formula of IPV^ω, whose free variables are contained in $\vec{z}$, such that $IPV^\omega + MP \vdash A(\vec{z})$ then there is a sequence $\vec{S}$ of closed terms of PV^ω so that

$$PV^\omega \vdash t_A(\vec{S}(\vec{z}), \vec{y}, \vec{z}) = 0,$$

where $A^D \stackrel{d}{\equiv} \exists\vec{x}\forall\vec{y}t_A(\vec{x}, \vec{y}, \vec{z}) = 0$.

(*proof*) We prove by induction on the IPV^ω proof of A. We first consider the logical axiom and rules.Let $\vec{R}, \vec{R_1}, \vec{R_2}, \vec{S}, \vec{S_1}, \vec{S_2}, \vec{T}, \vec{T_1}, \vec{T_2}, \vec{U}, \vec{X}, \vec{Y}, \vec{Z}$ be terms of PV^ω.

(1) **Axiom scheme 1**

Define as $\vec{S_1}(\vec{x}) = \vec{S_2}(\vec{x}) \stackrel{d}{\equiv} \vec{x}$ and for $1 \le i \le k$ where $\vec{y} = y_1, \cdots, y_k$, $T_i(\vec{x}\vec{y_1}\vec{y_2}) \stackrel{d}{\equiv} Cond(t_A(\vec{x}\vec{y_1}\vec{y_2}), (\vec{y_1})_i, (\vec{y_2})_i)$. By theorem 6.2.5,

$PV^\omega \vdash t_A(\vec{x}, \vec{y_2}) = 0 \supset t_A(\vec{x}, \vec{T}(\vec{x}\vec{y_1}\vec{y_2})) = t_A(\vec{x}, \vec{y_1}) \cdots\cdots$ ①

$PV^\omega \vdash t_A(\vec{x}, \vec{y_2}) \neq 0 \supset t_A(\vec{x}, \vec{T}(\vec{x}\vec{y_1}\vec{y_2})) = t_A(\vec{x}, \vec{y_2}) \cdots\cdots$ ②

By T43,

$PV^\omega \vdash t_A(\vec{x}, \vec{y_2}) = 0 \vee t_A(\vec{x}, \vec{y_2}) \neq 0$.

i) The case "$t_A(\vec{x}, \vec{y_2}) = 0$"

By ①, $t_A(\vec{x}, \vec{T}(\vec{x}\vec{y_1}\vec{y_2})) = 0 \supset t_A(\vec{x}, \vec{y_1}) = 0$ & $t_A(\vec{x}, \vec{y_2}) = 0$.

ii) The case "$t_A(\vec{x}, \vec{y_2}) \neq 0$"

By ②, $t_A(\vec{x}, \vec{T}(\vec{x}\vec{y_1}\vec{y_2})) = 0 \supset t_A(\vec{x}, \vec{y_1}) = 0$ & $t_A(\vec{x}, \vec{y_2}) = 0$.

By i), ii) and $t_A(\vec{x}, \vec{y_2}) = 0 \vee t_A(\vec{x}, \vec{y_2}) \neq 0$,

$PV^\omega \vdash t_A(\vec{x}, \vec{T}(\vec{x}\vec{y_1}\vec{y_2})) = 0 \supset t_A(\vec{x}, \vec{y_1}) = 0$ & $t_A(\vec{x}, \vec{y_2}) = 0$.

Hence

$IPV^\omega \vdash t_A(\vec{x}, \vec{T}(\vec{x}\vec{y_1}\vec{y_2})) = 0 \supset t_A(\vec{S_1}(\vec{x}), \vec{y_1}) = 0$ & $t_A(\vec{S_2}(\vec{x}), \vec{y_2}) = 0$.

Therefore

$IPV^\omega \vdash \exists\vec{S_1}\vec{S_2}\vec{T}\forall\vec{x}\vec{y_1}\vec{y_2}$
$[t_A(\vec{x}, \vec{T}(\vec{x}\vec{y_1}\vec{y_2})) = 0 \supset t_A(\vec{S_1}(\vec{x}), \vec{y_1}) = 0 \& t_A(\vec{S_2}(\vec{x}), \vec{y_2}) = 0]$.

Therefore If $IPV^\omega + MP \vdash A \to A \wedge A$ then $IPV^\omega \vdash (A \to A \wedge A)^D$.

(2) **Axiom scheme 2**

Define as $\vec{X}(\vec{u}\vec{v}) \stackrel{d}{\equiv} Cond(z, \vec{u}, \vec{v})$, $\vec{Y}(\vec{u}\vec{w}) \stackrel{d}{\equiv} \vec{w}$ and $\vec{Z}(\vec{v}\vec{w}) \stackrel{d}{\equiv} \vec{w}$. By theorem 6.2.5,

$PV^\omega \vdash z = 0 \supset t_A(\vec{X}(\vec{u}\vec{v}), \vec{w}) = t_A(\vec{u}, \vec{w})$

and

$PV^\omega \vdash z \neq 0 \supset t_A(\vec{X}(\vec{u}\vec{v}), \vec{w}) = t_A(\vec{v}, \vec{w})$.

Hence

$PV^\omega \vdash z = 0 \& t_A(\vec{u}, \vec{w}) = 0 \supset t_A(\vec{X}(\vec{u}\vec{v}), \vec{w}) = 0$

and

$PV^\omega \vdash z \neq 0 \& t_A(\vec{v}, \vec{w}) = 0 \supset t_A(\vec{X}(\vec{u}\vec{v}), \vec{w}) = 0.$

Hence

$PV^\omega \vdash (z = 0 \& t_A(\vec{u}, \vec{w}) = 0) \vee (z \neq 0 \& t_A(\vec{v}, \vec{w}) = 0) \supset t_A(\vec{X}(\vec{u}\vec{v}), \vec{w}) = 0.$

Hence

$IPV^\omega \vdash \exists z \vec{X}\vec{Y}\vec{Z} \forall \vec{u}\vec{v}\vec{w}$
$[(z = 0 \& t_A(\vec{u}, \vec{w}) = 0) \vee (z \neq 0 \& t_A(\vec{v}, \vec{w}) = 0) \supset t_A(\vec{X}(\vec{u}\vec{v}), \vec{w}) = 0].$

Therefore $IPV^\omega \vdash (A \vee A \to A)^D$.

(3) **Axiom scheme 3**

Define as $\vec{X}(\vec{u}\vec{v}) \stackrel{d}{\equiv} \vec{v}$, $\vec{Y}(\vec{u}\vec{w}) \stackrel{d}{\equiv} \vec{w}$ and $\vec{Z}(\vec{v}\vec{w}) \stackrel{d}{\equiv} \vec{w}$.

By $PV^\omega \vdash t_B(\vec{v}, \vec{w}) = 0 \supset t_B(\vec{v}, \vec{w}) = 0$,

$PV^\omega \vdash t_B(\vec{v}, \vec{Z}(\vec{v}\vec{w})) = 0 \supset t_B(\vec{X}(\vec{u}\vec{v}), \vec{w}) = 0.$

By T43,

$PV^\omega \vdash t_A(\vec{u}, \vec{Y}(\vec{u}\vec{w})) = 0 \& t_B(\vec{v}, \vec{Z}(\vec{v}\vec{w})) = 0 \supset t_B(\vec{X}(\vec{u}\vec{v}), \vec{w}) = 0.$

Hence

$IPV^\omega \vdash \exists \vec{X}\vec{Y}\vec{Z} \forall \vec{u}\vec{v}\vec{w}$
$[t_A(\vec{u}, \vec{Y}(\vec{u}\vec{w})) = 0 \& t_B(\vec{v}, \vec{Z}(\vec{v}\vec{w})) = 0 \supset t_B(\vec{X}(\vec{u}\vec{v}), \vec{w}) = 0].$

Therefore $IPV^\omega \vdash (A \wedge B \to B)^D$.

(4) **Axiom scheme 4**

Define as $\vec{X}(\vec{u}) \stackrel{d}{\equiv} \vec{u}$, $\vec{Y}(\vec{u}) \stackrel{d}{\equiv} \vec{u}$ and $\vec{Z}(\vec{u}\vec{v}\vec{w}) \stackrel{d}{\equiv} \vec{w}$.

By $PV^\omega \vdash t_B(\vec{u}, \vec{w}) = 0 \supset t_B(\vec{u}, \vec{w}) = 0$,

$PV^\omega \vdash t_B(\vec{u}, \vec{Z}(\vec{u}\vec{v}\vec{w})) = 0 \supset (1 \neq 0 \& t_B(\vec{Y}(\vec{u}), \vec{w}) = 0).$

By T43,

$PV^\omega \vdash t_B(\vec{u}, \vec{Z}(\vec{u}\vec{v}\vec{w})) = 0 \supset$
$(1 = 0 \& t_A(\vec{X}(\vec{u}), \vec{v}) = 0) \vee (1 \neq 0 \& t_B(\vec{Y}(\vec{u}), \vec{w}) = 0).$

Hence

$IPV^\omega \vdash \exists z \vec{X}\vec{Y}\vec{Z} \forall \vec{u}\vec{v}\vec{w}$
$[t_B(\vec{u}, \vec{Z}(\vec{u}\vec{v}\vec{w})) = 0 \supset (z = 0 \& t_A(\vec{X}(\vec{u}), \vec{v}) = 0) \vee (z \neq 0 \& t_B(\vec{Y}(\vec{u}), \vec{w}) = 0)].$

Therefore $IPV^\omega \vdash (B \to A \vee B)^D$.

(5) **Axiom scheme 5**

Define as $\vec{R}(\vec{x}\vec{y}\vec{v}) \stackrel{d}{\equiv} \vec{y}$, $\vec{S}(\vec{x}\vec{y}\vec{v}) \stackrel{d}{\equiv} \vec{v}$, $\vec{T}(\vec{u}) \stackrel{d}{\equiv} \vec{u}$ and $\vec{U}(\vec{x}) \stackrel{d}{\equiv} \vec{x}$.

By T43,

$PV^\omega \vdash t_A(\vec{x}, \vec{y}) = 0 \& t_B(\vec{u}, \vec{v}) = 0 \supset t_B(\vec{u}, \vec{v}) = 0 \& t_A(\vec{x}, \vec{y}) = 0.$

Hence

$PV^\omega \vdash t_A(\vec{x}, \vec{R}(\vec{x}\vec{y}\vec{v})) = 0 \& t_B(\vec{u}, \vec{S}(\vec{x}\vec{y}\vec{v})) = 0 \supset$
$t_B(\vec{T}(\vec{u}), \vec{v}) = 0 \& t_A(\vec{U}(\vec{x}), \vec{y}) = 0.$

Hence

$IPV^\omega \vdash \exists \vec{R}\vec{S}\vec{T}\vec{U} \forall \vec{x}\vec{y}\vec{u}\vec{v}$
$[t_A(\vec{x}, \vec{R}(\vec{x}\vec{y}\vec{v})) = 0 \& t_B(\vec{u}, \vec{S}(\vec{x}\vec{y}\vec{v})) = 0 \supset t_B(\vec{T}(\vec{u}), \vec{v}) = 0 \& t_A(\vec{U}(\vec{x}), \vec{y}) = 0].$

Therefore $IPV^\omega \vdash (A \wedge B \to B \wedge A)^D$.

(6) **Axiom scheme 6**

Define as $\vec{R}(\vec{x}\vec{y}\vec{v}) \stackrel{d}{\equiv} \vec{y}$, $\vec{S}(\vec{x}\vec{y}\vec{v}) \stackrel{d}{\equiv} \vec{v}$, $\vec{T}(\vec{u}) \stackrel{d}{\equiv} \vec{u}$ and $\vec{U}(\vec{x}) \stackrel{d}{\equiv} \vec{x}$.

By T43,

$PV^\omega \vdash (0 = 0 \& t_A(\vec{x}, \vec{y}) = 0) \vee (0 \neq 0 \& t_B(\vec{u}, \vec{v}) = 0) \supset (0 \neq 0 \& t_B(\vec{u}, \vec{v}) = 0)$.

Hence

$PV^\omega \vdash (0 = 0 \& t_A(\vec{x}, \vec{y}) = 0) \vee (0 \neq 0 \& t_B(\vec{u}, \vec{v}) = 0) \supset t_B(\vec{u}, \vec{v}) = 0$.

Therefore

$PV^\omega \vdash (0 = 0 \& t_A(\vec{x}, \vec{y}) = 0) \vee (0 \neq 0 \& t_B(\vec{u}, \vec{v}) = 0) \supset (0 = 0 \& t_B(\vec{u}, \vec{v}) = 0)$.

Hence

$PV^\omega \vdash (0 = 0 \& t_A(\vec{x}, \vec{y}) = 0) \vee (0 \neq 0 \& t_B(\vec{u}, \vec{v}) = 0) \supset$
$(0 = 0 \& t_B(\vec{u}, \vec{v}) = 0) \vee (0 \neq 0 \& t_A(\vec{x}, \vec{y}) = 0)$.

By definition of $\vec{R}, \vec{S}, \vec{T}, \vec{U}$,

$PV^\omega \vdash (0 = 0 \& t_A(\vec{x}, \vec{R}(\vec{x}\vec{y}\vec{v})) = 0) \vee (0 \neq 0 \& t_B(\vec{u}, \vec{S}(\vec{x}\vec{y}\vec{v})) = 0) \supset$
$(0 = 0 \& t_B(\vec{T}(\vec{u}), \vec{v}) = 0) \vee (0 \neq 0 \& t_A(\vec{U}(\vec{x}), \vec{y}) = 0)$.

Hence

$IPV^\omega \vdash \exists \vec{R}\vec{S}\vec{T}\vec{U}\forall \vec{x}\vec{y}\vec{u}\vec{v}$
$[(z = 0 \& t_A(\vec{x}, \vec{R}(\vec{x}\vec{y}\vec{v})) = 0) \vee (z \neq 0 \& t_B(\vec{u}, \vec{S}(\vec{x}\vec{y}\vec{v})) = 0) \supset$
$(z = 0 \& t_B(\vec{T}(\vec{u}), \vec{v}) = 0) \vee (z \neq 0 \& t_A(\vec{U}(\vec{x}), \vec{y}) = 0)]$.

Therefore $IPV^\omega \vdash (A \vee B \to B \vee A)^D$.

(7) **Axiom scheme 7**

Define as $\vec{X}(w) \stackrel{d}{\equiv} \vec{x}$, $\vec{X}(t) \stackrel{d}{\equiv} \vec{x}$, $\vec{Y}(\vec{X}(w)\vec{y}) \stackrel{d}{\equiv} \vec{y}$, $\vec{Z}(\vec{X}(t)) \stackrel{d}{\equiv} \vec{X}(w)$.

By $PV^\omega \vdash t_A(\vec{X}(w), \vec{y}) = 0 \supset t_A(\vec{X}(w), \vec{y}) = 0$,

$PV^\omega \vdash t_A(\vec{X}(w), \vec{Y}(\vec{X}(w)\vec{y})) = 0 \supset t_A(\vec{Z}(\vec{X}(t)), \vec{y}) = 0$.

Hence

$IPV^\omega \vdash \exists \vec{X}\vec{Y}\vec{Z}\forall w\vec{y}[t_A(\vec{X}(w), \vec{Y}(\vec{X}(w)\vec{y})) = 0 \supset t_A(\vec{Z}(\vec{X}(t)), \vec{y}) = 0]$.

Therefore $IPV^\omega \vdash (\forall w A \to A[t/w])^D$.

(8) **Axiom scheme 8**

Let free variables of $A(\vec{x}), \vec{y}, \vec{z})$ be contained in the list $\vec{z}$.

Define as $\vec{R}(\vec{x}\vec{y}) \stackrel{d}{\equiv} \vec{y}$ and $\vec{S}(\vec{x}) \stackrel{d}{\equiv} \vec{x}$. Let $\vec{z'}$ be replacement w in the list $\vec{z}$ to t.

By $PV^\omega \vdash t_A(\vec{x}, \vec{y}, \vec{z'}) \to t_A(\vec{x}, \vec{y}, \vec{z'})$ and definition of $\vec{R}$ and $\vec{S}$,

$PV^\omega \vdash t_A(\vec{x}, \vec{R}(\vec{x}\vec{y}), \vec{z'}) \to t_A(\vec{S}(\vec{x}), \vec{y}, \vec{z'})$.

Hence

$IPV^\omega \vdash \exists w \vec{R}\vec{S}\forall \vec{x}\vec{y}[t_A(\vec{x}, \vec{R}(\vec{x}\vec{y}), \vec{z'}) \to t_A(\vec{S}(\vec{x}), \vec{y}, \vec{z'})]$.

Therefore $IPV^\omega \vdash (A[t/w] \to \exists w A)^D$.

(9) **Axiom scheme 9**

By $PV^\omega \vdash Equ(0, 1) = 1$ and T43,

$PV^\omega \vdash Equ(0, 1) = 0 \supset t_A(\vec{U}(\vec{x}), \vec{v}) = 0$.

Hence

$IPV^\omega \vdash \exists \vec{U}\forall \vec{x}\vec{v}[Equ(0, 1) = 0 \supset t_A(\vec{U}(\vec{x}), \vec{v}) = 0]$.

Therefore $IPV^\omega \vdash (0 = 1 \to A)^D$.

(10) **Axiom scheme 17**

$PV^\omega \vdash Equ(x,x) = 0$. Therefore $IPV^\omega \vdash (x = x)^D$.

(11) **Axiom scheme 18**

Define as $\vec{R}_1(\vec{x}\vec{y}) \stackrel{d}{\equiv} \vec{y}$, $\vec{R}_2(\vec{x}\vec{y}) \stackrel{d}{\equiv} \vec{y}$, $\vec{T}_1(\vec{x}) \stackrel{d}{\equiv} \vec{x}$ and $\vec{T}_2(\vec{x}) \stackrel{d}{\equiv} \vec{x}$. Let $\vec{z'}$ be replacement u in the list $\vec{z}$ to v.

By $IPV^\omega \vdash Equ(u,v) = 0 \supset$

$[(t_A(\vec{x},\vec{y},\vec{z}) = 0 \supset t_A(\vec{x},\vec{y},\vec{z'}) = 0) \& (t_A(\vec{x},\vec{y},\vec{z'}) = 0 \supset t_A(\vec{x},\vec{y},\vec{z}) = 0)]$,

$IPV^\omega \vdash Equ(u,v) = 0 \supset [t_A(\vec{x},\vec{R}_1(\vec{x}\vec{y}),\vec{z}) = 0 \supset$

$(t_A(\vec{T}_1(\vec{x}),\vec{y},\vec{z'}) = 0 \& t_A(\vec{x},\vec{R}_2(\vec{x}\vec{y}),\vec{z'}) = 0 \supset t_A(\vec{T}_2(\vec{x}),\vec{y},\vec{z}) = 0)]$.

Hence

$IPV^\omega \vdash \exists \vec{R}_1 \vec{R}_2 \vec{T}_1 \vec{T}_2 \forall \vec{x}\vec{y}\vec{z}$

$(Equ(u,v) = 0 \supset [(t_A(\vec{x},\vec{R}_1(\vec{x}\vec{y}),\vec{z}) = 0 \supset t_A(\vec{T}_1(\vec{x}),\vec{y},\vec{z'}) = 0) \&$

$(t_A(\vec{x},\vec{R}_2(\vec{x}\vec{y}),\vec{z'}) = 0 \supset t_A(\vec{T}_2(\vec{x}),\vec{y},\vec{z}) = 0)])$.

Therefore $IPV^\omega \vdash (u = v \to (A \leftrightarrow A[v/x]))^D$.

(12) **Rule of inference 10**

Assume $PV^\omega \vdash t_A(\vec{x},\vec{y}) = 0, t_A(\vec{x},\vec{R}(\vec{x}\vec{v})) = 0 \supset t_B(\vec{Q}(\vec{x}),\vec{v}) = 0$. Then we need to find $\vec{X}$ and $\vec{Y}$ such that $PV^\omega \vdash t_B(\vec{X},\vec{Y}) = 0$. By $t_A(\vec{x},\vec{y}) = 0$ and $R4^\omega$,

$PV^\omega \vdash t_A(\vec{x},\vec{y})[\vec{R}(\vec{x}\vec{v})/\vec{y}] = 0[\vec{R}(\vec{x}\vec{v})/\vec{y}]$.

This is

$PV^\omega \vdash t_A(\vec{x},\vec{R}(\vec{x}\vec{v})) = 0$.

By this and hypothesis,

$PV^\omega \vdash t_B(\vec{Q}(\vec{x}),\vec{v}) = 0$.

Therefore it is good to take $\vec{Q}(\vec{x})$ and $\vec{v}$ as $\vec{X}$ and $\vec{Y}$.

Therefore If $IPV^\omega \vdash (A)^D$ and $(A \to B)^D$, then $IPV^\omega \vdash (B)^D$.

(13) **Rule of inference 11**

Assume $PV^\omega \vdash t_A(\vec{x},\vec{R}(\vec{x}\vec{v})) = 0 \supset t_B(\vec{Q}(\vec{x}),\vec{v}) = 0$ and

$t_B(\vec{u},\vec{T}(\vec{u}\vec{z})) = 0 \supset t_C(\vec{S}(\vec{u}),\vec{z}) = 0$. Then we need to find $\vec{N}$ and $\vec{P}$ such that $PV^\omega \vdash t_A(\vec{x},\vec{P}(\vec{x}\vec{z})) = 0 \supset t_C(\vec{N}(\vec{x}),\vec{z}) = 0$.

By $R4^\omega$,

$PV^\omega \vdash t_A(\vec{x},\vec{R}(\vec{x}\vec{v}))[\vec{T}(\vec{Q}(\vec{x})\vec{z})/\vec{y}] = 0 \supset t_B(\vec{Q}(\vec{x}),\vec{v})[\vec{T}(\vec{Q}(\vec{x})\vec{z})/\vec{y}] = 0$

and

$PV^\omega \vdash t_B(\vec{u},\vec{T}(\vec{u}\vec{z}))[\vec{Q}(\vec{x})/\vec{u}] = 0 \supset t_C(\vec{S}(\vec{u}),\vec{z})[\vec{Q}(\vec{x})/\vec{u}] = 0$.

By this and Rule 11,

$PV^\omega \vdash t_A(\vec{x},\vec{R}(\vec{x}\vec{T}(\vec{Q}(\vec{x})\vec{z}))) = 0 \supset t_C(\vec{S}(\vec{Q}(\vec{x})),\vec{z}) = 0$.

Therefore it is good to take $\vec{N} \stackrel{d}{\equiv} \lambda\vec{x}.\vec{S}(\vec{Q}(\vec{x}))$ and $\vec{P} \stackrel{d}{\equiv} \lambda\vec{x}\vec{z}.\vec{R}(\vec{x}\vec{T}(\vec{Q}(\vec{x})\vec{z}))$.

Therefore If $IPV^\omega \vdash (A \to B)^D$ and $(B \to C)^D$, then $IPV^\omega \vdash (A \to C)^D$.

(14) **Rule of inference 12**

Assume $PV^\omega \vdash t_A(\vec{u},\vec{Y}(\vec{u}\vec{w})) = 0 \& t_B(\vec{v},\vec{Z}(\vec{v}\vec{w})) = 0 \supset t_C(\vec{X}(\vec{u}\vec{v}),\vec{w}) = 0$.

Then we need to find $\vec{M}$, $\vec{N}$, $\vec{P}$ and $\vec{Q}$ such that

$PV^\omega \vdash t_A(\vec{u},\vec{M}(\vec{u}\vec{w})) = 0 \supset (t_B(\vec{N}(\vec{u}),\vec{P}(\vec{N}(\vec{u})\vec{w})) = 0 \supset t_C(\vec{Q}(\vec{N}(\vec{u})),\vec{w}) = 0)$.

By hypothesis and R12,
$PV^\omega \vdash t_A(\vec{u}, \vec{Y}(\vec{u}\vec{w})) = 0 \supset (t_B(\vec{v}, \vec{Z}(\vec{v}\vec{w})) = 0 \supset t_C(\vec{X}(\vec{u}\vec{v}), \vec{w}) = 0)$.
Therefore it is good to take $\vec{M} \stackrel{d}{\equiv} \vec{Y}$, $\vec{N} \stackrel{d}{\equiv} \lambda\vec{u}.\vec{v}$, $\vec{P} \stackrel{d}{\equiv} \vec{Z}$ and $\vec{Q} \stackrel{d}{\equiv} \vec{v}.\vec{X}(\vec{u}\vec{v})$.
Therefore If $IPV^\omega \vdash (A \wedge B \to C)^D$, then $IPV^\omega \vdash (A \to (B \to C))^D$.

(15) **Rule of inference 13**

Assume
$PV^\omega \vdash t_A(\vec{u}, \vec{M}(\vec{u}\vec{w})) = 0 \supset (t_B(\vec{N}(\vec{u}), \vec{P}(\vec{N}(\vec{u})\vec{w})) = 0 \supset t_C(\vec{Q}(\vec{N}(\vec{u})), \vec{w}) = 0)$.
Then we need to find $\vec{X}, \vec{Y}$ and $\vec{Z}$ such that
$PV^\omega \vdash (t_A(\vec{u}, \vec{Y}(\vec{u}\vec{w})) = 0 \& t_B(\vec{v}, \vec{Z}(\vec{v}\vec{w})) = 0) \supset t_C(\vec{X}(\vec{u}\vec{v}), \vec{w}) = 0$.
By hypothesis and R12,
$PV^\omega \vdash (t_A(\vec{u}, \vec{M}(\vec{u}\vec{w})) = 0 \& t_B(\vec{N}(\vec{u}), \vec{P}(\vec{N}(\vec{u})\vec{w})) = 0) \supset t_C(\vec{Q}(\vec{N}(\vec{u})), \vec{w}) = 0$.
Therefore it is good to take $\vec{X} \stackrel{d}{\equiv} \lambda\vec{u}\vec{v}.\vec{Q}(\vec{v})$, $\vec{Y} \stackrel{d}{\equiv} \vec{M}$ and $\vec{Z} \stackrel{d}{\equiv} \vec{P}$.
Therefore If $IPV^\omega \vdash (A \to (B \to C))^D$, then $IPV^\omega \vdash (A \wedge B \to C)^D$.

(16) **Rule of inference 14**

Assume $PV^\omega \vdash (t_A(\vec{u}, \vec{R}(\vec{u}\vec{v})) = 0 \supset t_B(\vec{T}(\vec{u}), \vec{v}) = 0$. Then we need to prove
$IPV^\omega \vdash \exists z\vec{M}\vec{N}\vec{P}\vec{Q}\forall\vec{x}\vec{y}\vec{u}\vec{v}$
$[(z = 0 \& t_C(\vec{x}, \vec{M}(\vec{x}\vec{y}\vec{v})) = 0) \vee (z \neq 0 \& t_A(\vec{u}, \vec{N}(\vec{u}\vec{y}\vec{v})) = 0) \supset$
$(z = 0 \& t_C(\vec{P}(\vec{x}), \vec{y}) = 0) \vee (z \neq 0 \& t_A(\vec{Q}(\vec{u}), \vec{N}(\vec{v})) = 0)]$.
For this we need to find $\vec{M}, \vec{N}, \vec{P}$ and $\vec{Q}$. Therefore it is good to take $\vec{M} \stackrel{d}{\equiv} \lambda\vec{x}\vec{y}\vec{v}.\vec{y}$, $\vec{N} \stackrel{d}{\equiv} \lambda\vec{u}\vec{y}\vec{v}.\vec{R}(\vec{u}\vec{v})$, $\vec{P} \stackrel{d}{\equiv} \lambda\vec{x}.\vec{x}$ and $\vec{Q} \stackrel{d}{\equiv} \lambda\vec{u}.\vec{T}(\vec{u})$.
By hypothesis,
$PV^\omega \vdash (1 \neq 0 \& t_A(\vec{u}, \vec{R}(\vec{u}\vec{v})) = 0) \supset (1 \neq 0 \& t_B(\vec{T}(\vec{u}), \vec{v}) = 0)$.
By Rule 14,
$PV^\omega \vdash (0 = 0 \& t_C(\vec{x}, \vec{y}) = 0) \vee (1 \neq 0 \& t_A(\vec{u}, \vec{R}(\vec{u}\vec{v})) = 0) \supset$
$(0 = 0 \& t_C(\vec{x}, \vec{y}) = 0) \vee (1 \neq 0 \& t_B(\vec{T}(\vec{u}), \vec{v}) = 0)$.
By definition of $\vec{M}, \vec{N}, \vec{P}$ and $\vec{Q}$,
$PV^\omega \vdash (0 = 0 \& t_C(\vec{x}, \vec{M}(\vec{x}\vec{y}\vec{v})) = 0) \vee (0 \neq 0 \& t_A(\vec{u}, \vec{N}(\vec{u}\vec{y}\vec{v})) = 0) \supset$
$(0 = 0 \& t_C(\vec{P}(\vec{x}), \vec{y}) = 0) \vee (0 \neq 0 \& t_A(\vec{Q}(\vec{u}), \vec{N}(\vec{v})) = 0)$.
Therefore If $IPV^\omega \vdash (A \to B)^D$, then $IPV^\omega \vdash (C \vee A \to C \vee B)^D$.

(17) **Rule of inference 15**

Assume $PV^\omega \vdash t_A(\vec{x}, \vec{Y}(\vec{x}\vec{v})) = 0 \supset t_B(\vec{U}(\vec{x}), \vec{v}) = 0$. We define $\vec{X} \stackrel{d}{\equiv} \lambda\vec{w}.\vec{U}(\vec{x})$.
By this and hypothesis,
$PV^\omega \vdash t_A(\vec{x}, \vec{Y}(\vec{x}\vec{v})) = 0 \supset t_B(\vec{X}(w), \vec{v}) = 0$.
Hence
$IPV^\omega \vdash \exists\vec{X}\vec{Y}\forall w\vec{x}\vec{v}[t_A(\vec{x}, \vec{Y}(\vec{x}\vec{v})) = 0 \supset t_B(\vec{X}(\vec{w}), \vec{v}) = 0]$.
Therefore If $IPV^\omega \vdash (A \to B)^D$, then $IPV^\omega \vdash (A \to \forall xB)^D$.

(18) **Rule of inference 16**

Assume $PV^\omega \vdash t_B(\vec{x}, \vec{R}(\vec{x}\vec{y})) = 0 \supset t_A(\vec{S}(\vec{x}), \vec{y}) = 0$. Then
$IPV^\omega \vdash \exists w\vec{R}\vec{S}\forall\vec{x}\vec{y}[t_B(\vec{x}, \vec{R}(\vec{x}\vec{y})) = 0 \supset t_A(\vec{S}(\vec{x}), \vec{y}) = 0]$.

is obvious.
Therefore If $IPV^\omega \vdash (B \to A)^D$, then $IPV^\omega \vdash (\exists x B \to A)^D$.

(19) **1)theorem of PV^ω and 2)axioms of IPV**
These are forms of $t = u$. Therefore $IPV^\omega \vdash (t = u)^D$ is obvious.

(20) **PIND$^\omega$**
Induction scheme has the form :

$$(A[0/x] \wedge \forall x(A[\lfloor \tfrac{1}{2}x \rfloor/x] \to A)) \to \forall x A$$

where A has the form $(\exists y \le t)u = v$, with t zero-order open. We shall write s as an abbreviation of the term $(Lesseq u(y,t) \& Equ(u,v))$; we write $s(p,q)$ for $s[p,q/x,y]$. With this convention, we need to prove that

$$IPV^\omega \vdash \exists T_3 S_1 T_1 \forall \vec{Z}[\{s(0,y_0) = 0 \& s(\lfloor \tfrac{1}{2}S_1(\vec{Z})\rfloor, T_1(\vec{Z})) = 0 \supset s(S_1(\vec{Z}), \vec{Y_2}(S_1(\vec{Z}), T_1(\vec{Z}))) = 0\} \supset s(x, T_3(\vec{Z})) = 0],$$

where $\vec{Z}$ abbreviates the vector $y_0 Y_2 x$.
Hence we need to find terms T_3, S_1 and T_1.

We define three terms, T_3, S_1 and an auxiliary term U by simultaneous recursion, using Theorem 6.2.6:

$$T_3(x) \stackrel{d}{\equiv} \begin{cases} If\ \ x = 0\ \ then\ \ y_0 \\ \quad else \\ Cond(< F, G, H > \dot{-} < t', x, 1 > 0, F, t') \end{cases}$$

$$S_1(x) \stackrel{d}{\equiv} \begin{cases} If\ \ x = 0\ \ then\ \ 0 \\ \quad else \\ Cond(< F, G, H > \dot{-} < t', x, 1 > 0, G, x) \end{cases}$$

$$T_1(x) \stackrel{d}{\equiv} T_3(\lfloor \tfrac{1}{2}x \rfloor)$$

$$U \stackrel{d}{\equiv} \begin{cases} If\ \ x = 0\ \ then\ \ s(0,y_0) \\ \quad else \\ Cond(< F, G, H > \dot{-} < t', x, 1 > 0, H, 1) \end{cases}$$

where F, G, H are defined as:

$$F \stackrel{d}{\equiv} \begin{cases} If\ \ U(\lfloor \tfrac{1}{2}x \rfloor) = 0\ \ then & \begin{cases} if\ \ s(x, Y_2(xT_3(\lfloor \tfrac{1}{2}x \rfloor))) = 0 \\ then\ \ Y_2(xT_3(\lfloor \tfrac{1}{2}x \rfloor)) \\ else\ \ T_3(\lfloor \tfrac{1}{2}x \rfloor) \end{cases} \\ \quad else\ \ T_3(\lfloor \tfrac{1}{2}x \rfloor) \end{cases}$$

$$G \stackrel{d}{\equiv} Cond(U(\lfloor \tfrac{1}{2}x \rfloor), x, S_1(\lfloor \tfrac{1}{2}x \rfloor))$$

$$H \stackrel{d}{\equiv} Cond(U(\lfloor \tfrac{1}{2}x \rfloor), s(x, Y_2(xT_3(\lfloor \tfrac{1}{2}x \rfloor))), 1),$$

where suppressed the free parameters y_0 and Y_2 in the definitions of T_3, S_1 and U, to simplify notation. And the term t' stands for a term which can be proved to obey the properties $t \le t', y_0 \le t', x \le y \supset t'(x) \le t'(y)$ in PV^ω. Such a term can be proved to exists by T206.

In remaining proof, we use the predicate symbols of IPV and classical propositional calculus, as we are entitled to do by T43 and Theorem 4.2.2.

We first prove $< F, G, H > \dot{-} < t', x, 1 > 0 = 0$. By definition of G and H, $G \leq x$ and $H \leq 1$. To prove $F \leq t'$, for $x > 0$, we first prove $T_3(x) \leq t'$, which holds by the definition of T_3. Now for $x > 0$, if $U(\lfloor \frac{1}{2}x \rfloor) = 0$ and $s(x, Y_2(xT_3(\lfloor \frac{1}{2}x \rfloor))) = 0$ then $Y_2(xT_3(\lfloor \frac{1}{2}x \rfloor)) \leq t$, so $F \leq t$; in other case, $F = T_3(\lfloor \frac{1}{2}x \rfloor) \leq t'(\lfloor \frac{1}{2}x \rfloor) \leq t'(x)$. It follows that $< F, G, H > \leq < t', x, 1 >$ so $< F, G, H > \dot{-} < t', x, 1 > 0 = 0$.

Hence

$T_3(x) \equiv Cond(x, y_0, F)$
$S_1(x) \equiv Cond(x, 0, G)$
$U(x) \equiv Cond(x, s(0, y_0), H)$

By definition of T_3, S_1 and U,

(A) $U(x) = 0 \supset U(\lfloor \frac{1}{2}x \rfloor) = 0$

(B) $U(x) = 0 \vee U(x) = 1$

(C) $U(\lfloor \frac{1}{2}x \rfloor) = 0 \supset S_1(x) = x$

(D) $U(x) = 1 \supset T_3(x) = T_3(\lfloor \frac{1}{2}x \rfloor)$

(E) $U(x) = 0 \supset s(x, T_3(x)) = 0$

(F) $U(x) = 1 \supset s(0, y_0) = 1 \vee$
$[s(\lfloor \frac{1}{2}S_1(x) \rfloor, T_1(x)) = 0 \wedge s(S_1(x), Y_2(S_1(x)T_1(x))) = 1]$.

Assume $s(0, y_0) = 0$ and $s(\lfloor \frac{1}{2}S_1(\vec{Z}) \rfloor, T_1(\vec{Z})) = 0 \supset s(S_1(\vec{Z}), \vec{Y_2}(S_1(\vec{Z}), T_1(\vec{Z}))) = 0$. And we define $\mathcal{H}$ as this hypothesis formulas. By (B),$U(x) = 0 \vee U(x) = 1$.

1) Assume $\mathbf{U(x) = 0}$

By (E), if $U(x) = 0$ then $\mathcal{H} \supset s(x, T_3(x)) = 0$.

2) Assume $\mathbf{U(x) = 1}$

By (F), $s(0, y_0) = 1 \vee [s(\lfloor \frac{1}{2}S_1(x) \rfloor, T_1(x)) = 0 \wedge s(S_1(x), Y_2(S_1(x)T_1(x))) = 1]$.

i)$\mathbf{s(0, y_0) = 1}$

By $s(0, y_0) = 0$ of hypothesis, $\mathcal{H} \supset 0 = 1$. Therefore $\mathcal{H} \supset s(x, T_3(x)) = 0$.

ii)$\mathbf{s(\lfloor \frac{1}{2}S_1(x) \rfloor, T_1(x)) = 0 \wedge s(S_1(x), Y_2(S_1(x)T_1(x))) = 1}$

By $s(\lfloor \frac{1}{2}S_1(x) \rfloor, T_1(x)) = 0$ and hypothesis, $s(S_1(\vec{Z}), \vec{Y_2}(S_1(\vec{Z}), T_1(\vec{Z}))) = 0$.
By this and $s(S_1(x), Y_2(S_1(x)T_1(x))) = 1$, $\mathcal{H} \supset 0 = 1$.
Therefore $\mathcal{H} \supset s(x, T_3(x)) = 0$.

By i) and ii), if $U(x) = 1$ then $\mathcal{H} \supset s(x, T_3(x)) = 0$.

By 1),2) and (B),

$$PV^\omega \vdash \{s(0,y_0)=0 \& s(\lfloor \tfrac{1}{2}S_1(\vec{Z})\rfloor, T_1(\vec{Z}))=0 \supset s(S_1(\vec{Z}), \vec{Y_2}(S_1(\vec{Z}),T_1(\vec{Z})))=0\} \supset s(x,T_3(\vec{Z}))=0.$$

Therefore $IPV^\omega \vdash ((A[0/x] \wedge \forall x(A[\lfloor \tfrac{1}{2}x\rfloor/x] \to A)) \to \forall x A)^D$

(21) **MP**

An instance of the scheme has the form $\neg\neg\exists\vec{x}A \to \exists\vec{x}A$, where A is an atomic formula of IPV^ω. Then $(\neg\neg\exists\vec{x}A)^D$ has the form $\exists\vec{x} \sim\sim t=0$, while $(\exists\vec{x}A)^D$ is $\exists\vec{x}t=0$. Therefore By T43, $IPV^\omega \vdash (\neg\neg\exists\vec{x}A \to \exists\vec{x}A)^D$.

∎

We think about *Felmat's "Little Theorem* as an example of use of *Dialectica* Interpretation.

We formulate Felmat's "Little Theorem" as the formula A:

$\forall a\forall n[\forall d(1 \neq d \wedge d \neq n \to \neg d|n) \to (0<a \wedge a<n \to a^{n-1} \bmod n = 1)]$.

The *Dialectica* translation A^D is essentially A with $\forall d$ removed and the remaining occurrences of d replaced by the term $D(a,n)$, where D has type $0 \to 0 \to 0$. Thus if $IPV \vdash A$, then by theorem 9.2.2 a polynomial time function $D(a,n)$ can be found which satisfies A^D. This function supplies the same information as the term D in DⓇB. Thus for Felmat's theorem, the *Dialectica* translation is interesting for both the statement itself and its contrapositive, while the realizability is interesting only for the contrapositive.

The *Dialectica interpretation* shows follows.

Proposition 9.2.3 $IPV \vdash A$ iff $IPV \vdash B$.

(*proof*)

By standard intuitionistic reasoning we have $IPV \vdash B \to A$. Conversely, if $IPV \vdash A$, then by theorem 9.2.2, $PV^\omega \vdash A^D(D)$ for some closed term D of IPV^ω. It is easy to see that

$$IPV^\omega \vdash A^D(D) \to B$$

and hence $IPV^\omega \vdash B$. By theorem 7.2.14, $IPV \vdash B$. ∎

9.3 Equivalent to the systems IS_1^2 and IS_1^2B

Theorem 9.3.1 $IPV^\omega + MP$ is a conservative extension of PV^ω.

(*proof*) Theorem of PV^ω has the form of $u=v$. Assume $IPV^\omega + MP \vdash u=v$ for any PV^ω formula $u=v$. Then by theorem 9.2.2, $PV^\omega \vdash Equ(u,v)=0$. By T126, $PV^\omega \vdash u=v$.

Therefore $\forall(u=v) \in L(PV^\omega)[IPV^\omega + MP \vdash u=v \Rightarrow PV^\omega \vdash u=v]$. ∎

Theorem 9.3.2 IPV is a conservative extension of PV^ω.

(*proof*) IPV^{ω} is an extension of IPV. Hence $\forall A \in L(IPV)[IPV \vdash A \Rightarrow IPV^{\omega} \vdash A]$.
And $L(PV) \subseteq L(IPV)$ because IPV is an extension of PV.
Hence $\forall A \in L(PV)[IPV \vdash A \Rightarrow IPV^{\omega} \vdash A]$.
By theorem 9.3.1 and theorem 6.2.22, IPV^{ω} is a conservative extension of PV. Therefore $\forall A \in L(PV)[IPV \vdash A \Rightarrow PV \vdash A]$. ∎

Definition 9.3.3 Let A be a formula of IPV or of IPV^{ω}. The **negative translation** of A, $A^{\neg\neg}$, is defined by induction on the complexity of A as follows:

(1) If A is atomic, $A^{\neg\neg} \stackrel{d}{\equiv} A$;

(2) $(A \wedge B)^{\neg\neg} \stackrel{d}{\equiv} (A^{\neg\neg} \wedge B^{\neg\neg})$;

(3) $(A \to B)^{\neg\neg} \stackrel{d}{\equiv} (A^{\neg\neg} \to B^{\neg\neg})$;

(4) $(\forall x A)^{\neg\neg} \stackrel{d}{\equiv} \forall x A^{\neg\neg}$;

(5) $(A \vee B)^{\neg\neg} \stackrel{d}{\equiv} \neg\neg(A^{\neg\neg} \vee B^{\neg\neg})$;

(6) $(\exists x A)^{\neg\neg} \stackrel{d}{\equiv} \neg\neg\exists x A^{\neg\neg}$.

Theorem 9.3.4 Let A be an any formula of IPV. Then $IPV + MP \vdash \neg\neg A^{\neg\neg} \to A^{\neg\neg}$. Same as IPV^{ω}.

(*proof*) We prove by induction on the complexity of A.

A) IPV

(1) A is atomic formula.
By MP, $IPV + MP \vdash \neg\neg A \to A$. By $A \equiv A^{\neg\neg}$, $IPV + MP \vdash \neg\neg A^{\neg\neg} \to A^{\neg\neg}$.

The remaining cases, assume $IPV + MP \vdash \neg\neg B^{\neg\neg} \to B^{\neg\neg}$ and $\neg\neg D^{\neg\neg} \to D^{\neg\neg}$.

(2) $A \equiv B \wedge D$
Then $A^{\neg\neg} \equiv B^{\neg\neg} \wedge D^{\neg\neg}$.
By $IPV + MP \vdash (B^{\neg\neg} \wedge D^{\neg\neg}) \wedge \neg B^{\neg\neg} \to \bot$,
$IPV + MP \vdash \neg B^{\neg\neg} \to \neg(B^{\neg\neg} \wedge D^{\neg\neg})$.
By this and $\vdash \neg\neg(B^{\neg\neg} \wedge D^{\neg\neg}) \wedge \neg B^{\neg\neg} \to \bot$,
$IPV + MP \vdash \neg\neg(B^{\neg\neg} \wedge D^{\neg\neg}) \to \neg\neg B^{\neg\neg}$.
Same as
$IPV + MP \vdash \neg\neg(B^{\neg\neg} \wedge D^{\neg\neg}) \to \neg\neg D^{\neg\neg}$.
Therefore
$IPV + MP \vdash \neg\neg(B^{\neg\neg} \wedge D^{\neg\neg}) \to \neg\neg B^{\neg\neg} \wedge \neg\neg D^{\neg\neg}$.
By hypothesis,
$IPV + MP \vdash \neg\neg(B^{\neg\neg} \wedge D^{\neg\neg}) \to B^{\neg\neg} \wedge D^{\neg\neg}$.

(3) $A \equiv B \to D$
Then $A^{\neg\neg} \equiv B^{\neg\neg} \to D^{\neg\neg}$.
By $IPV + MP \vdash [B^{\neg\neg} \wedge (B^{\neg\neg} \to D^{\neg\neg}) \wedge \neg D^{\neg\neg}] \to \bot$,
$IPV + MP \vdash (B^{\neg\neg} \wedge \neg D^{\neg\neg}) \to \neg(B^{\neg\neg} \to D^{\neg\neg})$.
Therefore
$IPV + MP \vdash [B^{\neg\neg} \wedge \neg D^{\neg\neg} \wedge \neg\neg(B^{\neg\neg} \to D^{\neg\neg})] \to \bot$.
Hence
$IPV + MP \vdash (B^{\neg\neg} \wedge (\neg\neg(B^{\neg\neg} \to D^{\neg\neg}))) \to \neg\neg D^{\neg\neg}$.
By Rule 12,
$IPV + MP \vdash \neg\neg(B^{\neg\neg} \to D^{\neg\neg}) \to (B^{\neg\neg} \to \neg\neg D^{\neg\neg})$
By hypothesis,
$IPV + MP \vdash \neg\neg(B^{\neg\neg} \to D^{\neg\neg}) \to (B^{\neg\neg} \to D^{\neg\neg})$

(4) $A \equiv \forall x B$
Then $A^{\neg\neg} \equiv \forall x B^{\neg\neg}$.
By $IPV + MP \vdash (\forall x B^{\neg\neg} \wedge \neg B^{\neg\neg}) \to \bot$,
$IPV + MP \vdash \neg B^{\neg\neg} \to \neg\forall x B^{\neg\neg}$.
Hence
$IPV + MP \vdash (\neg B^{\neg\neg} \wedge \neg\neg\forall x B^{\neg\neg}) \to \bot$.
By Rule 12,
$IPV + MP \vdash \neg\neg\forall x B^{\neg\neg} \to \neg\neg B^{\neg\neg}$.
By hypothesis,
$IPV + MP \vdash \neg\neg\forall x B^{\neg\neg} \to B^{\neg\neg}$.
By Rule 15,
$IPV + MP \vdash \neg\neg\forall x B^{\neg\neg} \to \forall x B^{\neg\neg}$.

(5) $A \equiv B \vee D$
Then $A^{\neg\neg} \equiv \neg\neg(B^{\neg\neg} \vee D^{\neg\neg})$.
We can prove $IPV + MP \vdash \neg\neg(\neg\neg M) \to (\neg\neg M)$ where M is any formula.
Therefore $IPV + MP \vdash \neg\neg(\neg\neg(B^{\neg\neg} \vee D^{\neg\neg})) \to \neg\neg(B^{\neg\neg} \vee D^{\neg\neg})$.

(6) $A \equiv \exists x B$
Then $A^{\neg\neg} \equiv \neg\neg\exists x B$.
$IPV + MP \vdash \neg\neg(\neg\neg(\exists x B)) \to \neg\neg(\exists x B)$ is obvious.

B) IPV^ω
Same as IPV. ∎

Definition 9.3.5 We shall denote by **CPV** the system obtained from IPV by adding all instances of the *law of excluded middle* $A \vee \neg A$ (axiom 20). $\mathbf{CPV}^\omega$ is obtained from IPV^ω in the same way. CPV is a conservative extension of S^1_2, by Theorem ?? . (CPV is equivalent to $S^1_2(PV)$ in Buss [1].)

Lemma 9.3.6 If $CPV \vdash A$ then $IPV + MP \vdash A^{\neg\neg}$. If $CPV^\omega \vdash A$ then $IPV^\omega + MP \vdash A^{\neg\neg}$.

(*proof*) We prove by induction on the length of the proof of A.

A) CPV

(1) **Axiom scheme 1**
$IPV+MP \vdash A^{\neg\neg} \to A^{\neg\neg} \wedge A^{\neg\neg}$ is obvious. Therefore $IPV+MP \vdash (A \to A \wedge A)^{\neg\neg}$.

(2) **Axiom scheme 2**
By theorem 5.2.14, $\neg\neg A^{\neg\neg} \to A^{\neg\neg}$. By this and $\neg\neg(A^{\neg\neg} \vee A^{\neg\neg}) \to \neg\neg A^{\neg\neg}$,
$IPV + MP \vdash \neg\neg(A^{\neg\neg} \vee A^{\neg\neg}) \to A^{\neg\neg}$.
Therefore $IPV + MP \vdash (A \vee A \to A)^{\neg\neg}$.

(3) **Axiom scheme 3**
$IPV+MP \vdash A^{\neg\neg} \wedge B^{\neg\neg} \to B^{\neg\neg}$ is obvious. Therefore $IPV+MP \vdash (A \wedge B \to B)^{\neg\neg}$.

(4) **Axiom scheme 4**
By $B^{\neg\neg} \to A^{\neg\neg} \vee B^{\neg\neg}$, $IPV + MP \vdash B^{\neg\neg} \wedge \neg(A^{\neg\neg} \vee B^{\neg\neg}) \to \bot$.
Therefore $IPV + MP \vdash B^{\neg\neg} \to \neg\neg(A^{\neg\neg} \vee B^{\neg\neg})$.
Therefore $IPV + MP \vdash (B \to A \vee B)^{\neg\neg}$.

(5) **Axiom scheme 5**
$IPV + MP \vdash A^{\neg\neg} \wedge B^{\neg\neg} \to B^{\neg\neg} \wedge A^{\neg\neg}$ is obvious.
Therefore $IPV + MP \vdash (A \wedge B \to B \wedge A)^{\neg\neg}$.

(6) **Axiom scheme 6**
By $IPV + MP \vdash A^{\neg\neg} \vee B^{\neg\neg} \to B^{\neg\neg} \vee A^{\neg\neg}$,
$IPV + MP \vdash \neg(A^{\neg\neg} \vee B^{\neg\neg}) \to \neg(B^{\neg\neg} \vee A^{\neg\neg})$.
By this,
$IPV + MP \vdash \neg\neg(A^{\neg\neg} \vee B^{\neg\neg}) \to \neg\neg(B^{\neg\neg} \vee A^{\neg\neg})$.
Therefore $IPV + MP \vdash (A \vee B \to B \vee A)^{\neg\neg}$.

(7) **Axiom scheme 7**
$IPV + MP \vdash \forall x A^{\neg\neg} \to A^{\neg\neg}[t/x]$ is obvious.
Therefore $IPV + MP \vdash (\forall x A \to A[t/x])^{\neg\neg}$.

(8) **Axiom scheme 8**
By $IPV + MP \vdash A^{\neg\neg}[t/x] \wedge \neg\exists x A^{\neg\neg} \to \bot$,
$IPV + MP \vdash A^{\neg\neg}[t/x] \to \neg\neg\exists x A^{\neg\neg} \to \bot$.
Therefore $IPV + MP \vdash (A[t/x] \to \exists x A)^{\neg\neg}$.

(9) **Axiom scheme 9**
$IPV + MP \vdash 0 = 1 \to A^{\neg\neg}$ is obvious. Therefore $IPV + MP \vdash (0 = 1 \to A)^{\neg\neg}$.

(10) **Axiom scheme 17**
$IPV + MP \vdash x = x$ is obvious. Therefore $IPV + MP \vdash (x = x)^{\neg\neg}$.

(11) **Axiom scheme 18**

$IPV + MP \vdash x = y \to ((A^{\neg\neg} \to A^{\neg\neg}[y/x]) \wedge (A^{\neg\neg}[y/x] \to A^{\neg\neg}))$ is obvious.
Therefore $IPV + MP \vdash (x = y \to (A \leftrightarrow A[y/x]))^{\neg\neg}$.

(12) **Axiom scheme 20**

By axiom 4,

$IPV + MP \vdash A^{\neg\neg} \to A^{\neg\neg} \vee \neg A^{\neg\neg}$.

Hence

$IPV + MP \vdash A^{\neg\neg} \wedge \neg(A^{\neg\neg} \vee \neg A^{\neg\neg}) \to \bot$.

Therefore

$IPV + MP \vdash \neg(A^{\neg\neg} \vee \neg A^{\neg\neg}) \to \neg A^{\neg\neg}$.

Hence

$IPV + MP \vdash \neg(A^{\neg\neg} \vee \neg A^{\neg\neg}) \to (A^{\neg\neg} \vee \neg A^{\neg\neg})$.

Hence

$IPV + MP \vdash \neg(A^{\neg\neg} \vee \neg A^{\neg\neg}) \wedge \neg(A^{\neg\neg} \vee \neg A^{\neg\neg}) \to \bot$.

Therefore

$IPV + MP \vdash \neg(A^{\neg\neg} \vee \neg A^{\neg\neg}) \to \bot$.

Hence

$IPV + MP \vdash \neg\neg(A^{\neg\neg} \vee \neg A^{\neg\neg})$.

Therefore $IPV + MP \vdash (A \vee \neg A)^{\neg\neg}$.

(13) **Rule of inference 10**

Assume $IPV + MP \vdash A^{\neg\neg}$ and $(A \to B)^{\neg\neg}$.
Then by $(A \to B)^{\neg\neg} \equiv A^{\neg\neg} \to B^{\neg\neg}$ and Rule 10,

$IPV + MP \vdash B^{\neg\neg}$.

Therefore If $IPV + MP \vdash A^{\neg\neg}$ and $(A \to B)^{\neg\neg}$, then $IPV + MP \vdash B^{\neg\neg}$.

(14) **Rule of inference 11-16**

Same as Rule of inference 10.

(15) **Definition** 4.1.2**(2)-(4)**

Non-logical axioms of IPV have the equivalent formula which have the form $u = v$.
Therefore
$IPV + MP \vdash (\text{Non-logical axioms})^{\neg\neg}$.

(16) **NP-Induction**

Since $\neg\exists x F$ and $\forall\neg x F$ are equivalent in intuitionistic logic, the negative translation of NP-Induction scheme is equivalent in IPV to a formula of the form:

$$[\neg\neg A(0) \wedge \forall x(\neg\neg A(\lfloor \tfrac{1}{2}x \rfloor) \to \neg\neg A(x))] \to \forall z \neg\neg A(z),$$

where A is of the form $(\exists y \leq t)u = v$.
By theorem 4.2.2, $(\exists y \leq t)u = v$ is equivalent in IPV to the formula $\exists y(Lesseq u(y,t) \& Equ(u,v) = 0)$, so that $\neg\neg A \leftrightarrow A$ by MP. Therefore the negative translation of NP-Induction scheme is derivable in $IPV + MP$.

B) CPV^{ω}

Same as CPV. ∎

Theorem 9.3.7 For each Σ_0^b formula A, if $CPV \vdash \exists \vec{x} A$ then $IPV \vdash \exists \vec{x} A$, and if $CPV^\omega \vdash \exists \vec{x} A$ then $IPV^\omega \vdash \exists \vec{x} A$.

(*proof*) Let A be any Σ_0^b formula of CPV. By theorem 4.2.3, there is a term t_A such that $IPV \vdash A \leftrightarrow t_A = 0$. Therefore if $CPV \vdash \exists \vec{x} A$, then $CPV \vdash \exists \vec{x}(t_A = 0)$. By lemma 9.3.6, $IPV + MP \vdash (\exists \vec{x}(t_A = 0))^{\neg\neg}$.
By MP

$$\begin{aligned} IPV + MP \vdash (\exists \vec{x}(t_A = 0))^{\neg\neg} &\leftrightarrow \neg\neg \exists x_1 (\exists x_2, \cdots, x_n (t_A = 0))^{\neg\neg} \\ &\leftrightarrow \exists x_1 \neg\neg \exists x_2 (\exists x_3, \cdots, x_n (t_A = 0))^{\neg\neg} \\ &\vdots \\ &\leftrightarrow \exists \vec{x}(t_A = 0). \end{aligned}$$

Therefore $IPV + MP \vdash \exists \vec{x}(t_A = 0)$.
By theorem 9.2.2, there exists $\vec{s}$ of zero-order open term of PV^ω such that $PV^\omega \vdash t_A[\vec{s}/\vec{x}] = 0$. By theorem 6.2.10, $PV^\omega \vdash t_A[\vec{s}^{PV}/\vec{x}] = 0$. By theorem 6.2.22, $PV \vdash t_A[\vec{s}^{PV}/\vec{x}] = 0$. Hence $IPV \vdash \exists \vec{x}(t_A = 0)$.
Therefore $IPV \vdash \exists \vec{x} A$.

For CPV^ω and IPV^ω, same as CPV and IPV. ∎

Theorem 9.3.8 CPV is a conservative extension of PV.

(*proof*) Theorem of PV has the form of $u = v$. Assume $CPV \vdash u = v$ for any PV formula $u = v$. Then by theorem 9.3.7, $IPV \vdash u = v$. By this and theorem 9.3.1, $PV \vdash u = v$. Therefore $\forall (u = v) \in L(PV)[CPV \vdash u = v \Rightarrow PV \vdash u = v]$. ∎

Theorem 9.3.9 CPV^ω is a conservative extension of PV^ω.

(*proof*) Same as theorem 9.3.8. ∎

Theorem 9.3.10 (First main theorem) The system IS_1^2 and $IS_1^2 B$ are equivalent.

(*proof*) We have already shown in theorem 2.3.11 that $H\Sigma_1^b - PIND$ *scheme* is derivable in IS_2^1. Thus it suffices to show that the remaining axioms of $IS_1^2 B$ are derivable in IS_1^2. Let $(A \to B)$ be a theorem of S_1^2, where both A and B are $H\Sigma_1^b$ formulas. By lemma 2.3.10, we may assume that A and B are both Σ_1^{b+}. Now if $IS_1^2 \vdash A \to B$ then $CPV \vdash A \to B$, and by lemma 4.2.11 and theorem 4.2.2, A and B are provably equivalent in IPV to formulas of the term $(\exists x \le t)(u = 0)$ and $(\exists y \le t)(v = 0)$. Thus

$$CPV \vdash (x \le t \wedge u = 0) \to (\exists y \le t)(v = 0)$$

so by classical logic,

$$CPV \vdash \exists y (x \le t \wedge u = 0) \to (y \le t \wedge v = 0).$$

By theorem 9.3.7,

$$IPV \vdash \exists y (x \le t \wedge u = 0) \to (y \le t \wedge v = 0).$$

Therefore

$$IPV \vdash A \to B.$$

By theorem 4.2.12,

$IS^1_2 \vdash A \to B$.

Hence

if A and B are HΣ^b_1-formulas and (A$\to$ B) is theorem of S^1_2,

then (A$\to$ B) is axiom of IS^1_2.

Therefore

$$\forall A \in L(IS^1_2 B)[IS^1_2 B \vdash A \Rightarrow IS^1_2 \vdash A].$$

Conversely, $BASIC$ *axioms* are provable in $IS^1_2 B$.

And By $L(\Sigma^{b+}_1) \subseteq L(H\Sigma^b_1)$, $\Sigma^{b+}_1 - PIND$ scheme is provable from $H\Sigma^b_1 - PIND$.

Therefore

$$\forall A \in L(IS^1_2)[IS^1_2 \vdash A \Rightarrow IS^1_2 B \vdash A]. \blacksquare$$

Theorem 9.3.11 (Second main theorem) Let A be a Σ^b_1 formula such that $CPV \vdash \forall \vec{x} \exists y A(\vec{x}, y)$. Then there is an n-place function symbol f of PV so that $IPV \vdash A(\vec{x}, f(\vec{x}))$.

(*proof*)

Assume $CPV \vdash \forall \vec{x} \exists y A(\vec{x}, y)$. Then $CPV \vdash \exists y A'(\vec{x}, y)$, where $A'(\vec{x}, y)$ is $POS(A'(\vec{x}, y))$.

By lemma 4.2.11, $A'(\vec{x}, y)$ is equivalent in IPV to a formula of the form $(\exists z \leq t)(u = v)$.

By theorem 9.3.7, $IPV \vdash \forall \vec{x} \exists y A'(\vec{x}, y)$. By lemma 2.3.2, $IPV \vdash \forall \vec{x} \exists y A(\vec{x}, y)$.

By theorem 8.3.3, $IPV \vdash A(\vec{x}, f(\vec{x}))$. $\blacksquare$

Chapter 10

Concluding Remarks

10.1 Results

In chapter 2 we defined arithmetic systems of Buss's IS^1_2B and Cook's IS^1_2. And we proved that two systems are equivalent in Chapter 9. And we proved that Σ^{b+}_1-definable functions in IS^1_2 are polynomial time computable functions and polynomial time computable functions are Σ^{b+}_1-definable functions in IS^1_2 in Chapter 2.

There is a big difference between "Σ^{b+}_1-definable function is polynomial time computable function" and "there exists a polynomial time computable function which is Σ^{b+}_1-definable". Hence we hoped that existence of polynomial time computable function is guaranteed. So we used two techniques same as computable function for this proof. In chapter 8 we used Troelstra's technique. So we proved "if $\forall\vec{x}\exists yA(\vec{x},y)$ is a closed theorem of IS^1_2, then there exists a polynomial time computable function f such that $\forall\vec{x}A(\vec{x},f(\vec{x}))$ is a theorem of IS^1_2" by realizability. In chapter 9 we used Gödel's technique. And we proved same property by *Dialectica* interpretation.

10.2 future subject

One of study of computational computability is to study the including relation of some classes. In this study there is the famous problem "$P = NP$ problem". This is a problem which relation between P and NP is "$P = NP$?" or "$P \subsetneqq NP$?" There are some classes besides P and NP. In these classes we direct my attention to classes which is definable by function algebra. For example, class K, T and $\mathcal{E}$ are definable by function algebra. In these classes it does not solve whether it is $T = K$ or $T \subsetneqq K$. So I want to express functions of each class by logical arithmetic like functions of class P by IS^2_1, and we want to solve including relation of some classes. Therefore first we find suitable hierarchy like Π^b_i and Σ^b_i in IS^1_2 because we know that class P and hierarchy are close relations. Next we construct logical arithmetic based on hierarchy. Next we show by use of function algebra that a function f is Σ'-definable iff a function f is a function of each class in each system. And we prove in system by realizability and *Dialectica* interpretation that there exists a function of each class which can Σ'-define. Finally using these, I want to

solve the relation of some classes. Then we need to study pure logic because we might be able to use tools of pure logic for study of computational complexity like realizability and *Dialectica* interpretation.

Bibliography

[1] Samuel R.Buss, *Bounded Arithmetic*, Ph.D. dissertation, Princeton University 1985; reprinted Biblopolis, Napoli, 1986.

[2] Samuel R.Buss, *The polynomial hierarchy and intuitionistic bounded arithmetic*, Springer-Verlag, Berlin, 1986.

[3] S.A.Cook, *Feasibly constructive proofs and the propositional calculus.*, Proc.7th A.C.M. Symposium on the Theory of Computation,(1975), pp.83-97.

[4] S.A.Cook, *Functional interpretation of feasibly constructive arithmetic*, Annals of Pure and Applied Logic, 63 (1993), pp.103-200.

[5] Kurt Gödel, Über *eine bifher noch nicht* benützte *erweiterung des finiten standpunktes*, J. of Philosophical Logic, 9 , pp.133-142.

[6] Victor Hindley and Jonathan P. Seldin, *Introduction to Combinators and λ-calculus*, Cambridge University Press, 1986.

[7] S.C.Kleene, *On the interpretation of intuitionistic number theory*, J. Symbolic Logic, 10 , pp.109-124.

[8] Mitsuru Tada, *Proof Theory in Bounded Arithmetic Systems*, PH.D. dissertation, Tohoku University 1998.

[9] Gaisi Takeuti, *Proof Theory*, North-Holland, second edition, 1987.

[10] A.S.Troelstra, *Metamathematical investigation of intuitionistic arithmetic and analysis*, Springer-Verlag Lecture Notes in Mathematics, No.344, 1973.