Università
degli Studi
di Padova

Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

Corso di Laurea Triennale in Matematica

Equiconsistency of ZF-Inf and PA

Relatore:
Dott. Samuele Maschio

Laureando: Flavio Valerio Saladino
Matricola: 2007261

Anno Accademico 2023/2024

19/04/2024

Contents

Chapter 0

Introduction

The equiconsistency of **ZF-Inf** and **PA** is part of the mathematical folklore, it appears for the first time in Akermann's "Die Widerspruchsfreiheit der allgemeinen Mengenlehre"[1], published in 1937. Ackermann's idea was to investigate the consistency of what he calls *general theory of sets*, i.e., Zermelo-Fraenkel theory without the axiom of infinity, by tracing it back to the consistency of arithmetic, consistency in which mathematicians had great confidence in that period. The heart of the Ackermann's idea is that it is possible to translate the general theory of sets into the formal theory of arithmetic and vice versa in a *syntactic* manner. To translate sets into natural numbers he had to find a way to codify the relation "$\in$" in arithmetical terms such that the translation of every axiom of **ZF-Inf** would be a theorem in **PA**. He found a translation of " $\in$ " - that is the so called *Ackermann Encoding* - by observing that every natural number a can be written as sums of power of 2: $a = 2^{b_0} + 2^{b_1} + ... + 2^{b_n}$, in which every b_i is either 0 or 1. Thus, he translated $i \in m$ into $b_i = 1$ where $m = 2^{b_0} + ... + 2^{b_n}$, that is: *$m \in n$ iff the m-th digit in the binary expansion of n is 1.* This translation is interesting not only because it works, but because it is also primitive recursive; thus, it only requires primitive recursive arithmetic as a meta-theoretic assumption to be formalized, and **PRA** is weaker than standard arithmetic. The translation of **PA** into **ZF-Inf** involves matching numbers with finite hereditary sets and restricting quantifiers accordingly. Subsequently the equiconsistency of **PA** and **ZF-Inf** became part of mathematics's folklore as "well-known" result, without having an extensive bibliographical reference. In 2007 Richard Kaye and Tin Lok Wong published a paper titled "On Interpretations of Arithmetic and Set Theory"[2] in which they argued the equiconsistency of **PA** and **ZF-Inf + ¬Inf** by proving that it is possible, using $\epsilon-$Induction, to construct two interpretations of **PA** in **ZF-Inf + ¬Inf** and vice versa, that are one the inverse of the other. In 2009 Richard Pettigrew published a paper called "On Interpretations of Bounded Arithmetic and Bounded Set Theory"[5] in which, starting from the bi-interpretability proved by Kaye and Wong, he defined a mutual interpretation for a bounded arithmetic theory and a sets theory obtained by **ZF-Inf - Repl + ¬Inf + WHP**, that is a slighted modified version of Mayberry's Euclidean Sets theory.

Our purpose is to treat the Ackermann proof together with the preliminary results necessary to formalize it. In Chapter 1 we will enunciate the general logical results necessary for our discussion. In Chapter 2, we will present and discuss both **ZF-Inf** and **PA** theories,

covering some basic results needed to conclude equiconsistency. In our treatment of Peano Arithmetic, we will explore recursive primitive functions and representable functions, ultimately establishing that all recursive primitive functions are representable. Thus, we will define **PA'**, a conservative extension of **PA** obtained by adding a symbol for each definition of a primitive recursive function. Regarding axiomatic set theory, we will introduce the Zermelo-Fraenkel axioms and explore results concerning ordinals, transfinite induction, and transfinite recursion within the framework of **ZF-Inf**. We will therefore move on to enunciate a conservative extension of **ZF-Inf** obtained by adding a symbol for 0, a symbol for the successor function and two symbols for sum and product of finite ordinals respectively, i.e. $\mathbf{ZF}_{ord}$**-Inf**. Finally, we will articulate a set of axioms equivalent to **ZF-Inf**, denoted as **ZF'-Inf**, in which we weaken the union and power axioms and eliminate certain non-independent axioms such as empty and pair. Therefore, in Chapter 3, we will develop the proof of equiconsistency. We will define two translations: one translating **PA** into $\mathbf{ZF}_{ord}$**-Inf** and another translating **ZF'-Inf** into **PA'**. Those translation, with some consideration about the equiconsistency of **ZF-Inf** with **ZF'-Inf** and $\mathbf{ZF}_{ord}$**-Inf** and **PA** with **PA'** yield to the equiconsistency of **PA** and **ZF-Inf**. In conclusion, in Chapter 4, we will discuss the consequences of the equiconsistency of **PA** and **ZF-Inf** in finite set theory. Therefore we will start from the definition of finite set, comparing different definitions of finiteness and infinity, and we will comment on the role of the axiom of choice. We will conclude the fourth chapter by briefly mentioning and commenting on the contemporary results that we mentioned in the first part of the introduction.
We will use, as mainly references in the literature, Kunen[3] for set theory, Mendelson[4] for logic and both Mendelson[4] and Takahshi[6] for formal arithmetic results.

Chapter 1

Logical Background

In this chapter we will introduce the logical framework necessary to develop our discussion, therefore we will define the concept of first order language and first order theory. In this chapter we will use definitions and results taken from Mendelson[4]

1.1 First Order Languages with equality

From an intuitive standpoint a formal language is a collection of symbols that can be put together by using a clear and formal set of rules. A first order language with equality $\mathcal{L}$ is defined by an alphabet of symbols (that is a collection of symbols intended to represent variables, constants, relations and functions), a set of terms (which are the "objects" of the theory) and a set of formulas.

An alphabet is defined by a collection $\langle \mathcal{C}, \mathcal{F}, \mathcal{R}, \mathcal{V} \rangle$ and a collection of logical symbols and auxiliaries symbols where:

- $\mathcal{V}$ is a countable set containing symbols for the variables. Usually the symbols used for variables are x_0 , x_1 , y_n, ...
- $\mathcal{F}$ is an arbitrary set containing symbols for the functions. Functions are usually denoted by $f^1, g^2, h^n, ...$
  The superscript in this signature represents the arity of function, that is the number of terms to whom the function applies.
- $\mathcal{R}$ is an arbitrary set of symbols used to represent relations. The relations are usually represented with capital Latin letters (such as Q, P, R) and they have the same notation for arity as the functions. $\mathcal{L}$ has a particular relation symbol A_1^2 that represents equality; we shall write $t = s$ instead of $A_1^2(t, s)$
- $\mathcal{C}$ is an arbitrary set containing the symbols representing constants.
- Logical symbols are the connectives: $\rightarrow$ (implication), $\neg$ (negation), and the universal quantifier $\forall$

- The auxiliary symbols are: (,) (Parenthesis) and ","

We can now imagine the terms of a formal language $\mathcal{L}$ as the structure elements of the theory, or the elements of $\mathcal{L}$ that form a closed set with respect to functions. So we can formalize this idea:
From an inductive point of view we can define the set of terms $T_{\mathcal{L}}$ saying:

1. every individual constant $a \in \mathcal{C}$ is a term

2. every variable $x \in \mathcal{V}$ is a term

3. if $t_1, ..., t_n$ are terms and f^n is a symbol for an n-ary function in $\mathcal{L}$ then $f^n\big(t_1, ..., t_n\big)$ is a term

4. no other element of $\mathcal{L}$ is a term

We can also define $T_{\mathcal{L}}$ as the smallest set that satisfies:

$$\mathcal{C} \cup \mathcal{V} \subseteq T_{\mathcal{L}} \quad and \quad (t_1, ..., t_n \in T_{\mathcal{L}} \quad and \quad f^n \in F) \Rightarrow f^n\big(t_1, ..., t_n\big) \in T_{\mathcal{L}} \tag{1.1}$$

From the definition of formal language we can imagine the idea of formulas as a finite sequence of symbols from a given alphabet that is in the formal language. Therefore, we can define the set of formulas over the language $\mathcal{L}$ as we do in definition of terms.
We can define the set of formulas over $\mathcal{L} = \big\langle \mathcal{C}, \mathcal{F}, \mathcal{R}, \mathcal{V} \big\rangle$ in an inductive way saying:

1. if $t, t' \in T_{\mathcal{L}}$, then $t = t'$ is a formula

2. if $t_1, ..., t_n \in T_{\mathcal{L}}$ and $R^n \in \mathcal{R}$ then $R^n(t_1, ..., t_n)$ is a formula

3. if ϕ and ψ are well formed formulas then $(\neg\phi), (\phi \to \psi), (\forall x\phi)$ are well formed formulas

We can conclude this section by explaining some conventions that we will use:
We do not need to introduce $\wedge$, $\vee$, $\leftrightarrow$ and $\exists$ since we can define them as abbreviations:

$$(\phi \wedge \psi) := (\neg(\phi \to (\neg\psi))) \tag{1.2}$$
$$(\phi \vee \psi) := ((\neg\phi) \to \psi) \tag{1.3}$$
$$(\phi \leftrightarrow \psi) := ((\phi \to \psi) \wedge (\psi \to \phi)) \tag{1.4}$$
$$(\exists x\phi) := (\neg(\forall x(\neg\phi))) \tag{1.5}$$

And we adopt the usual conventions regarding the elimination of parenthesis and the hierarchy order of operators

1.2 First order Theories With Equality

Now we have all the concepts necessary to define what is a First Order Theory $\mathscr{T}$ over a First Order language $\mathcal{L}$.

Definition 1.2.1 (First Order Theory With Equality Over with a First Order Language with Equality)**.** Let $\mathcal{L}$ be a first order language. A first order theory $\mathscr{T}$ in the language $\mathcal{L}$ is a set of formulas of $\mathcal{L}$, called the axioms of $\mathscr{T}$, together with some rules of inference. The axioms may be divided into logical axioms - axioms involving formulas, connectives, quantifiers and equality (which are common to all first order theories) - and proper axioms, which depend on the theory itself. If ϕ, ψ and θ are formulas of $\mathcal{L}$ than the *logical axioms* of $\mathscr{T}$ are

$$(A1) \quad (\phi \to (\psi \to \phi)) \tag{1.6}$$
$$(A2) \quad ((\phi \to (\psi \to \theta)) \to ((\phi \to \psi) \to (\phi \to \theta))) \tag{1.7}$$
$$(A3) \quad (((\neg\psi) \to (\neg\phi)) \to (((\neg\psi) \to \phi) \to \psi)) \tag{1.8}$$
$$(A4) \quad (\forall x_i)\phi(x_i) \to \phi(t) \tag{1.9}$$
$$(A5) \quad (\forall x_i)(\phi \to \psi) \to (\phi \to (\forall x_i)\psi) \tag{1.10}$$
$$(A6) \quad (\forall x_1)x_1 = x_1 \tag{1.11}$$
$$(A7) \quad x = y \to (\phi(x,x) \to \phi(x,y)) \tag{1.12}$$

In $(A4)$ $\phi(x_i)$ must be a formula of $\mathcal{L}$ for all i and $t \in T_{\mathcal{L}}$ must be free free for x_i in $\phi(x_i)$ while in $(A5)$ ϕ must not have free occurrences of x_i.
The proper axioms, as mentioned above, cannot be specified, since they depend on the objects and the meaning of $\mathscr{T}$. A first order theory without proper axioms is called first order *predicate calculus*
In conclusion, the rules of inference of $\mathscr{T}$ are:

(MP) Modus Ponens: ϕ follows from ψ and $\psi \to \phi$

(Gen) Generalization: $(\forall x_i)\phi$ follows from ϕ

Remark 1.2.2. Since now we will use "First Order Theory" instead of "First Order Theory with Equality"

Definition 1.2.3 (Proof)**.** We say that a formula ϕ follows in $\mathscr{T}$ from a set Γ of formulas if and only if there is a sequence $\phi_1, ..., \phi_k$ such that ϕ is ϕ_k and every ϕ_i for each i verifies: either ϕ_i is an axiom of $\mathscr{T}$, or ϕ_i is in Γ, or ϕ_i is direct consequence by Modus Ponens or Generalization of some of the preceding formulas in the sequence, with the proviso that every time Gen is used on a variable x_i, then there are no free occurrences of x_i in each formula in Γ preceding the use of Gen. The sequence is called *proof* (or *deduction*) of ϕ from Γ, and we write

$$\Gamma \vdash_{\mathscr{T}} \phi \tag{1.13}$$

The members of Γ are called *hypotheses* or *premises* of the proof.

Definition 1.2.4 (Theorem)**.** If $\Gamma \vdash_{\mathscr{T}} \phi$ and Γ is the empty set $\varnothing$ than instead of $\varnothing \vdash_{\mathscr{T}} \phi$ we can write $\vdash_{\mathscr{T}} \phi$. In this case we state that ϕ is a *theorem* of $\mathscr{T}$. That is, ϕ is a theorem in $\mathscr{T}$ if it follows from the axioms of $\mathscr{T}$ without any other assumptions.

Theorem 1.2.5 (Deduction Theorem)**.** Let $\Gamma \cup \{\phi, \psi\}$ a set of formulas of a first order language $\mathcal{L}$ and let $\mathscr{T}$ be a first order theory over $\mathcal{L}$

$$\Gamma \vdash_{\mathscr{T}} \phi \to \psi \iff \Gamma, \phi \vdash_{\mathscr{T}} \psi$$

Definition 1.2.6 (Consistency)**.** A theory $\mathscr{T}$ is *consistent* if no formula ϕ and its negation $\neg\phi$ are both provable in $\mathscr{T}$. We write Cons($\mathscr{T}$) if the theory is consistent and Incon($\mathscr{T}$) if it is not.

Definition 1.2.7 (Equiconsistency)**.** Let $\mathscr{T}$ and $\mathscr{K}$ be two first order theories, they are said to be *equiconsistent* if:

$$Cons(\mathscr{T}) \iff Cons(\mathscr{K}) \tag{1.14}$$

Remark 1.2.8. Since $\mathscr{T}$ proves two formulas ϕ, ψ if and only if proves their conjunction $\phi \wedge \psi$, the formulas such $\phi \wedge \neg\phi$ are said to be *contradictions*. It is possible to prove that all contradictions are equivalent. So it makes sense to introduce a symbol meaning "contradiction" $\perp$. Then it is clear that $\neg\phi$ is equivalent to $\phi \to \perp$.

1.3 Proprieties of First Order Theories

We shall now enunciate some important properties of first order theories that will be useful during our discussion

Proposition 1.3.1 (Particularization Rule A4)**.** If t is free for x in $\phi(x)$, then

$$\forall x(\phi(x)) \vdash_{\mathscr{T}} \phi(t)$$

Proposition 1.3.2 (Existential Rule E4)**.** Let t be a term that is free for x in formula $\phi(x,t)$, and let $\phi(t,t)$ arise from $\phi(x,t)$ by replacing all free occurrences of x by t. Then $\phi(t,t) \vdash (\exists x)\phi(x,t)$

Remark 1.3.3. By E4 the following holds:

$$\vdash_{\mathscr{T}} \exists x(x = x)$$

This establishes that the domain of the theory is not empty

Definition 1.3.4 (Rule C)**.** A rule C deduction in a first order theory $\mathscr{T}$ is defined in the following manner: $\Gamma \vdash_{\mathscr{T},C} \phi$ if and only if there is a sequence of formulas ϕ_1‘, ..., ϕ_n such that ϕ_n is ϕ and the following conditions hold:

1. For each $i < n$ either

(a) ϕ_i is an axiom of $\mathscr{T}$ or

(b) ϕ_i is in Γ

(c) ϕ_i follows by MP or Gen from preceding formulas in teh sequence with the clause that if Gen is used on x_i no preceding formulas in Γ has free occurrences of x_i

(d) there is a preceding formula $\exists x\psi(x)$ such that ϕ_i is $\psi(d)$, where d is a new individual constant (rule C)

2. As axioms in 1(a) we can also use all logical axioms that involve the new individual constant already introduced in the sequence by application of rule C

3. No application of Gen is made using a variable that is free in some $\exists x\psi(x)$ to which rule C has been previously applied

4. ϕ contains none of the new individual constants introduced in the sequence in any application of rule C

Proposition 1.3.5. If $\Gamma \vdash_{\mathscr{T},C} \phi$ then $\Gamma \vdash_{\mathscr{T}} \phi$

Proposition 1.3.6 (Definition of a new function symbol)**.** Let $\mathscr{K}$ be a First order theory with equality. Assume that $\vdash_{\mathscr{K}} (\exists! u)\phi(y_1, ..., y_n, u)$ let $\mathscr{K}^*$ be the theory with equality obtained by adding to $\mathscr{K}$ a new function symbol f^n and the proper axiom

$$(\forall u)(\phi(f^n(k_1, ..., k_n), y_1, ..., y_n)) \tag{1.15}$$

as well as every instance of (A1)-(A7) that involves f^n. There is an effective transformation mapping each formula ψ of $\mathscr{K}^*$ into a formula ψ^* of $\mathscr{K}$ such that:

a. If f does not occur in ψ, then ψ^* is ψ

b. $(\neg\psi)^*$ is $\neg(\psi^*)$

c. $(\psi \to \xi)^*$ is $\psi^* \to \xi^*$

d. $((\forall x)\psi)^*$ is $(\forall x)(\psi^*)$

e. $\vdash_{\mathscr{K}*} \psi^* \to \psi$

f. If $\vdash_{\mathscr{K}*} \psi$ then $\vdash_{\mathscr{K}} \psi^*$

Hence, if ψ does not contain f^n and $\vdash_{\mathscr{K}*} \psi$ then $\vdash_{\mathscr{K}} \psi$

Remark 1.3.7. It is possible to apply proposition 1.3.6 also to a set of new symbols corresponding to formulas that verify the hypotheses of the proposition obtain the same result

Chapter 2

Presentation of Formal Systems

2.1 Peano Arithmetic

The theory of numbers is one of the most immediate intuition of mathematics, therefore it is not surprising that the confidence of mathematicians regarding the consistency of arithmetic was unconditional at the beginning of the twentieth century. The first semi-axiomatic presentation of natural arithmetic was given by Dedekind in 1879; in a modified form it came as *Peano Arithmetic*. It can be defined through the following axioms:

PA1 0 is a natural number

PA2 If x is a natural number, there is another natural number denoted by x' and called the *successor of* x

PA3 $0 \neq x'$ for every natural number x

PA4 If $x' = y'$ then $x = y$

PA5 If Q is a property that may or may not hold for any given natural number, and if (I) 0 has the property Q and (II) whenever a natural number x has Q then even x' has Q, then all the natural numbers have the property Q (mathematical induction principle)

2.1.1 Peano Arithmetic Formal Theory

Now we can formally define *Peano Arithmetic* (PA)

Definition 2.1.1 (The language of arithmetic)**.** *The language of arithmetic*, $\mathcal{L}_A$ is the language that we will use to formalize arithmetic. $\mathcal{L}_A$ is a language of the first order with equality. $\mathcal{L}_A$ has a single individual constant a_1, we shall write 0 as alternative notation for a_1. Finally, $\mathcal{L}_A$ has three function letters: f_1^1, f_1^2 and f_2^2. We shall write t' instead of $f_1^1(t)$, $t + s$ instead of $f_1^2(t, s)$ and $t \cdot s$ instead of $f_2^2(t, s)$

Definition 2.1.2 (Proper Axioms of $\mathscr{S}$)**.** The proper axioms of $\mathscr{S}$ are the universal closure of:

$$\begin{aligned}
&(S1) && \forall x(0 \neq x) && (2.1)\\
&(S2) && \forall x_1 \forall x_2(x_1' = x_2' \to x_1 = x_2) && (2.2)\\
&(S3) && \forall x_1(x_1 + 0 = x_1) && (2.3)\\
&(S4) && \forall x_1 \forall x_2(x_1 + x_2' = (x_1 + x_2)') && (2.4)\\
&(S5) && \forall x_1(x_1 \cdot 0 = 0) && (2.5)\\
&(S6) && \forall x_1 \forall x_2((x_1 \cdot x_2') = (x_1 \cdot x_2) + x_1) && (2.6)\\
&(S7) && \phi(0) \to ((\forall x)(\phi(x) \to \phi(x')) \to (\forall x)\phi(x)) && (2.7)
\end{aligned}$$

in (S7) ϕ must be a formula of $\mathscr{S}$. Notice that (S1)-(S6) are formulas and (S7) is an axiom schema. [1]

Remark 2.1.3. Any theory that has the same theorem as $\mathscr{S}$ is often called *Penao Arithmetic*, or simply PA

Remark 2.1.4. From (S7) and (MP) we can derive the *induction rule*:

$$\phi(0), (\forall x_i)(\phi(x_i) \to \phi(x_i')) \vdash_{\mathscr{S}} (\forall x)(\phi x) \quad (2.8)$$

Proposition 2.1.5. For any terms t, r, s of $\mathcal{L}_A$ the following are theorems of $\mathscr{S}$

(S1') $0 \neq t'$

(S2') $t' = s' \to t = s$

(S3') $t + 0 = t$

(S4') $t + r' = (t + r)'$

(S5') $t \cdot 0 = 0$

(S6') $t \cdot r' = (t \cdot r) + t$

Proof. (S1')-(S6') follow from (S1)-(S6) applying rule A4 with the appropriate terms □

Proposition 2.1.6. For any terms t, r, s the following formulas are theorems of $\mathscr{S}$

a. $t = t$

[1] (S7) does not fully correspond to (PA5) since (PA5) refer to the $2^{\aleph_0}$ property of natural numbers while (S7) refers only to the denumerable property defined by formulas of $\mathcal{L}_A$. To completely correspond to (PA5) we would need an axiom such: $\forall X[(0 \in X \wedge \forall k(k \in X \to k' \in X)) \to \forall n(n \in X)]$. This formulation corresponds to mathematical induction, it can bee seen by matching every property Q to the set of all natural that satisfies Q K_Q. But we cannot use an axiom like this: in fact X in the formula is a subset of natural number, and so the quantifier are quantifying over a subset of theory's objects. Using arbitrary natural's subsets allows us to refer to $|\mathscr{P}(\mathbb{N})| = 2^{\aleph_0}$ proprieties. However, this is possible only in a second order theory, since in a first order theory we can quantify only over sets defined by formulas of $\mathcal{L}_A$, and so we will use (S7) instead of a complete axiomatization of (PA5).

b. $t = r \to r = t$

c. $t = r \to (r = s \to t = s)$

d. $r = t \to (s = t \to r = s)$

e. $t = r \to t + s = r + s$

f. $t = 0 + t$

g. $t' + r = (t + r)'$

h. $t + r = r + t$

i. $t = r \to s + t = s + r$

j. $(t + r) + s = t + (r + s)$

k. $t = r \to t \cdot s = r \cdot s$

l. $0 \cdot t = 0$

m. $t' \cdot r = t \cdot r + r$

n. $t \cdot r = r \cdot t$

o. $t = r \to s \cdot t = s \cdot r$

Proof.

a.	(1)	$t + 0 = t$	(S3')
	(2)	$(t + 0 = t) \to (t + 0 = t \to t = t)$	Equivalence Property
	(3)	$t + 0 = t \to t = t$	1, 2, MP
	(4)	$t = t$	1, 3, MP
b.	(1)	$t = r \to (t = t \to r = t)$	Equivalence Property
	(2)	$t = t \to (t = r \to r = t)$	1, tautology, MP
	(3)	$t = r \to r = t$	2, (a.), MP
c.	(1)	$r = t \to (r = s \to t = s)$	Equivalence Property
	(2)	$t = r \to r = t$	(b.)
	(3)	$t = r \to (r = s \to t = s)$	1, 2, tautology, MP

d.

(1)	$r = t \rightarrow (t = s \rightarrow r = s)$	(c.)
(2)	$t = s(r = t \rightarrow r = s)$	1, tautology, MP
(3)	$s = t \rightarrow t = s$	(b.)
(4)	$s = t \rightarrow (r = t \rightarrow r = s)$	2, 3, tautology, MP

e. Apply induction rule to $\phi(x)$: $x = y \rightarrow x + z = y + z$

i.

(1)	$x + 0 = 0$	(S3')
(2)	$y + 0 = 0$	(S3')
(3)	$x = y$	Hyp
(4)	$x + 0 = y$	1, 3, (c.), MP
(5)	$x + 0 = y + 0$	4, 2, (d.), MP
(6)	$\vdash_{\mathscr{S}} x = y \rightarrow x + 0 = y + 0$	1-5, deduction theorem

Thus, $\vdash_{\mathscr{S}} \phi(0)$

ii.

(1)	$x = y \rightarrow x + z = y + z$	Hyp
(2)	$x = y$	Hyp
(3)	$x + z' = (x + z)' + z' = (x + z)'$	(S4')
(4)	$y + z' = (y + z)'$	(S4')
(5)	$x + z = y + z$	1, 2, MP
(6)	$(x + z)' = (y + z)'$	5, equivalence property, MP
(7)	$x + z' = (y + z)'$	3, 6, (c.), MP
(8)	$x + z' = y + z'$	4, 7, (d.), MP
(9)	$\vdash_{\mathscr{S}} (x = y \rightarrow x + z = y + z) \rightarrow (x = y \rightarrow x + z' = y + z')$	1-8, deduction theorem

Thus, $\vdash_{\mathscr{S}} \phi(z) \rightarrow \phi(z')$ and, by Gen: $\vdash_{\mathscr{S}} (\forall z)(\phi(z) \rightarrow \phi(z'))$. Hence $\vdash_{\mathscr{S}} (\forall z)\phi(z)$ by induction rule. Therefore, by Gen and rule A4, $\vdash_{\mathscr{S}} t = r \rightarrow t + s = r + s$

f. Let $\phi(x)$ be $x = 0 + x$

i. $\vdash_{\mathscr{S}} 0 = 0 + 0$ by (S3'), (b.) and MP; thus $\vdash_{\mathscr{S}} \phi(0)$

ii.

(1)	$x = 0 + x$	Hyp
(2)	$0 + x' = (0 + x)'$	(S4')

(3)	$x' = (0 + x)'$	1, Equivalence Property, MP
(4)	$x' = 0 + x'$	3, 2, (d.), MP
(5)	$\vdash_{\mathscr{S}} x = 0 + x \rightarrow x' = 0 + x'$	1-4, deduction theorem

Thus, $\vdash_{\mathscr{S}} \phi(x) \rightarrow \phi(x')$ and, by Gen, $\vdash_{\mathscr{S}} (\forall x)(\phi(x) \rightarrow \phi(x'))$. So, by (i), (ii) and the induction rule, $\vdash_{\mathscr{S}} (\forall x)(x = 0 + x)$. Then, by rule A4, $\vdash_{\mathscr{S}} t = 0 + t$

g. Let $\phi(x)$ be $x' + y = (x + y)'$

i.

(1)	$x' + 0 = x'$	(S3')
(2)	$x + 0 = x$	(S3')
(3)	$(x + 0)' = x'$	2, Equivalence Property, MP
(4)	$x' + 0 = (x + 0)'$	1, 3, (d.), MP

Thus, $\vdash_{\mathscr{S}} \phi(0)$

ii.

(1)	$x' + y = (x + y)'$	Hyp
(2)	$x' + y' = (x' + y)'$	(S4')
(3)	$(x' + y)' = (x + y)''$	1,Equivalence Property, MP
(4)	$x' + y' = (x + y)''$	2, 3, (c.), MP
(5)	$x + y' = (x + y)'$	(S4)'
(6)	$(x + y')' = (x + y)''$	5, Equivalence Property, MP
(7)	$x' + y' = (x + y)''$	4, 6, (d.), MP
(8)	$\vdash_{\mathscr{S}} x' + y = (x + y)' \rightarrow x' + y' = (x + y')'$	1-7, deduction theorem

Thus, as in f. by Gen we can apply induction rule, and we can end the proof using Gen and rule A4

h. Let $\phi(x)$ be $x + y = y + x$

i.

(1)	$x + 0 = x$	(S3')
(2)	$x = 0 + x$	(f.)
(3)	$x + 0 = 0 + x$	1, 2, (c.), MP

Thus, $\vdash_{\mathscr{S}} \phi(0)$

ii.	(1)	$x+y=y+x$	Hyp
	(2)	$x+y'=(x+y)'$	(S4')
	(3)	$y'+x=(y+x)'$	1, Equivalence property, MP
	(4)	$(x+y)'=(y+x)'$	1, equivalence property, MP
	(5)	$x+y'=(y+x)'$	2, 4, (c.), MP
	(6)	$x+y'=y'+x$	5, 3, (d.), MP
	(7)	$\vdash_{\mathscr{S}} x+y=y+x \rightarrow x+y'=y'+x$	1-6, deduction theorem

By Gen $\vdash_{\mathscr{S}} \forall y(\phi(y) \rightarrow \phi(y'))$. So, by (i), (ii) and the induction rule $\vdash_{\mathscr{S}} (\forall y)(x+y = y+x)$. Then, by rule A4 and Gen $\vdash_{\mathscr{S}} t+r=r+t$

We will leave out the (j)-(o) poofs, since they take place like the ones above □

Proposition 2.1.7. For any terms t, r, s, the following formulas are theorems of $\mathscr{S}$

a. $t\cdot(r+s)=(t\cdot r)+(t\cdot s)$ (distributivity)

b. $(r+s)\cdot t=(r\cdot t)+(s\cdot t)$ (distributivity)

c. $(t\cdot r)\cdot s=t\cdot(r\cdot s)$ (associativity of $\cdot$)

d. $t+s=r+s \rightarrow t=r$ (cancellation law for +)

Proof. Omitted, see E.Mendelson: "Introduction To Mathematical logic", sixth edition, 2015[4] □

Definition 2.1.8. We can define an inequality in $\mathscr{S}$: $t<s$ for $(\exists w)(w \neq 0 \wedge w+t=s)$, $t \leqslant s$ for $t<s \vee t=s$, $t>s$ for $s<t$ and $t \geqslant s$ for $s \leqslant t$

Proposition 2.1.9. For any terms t,r,s, the following are theorems: $\neg(t<t)$, $t<s \rightarrow (s<r \rightarrow t<r)$, $t<s \rightarrow (\neg(s<t))$, $t<s \rightarrow t+r<s+r$, $t \leqslant t$, $t \leqslant s \rightarrow (s \leqslant r \rightarrow t \leqslant r)$, $0 \leqslant t$, $0<t$, $t<r \leftrightarrow t' \leqslant r$, $t \leqslant s \leftrightarrow t' \leqslant r$, $t<t'$, $0<\overline{1}, \overline{1}<\overline{2}, ...$, $t \neq r \rightarrow (t<r \vee r<t)$, $t=r \vee t<r \vee r<t$, $t \leqslant r \vee r \leqslant t$, $t+r \geqslant t$, $r \neq 0 \rightarrow t+r\,t$, $r \neq 0 \rightarrow t\cdot r \geqslant t$, $r \neq 0 \leftrightarrow r>0$, $r>0 \rightarrow (t>0 \rightarrow r\cdot t>0)$, $r \neq 0 \rightarrow (t>1 \rightarrow t\cdot r>r)$, $r \neq 0 \rightarrow (t<s \leftrightarrow t\cdot r<s\cdot r)$, $r \neq 0 \rightarrow (t \leqslant s \leftrightarrow t\cdot r \leqslant s\cdot r)$, $\neg(t<0)$, $t \leqslant r \wedge r \leqslant t \rightarrow t=r$

Proof. Omitted, see E.Mendelson: "Introduction To Mathematical logic", sixth edition, 2015[4] □

Definition 2.1.10. We define the ordinal $\bar{n}$ as $\underbrace{(((0)')'\cdots)'}_{\text{n times}}$

Proposition 2.1.11.

a. For any natural number k, $\vdash_{\mathscr{S}} x = 0 \vee ... \vee x = \overline{k} \leftrightarrow x \leqslant \overline{k}$

a'. For any natural number $k > 0$ and for any formula ϕ, $\vdash_{\mathscr{S}} \phi(0) \wedge \phi(1) \wedge ... \wedge \phi(\overline{k}) \leftrightarrow (\forall x)(x \leqslant \overline{k} \to \phi(x))$

b. For any natural number $k > 0$, $\vdash_{\mathscr{S}} x = 0 \vee ... \vee x = (\overline{k-1}) \leftrightarrow x < \overline{k}$

b'. For any natural number $k > 0$ and any formula ϕ, $\vdash_{\mathscr{S}} \phi(0) \wedge ... \wedge \phi(\overline{k-1}) \leftrightarrow (\forall x)(x < \overline{k} \to \phi(x)$

c. $\vdash_{\mathscr{S}} ((\forall x)(x < y \to \phi(x)) \wedge (\forall x)(x \geqslant y \to \psi(x))) \to (\forall x)(\phi(x) \vee \psi(x))$

Proof. Omitted, see E.Mendelson: "Introduction To Mathematical logic", sixth edition, 2015[4] □

Proposition 2.1.12.

a. *Complete induction*: $\vdash_{\mathscr{S}} (\forall x)((\forall z)(z < x \to \phi(z)) \to \phi(x)) \to (\forall x)(\phi(x))$

b. *Least number principle*: $\vdash_{\mathscr{S}} (\exists x)\phi(x) \to (\exists y)\phi(y) \wedge (\forall z)(z < y \to \neg\phi(z))$

Proof. a. Let $\psi(x)$ be $(\forall z)(z \leqslant x \to \phi(z))$

i.

(1)	$(\forall x)((\forall z)(z < x \to \phi(z)) \to \phi(x))$	Hyp
(2)	$(\forall z)(z < 0 \to \phi(z)) \to \phi(0)$	1, rule A4
(3)	$\neg(z < 0)$	Proposition 2.1.9
(4)	$(\forall z)(z < 0 \to \phi(z))$	3, tautology, Gen
(5)	$\phi(0)$	2-4, MP
(6)	$(\forall z)(z \leqslant 0 \to \phi(z))$, i.e $\psi(0)$	5, Proposition 2.1.11
(7)	$(\forall x)((\forall z)(z < x \to \phi(z)) \to \phi(x) \vdash_{\mathscr{S}} \psi(0)$	1-6

ii.

(1)	$(\forall x)((\forall z)(z < x \to \phi(z) \to \phi(x))$	Hyp
(2)	$\psi(x)$, i.e., $(\forall z)(z \leqslant x \to \phi(z))$	Hyp
(3)	$(\forall z)(z < x' \to \phi(z))$	2, Proposition 2.1.9
(4)	$(\forall z)(z < x' \to \phi(z)) \to \phi(x')$	1, Rule A4
(5)	$\phi(x')$	3, Rule A4
(6)	$z \leqslant x' \to z < x' \vee z = x'$	Definition, tautology
(7)	$z < x' \to \phi(z)$	3, rule A4
(8)	$z = x' \to \phi(z)$	5, (A7), substitutability of equality

(9)	$(\forall z)(z \leqslant x' \to \phi(z))$, i.e. $\psi(x')$	6, 7, 8, tautology, Gen
(10)	$(\forall x)((\forall z)(z < x \to \phi(z)) \to \phi(x)) \vdash_{\mathscr{S}} (\forall x)(\psi(x) \to \psi(x'))$	1-9, deduction theorem

By (i.) and (ii.), and the induction rule, we obtain $\xi \vdash_{\mathscr{S}} (\forall x)(\psi(x))$, that is, $\xi \vdash_{\mathscr{S}} (\forall x)(\forall z)(z \leqslant x\phi(z))$, where ξ is $(\forall x)((\forall z)(z < x \to \phi(z)) \to \phi(x))$. Hence, by rule A4 twice, $\xi \vdash_{\mathscr{S}} x \leqslant x \to \phi(x)$. But $\vdash_{\mathscr{S}} x \leqslant x$. So, $\xi \vdash_{\mathscr{S}} \phi(x)$, and, by Gen and the deduction theorem $\vdash_{\mathscr{S}} \xi \to (\forall x)(\phi(x))$

b. Omitted, see E.Mendelson: "Introduction To Mathematical logic", sixth edition, 2015[4]

□

In the next proposition we will prove the existence of the division and the reminder in **PA**.

Proposition 2.1.13.

$$\vdash_{\mathscr{S}} y \neq 0 \to (\exists u)(\exists v)[x = y \cdot u + v \wedge v < y \wedge (\forall u_1)(\forall v_1)((x = y \cdot u_1 + v_1 \wedge v_1 < y) \to u = u_1 \wedge v = v_1)] \tag{2.9}$$

Proof. Let $\phi(x)$ be $y \neq 0 \to (\exists u)(\exists v)(x = y \cdot u + v \wedge v < y)$

i.

(1)	$y \neq 0$	Hyp
(2)	$0 = y \cdot 0 + 0$	(S3'), (S5')
(3)	$0 < y$	1, Proposition 2.1.9
(4)	$0 = y \cdot 0 + 0 \wedge 0 < y$	2, 3, conjunction
(5)	$(\exists u)(\exists v)(0 = y \cdot u + v \wedge v < y)$	4, rule E4 twice
(6)	$y \neq 0 \to (\exists u)(\exists v)(0 = y \cdot u + v \wedge v < y)$	1-5, deduction theorem

ii.

(1)	$\phi(x)$, i.e., $y \neq 0 \to (\exists u)(\exists v)(x = y \cdot u + v \wedge v < y)$	Hyp
(2)	$y \neq 0$	Hyp
(3)	$(\exists u)(\exists v)(x = y \cdot u + v \wedge v < y)$	1, 2, MP
(4)	$x = y \cdot a + b \wedge b < y$	3, rule C twice
(5)	$b < y$	4, conjunction elimination
(6)	$b' \leqslant y$	5, Prop 2.1.9.
(7)	$b' < y \vee b' = y$	6, Definition

(8)	$b' < y \to (x' = y \cdot a + b' \wedge b' < y)$	4, (S4'), derived rules
(9)	$b' < y \to (\exists u)(\exists v)(x' = y \cdot u + v \wedge v < y)$	8, rule E4, deduction theorem
(10)	$b' = y \to x' = y \cdot a + y \cdot \overline{1}$	4, (S4'), Theorem[a] [a] In $\mathscr{S}$, $t \cdot \overline{1} = x$ is a theorem
(11)	$b' = y \to (x' = y \cdot (a + \overline{1}) + 0 \wedge 0 < y)$	10, Proposition 2.1.7, theorem, (S3')[a] [a] same as above
(12)	$b' = y \to (\exists u)(\exists v)(x' = y \cdot u + v \wedge v < y)$	11, rule E4 twice, deduction theorem
(13)	$(\exists u)(\exists v)(x' = y \cdot u + v \wedge v < y)$	7, 9, 12, disjunction elimination
(14)	$\phi(x) \to (y \neq 0 \to (\exists u)(\exists v)(x' = y \cdot u + v \wedge v < y))$, i.e., $\phi(x) \to \phi(x')$	1-13, deduction theorem

By (i.), (ii.), Gen and the induction rule, $\vdash_{\mathscr{S}} (\forall x)\phi(x)$. This establishes the existence of a quotient u and a reminder v. To prove uniqueness: assume $y \neq 0$. Assume $x = y \cdot u + v \wedge v < y$ and $x = y \cdot u_1 + v_1 \wedge v_1 < y$. Now: $u = u_1$ or $u < u_1$ or $u_1 < u$. If $u_1 = u$ then $v = v_1$ by Proposition 2.2.3. If now $u < u_1$, then $u_1 = u + w$ for some $w \neq 0$. Then $y \cdot u + v = y \cdot (u + w) + v_1 = y \cdot u + y \cdot w + v_1$. Hence, $v = y \cdot w + v_1$. Since $w \neq 0$, $y \cdot w \geqslant y$. So, $v = y \cdot w + v_1 \geqslant y$, contradicting $v < y$. Hence $\neg(u < u_1)$. Similarly $\neg(u_1 < u)$. Thus, $u = u_1$. Since $y \cdot u + v = x = y \cdot u_1 + v_1$, it follows that $v = v_1$ □

Now, we have defined Peano Arithmetic, but in order to simplify future proofs we may need a conservative extension of **PA** obtained by adding a symbol for every definition of primitive recursive function of **PA**

2.1.2 Representable, Primitive Recursive and Recursive Functions

Definition 2.1.14 (Representable functions)**.** Let $\mathscr{K}$ be a first order theory with equality in the language $\mathscr{L}_A$ (language of arithmetic). A number theoretic function f of n arguments is said to be *representable* in $\mathscr{K}$ if and only if there is a formula $\phi(x_1, ..., x_n, y)$ of $\mathscr{K}$ with free variables $x_1, ..., x_n, y$ such that, for any natural numbers $k_1, ..., k_n, m$, the following hold:

1. If $f(k_1, ..., k_n) = m$, then $\vdash_{\mathscr{K}} \phi(\overline{k_1}, ..., \overline{k_n}, \overline{m})$
2. $\vdash_{\mathscr{K}} (\exists! y)\phi(\overline{k_1}, ..., \overline{k_n}, y)$

Definition 2.1.15 (Strongly representable functions)**.** A representable number theoretic function is said to be *strongly representable* if the following holds:

2' $\vdash_{\mathscr{K}} (\exists! y)\phi(x_1,...,x_n,y)$

Remark 2.1.16. We can notice that strongly representability implies representability; in fact we can obtain the representability with generalization and $(\forall x)\psi(x) \vdash \psi(t)$ (t is free in ψ)

Proposition 2.1.17 (V.H. Dyson)**.** If $f(x_1,...,x_n)$ is representable in $\mathscr{K}$, then is strongly representable in $\mathscr{K}$

Proof. Assume f representable in $\mathscr{K}$ by a formula $\phi(x_1,...,x_n,y)$. Then f is strongly representable in $\mathscr{K}$ by the formula $\psi(x_1,...,x_n,y)$:

$$([(\exists! y)\phi(x_1,...,x_n,y)] \wedge \phi(x_1,...,x_n,y)) \vee (\neg[(\exists! y)\phi(x_1,...,x_n,y)] \wedge y = 0) \tag{2.10}$$

1. Assume $f(k_1,...,k_n) = m$. Then $\vdash_{\mathscr{K}} \phi(\overline{k_1},...,\overline{k_n},\overline{m})$ and $\vdash_{\mathscr{K}} (\exists! y)\phi(\overline{k_1},...,\overline{k_n},y)$. So, by conjunction introduction and disjunction introduction, we get

$$\vdash_{\mathscr{K}} \psi(\overline{k_1},...,\overline{k_n},\overline{m})$$

2' We must show that $\vdash_{\mathscr{K}} (\exists! y)\phi(x_1,...,x_n,y)$

Case 1. Take $(\exists! y)\phi(x_1,...,x_n,y)$ as hypothesis. (i) It is easy, using rule C, to obtain $\phi(x_1,...,x_n,b)$, where b is a new individual constant. Together with our hypothesis and conjunction and disjunction introduction, this yield $\psi(x_1,...,x_m,b)$ and then, by rule E4 $(\exists y)\psi(x_1,..,x_m,y)$. (ii) Assume $\psi(x_1,...,x_m,u) \wedge \psi(x_1,...,x_m,v)$. Now, from $\psi(x_1,...,x_m,u)$ and our hypothesis we obtain $\phi(x_1,...,x_m,u)$ and, in the same way, from $\psi(x_1,...,x_m,v)$ we obtain $\phi(x_1,...,x_m,v)$ and so, since f is representable, we get $u = v$. The deduction theorem yields $\psi(x_1,...,x_m,u) \wedge \psi(x_1,...,x_m,v) \to u = v$. Now, from (i) and (ii) $\exists! y)(\psi(x_1,...,x_m,y))$; thus we have proved

$$\vdash_{\mathscr{K}} (\exists! y)\phi(x_1,...,x_n,y) \to (\exists! y)\psi(x_1,...,x_n,y)$$

Case 2. Take $\neg(\exists! y)\phi(x_1,...,x_n,y)$ as hypothesis. (i) Our hypothesis, together with $0 = 0$ (which is a theorem in $\mathscr{K}$) yields, by conjunction introduction, $\neg(\exists! y)(\phi(x_1,..x_m,y) \wedge 0 = 0))$. By disjunction introduction, $\psi(x_1,...,x_n,0)$ and, by rule E4, $(\exists y)\psi(x_1,...,x_n,y)$. (ii) Assume $\psi(x_1,...,x_n,u) \wedge \psi(x_1,...,x_n,v)$; then from $\psi(x_1,...,x_n,u)$ and our hypothesis follows that $u = 0$ and so, from $\psi(x_1,...,x_n,v)$ follows $v = 0$. Hence $u = v$. By deduction theorem $\psi(x_1,..,x_n,u) \wedge \psi(x_1,...,x_n,v) \to u = v$. From (i) and (ii), $(\exists! y)(\psi(x_1,...,x_n,y))$. Thus, we have proved $\vdash_{\mathscr{K}} \neg(\exists! y)\phi(x_1,...,x_n,y) \to (\exists! y)\psi(x_1,...,x_n,y)$

Now, by case 1 and 2 and an instance of the tautology $[(\psi \to \psi) \wedge (\neg\psi \to \phi)] \to \psi$, we can obtain $\vdash_{\mathscr{K}} (\exists! y)\psi(x_1,...,x_n,y)$. Then f is a strongly representable functions. □

Remark 2.1.18. Since representable and strongly representable are equivalent we shall use only "representable function" to refers to both representable and strongly representable

Definition 2.1.19 (Initial Functions)**.** The following functions are called *initial functions*

I. The *zero function*, $Z(x) = 0$ for all x

II. The *successor function*, $N(x) = x + 1$ for all x

III. The *projection functions*, $U_i^n(x_1, ..., x_n) = x_i$ for all $x_1, ..., x_n$

Definition 2.1.20. From the initial functions we can obtain new functions by:

i. *Substitution:* if $f(x_1, .., x_n) = g(h(x_1, ..., x_n), ..., h_m(x_1, ..., x_n))$ then f is said to be obtained by substitution from the function

$$g(y_1, ..., y_m), h_1(x_1, ..., x_n), ..., h_m(x_1, ..., x_n)$$

ii. *Recursion:*

$$f(x_1, ..., x_n, 0) = g(x_1, ..., x_n)$$
$$f(x_1, ..., x_n, y + 1) = h(x_1, ..., x_n, y, f(x_1, ..., x_n, y)$$

Here, we allow $n = 0$, in which case we have $f(0) = k$ where k is a fixed natural number.

$$f(y + 1) = h(y, f(y)$$

We shall say that f is obtained from g and h (in the case in which $n = 0$ just h alone) by recursion. The *parameters* of recursion are $x_1, ..., x_n$. Notice that f is well defined: $f(x_1, ..., x_n, 0)$ is given by the first equation, and if we already know $f(x_1, ..., x_n, y)$ then we can obtain $f(x_1, ..., x_n, y + 1)$ by the second equation.

Definition 2.1.21 (Primitive Recursive Function)**.** A function f is said to be *primitive recursive* if and only if it can be obtained from the initial functions by any finite number of substitutions (i.) and recursions (ii.) - that is, if there is a finite sequence of functions $f_0, ..., f_n$ such that $f_n = f$ and for $0 \leqslant i \leqslant n$, either f_i is an initial function or f_i comes from the preceding functions in the sequence by an application of rules (i.) or (ii.)

We shall show that the class of recursive functions is identical with the class of representable functions $\mathscr{S}$

Remark 2.1.22. The initial functions are representable

Proof.

1. The zero function, $Z(x) = 0$, is representable in $\mathscr{K}$ by the formula formula $x_1 = x_1 \wedge y = 0$. For any k and m, if $Z(k) = m$, then $m = 0$ and $\vdash_{\mathscr{K}} \overline{k} = \overline{k} \wedge 0 = 0$; that is, condition 1 (in definition 2.1.14) holds. Also it is easy to show that $\vdash_{\mathscr{K}}$ $(\exists! y)(x_1 = x_1 \wedge y = 0)$. Thus, condition 2' (in definition 2.1.15) holds; so zero function is representable.

2. The successor function $N(x) = x + 1$, is representable in $\mathscr{K}$ by the formula formula $y = x_1'$. For any k and m, if $N(k) = m$ then $m = k + 1$; hence, $\overline{m}$ is $\overline{k}'$. Then $\vdash_{\mathscr{K}}$ $\overline{m} = \overline{k}'$. It is easy to verify $\vdash_{\mathscr{K}}$ $(\exists! y)(y = x_1')$. Then successor function is representable.

3. The projection function $U_j^n(x_1, ..., x_n) = x_j$ is representable in $\mathscr{K}$ by $x_1 = x_1 \wedge x_2 = x_2 \wedge ... \wedge x_n = x_n \wedge y = x_j$. If $U_j^n(k_1, ..., k_n) = m$, then $k_j = m$. Hence $\vdash_{\mathscr{K}} \overline{k_1} = \overline{k_1} \wedge ... \wedge \overline{k_n} = \overline{k_n} \wedge \overline{k_j} = \overline{m}$. Thus, condition 1 (in definition 2.1.14) holds. Also, $\vdash_{\mathscr{K}} (\exists! y)(x_1 = x_2 \wedge ... \wedge x_n = x_n \wedge x_j = y)$, that is, the condition 2' (in definition 2.1.15) holds. Thus, projector functions are representable

□

Remark 2.1.23. Functions obtained by substitution on representable functions are representable

Proof. Assume that the functions $g(x_1, ..., x_m), h_1(x_1, ..., x_n), ..., h_m(x_1, ..., x_n)$ are representable in the theory with equality $\mathscr{K}$ by the formulas

$$\phi(x_1, ..., x_m, z), \psi_1(x_1 ..., x_n, y_1), ..., \psi_m(x_1, ..., x_n, y_m)$$

Define f by substitution:

$$f(x_1, ..., x_n) = g(h_1(x_1, ..., x_n), ..., h_m(x_1, ..., x_n))$$

Then f is strongly representable by formula $\xi(x_1, ..., x_n, z)$:

$$(\exists y_1)...(\exists y_m)(\psi_1(x_1, ..., x_n, y_1) \wedge ... \wedge \psi_m(x_1, ..., x_n, y_m) \wedge \phi(x_1, ..., x_m, z))$$

To prove condition 1 (in definition 2.1.14), let $f(k_1, ..., k_n) = p$. Let $h_j(k_i, ..., k_n) = r_j$ for $1 \leqslant j \leqslant m$; then $g(r_1, ..., r_m) = p$. Since $\phi, \psi_1, ..., \psi_m$ represent $g, h_1, ..., h_m$, we have $\vdash_{\mathscr{K}} \psi_j(\overline{k_1}, ..., \overline{k_n}, \overline{r_j})$ for $1 \leqslant j \leqslant m$, and $\vdash_{\mathscr{K}} \phi(\overline{r_1}, ..., \overline{r_m}, \overline{p})$. So, by conjunction introduction, $\vdash_{\mathscr{K}} \psi_1(\overline{k_1}, ..., \overline{k_n}, \overline{r_1}) \wedge ... \wedge \psi_m(\overline{k_1}, ..., \overline{k_n}, \overline{r_m}) \wedge \phi(\overline{r_1}, ..., \overline{r_m}, \overline{p})$. Hence, by rule E4, $\vdash_{\mathscr{K}} \xi(\overline{k_1}, ..., \overline{k_n}, \overline{p})$. Thus, condition 1 holds. Now we shall prove the condition 2' (in definition 2.1.15). Assume $\xi(x_1, ..., x_n, u) \wedge \xi(x_1, ..., x_n, v)$, that is

$$(\exists y_1)...(\exists y_m)(\psi_1(x_1, ..., x_n, y_1) \wedge ... \wedge \psi_m(x_1, ..., x_n, y_m) \wedge \phi(x_1, ..., x_m, u)) \tag{2.11}$$

and

$$(\exists y_1)...(\exists y_m)(\psi_1(x_1, ..., x_n, y_1) \wedge ... \wedge \psi_m(x_1, ..., x_n, y_m) \wedge \phi(x_1, ..., x_m, v)) \tag{2.12}$$

By remark 2.11, using rule C m times:

$$\psi_1(x_1, ..., x_n, b_1) \wedge ... \wedge \psi_m(x_1, ..., x_n, b_m) \wedge \phi(b_1, ..., b_m, u) \tag{2.13}$$

By remark 2.12, using rule C again:

$$\psi_1(x_1, ..., x_n, c_1) \wedge ... \wedge \psi_m(x_1, ..., x_n, c_m) \wedge \phi(c_1, ..., c_m, v) \tag{2.14}$$

Since $\vdash_{\mathscr{K}} (\exists! y)\psi_j(x_1, ..., x_n, y_j)$ we obtain from $\psi_j(x_1, ..., x_n, b_j)$ and $\psi_j(x_1, ..., x_n, c_j)$ that $b_j = c_j$. From $\phi(b_1, ..., b_m, u)$ and $b_1 = c_1, ..., b_m = c_m$ we have $\phi(c_1, ..., c_m, u)$; this, with $\vdash_{\mathscr{K}} (\exists! y)(\phi(x_1, ..., x_m, z))$ and $\phi(c_1, ..., c_m, v)$, yields $u = v$. Thus, we have shown $\vdash_{\mathscr{K}} \xi(x_1, ..., x_n, u) \wedge \xi(x_1, ..., x_n, v) \rightarrow u = v$. Now, it is easy to prove that $\vdash_{\mathscr{K}} (\exists z)\xi(x_1, ..., x_n, z)$. Hence, $\vdash_{\mathscr{K}} (\exists! z)\xi(x_1, ..., x_n, z)$. So condition 2' (in definition 2.1.15) is proven, and then f is representable. □

Proposition 2.1.24. Let $g(y_1, ..., y_n)$ be primitive recursive. Let $x_1, ..., x_n$ be distinct variables and, for $1 \leqslant i \leqslant k$, let z_i be one of $x_1, ..., x_n$. The the function f such that $f(x_1, ..., x_n) = g(z_1, ..., z_k)$ is primitive recursive (or recursive)

Proof. Let $z_i = x_{j_i}$, where $1 \leqslant j_i \leqslant n$. Then $z_i = U^n_{j_i}(x_1, ..., x_n)$. Thus,

$$f(x_1, ..., x_n) = g(U^n_{j_1}(x_1, ..., x_n), ..., U^n_{j_k}(x_1, ..., x_n))$$

and therefore f is a primitive recursive (or recursive), since it arise from $g, U^n_{j_1}, ..., U^n_{j_k}$ by substitution. □

Corollary 2.1.25.

a. The zero function $Z_n(x_1, ..., x_n) = 0$ is primitive recursive

b. The constant function $C^n_k(x_1, ..., x_n) = k$, where k is a fixed natural number, is primitive recursive

c. The substitution rule can be extended to the case where each h_i may be a function of some but not not necessarily all of the variables. Likewise, in the recursione rule, the function g may not involve all the variables $x_1, ..., x_n, y$ or $f(x_1, ..., x_n, y)$ and h may not involve all of the variables $x_1, ..., x_n, y$, or $f(x_1, ..., x_n, y)$

Proof.

a. In Proposition 2.2.2, let g be the zero function Z; then $k = 1$. Take z_1 to be x_1

b. Use mathematical induction. For $k = 0$, this is part (a). Assume C^n_k primitive recursive. Then $C^n_{k+1}(x_1, ..., x_n)$ is primitive recursive by the substitution $C^n_{k+1}(x_1, ..., x_n) = N(C^n_k(x_1, ..., x_n))$

c. By Proposition 2.2.2, any possible variables among $x_1, ..., x_n$ not involved in a function can be added as dummy variables. For examples, if $h(x_1, x_3)$ is primitive recursive, then $h^*(x_1, x_2, x_3) = h(x_1, x_2) = h(U^3_1(x_1, x_2, x_3), U^3_3(x_1, x_2, x_3))$ is also primitive recursive since it is obtained by a substitution.

□

Proposition 2.1.26. The following functions are primitive recursive:

a. $x + y$

b. $x \cdot y$

c. x^y

d. $\delta(x) = \begin{cases} x - 1 & \text{if } x > 0 \\ 0 & \text{if } x = 0 \end{cases}$
δ is called predecessor function

e. $x \dot{-} y = \begin{cases} x - y & \text{if } x \geqslant y \\ 0 & \text{if } x < 0 \end{cases}$

f. $|x - y| = \begin{cases} x - y & \text{if } x \geqslant y \\ y - x & \text{if } x < y \end{cases}$

g. $sg(x) = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{if } x \neq 0 \end{cases}$

h. $\overline{sg}(x) = \begin{cases} 1 & \text{if } x = 0 \\ 0 & \text{if } x \neq 0 \end{cases}$

i. $x!$

j. $min(x, y)$ = minimum of x and y

k. $min(x_1, ..., x_n)$

l. $max(x, y)$ = maximum of x and

m. $max(x_1, ..., x_n)$

n. $rm(x, y)$ = remainder upon division of y by x

o. $qt(x, y)$ = quotient upon division of y by

p. $f(x, y) = rm(qt(y, 2^x), 2)$

Proof.

a. Apply recursion rule: $x + 0 = 0$ or $f(x, 0) = U_1^1(x)$ and $x + (y + 1) = N(x + y)$ or $f(x, y + 1) = N(f(x, y))$[4]

b. Using (a): $x \cdot 0 = 0$ or $g(x, 0) = Z(x)$ and $x \cdot (y + 1) = (x \cdot y) + x$ or $g(x, y + 1) = f(g(x, y), x)$

c. $x^0 = 1$, $x^{(y+1)} = (x^y) \cdot (x)$[5]

d. $\delta(0) = 0$, $\delta(y + 1) = y$

e. $x \dot{-} 0 = x$, $x \dot{-} (y + 1) = \delta(x \dot{-} y)$

f. $|x - y| = (x \dot{-} y) + (y \dot{-} x)$ (substitution)

g. $sg(x) = x \dot{-} \delta(x)$ (substitution)

h. $\overline{sg}(x) = 1 \dot{-} sg(x)$

[4] since we are working in $\mathscr{S}$, every nonzero element can be expressed as successor of another element
[5] since now we will imply functional notation

i. $0! = 1$, $(y+1)! = (y+1) \cdot (y!)$

j. $min(x, y) = x \dot{-} (x \dot{-} y)$

k. Assume $min(x_1, ..., x_n, x_{n+1})$ already shown primitive recursive, then:

$$min(x_1, ..., x_{n+1}) = min(min(x_1, ...x_n), x_{n+1})$$

l. $max(x, y) = y + (x \dot{-} y)$

m. As in (k): $max(x_1, ..., x_{n+1}) = max(max(x_1, ..., x_n), x_{n+1})$

n. $rm(x, 0) = 0$, $rm(x, y+1) = N(rm(x, y)) \cdot sg(|x - N(rm(x, y))|)$

o. $qt(x, 0) = 0$, $qt(x, y+1) = qt(x, y) + \overline{sg}(|x - N(rm(x, y))|)$

p. $f(x, y)$ is obtained by substitution over remainder and exponentiation, that are primitive recursive functions

To justify (n) and (o): if q and r are the quotient and the reminder upon the division of y by x, then $y = qx + r$, and $0 \leqslant r < x$. So, $y + 1 = qx + (r + 1)$. If $r + 1 < x$ (that is $|x - N(rm(x, y))| > 0$) then the quotient and the reminder upon the division of $y + 1$ by x are q and $r + 1$. If $r + 1 = x$ (that is $|x - N(rm(x, y))| = 0$) then $y + 1 = (q + 1)x$ and quotient and reminder are $q + 1$ and 0 □

Definition 2.1.27. Now we can define a primitive recursive relation that will be fundamental for our discussion. We say that $x \Subset y$ iff $rm(qt(y, 2^x), 2) = 1$.

Remark 2.1.28. $x \Subset y$ is a primitive recursive relation since $rm(qt(y, 2^x), 2)$ is a primitive recursive function

Lemma 2.1.29 (Gödel's β-Function)**.** Let $\beta(x_1, x_2, x_3) = rm(1 + (x_3 + 1) \cdot x_2, x_1)$. Then β is primitive recursive, by proposition 2.1.26. Also, β is strongly representable in $\mathscr{S}$ by the following formula formula $Bt(x_1, x_2, x_3, y)$:

$$(\exists w)((x_1 = (1 + (x_3 + 1) \cdot x_2) \cdot w + y) \wedge (y < 1 + (x_3 + 1) \cdot x_2)) \tag{2.15}$$

Proof. By Proposition 2.1.13 $\vdash_{\mathscr{S}} (\exists! y)Bt(x_1, x_2, x_3, y)$. Assume $\beta(k_1, k_2, k_3) = m$. Then $k_1 = (1 + (k_3 + 1) \cdot k_2) \cdot k + m$ for some k, and $m < 1 + (k_3 + 1) \cdot k_2$. So, $\vdash_{\mathscr{S}} \overline{k_1} = (\overline{1} + (\overline{k_3} + \overline{1}) \cdot \overline{k_2}) \cdot \overline{k} + \overline{m}$ by numerals property. Moreover, $\vdash_{\mathscr{S}} \overline{m} < \overline{1} + (\overline{k_3} + \overline{1}) \cdot \overline{k_2}$ by expressibility of $<$ and numerals property. Hence, $\vdash_{\mathscr{S}} \overline{k_1} = (\overline{1} + (\overline{k_3} + \overline{1}) \cdot \overline{k_2}) \cdot \overline{k} + \overline{m} \wedge \overline{m} < \overline{1} + (\overline{k_3} + \overline{1}) \cdot \overline{k_2}$ from which, by rule E4, $\vdash_{\mathscr{S}} Bt(\overline{k_1}, \overline{k_2}, \overline{k_3}, \overline{m})$. Thus, by Bt, β is strongly representable in $\mathscr{S}$ □

Lemma 2.1.30. For any sequence of natural number $k_0, k_1, ..., k_n$, there exist natural numbers b and c such that $\beta(b, c, i) = k_i$ for $0 \leqslant i \leqslant n$

Proof. Let $j = max(n, k_1, .., k_n)$ and let $c = j!$. Consider the numbers $u_i = 1 + (i+1)c$ for $0 \leqslant i \leqslant n$; no two of them have a factor in common other than 1. In fact, if p where a prime dividing both $1 + (i+1)c$ and $1 + (m+1)c$ with $0 \leqslant i < m \leqslant n$, then p would divide their difference $(m - i)c$. Now, p does not divide c, since, in that case p would divide both $(i+1)c$ and $1+(i+1)c$, and so would divide 1, which is impossible. Hence, p also does divide $(m-i)$; for $m-i \leqslant n \leqslant j$ and so, $m-i$ divides $j! = c$. If p divided $m-i$, then p would divide c. Therefore, p does not divide $(m-i)c$ which yields a contradiction. Thus, the numbers u_i, $0 \leqslant i \leqslant n$, are relatively prime in pairs. Also, for $0 \leqslant i \leqslant n$, $k_i \leqslant j \leqslant j! = c < 1 + (i+1)c = u_i$; that is, $k_i < u_i$. Now, by the Chinese remainder theorem, there is a number $b < u_0 u_1 ... u_n$ such that $rm(u_i, b) = k_i$ for $0 \leqslant i \leqslant n$. But $\beta(b, c, i) = rm(1 + (i+1)c, b) = rm(u_i, b) = k_i$. □

The lemmas 2.1.29 and 2.1.30 allows us to express in $\mathscr{S}$ assertion about finite sequences of natural numbers, and this is crucial to to prove the representability of recursive functions

Proposition 2.1.31. Every primitive recursive function in $\mathscr{S}$ is representable in $\mathscr{S}$.

Proof. The initial functions Z, N and U^i_n are representable in $\mathscr{S}$, by remark 2.1.22. The substitution rule does not lead out of the class of representable function, by remark 2.1.23. For the recursion rule, assume that $g(x_1, ..., x_n)$ and $h(x_1, ..., x_n, y, z)$ are representable in $\mathscr{S}$ by formula $\phi(x_1, .., x_{n+1})$ and $\psi(x_1, ..., x_{n+3})$, respectively, and let

$$f(x_1, ..., x_n, 0) = g(x_1, ..., x_n) \tag{2.16}$$

$$f(x_1, ..., x_n, y+1) = h(x_1, ..., x_n, y, f(x_1, ..., x_n, y)) \tag{2.17}$$

Now, $f(x_1, ..., x_n, y) = z$ if and only if there is a finite sequence of numbers $b_0, ..., b_y$, such that $b_0 = g(x_1, ..., x_n)$, $b_{w+1} = h(x_1, ..., x_n, w, b_w)$ for $w + 1 \leqslant y$, and $b_y = z$. But, by lemma 2.1.30, reference to finite sequences can be formulated in therms of the function β and, by lemma 2.1.29, β is representable in $\mathscr{S}$ by the formula $Bt(x_1, x_2, x_3, y)$. We now shall show that $f(x_1, ..., x_n, x_{n+1})$ is representable in $\mathscr{S}$ by the formula $\xi(x_1, ..., x_{n+2})$:

$$\begin{aligned}&(\exists u)(\exists v)[((\exists w)(Bt(u, v, 0, w) \wedge \phi(x_1, ..., x_n, w))) \wedge Bt(u, v, x_{n+1}, x_{n+2})\\ &\wedge (\forall w)(w < x_{n+1} \rightarrow (\exists y)(\exists z)(Bt(u, v, w, y) \wedge Bt(u, v, w', z) \wedge \psi(x_1, ..., x_n, w, y, z)))]\end{aligned} \tag{2.18}$$

i. First, assume that $f(x_1, ..., x_n, p) = m$. We wish to show that $\vdash_{\mathscr{S}} \xi(\overline{k_1}, ..., \overline{k_n}, \overline{p}, \overline{m})$. If $p = 0$, then $m = g(k_1, ..., k_n)$. Consider the sequence consisting of m alone. By lemma 2.1.30, there exist b and c such that $\beta(b, c, 0) = m$. Hence, by lemma 2.1.29:

$$\vdash_{\mathscr{S}} Bt(\overline{b}, \overline{c}, 0, \overline{m}) \tag{2.19}$$

Also, since $m = g(k_1, ..., k_n)$, we have $\vdash_{\mathscr{S}} \phi(\overline{k_1}, ..., \overline{k_n}, \overline{m})$. Hence, by rule E4,

$$\vdash_{\mathscr{S}} (\exists w)(Bt(\overline{b}, \overline{c}, 0, w) \wedge \phi(\overline{k_1}, ..., \overline{k_n}, w)) \tag{2.20}$$

In addition, since $\vdash_{\mathscr{S}} \neg(w < 0)$, a tautology and Gen yield

$$(\forall w)(w < 0 \rightarrow (\exists y)(\exists z)(Bt((\overline{b}, \overline{c}, w, y) \\ \wedge (Bt(\overline{b}, \overline{c}, w', z) \wedge \psi(\overline{k_1}, ..., \overline{k_n}, w, y, z)))) \tag{2.21}$$

Applying rule E4 to conjunction of 2.38, 2.39, 2.40, we obtain $\vdash_{\mathscr{S}} \xi(\overline{k_1}, ..., \overline{k_n}, 0, \overline{m})$. Now, for $p > 0$, $f(k_1, ..., k_n, p)$ is calculated from the equation 2.36 in $p + 1$ steps. Let $r_i = f(k_1, ..., k_n, i)$. For the sequence of numbers $r_0, r_1, ..., r_p$, there are, by lemma 2.1.29, numbers b, and c such that $\beta(b, c, i) = r_i$ for $0 \leqslant i \leqslant p$. Hence, by Lemma 2.1.30, $\vdash_{\mathscr{S}} Bt(\overline{b}, \overline{c}, \overline{i}, \overline{r_i})$. In particular, $\beta(b, c, 0) = r_0 = f(k_1, ..., k_n, 0) = g(k_1, ..., k_n)$. Therefore, $\vdash_{\mathscr{S}} Bt(\overline{b}, \overline{c}, 0, \overline{r_0}) \wedge \phi(\overline{k_1}, ..., \overline{k_n}, \overline{r_0})$, and, by rule E4,

$$\text{(i)} \vdash_{\mathscr{S}} (\exists w)(Bt(\overline{b}, \overline{c}, 0, y) \wedge \phi(\overline{k_1}, ..., \overline{k_n}, w))$$

Since $r_p = f(k_1, ..., k_n, p) = m$, we have $\beta(b, c, p) = m$. Hence,

$$\text{(ii)} \vdash_{\mathscr{S}} Bt(\overline{b}, \overline{c}, \overline{p}, \overline{m}).$$

For $0 \wedge i \wedge p - 1$, $\beta(b, c, i) = r_i = f(k_i, ..., k_n, i)$ and

$$\beta(b, c, i + 1) = r_{i+1} = f(k_1, ..., k_n, i + 1) = \\ h(k_1, ...k_n, i, f(k_1, ..., k_n, i)) = h(k_1, ..., k_n, i, r_i)$$

Therefore, $\vdash_{\mathscr{S}} Bt(\overline{b}, \overline{c}, \overline{i}, \overline{r_i}) \wedge Bt(\overline{b}, \overline{c}, \overline{i'}, \overline{i+1}) \wedge \psi(\overline{k_1}, ..., \overline{k_n}, \overline{i}, \overline{r_i}, \overline{r_{i+1}})$. By rule E4, $\vdash_{\mathscr{S}} (\exists y)(\exists z)(Bt(\overline{b}, \overline{c}, \overline{i}, y) \wedge Bt(\overline{b}, \overline{c}, \overline{i'}, z) \wedge \psi(\overline{k_1}, ..., \overline{k_n}, \overline{i}, y, z))$. So, by Proposition 2.1.11,

$$\text{(iii)} \vdash_{\mathscr{S}} (\forall w)(w < \overline{p} \rightarrow (\exists y)(\exists z)(Bt(\overline{b}, \overline{c}, w, y) \wedge Bt(\overline{b}, \overline{c}, w', z) \wedge \psi(\overline{k_1}, ..., \overline{k_n}, w, y, z))).$$

Then applying rule E4 twice to the conjunction of (i), (ii) and (iii), we obtain $\vdash_{\mathscr{S}} \xi(\overline{k_1}, ..., \overline{k_n}, \overline{p}, \overline{m})$. Thus, we have verified condition 1 in definition 2.1.14

ii. We must show that $\vdash_{\mathscr{S}} (\exists! x_{n+2})\xi(\overline{k_1}, \overline{k_n}, \overline{p}, x_{n+2})$. The proof is by induction of p in the metalanguage. Notice that, by what we have proved above, it suffices to prove only uniqueness.
The case of $p = 0$ is trivial. Assume $\vdash_{\mathscr{S}} (\exists! x_{n+2})\xi(\overline{k_1}, ..., \overline{k_n}, \overline{p}, x_{n+2})$. Let $\alpha = g(k_1, ..., k_n)$, $\beta = f(k_1, ..., k_n, p)$, and $\gamma = f(k_1, ..., k_n, p + 1) = h(k_1, ..., k_n, p, \beta)$. Then

1. $\vdash_{\mathscr{S}} \psi(\overline{k_1}, ..., \overline{k_n}, \overline{p}, \overline{\beta}, \overline{\gamma})$
2. $\vdash_{\mathscr{S}} \phi(\overline{k_1}, ..., \overline{k_n}, \overline{\alpha})$
3. $\vdash_{\mathscr{S}} \xi(\overline{k_1}, ..., \overline{k_n}, \overline{p}, \overline{\beta})$
4. $\vdash_{\mathscr{S}} \xi(\overline{k_1}, ..., \overline{k_n}, \overline{p+1}, \overline{\gamma})$
5. $\vdash_{\mathscr{S}} (\exists! x_{n+2})\xi(\overline{k_1}, ..., \overline{k_n}, \overline{p}, x_{n+2})$

Now, assume

$$\xi(\overline{k_1}, ..., \overline{k_n}, \overline{p+1}, x_{n+2}) \tag{2.22}$$

We must prove $x_{n+2} = \overline{\gamma}$. From 2.41, by rule C,

a. $(\exists w)(Bt(b, c, 0, w) \wedge \phi(\overline{k_1}, ..., \overline{k_n}, w))$
b. $Bt(b, c, \overline{p+1}, x_{n+2})$
c. $(\forall w)(w < \overline{p+1} \rightarrow (\exists y)(\exists z)(Bt(b, c, w, y) \wedge Bt(b, c, w', z) \wedge \psi(\overline{k_1}, ..., \overline{k_n}, w, y, z)))$
d. From (c): $(\forall w)(w < \overline{p} \rightarrow (\exists y)(\exists z)(Bt(b, c, w, y) \wedge Bt(b, c, w', z) \wedge \psi(\overline{k_1}, ..., \overline{k_n}, w, y, z)))$
e. From (c) by rule A4 and rule C:

$$Bt(b, c, \overline{p}, d) \wedge Bt(b, c, \overline{p+1}, e) \wedge \psi(\overline{k_1}, ..., \overline{k_n}, \overline{p}, d, e)$$

f. From (a), (d), and (e): $\xi(\overline{k_1}, ..., \overline{k_n}, \overline{p}, d)$
g. From (f), (5) and (3): $d = \overline{\beta}$
h. From (e) and (g), $\psi(\overline{k_1}, ..., \overline{k_n}, \overline{\beta}, e)$
i. Since β represents h, we obtain from (1) and (h): $\overline{\gamma} = e$
j. From (e) and (i): $Bt(b, c, \overline{p+1}, \overline{\gamma})$
k. From (b), (j) and Lemma 2.1.29: $x_{n+2} = \overline{\gamma}$

This concludes the induction.

□

2.1.3 Extended Peano Arithmetic Theory

Ackermann encoding translates the membership relation into a primitive recursive relation based on binary expansion in **PA**. Therefore we will need an extension of **PA** that has a symbol for each definition of recursive primitive function, and which therefore can internalize the translation of the set-theoretic membership relation via Ackermann encoding. This subsection will be dedicated to define this conservative extension, namely *Extended Peano Arithmetic* (**PA'**), and to prove that **PA** and **PA'** are equiconsistent

Definition 2.1.32. Let $\mathcal{L}_A$ be the language of arithmetic (definition 2.1.1), then let $\mathcal{L'}_A$ be the language obtained adding to $\mathcal{L}_A$ a functional symbol f_i^n for every definition of primitive recursive function f on $\mathscr{S}$[6]

Definition 2.1.33. Let $\mathcal{L'}_A$ be the language in definition 2.1.32, then we can define a first order theory $\mathscr{T}$ over $\mathcal{L'}_A$ with the same logical axioms of $\mathscr{S}$ and, for proper axioms:

[6]Since the classes of recursive and representable functions are the same we can notice that we are adding at least $\aleph_0$ new symbols

- The same axioms of $\mathscr{S}$, as well as every instance of them involving terms of the extended language, and:
- Let f be a symbol for a definition of a primitive recursive function of arity n in $\mathscr{S}$ with $\phi_i(x_1, ..., x_n, y)$ the formula that represents f in $\mathscr{S}$, where ϕ_i is constructed as in the proof of Proposition 2.1.31[7]. Now, let f_i^n be the functional symbol corresponding to the definition of f. Then, for f_i^n we shall add the proper axiom:

$$\forall x_1, ..., \forall x_n \phi_i(x_1, ..., x_n, f_i^n(x_1, ..., x_n)) \tag{2.23}$$

The theory $\mathscr{T}$ is called *Extended Peano Arithmetic*

Proposition 2.1.34. Let f be a primitive recursive function defined by recursion over g, h and let ϕ the formula that represent f according to proposition 2.1.31. Let ϕ_1, ϕ_2 the formulas that represent respectively g and h, then the following hold:

$$\vdash_{\mathscr{S}} \phi(x_1, ..., x_n, 0, h) \leftrightarrow \phi_1(x_1, ..., x_n, h)$$
$$\vdash_{\mathscr{S}} \phi(x_1, ..., x_n, y+1, h) \leftrightarrow \exists z(\phi_2(x_1, ..., x_n, y, h_1, h) \wedge \phi(x_1, ..., x_n, y, z))$$

where h_1 is such $\phi(x_1, .., x_n, y, h_1)$

Proof. Let $\vdash_{\mathscr{S}} \phi(x_1, ..., 0, h)$. Then, since $\vdash_{\mathscr{S}} \forall w \neg(w < 0)$

$$\phi(x_1, ..., 0, h) \vdash_{\mathscr{S}} \exists u \exists v(\exists w(Bt(u, v, 0, w) \wedge \phi_1(x_1, ..., x_n, w)) \wedge Bt(u, v, 0, h))$$

Now, since $\vdash_{\mathscr{S}} \exists! y Bt(x_1, x_2, x_3, y)$, w and h must be equal. Thus:

$$\phi(x_1, ..., x_n, 0, h) \vdash_{\mathscr{S}} \phi_1(x_1, ..., x_n, h)$$

Now, let $\vdash_{\mathscr{S}} \phi_1(x_1, ..., x_n, h)$. Then, let $k_0 = h$ be a sequence of only one natural, then, by lemma 2.1.29:

$$(i) \quad \vdash_{\mathscr{S}} \exists u \exists v(Bt(\overline{u}, \overline{v}, 0, \overline{h}))$$

And, by Hypotheses:

$$(ii) \quad \phi_1(x_1, ..., x_n) \vdash_{\mathscr{S}} \exists u \exists v(Bt(\overline{u}, \overline{v}, 0, h) \wedge \phi_1(\overline{x_1}, ..., \overline{x_n}, h))$$

Then, since $\vdash_{\mathscr{S}} \forall w \neg(w < 0)$, by a tautology and Gen:

$$(iii) \quad \forall w(w < 0 \to (\exists y)(\exists z)(Bt(\overline{b}, \overline{c}, w, y)) \wedge (Bt(\overline{b}, \overline{c}, w', z) \wedge \phi_2(\overline{k_1}, ..., \overline{k_n}, w, y, z)))$$

Applying rule C on (ii) and E4 twice to the conjunction of (i), (ii) and (iii), we obtain $\phi(x_1, ..., x_n) \vdash_{\mathscr{S}} \phi(x_1, ..., x_n)$. Thus $\vdash_{\mathscr{S}} \phi(x_1, ..., x_n, 0, h) \leftrightarrow \phi_1(x_1, ..., x_n, h)$

Now, we have to prove $\vdash_{\mathscr{S}} \phi(x_1, ..., x_n, y+1, h) \leftrightarrow \phi_2(x_1, ..., x_n, y, h_1, h)$.
Let $\vdash_{\mathscr{S}} \phi(x_1, ..., x_n, 0+1, h)$, then, by definition of ϕ in 2.1.31 the following holds:

$$(\exists u)(\exists v)[((\exists w)(Bt(u, v, 0, w) \wedge \phi_1(x_1, ..., x_n, w))) \wedge Bt(u, v, 1, h)$$
$$\wedge (\forall w)(w < 1 \to (\exists a)(\exists b)(Bt(u, v, w, a) \wedge Bt(u, v, w', b) \wedge \phi_2(x_1, .., x_n, a, b)))]$$

[7]Considering also the equivalence between representable and strongly representable functions

Then, we have that w in the last part of the sentence could be only 0, and in that case we would have

$$(\exists u)(\exists v)[((\exists m)(Bt(u,v,0,m) \wedge \phi_1(x_1,...,x_n,m))) \wedge Bt(u,v,1,h) \\ \wedge (0 < 1 \to (\exists a)(\exists b)(Bt(u,v,0,a) \wedge Bt(u,v,0+1,b) \wedge \phi_2(x_1,..,x_n,a,b)))]$$

from which, by $\vdash_{\mathscr{S}} \exists! y Bt(x_1,x_2,x_3,y)$, $a = m$ and $h = b$. Then, by property of the conjunction, $\phi(x_1,...,x_n,0+1,h) \vdash_{\mathscr{S}} \phi_1(x_1,...,x_n,m,h)$. Now, we can generalize this prove. Let $\vdash_{\mathscr{S}} \phi(x_1,...,x_n,y+1,h)$, then

$$(\exists u)(\exists v)[((\exists w)(Bt(u,v,0,w) \wedge \phi_1(x_1,...,x_n,w))) \wedge Bt(u,v,y+1,h) \\ \wedge (\forall w)(w < y+1 \to (\exists a)(\exists b)(Bt(u,v,w,a) \wedge Bt(u,v,w',b) \\ \wedge \phi_2(x_1,..,x_n,a,b)))]$$

We can define for every, $w < y+1$, a_w and b_w such as

$$(w < y+1 \to (\exists a)(\exists b)(Bt(u,v,w,a) \wedge Bt(u,v,w',b) \wedge \phi_2(a,b)))$$

Then, since Bt is representable, $a_i = b_{i-1}$, $a_0 = m$, $b_y = h$. Also, for all w, by conjunction proprieties $\phi \vdash_{\mathscr{S}} \phi_2(x_1,...,x_n,b_{w-1},b_w)$ in particular $\phi \vdash_{\mathscr{S}} \phi_2(x_1,...,x_n,b_{y-1},h)$.
In order to conclude the proof we can work as in proposition 2.1.31 to prove

$$\phi_1(x_1,...,x_n,b_{w+1},h) \vdash_{\mathscr{S}} \phi(x_1,...,x_n,y+1,h)$$

□

Remark 2.1.35. Let f^n be a functional symbol in $\mathcal{L}'_A$ defined in $\mathscr{T}$ by

$$\forall x_1,...,\forall x_n \phi_i(x_1,...,x_n,f_i^n(x_1,...,x_n))$$

then, if ϕ_i is defined as in proposition 2.1.31, that is, if it is defined by recursion in $\mathscr{S}$, the following hold:

$$\vdash_{\mathscr{T}} f(x_1,...,x_n,0) = g(x_1,...,x_n) \\ \vdash_{\mathscr{T}} f(x_1,...,x_n,y+1) = h(x_1,...,x_n,y,f(x_1,...,x_n,y))$$

where g and h are functional symbols defined by ϕ_1, ϕ_2 involved in ϕ_i

Proof. By proposition 2.1.34 the following hold

$$\vdash_{\mathscr{S}} \phi(x_1,...,x_n,0,h) \leftrightarrow \phi_1(x_1,...,x_n,h) \\ \vdash_{\mathscr{S}} \phi(x_1,...,x_n,y+1,h) \leftrightarrow \phi_2(x_1,...,x_n,y,h_1,h)$$

But, by proposition 1.3.6

$$\vdash_{\mathscr{T}} \phi(x_1,...,x_n,0,h) \leftrightarrow \phi_1(x_1,...,x_n,h) \\ \vdash_{\mathscr{T}} \phi(x_1,...,x_n,y+1,h) \leftrightarrow \phi_2(x_1,...,x_n,y,h_1,h)$$

But we have as proper axioms

$$\forall x_1, ..., \forall x_n \phi_i(x_1, ..., x_n, f(x_1, ..., x_n))$$
$$\forall x_1, ..., \forall x_n \phi_1(x_1, ..., x_n, g(x_1, ..., x_n))$$
$$\forall x_1, ..., \forall x_n \phi_2(x_1, ..., x_n, h(x_1, ..., x_n))$$

Then

$$\vdash_{\mathscr{T}} f(x_1, ..., x_n, 0) = g(x_1, ..., x_n)$$
$$\vdash_{\mathscr{T}} f(x_1, ..., x_n, y+1) = h(x_1, ..., x_n, y, f(x_1, ..., x_n, y))$$

□

Lemma 2.1.36. The following are theorems of **PA'**:

$$\text{PA'} \vdash 2^0 = 1$$
$$\text{PA'} \vdash qt(b, 1) = b$$
$$\text{PA'} \vdash qt(2c, 2^{a+1}) = qt(c, 2^a)$$
$$\text{PA'} \vdash qt(2c+1, 2^{a+1}) = qt(c, 2^a)$$

Then, we have:

$$\text{PA'} \vdash (a+1) \equiv 2c \leftrightarrow a \equiv c$$
$$\text{PA'} \vdash (a+1) \equiv (2c+1) \leftrightarrow a \equiv c$$

Lemma 2.1.37. In **PA'** the following holds:

$$\text{PA'} \vdash b \leqslant a \to b < 2^a$$
$$\text{PA'} \vdash b < 2^a \to qt(b, 2^a) = 0$$

Thus,

$$\text{PA'} \vdash a \equiv b \to a < b$$

Proposition 2.1.38. The extended Peano arithmetic $\mathscr{T}$ is a conservative extension of Peano arithmetic $\mathscr{S}$

$$\mathscr{S} \lhd \mathscr{T} \tag{2.24}$$

Proof. By definition 2.1.32 $\mathcal{L}_A \subset \mathcal{L}'_A$. Let ϕ be a sentence in $\mathcal{L}_A$, that is, a sentence that does not contain any f_i^n. Then, by definition 2.1.32 $\vdash_{\mathscr{T}} \phi \Rightarrow \vdash_{\mathscr{S}} \phi$. Since every proper axiom of $\mathscr{S}$ is also a proper axioms of $\mathscr{T}$, then, if ϕ does not contain any f_i^n, $\vdash_{\mathscr{S}} \phi \Rightarrow \vdash_{\mathscr{T}} \phi$. Thus, $\mathscr{S} \lhd \mathscr{T}$ □

Remark 2.1.39. Since $\mathscr{T}$ is a conservative extension of $\mathscr{S}$, then

$$Cons(\mathscr{S}) \Rightarrow Cons(\mathscr{T}) \tag{2.25}$$

Theorem 2.1.40. $\mathscr{S}$ and $\mathscr{T}$ are equiconsistent

$$Cons(\mathscr{S}) \iff Cons(\mathscr{T}) \tag{2.26}$$

Proof. From Definition 1.2.6, since $\vdash_{\mathscr{S}} 0 \neq 1$ by (S1), $\mathscr{S}$ is inconsistent if and only if $\vdash_{\mathscr{S}} 0 = 1$. Now, since $0 = 1$ involves only terms of $\mathcal{L}_A$ and $\mathscr{S} \lhd \mathscr{T}$, then $\vdash_{\mathscr{S}} 0 = 1 \iff \vdash_{\mathscr{T}} 0 = 1$. Thus, $Incon(\mathscr{T}) \iff \vdash_{\mathscr{T}} 0 = 1$. This yields to $Incon(\mathscr{T}) \iff Incon(\mathscr{S})$, and then: $Cons(\mathscr{T}) \iff Cons(\mathscr{S})$

□

Remark 2.1.41. Since now we will use **PA** instead of $\mathscr{S}$ and **PA'** instead of $\mathscr{T}$

2.1.4 Primitive Recursive Aritithmetic

Primitive Recursive Arithmetic (**PRA**) is a finitistic formalization of the natural numbers, proposed by Skolem in 1923. It is weaker than **PA** since it does not have quantifier and can only formalize primitive recursive arguments. We will use **PRA** as meta-theoretic assumption to formalize our translations between **ZF-Inf** and **PA**, this means that our equiconsistency proof can be proved finistically

Definition 2.1.42. The language of **PRA** consists of

- A countably infinite number of variables
- The propositional connective
- A predicate letter A_1^2 also written as $=$, an individual constant 0, a functional symbol with arity 1 f_1^1 also written as $S()$ - successor function - and a functional symbol f_i^n for every definition of primitive recursive funciton

Definition 2.1.43. The logical axioms of **PRA** are:

- Tautologies of the propositional calculus
- Usual axioms of equality for " = "

The logical rules are the modus ponens and the variable substitution

Definition 2.1.44. The non logical axiom of **PRA** are:

- $S(x) \neq 0$
- $S(x) = S(y) \to x = y$

as well as every recursive definition of every primitive recursive function, that is:

- $f(x_1, ..., x_n, 0) = g(x_1, ..., x_n)$
- $f(x_1, ..., x_n, S(y)) = h(x_1, ..., x_n, y, f(x_1, ..., x_n, y))$

PRA replaces the axiom of induction with the rule of induction:

$$\frac{\phi(0) \qquad \phi(x) \to \phi(S(x))}{\phi(x)}$$

Remark 2.1.45. Lemmas 2.1.36 and 2.1.37 are still valid in **PRA**. Since $m \equiv n$ is a primitive recursive relation, then it is formalized in **PRA** as well as other primitive recursive functions and relations

2.2 Zermelo-Fraenkel Without Infinity Axiomatic Set Theory

In this section, we will define the axiomatic theory of sets by Zermelo-Fraenkel without the axiom of infinity. We will develop some results regarding ordinals, transfinite induction, and transfinite recursion with the aim of defining a conservative extension of **ZF-Inf**, denoted as $\mathbf{ZF}_{ord}$**-Inf**, which includes symbols for finite ordinals and their operations. We will conclude the section by elaborating on a theory equivalent to **ZF-Inf**, called **ZF'-Inf**, obtained by weakening the axioms of union and power and eliminating some non-independent axioms such as the axiom of empty set and pair.

2.2.1 Zermelo-Fraenkel Theory

Definition 2.2.1. Let $\mathcal{L}$ be a first order language with two predicate letters A_1^2 (in future we will write $a = b$ instead of $A_1^2(a, b)$) and A_2^2 (we will write $a \in b$ instead of $A_2^2(a, b)$). $\mathcal{L}$ is the *language of ZF*

Definition 2.2.2 (ZF)**.** Let $\mathcal{L}$ be the first order language in definition 2.2.1. Then the *Zermelo Fraenkel theory*, **ZF**, is the first order theory over $\mathcal{L}$ with equality (in which A_1^2 is the equality), with the following proper axioms

ZF 1. Extensionality.

$$\forall z(z \in x \leftrightarrow z \in y) \to x = y \tag{2.27}$$

ZF 2. Empty Set.

$$\exists x \forall y(y \notin x) \tag{2.28}$$

ZF 3. Foundation.

$$\exists y(y \in x) \to \exists y(y \in x \wedge \neg \exists z(z \in x \wedge z \in y)) \tag{2.29}$$

ZF 4. Paring.

$$\forall x \forall y \exists z(w \in z \leftrightarrow (w = x \vee w = y)) \tag{2.30}$$

ZF 5. Union.

$$\forall x \exists y \forall z(z \in y \leftrightarrow \exists v \in x \wedge z \in v) \tag{2.31}$$

ZF 6. Power Set.

$$\forall z \exists y(\forall w(w \in z \to w \in x) \leftrightarrow z \in y) \tag{2.32}$$

ZF 7. Separation Scheme. For each formula ϕ without y free,

$$\forall x \exists y \forall z (z \in y \leftrightarrow z \in x \wedge \phi(z)) \tag{2.33}$$

ZF 8. Replacement Scheme. Let φ be a formula formula of $\mathcal{L}$

$$\forall x \exists! y \varphi(x,y) \rightarrow \forall a \exists b \forall y (y \in b \leftrightarrow \exists x \in a \varphi(x,y)) \tag{2.34}$$

ZF 9. Infinity.

$$\exists x (\exists u (u \in x \wedge (\forall v (v \notin u))) \wedge \forall z (z \in x \rightarrow \exists y (y \in x \wedge \forall w (w \in y \leftrightarrow (w \in z \vee w = z))))) \tag{2.35}$$

Remark 2.2.3. From now we will use $\subseteq$, $\subset$, $\mathcal{P}(x)$ and $\varnothing$ with the usual meaning

Definition 2.2.4 (ZFC)**.** We can define **ZFC** as **ZF** with the addition of **axiom of choice**

$$x \neq 0 \wedge a \subseteq \mathcal{P}(x) \backslash \varnothing \wedge a \neq \varnothing \rightarrow \exists c : a \rightarrow x \forall z \in a (c(z) \in z) \tag{2.36}$$

Definition 2.2.5. We denote **ZF** with the axiom of infinity deleted as **ZF-Inf**

Remark 2.2.6. Since now we will work, unless otherwise specified, in **ZF-Inf**

Now we will develop some set theoretic results, necessary for our discussion. We take the book by Kunen[3] as reference.

Definition 2.2.7 (successor)**.** Let x a set, than we can define is *successor* as $s(x) = x \cup \{x\}$

Definition 2.2.8. Using Pair, Empty and Union we can define naturals numbers in terms of sets

$$0 = \varnothing \qquad 1 = \{0\} = \{\varnothing\} = s(0) \qquad 2 = \{0,1\} = \{\varnothing, \{\varnothing\}\} = s(1)$$

we can define the natural number n as $n = \underbrace{s(s(\cdots(0)))}_{\text{k times}}$. They are called *finite ordinals*

Definition 2.2.9 (sums and products of finite ordinals)**.** Let x and y (since y is a finite ordinal $y = 0$ or $\exists z\, y = s(z)$) be two finite ordinal, then we define sums and products as

$$x + 0 = x$$
$$x + s(z) = s(x + z)$$

and

$$x \cdot 0 = 0$$
$$x \cdot s(z) = x \cdot z + x$$

Remark 2.2.10. We gave an informal definition of sum and product of finite ordinals; it would be natural to justify it by recursion on ω. But ω is not a set in **ZF-Inf**. To justify a recursive definition over a class we will need the transfinite recursion theorem, that we will discuss in the next section

Definition 2.2.11. x is transitive if $\forall y \in x(y \subseteq x)$

Definition 2.2.12 (Ordinals)**.** α is a ordinal if α is transitive and it is totally ordered by $\in$[8]

Proposition 2.2.13. α is an ordinal if and only if α is transitive and is well ordered by $\in$[9]

Lemma 2.2.14. If α is an ordinal, then $s(\alpha)$ is an ordinal. Hence, the sets $0, 1, ...s(\alpha)$ are all ordinals

Definition 2.2.15. Let α and β be ordinals, then we define $\alpha < \beta$ as $\alpha \in \beta$ and $\alpha \leqslant \beta$ as $\alpha \in \beta \vee \alpha = \beta$. ON denotates the proper class of all ordinals[10]

Proposition 2.2.16. ON is well order by $\in$

Proposition 2.2.17. if X is a subset of ON and X is transitive, then X$\in$ON

Lemma 2.2.18. If α,β are ordinals, then $\alpha \cup \beta$ and $\alpha \cap \beta$ are ordinals, with $\alpha \cup \beta = max(\alpha, \beta)$ and $\alpha \cap \beta = min(\alpha, \beta)$

Lemma 2.2.19. If α is any ordinal, then $S(\alpha)$ is an ordinal, $\alpha \in S(\alpha)$ and, for all ordinals γ: $\gamma < s(\alpha)$ if and only if $\gamma \leqslant \alpha$

Lemma 2.2.20. If α and β are ordinals and $s(\alpha) = s(\beta)$ then $\alpha = \beta$

Proof. We can proceed by contradiction. Let us suppose $\alpha \neq \beta$. Then, by definition of successor function $\alpha \in s(\alpha)$, but $s(\alpha) = s(\beta)$. Thus, $\alpha \in s(\beta)$. Now, since $\alpha \neq \beta$ then $\alpha \in \beta$. In the same way we get $\beta \in \alpha$. This contradicts the axiom of foundation. □

Definition 2.2.21. An ordinal β is

- a *successor ordinal* if $\beta = s(\alpha)$ for some α
- a *limit ordinal* if $\beta \neq 0$ and β is not a successor ordinal
- a *natural number* if every $\alpha \leqslant \beta$ is either 0 or a successor

Lemma 2.2.22. If n is a natural number, then $s(n)$ is also a natural number and every element of n is a natural number

Definition 2.2.23. We can define the class of natural number as

$$\omega = \{n : \text{n is a natural number}\}$$

Remark 2.2.24. Without assuming the axiom of infinity we cannot claim that ω exists (that is, ω is a set). But we can prove induction also on class

[8]that is, $\forall y \forall z(y = z \vee y \in z \vee z \in y)$

[9]That is, every subset of x has minimum for $\in$

[10]By proper class we mean an informal collection of objects. A proper class is not a set and it is not an object of the theory; so it is a way to talk about an arbitrary collection of elements in a complete informal way

Theorem 2.2.25 (Principle of Ordinary Induction)**.** For any class X: if $\varnothing \in X$ and $\forall y \in X(s(y) \in X)$, then X contains all natural numbers

Proof. Suppose that n is a natural number and $n \notin X$. Then $n \in s(n)\backslash X$, so $s(n)\backslash X \neq \varnothing$. $s(n)$ is well ordered, so, let m be the least element of $s(n)\backslash X$. Then $m \neq 0$ since $0 \in X$, and $m \neq s(y)$ for any y, so m is not a natural number, contradicting lemma 2.2.22 □

In **ZF-Inf** it is impossible to prove that ω is a set, thus we need to justify the definition of sums and products of finite ordinals given in 2.2.9. From an informal standpoint it is clear that our definition of sums and products is given by recursion, but we need to justify it in terms of transfinite recursion.

Definition 2.2.26. R is a binary relation if R is a set of ordinate pair, that is,

$$\forall u \in R \exists x \exists y [u =< x, y >]$$ [11]

xRy stances for $< x, y >\in R$
R is sad to be *transitive* iff $\forall x \forall y \forall z \in A[xRy \wedge yRz \rightarrow zRz]$

Definition 2.2.27. For any set R, we can define:

$$dom(R) = \{x : \exists y[(x, y) \in R]\} \qquad ran(R) = \{y : \exists y[(x, y) \in R]\}$$

Definition 2.2.28. $R \upharpoonright A := \{(x, y) \in R : x \in A\}$

Definition 2.2.29. R is well-founded on A if every non empty subset of A contains an R-minimal element

Remark 2.2.30. In this definition we are not asking that A is a set

Lemma 2.2.31. The axiom of foundation is equivalent to the statement that $\in$ relation is well-founded on $V = \{x : x = x\}$

Definition 2.2.32. Let R be a relation on a class A. If $y \in A$, let $y \downarrow= pred_R(y) = pred_{A,R}(y) = \{x \in A : xRy\}$. Then R is set-like on A if $y \downarrow$ is a set for all $y \in A$

Remark 2.2.33. If A=ON and R is the membership, then $y \downarrow= y$, then $\in$ is set-like on ON

Definition 2.2.34. For a relation R and a class A:

1. s is a *path* (or, R-path) of n steps in A if $n \in \omega$, $n \geqslant 1$, s is a function, $dom(s) = n+1$, $ran(s) \subseteq A$ and $\forall j < n[s(j)Rs(j + 1)]$

2. The s in (1) is called path from s(0) to s(n)

3. The transitive closure of R on A is the relation $R^* = R^*_A$ on A defined by xR^*y iff there exists a path in A from x to y

Lemma 2.2.35. For a relation R and a class A:

[11] the notion of ordinate pair is formalizeb by Kuratowsky's definition, i.e. $< x, y >:= \{\{x\}, \{x, y\}\}$

1. R^* is transitive on A
2. If R is set like on A, then R^* is set-like on A

Theorem 2.2.36 (Transfinite Induction on Well-Founded Relations). Assume that R is well-founded and set-like on a class A, and let X be a non empty sub-class of A. Then X has an R-minimal element.

Proof. Fix any $a \in X$. Let b be an R-minimal element of the *set* $\{a\} \cup (pred_{R^*}(a) \cap X)$. Then b is an R-minimal element of X, since $yRb \to y \in pred_{R^*}(a)$ □

Theorem 2.2.37 (Transfinite Recursion on Well-founded Relation). Let R be a well-founded and set-like relation on A, and $\forall x \forall s \exists ! y \phi(x, s, y)$. Define $G(x, s)$ to be the unique y such that $\phi(x, s, y)$. Then we can write a formula ψ for which the following are provable:

- $\forall x \exists ! \psi(x, y)$, so ψ defines a function F, where $F(x)$ is the y such that $\psi(x, y)$
- $\forall a \in A[F(a) = G(a, F \restriction (a \downarrow)]$.

Proof. For set d, h, let $App(h, d)$ say that h is a function and $dom(h) = D \subseteq A$. $\forall y \in d[y \downarrow \subseteq d]$, and $\forall y \in d[h(y) = G(y, h \restriction (y \downarrow))]$; so, we are saying that h is an *approximation* to F defined on some set d. Here $y \downarrow$ abbreviates $pred_{A,R}(y)$ as before. Note that the property $\forall y \in d[y \downarrow \subset d]$ implies also $\forall y \in d[pred_{A,R^*}(y) \subseteq d]$. An important set with this property is:

$$d_x := x \cup pred_{A,R^*}(x)$$

for any $x \in A$; this is a set because R^* is set like by Lemma 2.2.35
Assuming that the theorem is true, $App(d, h)$ implies that $h = F \restriction d$, since $h(y) = F(y)$ for all $y \in d$ is easily proved by transfinite induction. Since we do not know yet that the theorem is true, we shall prove the theorem by using this $App(d, h)$ to write down the definition of ψ:

$$\psi(x, y) \iff [x \notin A \wedge y = \emptyset] \vee [x \in A \wedge \exists d \exists h[App(d, h) \wedge x \in d \wedge h(x) = y]]$$

We now need to check that this definition works, which will be easy one we have verified the *existence* and the *uniqueness* of these approximation.
Uniqueness means that all the approximations agree wherever the are defined:

$$App(d, h) \wedge App(d', h') \to App(d \cap d', h \cap h') \tag{U}$$

To verify this, note first that $\forall y \in (d \cap d')[y \downarrow \subset (d \cap d')]$. Then, note that $h(y) = h'(y)$ for all $y \in (d \cap d')$, since a R-minimal element of $\{y \in d \cap d' : h(y) \neq h'(y)\}$ would be contradictory, using $h(y) = G(y, h \restriction (y \downarrow))$. So, the intersection $h \cap h'$ is really a function with domain $d \cap d'$ that takes $y \in d \cap d'$ to $h(y) = h'(y)$. Then $App(d \cap d', h \cap h')$ is clear. By (U), we know that for all x, there is at most one y such that $\psi(x, y)$. To prove that such y always exists, use:

$$\forall x \in A \exists d \exists h[App(d, h) \wedge x \in d] \tag{E}$$

To prove (E) we apply transfinite induction on R, using theorem 2.2.36. First observe that $App(d,h) \wedge x \in d \rightarrow App(d_x, h_x)$, where $h_x = h \upharpoonright d_x$. Assuming that (E) is false, let $X = \{x \in A : \neg\exists d \exists h[App(d,h) \wedge x \in d]\} \neq \emptyset$. Observe that for all $x \notin X$, we have a h_x such that $App(d_x, h_x)$, and h_x is unique by (U). Let $a \in X$ be a R-minimal element of X. Let $\tilde{b} := pred_{A,R^*}(a) = \bigcup\{d_x : xRa\}$. By minimality $xRa \rightarrow x \notin X$, so, by Replacement axiom we may define a set $\tilde{h} := \bigcup\{h_x : xRa\}$ which is a function by (U), and it is easy to verify that $App(\tilde{d}, \tilde{h})$. Now, $a \notin \tilde{d}$, but $a \downarrow\subseteq \tilde{d}$. Informally $F \upharpoonright \tilde{d}$ "should be" $\tilde{h}$, so $F(a)$ "Should be" $G(a, \tilde{h} \upharpoonright (a \downarrow))$. Formally, let $d = \tilde{d} \cup \{a\}$ and let $h = \tilde{h} \cup \{(a, G(a, \tilde{h} \upharpoonright (a \downarrow)))\}$. Then $App(d,h)$ and $a \in d$ contradicting $a \in X$.
Combining (U) and (E), we know that $\forall x \exists! y \psi(x,y)$, so y defines a function F as in (1). Then (2) follows from the definition of $App(d,h)$ □

Remark 2.2.38. Let $A = ON$, and R usual order, then $\alpha \downarrow= \alpha$, and so the recursion scheme is usually written as $F(\alpha) = G(F \upharpoonright \alpha)$

Lemma 2.2.39. In theorem 2.2.37, suppose that F and F' both satisfy :

$$F(a) = G(a, F \upharpoonright (a \downarrow)) = G(a, F' \upharpoonright (a \downarrow)) = F'(a)$$

Then $\forall a(F(a) = F'(a))$

Proof. If not, and a is R-minimal in $\{a \in A : F(x) \neq F'(x)\}$, then

$$F(a) = G(a, F \upharpoonright (a \downarrow)) = G(a, F' \upharpoonright (a \downarrow)) = F'(a)$$

That is a contradiction □

Now, we can redefine sums and products of finite ordinals (for witch we have given an informal definition in 2.2.9) in therms of transfinite induction.

Definition 2.2.40. $p(\beta)$ is β if $\beta = 0$ and $p(\beta) = \gamma$ if $\beta = s(\gamma)$

Lemma 2.2.41. Sums and Products of finite ordinals exist

Proof. Let α be a fixed ordinal, then we can define $\phi_+(\alpha, x, y) = \phi_{\alpha,+}(x,y)$ as:

$$\begin{aligned}
&((Ord(\alpha) \wedge Fun(x) \wedge \exists\beta(Ord(\beta) \wedge Dom(x) = \beta)) \rightarrow \\
&((\exists\gamma(\beta = s(\gamma))) \rightarrow y = s(x(\gamma))) \wedge ((\beta = 0) \rightarrow y = 0)) \\
&\wedge (\neg(Ord(\alpha) \wedge Func(x) \wedge \exists\beta(Ord(\beta) \wedge Dom(x) = \beta)) \rightarrow y = 0)
\end{aligned}$$

Now, by uniqueness of predecessor and successor it is clear that $\phi_{\alpha,+}$ is a functional formula; that is, ZF-Inf $\vdash \forall x \exists y \phi_{\alpha,+}(x,y)$. Therefore, by transfinite recursion (theorem 2.2.37) there exists a formula $\psi_{\alpha,+}(x,y) = \psi_+(\alpha, x, y)$ such that, if F is the function defined by $\psi_{\alpha,+}$ and G is the function defined by $\phi_{\alpha,+}$, then $\forall\beta(F_\alpha(\beta) = G(F \upharpoonright \beta))$. We can apply transfinite recursion for every α. In functional therms: for each α we can define G_α so that $G_\alpha(x) = 0$ unless x is a function with domain some ordinal β, in which case $G_\alpha(x)$ is α if $\beta = 0$ and is $s(x(p(\beta)))$ if $\beta = s(\gamma)$ for an ordinal γ. Then, Theorem 2.2.37 yields to the existence of a unique F_α such that $\forall\beta(F_\alpha(\beta) = G(F \upharpoonright \beta))$. Thus, we have

defined $G_\alpha(\beta) = \alpha + \beta$ (we can conclude this equality since G_α is unique).
In the same way we can obtain the existence of the product $\alpha \cdot \beta$. Define $\phi_\bullet(\alpha, x, y) = \phi_{\alpha,\bullet}(x, y)$ as[12]

$$\begin{aligned}&(((Ord(\alpha) \wedge Fun(x) \wedge \exists\beta(Ord(\beta) \wedge Dom(x) = \beta)) \rightarrow\\&((\exists\gamma(Ord(\gamma) \wedge \beta = s(\gamma)) \rightarrow y = x(\gamma) + \alpha) \wedge (\beta = 0 \rightarrow y = 0)))\\&\wedge (\neg(Ord(\alpha) \wedge Fun(x) \wedge \exists\beta(Ord(\beta) \wedge Dom(x) = \beta)) \rightarrow y = 0)\end{aligned}$$

By uniqueness of successor ZF-Inf $\vdash \forall x\exists! y\phi_{\alpha,\bullet}(x, y)$. Therefore we can apply transfinite recursion, and so there exists a functional formula $\psi_{\alpha,\bullet}(x, y)$ such that, if F is the function defined by $\psi_{\alpha,\cdot}$ and G is the function defined by $\phi_{\alpha,\bullet}$, then $\forall\beta(F_\alpha(\beta) = G(F \upharpoonright \beta))$. In functional therms: for each α let be $G_\alpha(x)$ be 0 unless x is a function with domain some ordinal β, in which case $G_\alpha(x) = 0$ if $\beta = 0$ and $G_\alpha(x)$ is $x(\beta) + \alpha$. Thus, Theorem 2.2.37 ensure us that $G_\alpha(\beta) = F(G \upharpoonright \beta) = \alpha \cdot \beta$ exists. □

This definition through transfinite recursion ensures that functional formulas exist which define sums and products of ordinals.

2.2.2 Ordinal Extension of ZF-Inf

In the next chapter, we will define a translation of **PA** into **ZF-Inf**. To accomplish this, we need functions to translate the successor, sum, and product functions of **PA**. Therefore, we will now define a conservative extension of **ZF-Inf**, including symbols for ordinals, the successor function, and sums and products of ordinals.

Definition 2.2.42. Let $\mathcal{L}$ be the language of the sets (Definition 2.2.1), then we can define $\mathcal{L}_{ord}$ as the language that contains $\mathcal{L}$, a new individual constant 0, an unary function symbol $s(x)$, and two binary function symbols: " + " and " · ". Then we can define **ZF$_{ord}$-Inf** as the first order theory that has the same logical and proper axioms of **ZF-Inf** and the following proper axioms:

- $\forall z(z \notin 0)$
- $\forall z\forall y(y \in s(z) \leftrightarrow (y \in z \vee y = z))$
- $\forall x\forall y(\psi_+(x, y), (x + y))$
- $\forall x\forall y(\psi_\bullet(x, y), (x \cdot y))$

The existence of ψ_+ and $\psi_\bullet$ is provided by transfinite recursion, as seen in lemma 2.2.41

Proposition 2.2.43. **ZF$_{ord}$-Inf** is a conservative extension of **ZF-Inf**

$$\textbf{ZF-Inf} \lhd \textbf{ZF}_{ord}\textbf{-Inf}$$

[12]The function + that appears in the formula is the one defined above

Proof. Let $\phi(x,z) := \forall y(z \in z \leftrightarrow (y = x \vee y \in x))$, then by extensionality we easily get ZF-Inf $\vdash \forall x \exists! z \phi(x,z)$. Now, by lemma 2.2.41 ZF-Inf $\vdash \forall x \forall y \exists! z(\psi_+(x,y,z))$ and ZF-Inf $\vdash \forall x \forall y \exists! z(\psi_.(x,y,z))$. Thus we can apply proposition 1.3.6, therefore if ϕ does not contain neither $s(.)$ nor + nor ·, then ZF$_{ord}$-Inf $\vdash \phi \Rightarrow$ ZF-Inf $\vdash \phi$. Now, by definition $\mathcal{L} \subset \mathcal{L}_{ord}$. This yields to **ZF-Inf** $\lhd$ **ZF$_{ord}$-Inf** □

Theorem 2.2.44. **ZF - Inf** and **ZF$_{ord}$-Inf** are equiconsistent

$$\text{Cons(ZF-Inf)} \iff \text{Cons(ZF}_{ord}\text{-Inf)}$$

Proof. **ZF - Inf** is inconsistent if, and only if, ZF-Inf $\vdash \exists x(x \in x)$. Then also ZF$_{ord}$-Inf $\vdash \exists x(x \in x)$, thus: Incon(ZF-Inf) $\Rightarrow$ Incon(ZF$_{ord}$-Inf). Now , since ZF-Inf $\lhd$ ZF$_{ord}$-Inf then ZF$_{ord}$-Inf $\vdash \exists x(x \in x) \Rightarrow$ ZF-Inf $\vdash \exists x(x \in x)$ holds. Therefore we have proved the equiconsistency of **ZF-Inf** and **ZF$_{ord}$-Inf** □

2.2.3 A Lighter Axiomatic Presentation of ZF-Inf

As we will see in the next chapter a lighter presentation of **ZF-Inf** may be really helpful to conclude that if **ZF-Inf** is consistent than PA is also **consistent**. This section is dedicated to enunciate this lighter presentation of **ZF-Inf** and to prove that is equivalent to **ZF-Inf**

Definition 2.2.45 (ZF'). Let $\mathcal{L}$ be the language of set theory in Definition 2.2.1, then **ZF'-Inf** is the first order theory with equality over $\mathcal{L}$ whith the proper axioms:

ZF' 1. Extensionality.

$$\forall z(z \in x \leftrightarrow z \in y) \rightarrow x = y \tag{2.37}$$

ZF' 2. Foundation.

$$\exists y(y \in x) \rightarrow \exists y(y \in x \wedge \neg \exists z(z \in x \wedge z \in y)) \tag{2.38}$$

ZF' 4. Weakened Union.

$$\forall x \exists y \forall c \in x \forall z \in c(z \in y) \tag{2.39}$$

ZF' 5. Weakened Power.

$$\forall x \exists y \forall z(\forall w(w \in z \rightarrow w \in x) \rightarrow z \in y) \tag{2.40}$$

ZF' 6. Separation Scheme. For each formula ϕ without y free,

$$\forall x \exists y \forall z(z \in y \leftrightarrow z \in x \wedge \phi(z)) \tag{2.41}$$

ZF' 7. Replacement Scheme. Let φ be a formula formula of $\mathcal{L}$

$$\forall x \exists! y \varphi(x,y) \rightarrow \forall a \exists b \forall y(y \in b \leftrightarrow \exists x \in a \varphi(x,y)) \tag{2.42}$$

Theorem 2.2.46. **ZF-Inf** and **ZF'-Inf** are equivalent

$$\textbf{ZF-Inf} \equiv \textbf{ZF'-Inf}$$

Proof.

i. We will prove that ZF-Inf $\vdash$ ZF'-Inf.
Since Extensionality, Foundation, Separation and Replacement do not change, for they there are nothing to prove.
ZF' 4. ZF $\vdash \forall x \exists y \forall z(z \in y \leftrightarrow \exists v \in x(z \in v))$ by ZF 5; then ZF $\vdash \forall x \exists y \forall z(z \in y \leftarrow \exists v \in x(z \in v))$. Then ZF $\vdash \forall x \exists y \forall c \in x \forall z \in c(z \in y)$
ZF' 5. ZF' 5 consist of only one implication of Power Axiom, so is trivially valid in ZF-Inf

ii. Now, we need to prove that ZF'-Inf $\vdash$ ZF-Inf. Since Extensionality, Foundation, Separation and Replacement do not change, for them there is nothing to prove.
Empty set. It follows for Separation: $ZF' \vdash \forall x \exists y(z \in y \leftrightarrow z \in x \wedge \phi(z))$. Let $\phi(z)$ be $z \neq z$. Since ϕ is a logical contradiction: $ZF' \vdash \exists y \forall z(z \notin y)$. We are allowed to use Separation since, by Remark 1.3.3, there exists at least one set.
Union. From ZF'4: $ZF' \vdash \forall x \exists y \forall c \in x \forall z \in c(z \in y)$, then, by Separation on y using $\phi(w)$:$\exists u \in x \wedge w \in u$ we get ZF' $\vdash \forall x \exists y \exists A((\forall c \in x \forall z \in c(z \in y)) \wedge (w \in A \leftrightarrow w \in y \wedge (\exists u \in x \wedge w \in u))$. Since, by definition ZF' $\vdash A \subseteq y$ (where y is the set provided by ZF' 5 and A is union set as described ZF 5) then ZF' $\vdash \forall x \exists y \forall z(z \in y \leftrightarrow \exists v \in x \wedge z \in v)$
Power. It follows from ZF' 5 by Separation (we need to add $z \in y \rightarrow z \subseteq x$)
Paring. It follows from Union, Power and Replacement. Let $\varnothing$ be the set provided by Axiom of Empty Set, and $\mathcal{P}(x)$ the set provided by Power Set Axiom. Now, we can define a formula $\phi(u, v, x, y) := (u = \varnothing \wedge v = x) \vee (u = \{\varnothing\} \wedge v = y\})$. By replacement on $\mathcal{P}(\mathcal{P}(\varnothing))$ we get the pair set of x and y

□

Corollary 2.2.47. Since **ZF-Inf** $\equiv$ **ZF'-Inf**

$$\text{Cons(ZF-Inf)} \iff \text{Cons(ZF'-Inf)}$$

2.3 Preliminary conclusions

In this section, we have defined **ZF-Inf** and PA, and for both, we have defined other equiconsistent systems. For **ZF-Inf**, we have defined a conservative extension, **ZF**$_{ord}$**-Inf**, and an equivalent one, **ZF'-Inf**. For **PA**, we have defined a conservative extension, **PA'**, obtained by adding a symbol for every primitive recursive function. The next chapter will be dedicated to concluding the equiconsistency: in order to obtain the equiconsistency, we will translate **ZF**$_{ord}$**-Inf** into **PA** and **PA'** into **ZF'-Inf**. **ZF**$_{ord}$**-Inf** into **PA** and **PA'** into **ZF'-Inf**.

Chapter 3

Equicontistency of PA and ZF-Inf

In this chapter we will prove that there exists a translation of **PA** into $\mathbf{ZF}_{ord} - \mathbf{Inf}$ and that there exists a translation of **ZF'-Inf** into **PA'**. The existence of these translations will provide us the equiconsistency of **PA** and **ZF-Inf**. Our proof will be just a syntactic proof. This allows us to rely on a very weak meta-theory; in fact the translations we present can be formalized in **PRA**.

3.1 Ordinal Translation

Definition 3.1.1. Let $\mathcal{I}$ be a translation of **PA** into $\mathbf{ZF}_{ord}$**-In** for which:

- The constant of 0 **PA** is translated to 0 in $\mathbf{ZF}_{ord}$**-Inf**. $\mathcal{I}(0_{\text{Pa}}) = 0_{\text{ZF}_{ord}\text{-Inf}}$
- The successor function $(\cdot)'$ in **PA** is translated to $s(\mathcal{I}(x))$, i.e: $\mathcal{I}(x') = s(\mathcal{I}(x))$
- The functions $+$ and $\cdot$ in **PA** are translated to sum and product of finite ordinals in $\mathbf{ZF}_{ord}$**-Inf**, i.e. $\mathcal{I}(a+b) = \mathcal{I}(a) + \mathcal{I}(b)$ and $\mathcal{I}(a \cdot b) = \mathcal{I}(a) \cdot \mathcal{I}(b)$
- $\mathcal{I}(\phi \to \psi) = \mathcal{I}(\phi) \to \mathcal{I}(\psi)$ and $\mathcal{I}(\neg\phi) = \neg\mathcal{I}(\phi)$
- Quantified formulas $\forall x P(x)$ in **PA** are translated to $\forall x(Nat(x) \to \mathcal{I}(P(x)))$ where $Nat(x) := ord(x) \wedge (y = 0 \vee (succ(y) \wedge \forall x(x \in y \to x = 0 \vee succ(x)))$ in $\mathbf{ZF}_{ord}$**-Inf**.[1]

Proposition 3.1.2. **PA** $\vdash \phi \Rightarrow \text{ZF}_{ord}\text{-Inf} \vdash \mathcal{I}(\phi)$

Proof. We have to prove that in $\mathbf{ZF}_{ord}$**-Inf** the translation of each PA axiom holds.

- $\text{ZF}_{ord}\text{-Inf} \vdash \forall x(Nat(x) \to (0 \neq s(x))$. We can prove this by contradiction: if $Nat(z)$ and $0 = s(z)$, then $z \in 0 = \varnothing$ by the proper axiom of $s()$, contradicting the proper axiom for the ordinal 0.
- ZF-Inf $\vdash \forall x_1(Nat(x) \to (\forall x_2(Nat(x_2) \to (s(x_1) = s(x_2) \to x_1 = x_2))))$. This follows directly from Lemma 2.2.20

[1] $succ(y)$ means "y is a successor", that is $\exists z(s(z) = x)$. $ord(y)$ means "y is a ordinal", that is $(\forall z \in y(z \subseteq y)) \wedge (\forall x \in y \forall z \in y(x = z \vee x \in z \vee z \in x))$

- (S3)-(S6) are trivially verified by definition of sums and products of finite ordinals
- Let ϕ be a formula formula. Then (S7) is verified by Theorem 2.2.25. Let X be the class of naturals defined by $\mathcal{I}(\phi)$, then, by ordinary induction principle if $\varnothing \in X$ and $\forall y \in X(s(y) \in X)$ then X contains every natural number.

□

Theorem 3.1.3. If **ZF**$_{ord}$**-Inf** is consistent, then **PA** is consistent

$$\text{Cons}(\text{ZF}_{ord}\text{-Inf}) \Rightarrow \text{Cons}(\text{PA})$$

Proof. Let **PA** be inconsistent, then PA $\vdash \phi \wedge \neg\phi$ and so, by Proposition 3.1.2 ZF$_{ord}$-Inf $\vdash \mathcal{I}(\phi \wedge \neg\phi)$. Therefore, since $\mathcal{I}$ does not change $\rightarrow$ and $\neg$, ZF$_{ord}$-Inf $\vdash \mathcal{I}(\phi) \wedge \neg\mathcal{I}(\phi)$. Thus, Incon(PA) $\Rightarrow$ Incon(ZF$_{ord}$-Inf). This yields to:

$$\text{Cons}(\text{ZF}_{ord}\text{-Inf}) \Rightarrow \text{Cons}(\text{PA})$$

□

3.2 Ackermann Translation

In this section we will define a translation of **ZF'-Inf** into **PA'**, and we will show that any sentence in **ZF'-Inf** can be syntactically translated into a sentence of **PA'**. In order to do this we will use the "Ackermann Encoding" to translate the membership relation of sets and we will prove that this translation preserves the provability; that is, if a sentence is a theorem in **ZF'-Inf** then also its translation will be a theorem in **PA'**

Idea (**Ackermann Encoding**)**.** From an informal standpoint the Ackermann Encoding asserts that: $n \in m$ if the nth digit in the binary expansion of m is 1. For example let be $x = 0$, then, since $\forall y(y \notin x)$, $\mathcal{A}(0) = 0$. Let now $x = \bar{1} = \{0\}$, by definition of $\bar{1}$ the only z such $z \in \bar{1}$ is 0. Thus, the 0th digit of the binary expansion of $\mathcal{A}(\bar{1})$ must be 1 and, since not other sets belong to $\bar{1}$ all the other digits bust be 0. Thus $\mathcal{A}(\bar{1}) = (1)_2 = (1)_{10}$. In the following table, we list some examples of translations:

Example of Some Translation		
Set	Binary Encoding	Decimal Number
$0 = \varnothing$	0	0
$\bar{1} = \{0\}$	1	1
$\{\bar{1}\}$	10	2
$\bar{2} = \{0, \bar{1}\}$	11	3
$\{0, \bar{2}\}$	1001	9
$\{0, \{\bar{1}\}\}$	101	5
$\bar{3} = \{0, \bar{1}, \bar{2}\}$	1011	11
$\{\bar{1}, \bar{2}, \{0, \{\bar{1}\}\}\}$	101010	42

Now, we need to define a translation of **ZF'-Inf** in **PA'** in a formal way

Definition 3.2.1 (Ackermann Translation)**.** Let $\mathcal{A}$ be the translation of **ZF'-Inf** in **PA'** for which:

- $\mathcal{A}(x_1 = x_2)$ is $\mathcal{A}(x_1) = \mathcal{A}(x_2)$.
- $\mathcal{A}(n \in m)$ is $n \Subset m := \mathrm{rm}(\mathrm{qt}(m, 2^n), 2) = 1$. This is the Ackermann Encoding written in terms of primitive recursive functions in **PA'**
- $\mathcal{A}(\phi \to \psi)$ is $\mathcal{A}(\phi) \to \mathcal{A}(\psi)$, $\mathcal{A}(\neg\phi)$ is $\neg\mathcal{A}(\phi)$ and $\mathcal{A}(\forall x \phi(x))$ is $\forall x \mathcal{A}(\phi(x))$

$\mathcal{A}$ is called the *Ackermann Translation.*

Proposition 3.2.2. ZF'-Inf $\vdash \phi \Rightarrow$ PA' $\vdash \mathcal{A}(\phi)$

Proof. We need to prove that in **PA'** the translation of every axiom of **ZF'-Inf** holds. The following arguments can be fully internalized in **PRA**.

- **Extensionality.** Let be x, y such that $\forall z(z \Subset x \leftrightarrow z \Subset y)$. Now, from an informal standpoint this means that x and y has a 1 in the same nth place in binary representation. Since two numbers with the same binary representation are the same, then $x = y$. From a formal point of view we need to prove that:

$$\text{PA'} \vdash \forall x(x = \sum_{i \Subset x} 2^i)$$ [2]

We can prove this by induction:

- since PA' $\vdash i \Subset x \to i < x$ and PA' $\vdash \forall x \neg(x < 0)$ then PA' $\vdash \forall i \neg(i \Subset 0)$. Thus,

$$\text{PA'} \vdash 0 = \sum_{i \Subset 0} 2^i$$

- let us suppose $x = \sum_{i \Subset x} 2^i$, then, by product property and exponential definition $2x = \sum_{i \Subset x} 2^{i+1}$. By Lemma 2.1.36 $2x = \sum_{i+1 \Subset 2x} 2^{i+1}$, then, PA' $\vdash x = \sum_{i \Subset x} 2^i \to 2x = \sum_{j \Subset 2x} 2^j$. Now, as above, by Lemma 2.1.36 PA' $\vdash x = \sum_{i \Subset x} 2^i \to 2x + 1 = \sum_{j \Subset (2x+1)} 2^j$. Then by induction scheme:[3]

$$\text{PA'} \vdash \forall x(x = \sum_{i \Subset x} 2^i)$$

Thus, we have proved that

$$\text{PA'} \vdash \forall x \forall y \forall z((z \Subset x \leftrightarrow z \Subset t) \to x = y)$$ [4]

[2]this sum make sense in **PA'** since "$i \Subset x$" is a primitive recursive relation

[3]$\phi(0) \wedge (\forall x((\phi(x) \to (\phi(2x)) \wedge (\phi(x) \to \phi(2x+1)))9) \to \forall x \phi(x)$ is equivalent to induction scheme

[4]We may notice that, without referring to any quantifier, the theorem about binary expansion is still valid in **PRA**, since we can use an equivalent of the induction rule:

$$\frac{\phi(0) \qquad \phi(x) \to \phi(2x) \qquad \phi(x) \to \phi(2x+1)}{\phi(x)}$$

- **Foundation.** Let $x \neq 0$ and $\phi(n) := n \Subset x$. Since $x \neq 0$ there exist at least one place in its binary representation with digit 1, that is $\exists u \phi(u)$. Now, by Proposition 2.1.12(b): PA', $\exists u\phi(u) \vdash \exists n(\phi(n) \wedge (\forall z)(z < n \rightarrow \neg\phi(n)))$. Since $m \Subset n \rightarrow m \leqslant n$ if existed m such that $m \Subset x \wedge m \Subset n$ then we would have $m \leqslant n \wedge \phi(m)$, and so or $m = n$ or we would contradict the minimality of n. Thus, n is the minimal element for "$\Subset$" in x, in other words:

$$\text{PA}, \exists u \Subset x \vdash \exists y(y \Subset x \wedge \neg\exists z(z \Subset x \wedge z \Subset y))$$

- **Weakened Union.** From an informal standpoint the axiom of weakened union asserts the existence of an upper bound of the union set, that is, we need to prove that PA' $\vdash \forall x\exists y\forall u \Subset x\forall z \Subset u(z \Subset y)$. Now, let x be a natural, then $\forall i \neq x\neg(i \Subset 2^x)$ (this follows from the observation on the binary expansion in the proof of **Extensionality**, since $2^x = \sum_{i \Subset x} 2^i$ the only natural such that $i \Subset 2^x$ is x). Now, let us prove by induction than $\forall i(i \leqslant x \rightarrow (i \Subset 2^x - 1))$. We will prove by induction that PA $\vdash 2^x - 1 = \sum_{i<x} 2^i$ and then, since PA $\vdash \forall x(x = \sum_{i \Subset x} 2^i)$, PA $\vdash \forall i(i < x \rightarrow i \Subset 2^x - 1)$.

  - $2^0 - 1 = 0 = \sum_{i \Subset 0} 2^i$
  - Let $2^x - 1 = \sum_{i<x} 2^i$. Then:

$$\begin{aligned} 2^{x'} - 1 &= 2^x \cdot 2 - 1 = (2^x + 1 - 1) \cdot 2 - 1 \\ &= (2^x - 1) \cdot 2 + 1 = \sum_{i<x} 2^{i+1} + 2^0 \\ &= \sum_{i<x'} 2^i \end{aligned}$$

  Thus, PA $\vdash \forall x(2^x - 1 = \sum_{i<x} 2^i)$. Now, since PA' $\vdash \forall x(x = \sum_{i \Subset x} 2^i)$:

$$\text{PA'} \vdash \forall i(i < x \rightarrow i \Subset 2^x - 1)$$

  Now, by Lemma 2.1.37 PA' $\vdash \forall n\forall m(n \Subset m \rightarrow n < m)$. Then:

$$\forall z(z \Subset u \Subset x \rightarrow z < u < x)$$

  and then $\forall u \Subset x\forall z \Subset u(z \Subset 2^x - 1)$. Thus, we have proved that

$$\text{PA'} \vdash \forall x\exists y\forall u \Subset x\forall z \Subset u(z \Subset y)$$

- **Weakened Power.** We should start specifying what the interpretation of $y \subseteq x$ is. By definition $(y \subseteq x) \iff (\forall z(z \in y \rightarrow z \in x))$. This is interpreted in $(y \sqsubseteq x) \iff (\forall z(z \Subset y \rightarrow z \Subset x))$. I.e. "$y \sqsubseteq x$ if, for every z, the z-th digit of the binary representation of y is 1 implies that the z-th digit of the binary representation of x is 1". In other words $y \sqsubseteq x$ if, and only if, the binary representation of y is contained in the binary representation of x. Now, in order to satisfy the weakened power axiom, we need to find an upper bound for power set. We can work as in

Weakened Union:
Since $\forall y \forall x (y \sqsubseteq x \rightarrow y \leqslant x)$ (This follows from Lemma 2.1.37), then $\forall y \forall x (y \sqsubseteq x \rightarrow y \sqsubset 2^{x+1} - 1$. Thus we have found an upper bound for power set. This yields to:

$$\text{PA'} \vdash \forall x \exists y \forall z (z \sqsubseteq x \rightarrow z \sqsubset y)$$

- **Separation Scheme.** We need to prove that for all formula ϕ (in $\mathcal{L'}_A$) without y free:

$$\forall x \exists y \forall z (z \sqsubset y \leftrightarrow z \sqsubset x \wedge \phi(z))$$

We can proceed by complete induction (Proposition 2.1.12):
let $\psi(x) := \exists y \forall z (z \sqsubset y \leftrightarrow z \sqsubset x \wedge \phi(z))$, then: Suppose that $\forall w (w < x \rightarrow \psi(z))$. Now, let be $x = \sum_{i \sqsubset x} 2^i$. Since, $i > x \rightarrow \neg(i \sqsubset x)$ holds there are finite i_n such that $i_n \sqsubset x$. This allows us to define $\square(x) := x - 2^{m(x)}$, where $m(x)$ is the maximum natural such $m(x) \sqsubset x$[5]

$$m(x) = n - \sum_{y=o}^{n} \bar{sg}(\sum_{i=0}^{y} rm(qt(x, 2^{x-i}), 2))$$

$m(x)$ is, by definition, primitive recursive. Thus we can conclude that $\square(x)$ is primitive recursive since it is obtained by substitution on primitive recursive functions. Now, if $x = \sum_{i \sqsubset x} 2^i$ then $\square(x) = \sum_{i \sqsubset x \wedge i < m(x)} 2^i$; thus $\square(x) \sqsubset x$. The maximality of $\square(x)$ is guaranteed by the maximality of $m(x)$. We know from the inductive hypothesis that $\psi(z)$ holds for every $z < x$, so $\psi(\square(x))$ holds. Now, we need to prove that $\psi(x)$ holds. Let y be the natural provided by $\phi(\square(x))$, then $\forall z (z \sqsubset y \leftrightarrow z \sqsubset \square(x) \wedge \phi(z))$. Now, we can define:

$$u = \begin{cases} y + 2^{m(x)} & \text{if } \phi(m(x)) \\ y & \text{otherwise} \end{cases}$$

Then, since $\square(x) \sqsubset x$, $\forall z (z \sqsubset u \leftrightarrow (z \sqsubset x \wedge \phi(z)))$, and so: PA' $\vdash \forall x (\forall z (z < x \rightarrow \psi(x)) \rightarrow \psi(x))$. This concludes the induction:

$$\text{PA'} \vdash \forall x \exists y \forall z (z \sqsubset y \leftrightarrow z \sqsubset x \wedge \phi(z))$$

- **Replacement Scheme.** We need to prove the Replacement Scheme:

$$\forall u \exists ! v \phi(u, v) \rightarrow \forall x \exists y \forall b (b \sqsubset y \leftrightarrow \exists a \sqsubset x \phi(a, b))$$

We can work as in **Separation Scheme** by complete induction:
Let $\psi(x) := \forall u \exists ! v \phi(u, v) \rightarrow \exists y \forall b (b \sqsubset y \leftrightarrow \exists a \sqsubset x \phi(a, b))$ and let us suppose $\forall z (z < x \rightarrow \psi(z))$. We can define, as above, $\square(x)$. By induction hypothesis $\psi(\square(x))$

[5]From a meta-theoretical standpoint it is trivial that $m(x) = log_2(x)$, in which the logarithm is defined over natural numbers in a recursive way. Nevertheless it is not trivial to prove that **PA'** proves the maximally of $log_2(x)$ as exponent in the binary expansion of x

holds, so there is an y such that $\forall b(b \in y \leftrightarrow \exists a \in \square(x)(\phi(a,b))$. Then we can define $u := y + 2^b$ in which b is the only natural such $\phi(a,b)$ (we have supposed that PA' $\vdash \forall u \exists! v \phi(u,v)$). Thus, PA' $\vdash \forall x(\forall z(z < x \rightarrow \psi(z)) \rightarrow \psi(x))$. This concludes the induction:

$$\text{PA'} \vdash \forall u \exists! v \phi(u,v) \rightarrow \forall x \exists y \forall b(b \in y \leftrightarrow \exists a \in x \phi(a,b))$$

□

Theorem 3.2.3. If **PA'** is consistent, then also **ZF'-Inf** is consistent

$$\text{Cons(PA')} \Rightarrow \text{Cons(ZF'-inf)}$$

Proof. Let **ZF'-Inf** be inconsistent, then ZF'-Inf $\vdash \phi \wedge \neg\phi$. Thus, by Proposition 3.2.2 PA' $\vdash \mathcal{A}(\phi \wedge \neg\phi)$. By definition of Ackermann Translation: PA' $\vdash \mathcal{A}(\phi) \wedge \neg\mathcal{A}(\phi)$. Thus, Incon(ZF'-Inf) $\Rightarrow$ Incon(PA'). And so

$$\text{Cons(PA')} \Rightarrow \text{Cons(ZF'-Inf)}$$

□

3.3 Conclusions Regarding Equiconsistency

In this chapter we have proved that Cons(ZF_{ord}-Inf) $\Rightarrow$ Cons(PA) and Cons(PA') $\Rightarrow$ Cons(ZF'-Inf). This information with the results of Chapter 2 yields to

Theorem 3.3.1. ZF-Inf and **PA** are equiconsistent

$$\text{Cons(ZF-Inf)} \iff \text{Cons(PA)}$$

Proof. By Theorem 3.1.3 Cons(ZF_{ord}-Inf) $\Rightarrow$ Cons(PA). Thus, by 2.2.44 ZF-Inf $\Rightarrow$ PA. Now, by Theorem 2.1.40 Cons(PA) $\iff$ Cons(PA'), by Theorem 3.2.3 Cons(PA') $\Rightarrow$ Cons(ZF'-Inf) and by Theorem 2.2.47 Cons(ZF'-Inf) $\iff$ Cons(ZF-Inf). Thus, Cons(PA) $\Rightarrow$ Cons(ZF-Inf). □

We have obtained the equiconsistency of **ZF-Inf** and **PA**, but we have not explicitly discussed our meta-theoretic assumption. We said that both translation were *primitive recursive*. Thus, all the proof of equiconsistency needs only primitive recursive arithmetic to be formalized, that is:

$$\text{PRA} \vdash \text{Cons(ZF-Inf)} \iff \text{Cons(PA)}$$

Chapter 4

Consequences in Finite Set Theory and Other Results

4.1 Zermelo Fraenkel with the negation of Axiom of infinity

Our discussion until now took place in **ZF-Inf**. But **ZF-Inf** is not a Finite Set Theory, there are model of **ZF-Inf** with infinite sets and models without them. In this section we will discuss different definitions of infinity, and prove that the Ackermann models of **ZF-Inf** prove an axiom of finiteness; then we will discuss the role of the axiom of choice. In his original work Ackermann discusses the axiom of choice explicitly proving that its translation holds in **PA'**. We will propose a different argument. A rapid development of a finite sets theory proves that the finite choice is a theorem; therefore, if the translation of an axiom of finiteness is valid in **PA'**, consequently we obtain the validity of the translation of the axiom of choice

4.1.1 Finite Set Theory

While defining **ZF** we stated the axiom of infinity as:

$$\exists x(\exists u(u \in x \wedge (\forall v(v \notin u))) \wedge \forall z(z \in x \rightarrow \exists y(y \in x \wedge \forall w(w \in y \leftrightarrow (w \in z \vee w = z)))))$$

That is, we state the existence of ω, that is obtained by Separation.
Now, in literature there are some definitions of mathematical infinity; some of those assume the axiom of infinity

Definition 4.1.1. We say that x is $\omega-$finite iff the following holds

$$Fin^{\omega}(x) := \neg\exists f(Func(f) \wedge Inj(f) \wedge Dom(f) = \omega \wedge Ran(f) \subseteq x)^1$$

This definition is obviously not useful for our purpose since ω does not exists if Axiom of Infinity does not holds. But there are other definition of infinity not involving neither ω nor the assumption of axiom of infinity

[1]Here "Func(f)" stances for "f is a function" and "Inj(f)" stances for "f is injiective"

Definition 4.1.2. We say that x is f-finite if the following holds:

$$Fin^f(x) := \exists f \exists n(Fun(f) \wedge Inj(f) \wedge Nat(n) \wedge Dom(f) = n \wedge Ran(f) = x)$$

And we have the Dedekind finiteness:

Definition 4.1.3. We say that x is Dedekind-Finite iff the following holds:

$$Fin^D(x) := \neg\exists f \exists y(x \supseteq y \wedge y \neq x \wedge Fun(f) \wedge Inj(f) \wedge Dom(f) = x \wedge Ran(f) = y)$$

Now we have some preliminary well-known results about the characterization of finiteness:

Lemma 4.1.4. ZF $\vdash \forall x(Fin^\omega(x) \leftrightarrow Fin^D(x))$

Lemma 4.1.5. ZF-Inf $\vdash \forall x(Fin^f(x) \rightarrow Fin^D(x))$

Lemma 4.1.6. ZF-Inf $\vdash \forall x Fin^D(x) \rightarrow \neg$Inf

Therefore

Corollary 4.1.7. ZF-Inf $\vdash \forall x Fin^f(x) \rightarrow \neg$Inf

Thus we can define a Finite Set Theory by using f-finiteness as finiteness axiom

$$Fin := \forall x Fin^f(x)$$

Definition 4.1.8. WO is the sentence that every set can be well ordered, formally:

$$WO := \forall x \exists \alpha \exists f(On(\alpha) \wedge Fun(f) \wedge Dom(f) = \alpha \wedge Ran(f) = x \wedge Inj(f))$$

Lemma 4.1.9. ZF-Inf + Fin $\vdash$ WO

Proof. This easily follows from **Fin**, since **Fin** provides the existence of a bijection between every x and a natural n, and a natural numbers is also an ordinal. □

Proposition 4.1.10. ZF-Inf $\vdash$ WO $\leftrightarrow$ AC

Proof. Omitted, see K.Kunen: "Set Theory", 2013[3] □

Now we will prove that the Ackermann model of **ZF-Inf** satisfies $\forall x Fin^f(x)$. To discuss $\forall x Fin^f(x)$ we need to make clear what the translation of a function is.

Remark 4.1.11. In **ZF-Inf** we can define a function f as a subset of the Cartesian product of two other sets A,B for which $\forall x \in A \exists! y \in B((x, y) \in f)$. Now, the definition of order pair is $(a, b) := \{\{a\}, \{a, b\}\}$. Therefore the Ackermann translation of (a, b) is

$$\mathcal{A}((a, b)) = \mathcal{A}(\{\{a\}, \{a, b\}\}) = 2^{2^{\mathcal{A}(a)}} + 2^{2^{\mathcal{A}(a)} + 2^{\mathcal{A}(b)}} = 2^{2^{\mathcal{A}(a)}}(1 + 2^{2^{\mathcal{A}(b)}})$$

if $a \neq b$ and

$$\mathcal{A}((a, a)) = \mathcal{A}(\{\{a\}\}) = 2^{2^{\mathcal{A}(a)}}$$

Otherwise.
Thus, if f is a function, then

$$\mathcal{A}(f) = \sum_{\substack{(a,b)\in f \\ a\neq b}} 2^{(2^{2^{\mathcal{A}(a)}}(1+2^{2^{\mathcal{A}(b)}}))} + \sum_{\substack{(a,b)\in f \\ a=b}} 2^{2^{2^{\mathcal{A}(a)}}}$$

Therefore the domain and the range of a function f are translated in

$$\mathcal{A}(dom(f)) = \sum_{\substack{a\in A \\ \exists b\in B\,(a,b)\in f}} 2^{\mathcal{A}(a)} \qquad \mathcal{A}(ran(f)) = \sum_{\substack{b\in B \\ \exists a\in A\,(a,b)\in f}} 2^{\mathcal{A}(b)}$$

Theorem 4.1.12. PA' $\vdash \forall x \mathcal{A}(Fin^f(x))$

Proof. We need some preliminary results:

1. There exists a primitive recursive function $f(x)$ that counts the 1-digit in the binary expansion of x.

$$f(x) = \sum_{i<x} rm(qt(x, 2^i), 2)$$

   f is primitive recursive since it is a bounded sum of primitive recursive functions

2. We can define by recursion a function g such that PA' $\vdash \forall x(\mathcal{A}(Nat(y))[g(x)/y]$ as:

$$g(0) = 0$$
$$g(n+1) = g(n) + 2^{g(n)}$$

By composing g with f we obtain a primitive recursive function that sends every natural x of the arithmetic seen as a code for a set, in a natural number which is the code for the cardinality of x. To prove the theorem we need to construct the code of a bijective function from x to $g(f(x))$. We can proceed by complete induction.

- Let $x = 0$, then $h_0 = 0$ is the code of a bijective function from 0 to $g(f(0)) = 0$.
- Suppose that for all $y < x$ there exists a bijection $h : y \to g(h(y))$. Then we can define in the same way as in proof of Proposition 3.2.2 $\square(x)$ and $m(x)$. Therefore there must exists the code for a bijective $h_{\square(x)}$ from $\square(x)$ to $g(f(\square(x)))$. Thus we can define h_x as:

$$h_x = h_{\square(x)} + 2^{<<(m(x), g(f(\square(x))))>>}$$

  where $<< (m(x), g(f(\square(x)))) >>$ is the code for the ordered pair of the sets encoded by $m(x)$ and $g(f(\square(x)))$.
  Now, $dom(h_x) = dom(h_{\square(x)}) + 2^{m(x)} = \square(x) + 2^{m(x)} = x$ and $ran(h_x) = ran(h_{\square(x)}) + 2^{g(f(\square(x)))} = g(f(x))$.

□

We have proved that the Ackermann model **ZF-Inf** proves the axiom of finiteness. By lemmas 4.1.9 and 4.1.10, ZF - Inf + Fin $\vdash$ AC, thus PA' $\vdash \mathcal{A}$(AC).

Corollary 4.1.13. Cons(PA') $\Rightarrow$ Cons(ZF-Inf + Fin)

4.2 An Inverse of Ackermann Translation

In 2007 Kayne and Wong proposed an inverse of the Ackermann interpretation and observed that the definition of this inverse needs the assumption of the ϵ-Induction or the transitive containment. In this section we will develop and present their results, in order to define and inverse of the Ackerman translation defined from **PA** to **ZF - Inf + ¬Inf + TC**. Therefore, for the omitted proof in this section and any further information, we refer to Kaye and Wong[2]

4.2.1 ϵ-Induction and Transitive Containment

In order to define an inverse for the Ackermann translation we need to consider the ϵ-induction.

Definition 4.2.1. For a formula formula $\psi(x, y)$, the epsilon induction affirms:

$$\forall y(\forall x(\forall w \in x\phi(w, y) \to \phi(x, y)) \to \forall x\phi(x, y))$$

$\epsilon-$Induction, however, is not a theorem of **ZF-Inf + ¬Inf**, this can be proved by using the notion of *transitive closure* of a set

Definition 4.2.2. Define $y = TC(x)$ ("y is the transitive closure of x") to be

$$y \supseteq x \wedge Trans(y) \wedge \forall y'(y' \supseteq x \wedge Trans(y') \to y' \supseteq y)$$

TC is the axiom: $\forall x \exists u(x \subseteq u \wedge Trans(u))$

Lemma 4.2.3. ZF-Inf $\vdash \forall x(\exists y(y \supseteq x \wedge Trans(y)) \to \exists y(TC(x) = y))$

Proposition 4.2.4. ϵ-Induction and **TC** are equivalent over **ZF-Inf**

Theorem 4.2.5. TC is independent from **ZF -Inf + ¬Inf**

The assumption of transitive closure is fundamental in order to define an inverse of the Ackermann translation.

Proposition 4.2.6. Let $\mathcal{A}$ be the Ackermann translation. Then PA' $\vdash \mathcal{A}$(TC)

Proof. Let x be a natural, then $2^{x+1} - 1$ satisfies $\mathcal{A}(TC)$. As said in Proposition 3.2.2: PA' $\vdash \forall i(i \leqslant x \to i \Subset 2^{x+1} - 1)$, thus PA' $\vdash x \Subset 2^{x+1} - 1$. Therefore, since PA' $\vdash \forall i \Subset x \forall j \Subset i(j \Subset 2^{x+1} - 1)$, then $2^{x+1} - 1$ is also transitive. Thus,

$$\text{PA'} \vdash \mathcal{A}(TC)$$

□

Remark 4.2.7. Since Proposition 4.2.6 we cannot define an inverse of Ackermann translation without the assumption of the transitive closure. We can prove this by contradiction. Let $\mathcal{B}$ be the inverse of Ackermann translation, i.e. a translation from **PA** onto **ZF-Inf + ¬Inf** such

$$\text{PA'} \vdash \mathcal{A}(\phi) \Rightarrow \text{ZF - Inf} + \neg\text{Inf} \vdash \mathcal{B}(\mathcal{A}(\phi)) = \phi$$

Then, since PA' $\vdash \mathcal{A}$(**TC**) we would have **ZF-Inf+¬Inf** $\vdash \mathcal{B}(\mathcal{A}(\textbf{TC})) = \textbf{TC}$; this would contradicts theorem 4.2.5

4.2.2 The inverse of Ackermann Translation

Now we will report the inverse of the Ackermann translation proposed by Kayne and Wong. The basic idea is similar to the one proposed by us, although there are some differences. Kayne and Wong do not give an explicit translation of the successor function, so they give a translation directly from **ZF-Inf** (which they also define by negating Inf) to **PA**. For the reverse a similar thing happens: they do not give a translation for the successor function, but rather focus on the translation of the order, not defining any intermediate system

Definition 4.2.8. Let, in **ZF-Inf*** :=**ZF - Inf + ¬Inf + TC**, $\mathcal{P}(On)$ denotes the class of sets of ordinals. And let $\hat{\Sigma} : On \times \mathcal{P}(On) \to On$ be the class function defined recursively by

$$\hat{\Sigma}(0, x) = 0$$

for all $x \in \mathcal{P}(On)$, and

$$\hat{\Sigma}(s(c), x) = \begin{cases} \hat{\Sigma}(c, x) & \text{if } s(c) \notin x \\ \hat{\Sigma}(c, x) + s(c) & \text{if } s(c) \in x \end{cases}$$

for all $c \in On$ and $x \in \mathcal{P}(On)$. Also, let $\Sigma : \mathcal{P}(On) \to On$ the function defined by

$$\Sigma(x) = \hat{\Sigma}(\bigcup x, x)$$

Informally, this defines

$$\Sigma(x) = \sum_{y \in x} y$$

In which the sums refers to the ordinal sum. By transfinite induction it is possible to justify the definition of $\hat{\Sigma}$ and Σ

Definition 4.2.9. Define $\mathcal{H}(x) : V \to On$ recursively by

$$\mathcal{H}(x) = \Sigma(\{2^{\mathcal{H}(y)} \in On : y \in x\})$$

To justify the definition of $\mathcal{H}$ we need epsilon induction.

Proposition 4.2.10. **ZF-Inf*** proves that $\mathcal{H}$ is a bijective class function $V \to On$

Definition 4.2.11. We can define the translation $\mathcal{B}$ of **PA** into **ZF-Inf** as

- $\mathcal{B}(a + b) = \mathcal{H}(a) + \mathcal{H}(b)$
- $\mathcal{B}(a \cdot b) = \mathcal{H}(a) \cdot \mathcal{H}(b)$
- $\mathcal{B}(\phi \to \psi) = \mathcal{B}(\phi) \to \mathcal{B}(\psi)$ and $\mathcal{B}(\forall x(\phi))$ is $\forall x \mathcal{B}(\phi)$
- $\mathcal{B}(\phi = \psi)$ is $\mathcal{B}(\phi) = \mathcal{B}(\psi)$
- $\mathcal{B}(x < y)$ is $\mathcal{H}(x) < \mathcal{H}(y)$

In which the target relations and operations of <,+ and × are the usual ones on ordinal.

Proposition 4.2.12. The translation $\mathcal{I}$ and $\mathcal{B}$ are inverse each other

Bibliography

[1] Wilhelm Ackermann. "Die widerspruchsfreiheit der allgemeinen mengenlehre". In: *Mathematische Annalen* 114.1 (1937), pp. 305–315.

[2] Richard Kaye and Tin Lok Wong. "On interpretations of arithmetic and set theory". In: *Notre Dame Journal of Formal Logic* 48.4 (2007), pp. 497–510.

[3] Kenneth Kunen. *Set theory an introduction to independence proofs*. Elsevier, 2014.

[4] Elliott Mendelson. *Introduction to Mathematical Logic*. Chapman and Hall/CRC, 2015.

[5] Richard Pettigrew. "On interpretations of bounded arithmetic and bounded set theory". In: *Notre Dame Journal of Formal Logic* 50.2 (2009), pp. 141–151.

[6] Moto-O. Takahashi. "A Foundation of Finite Mathematics". In: *Publications of The Research Institute for Mathematical Sciences* 12 (1976), pp. 577–708.