Induction Models on $\mathbb{N}$*

A. Dileep[1], Kuldeep S. Meel[2], and Ammar F. Sabili[2]

[1] Indian Institute of Technology Delhi, India
[2] National University of Singapore, Singapore

Abstract

Mathematical induction is a fundamental tool in computer science and mathematics. Henkin [11] initiated the study of formalization of mathematical induction restricted to the setting when the base case B is set to singleton set containing 0 and a unary generating function S. The usage of mathematical induction often involves wider set of base cases and $k-$ary generating functions with different structural restrictions. While subsequent studies have shown several Induction Models to be equivalent, there does not exist precise logical characterization of reduction and equivalence among different Induction Models. In this paper, we generalize the definition of Induction Model and demonstrate existence and construction of S for given B and vice versa. We then provide a formal characterization of the reduction among different Induction Models that can allow proofs in one Induction Models to be expressed as proofs in another Induction Models. The notion of reduction allows us to capture equivalence among Induction Models.

1 Introduction

Mathematical induction is a fundamental tool in automated reasoning, and more broadly in computer science and mathematics [2, 3, 9, 13]. To prove that a mathematical object $\mathcal{A}$ satisfies the property P by mathematical induction, one proceeds by a careful, and often *creative* design of induction hypothesis and associated base case B [11]. The property is first shown to hold over the base case and then shown to hold under induction hypothesis [9]. While mathematical induction is often taught to involve creativity in the design of inductive hypothesis [6, 10], modern automated theorem proves employ mathematical induction as a core technique.

The widespread usage of mathematical induction has led to plethora of Induction Models defined as tuples of base case and the associated generating functions [1, 12]. The existence of plethora of Induction Models begs for a formal analysis of Induction Models. The seminal work of Henkin [11] provided the earliest definition of Induction Model on $\mathbb{N}$ where the base case is restricted 0 and the associated generating function S is unary. Subsequent work of Doornbos, Backhouse, and Woude [5] presented several different formulations of mathematical inductions and demonstrated their equivalence.

Motivated by the usage of several different Induction Models and their equivalence, we carry forth Henkin's work by providing a logical foundation of reduction and equivalence among different Induction Models. To this end, we generalize Henkin's definition of an Induction Model. While designing an appropriate the induction hypothesis may seem matter of human creativity, we discuss the properties of the base case B and generating set S for the tuple $\langle B, S\rangle$ to be a Induction Model. We then discuss reduction and equivalence among different Induction Models. While the focus of this paper is to lay a formal foundation of Induction Models, we briefly discuss motivations and potential applications of the primary contributions of this paper: Theorem 1.1 and Theorem 1.2.

*The author list has been sorted alphabetically by last name; this should not be used to determine the extent of authors contributions.

1.1 What makes $\langle B, S\rangle$ an $\mathbb{N}$-Induction Model?

The first principle of induction can be written as $\langle\{1\}, S : x \to x+1\rangle$. Other examples of models of induction are $\langle\{1,2,\ldots,m\}, S : x \to x+m\rangle$ and $\langle A, S : x \to x-1\rangle$, where A is a infinite subset of $\mathbb{N}$. What subsets $B \subset \mathbb{N}$ and $S : \mathbb{N}^k \to \mathbb{Z}$ can give us an Induction Model? Henkin's formulation[11] defines an Induction Model for the case where the base set contains just the element 0 and the generating function S is unary. We make this definition more general by allowing B to be any subset of $\mathbb{N}$ and S to be a k-ary function, and in particular, formalize the notion of $\mathbb{N}$-induction model.

An important contribution of this paper is study of existence and construction of B for a given S and vice versa under different restrictions on the structure of S. (See Definitions 2.1, 2.2, and 2.3 for the formal definitions of *self-loop function*, *additive structure*, and *multiplicative structure*).

Theorem 1.1. *1. For every non-self loop function $S : \mathbb{N}^k \to \mathbb{Z}$, there exists a $B \subset \mathbb{N}$ such that $\langle B, S\rangle$ is an $\mathbb{N}$-I.M. So this is true for S with additive and multiplicative structures as well.*

2. For any non-empty $B \subset \mathbb{N}$, there exists a function $S : \mathbb{N}^k \to \mathbb{Z}$ (for some k) such that $\langle B, S\rangle$ is an $\mathbb{N}$-I.M. We can find such an S with additive structure as well. If $|B| \geq 2$, this is also true for S with multiplicative structure.

Open Question: Does there always exist S with multiplicative structure for $B = 1$.

Potential Applications The proof of Theorem 1.1 is constructive and provides general recipe for finding S with appropriate structure for a given B and vice versa. We expect such a recipe to lead to algorithmic results in the context of automated mathematical induction [1] providing where one knows that a given property P holds for some generating function S and now needs to find the corresponding B such that once P is shown to hold over B, we can conclude that P holds for all $n \in \mathbb{N}$.

1.2 A Classification Among Induction Models

The following are some well known Induction Models (except maybe Definition 1.4).

Definition 1.1 (First principle of induction)**.** Let $P(n)$ be a statement. If

(i) $P(1)$ is true

(ii) $P(k)$ is true $\implies P(k+1)$ is true

then $P(n)$ is true $\forall\ n \in \mathbb{N}$.

Definition 1.2 (Strong form of induction)**.** Let $P(n)$ be a statement. If

(a) $P(1)$ is true

(b) $P(1), P(2), \ldots, P(k)$ is true $\implies P(k+1)$ is true

then $P(n)$ is true $\forall\ n \in \mathbb{N}$.

Definition 1.3 (Backward induction)**.** Let $A \subseteq \mathbb{N}$ be an infinite subset. If

(c) $P(a)$ is true $\forall\ a \in A$

(d) $P(k)$ is true $\implies$ $P(k-1)$ is true

then $P(n)$ is true $\forall\ n \in \mathbb{N}$.

Definition 1.4 (Prime Induction)**.** Let $\mathbb{P}$ be be the set of all primes. If

(e) $P(a)$ is true $\forall\ a \in \mathbb{P} \cup \{1\}$

(f) $P(i), P(j)$ is true $\implies$ $P(ij)$ is true

then $P(n)$ is true $\forall\ n \in \mathbb{N}$.

It is easy to show that the first principle and strong form of induction are equivalent. If we assume that Definition 1.1 holds, then we could construct a new statement $Q(k) = P(1) \wedge P(2) \wedge \ldots P(k)$. We can apply the first principle on $Q(n)$ to show that $Q(n)$ is true for all $n \in \mathbb{N}$. So, $P(n)$ is true for all $n \in \mathbb{N}$. For the other way, if we know that (i) and (ii) hold, then (a) and (b) also hold. So, Definitions 1.1 and 1.2 are equivalent. Now given any Induction Model, is it equivalent to the first principle of induction? The key to the proof above was coming up with the new statement Q. But it might not be easy to construct one for any general Induction Model. For example, can a similar proof be given for the backward Induction Model and the first principle of induction (if they are equivalent)? To this end, we formalize the concept of reduction and equivalence among different Induction Models. In formally, let $\langle B_1, S_1\rangle$ and $\langle B_2, S_2\rangle$ be two Induction Models, then if $\langle B_1, S_1\rangle$ can be reduced to $\langle B_2, S_2\rangle$ (according to our definition), we show that any proof for a statement $P(n)$ which uses $\langle B_1, S_1\rangle$ can be converted into a proof that uses $\langle B_2, S_2\rangle$. For example, by demonstrating equivalence among the Backward Induction and Prime Induction Models, our method can be used to convert a proof that uses one model into a proof that uses the other one.

If $\langle B, S\rangle$ is an Induction Model, we show in Section 3 that we have $\bigcup_{i=0}^{\infty} S^i(B) = \mathbb{N}$. We can associate a number, $n(\langle B, S\rangle)$, with each Induction Model based on how many times S needs to be applied on B to reach $\mathbb{N}$. For example, for the first principle of induction, we need to apply S $\aleph_0$ many times.

Theorem 1.2. *Let $\langle B_1, S_1\rangle$ and $\langle B_2, S_2\rangle$ be Induction Models. Then, $\langle B_1, S_1\rangle$ can be reduced to $\langle B_2, S_2\rangle$ iff $n(\langle B_1, S_1\rangle) \leq n(\langle B_2, S_2\rangle)$. Moreover, $\langle B_1, S_1\rangle$ is equivalent to $\langle B_2, S_2\rangle$ iff $n(\langle B_1, S_1\rangle) = n(\langle B_2, S_2\rangle)$.*

Potential Applications To the best of our knowledge, Theorem 1.2 provides the first characterization for reduction and equivalence of different Induction Models. The proof of Theorem 1.2 is constructive and provides a recipe to convert a proof in one inductive model to a proof in another inductive model. We perceive such a recipe may be used to compose proofs of different lemmas since being able to reuse parts of the proofs is a major challenge [1].

The rest of the paper is organized as follows: We discuss the notations used in the paper in section 2 and we formally define Induction Models in section 3. We discuss characterisation of Induction Models in section 4, reduction and equivalence in section 5. We finally conclude in section 6.

2 Preliminaries

We first lists the symbols and notations used in this paper on the following table.

Notation	Description
$\emptyset$	Empty set, $\emptyset = \{\}$
B	Base case
I.M.	(abbr. of) Induction Model
$\mathbb{N}$	A set of natural numbers, $\mathbb{N} = \{1, 2, 3, \dots\}$
$\mathbb{N}$-I.M.	(abbr. of) $\mathbb{N}$-Induction Model
$\aleph_0$	The cardinality of $\mathbb{N}$
$\mathbb{P}$	A set of prime numbers, $\mathbb{P} = \{2, 3, 5, 7, 11, \dots\}$
$P(i)$	Property of i
S	Generating function
$\mathbb{Z}$	A set of integers, $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$

For any sets A and B, 2^A denotes the power set of A and $A \setminus B$ denotes set A minus set B, i.e. $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$. We also give some definitions on specific functions called self-loop function, non-self-loop function, function with additive structure, and function with multiplicative structure.

Definition 2.1 (Self-loop and non-self-loop function)**.** A function $F : \mathbb{N}^k \to \mathbb{Z}$ is said to be a self-loop function if for every $(x_1, x_2, \dots x_k) \in \mathbb{N}^k$, $F(x_1, x_2, \dots x_k) \in \{x_1, x_2, \dots x_k\}$. A function which is not a self-loop function is said to be a non-self-loop function.

Remark. Identity function $F(x) = x$ is the only unary self-loop function. Another example of a self-loop function is $F(x_1, x_2, \dots, x_k) = max(\{x_1, x_2, \dots, x_k\})$.

Definition 2.2 (Additive Structure)**.** A function $F : \mathbb{N}^k \to \mathbb{Z}$ is said to have an additive structure if it is of the form:

$$F : (x_1, x_2, \dots x_k) \to a_0 + a_1x_1 + a_2x_2 + \dots a_kx_k$$

where $a_i \in \mathbb{Z}$ and $a_i \neq 0$ for $1 \leq i \leq k$.

Definition 2.3 (Multiplicative Structure)**.** $F : \mathbb{N}^k \to \mathbb{Z}$ is said to have a multiplicative structure if it is of the form:

$$F(x_1, x_2, \dots, x_k) = \sum_{\mathbf{i} \in 2^{[1,k]}} a_{\mathbf{i}} \cdot (\prod_{j \in \mathbf{i}} x_j)$$

where $a_{\mathbf{i}} \in \mathbb{Z}$ and the leading coefficient of F i.e. the coefficient of $x_1x_2 \cdots x_k$ is non-zero.

Example 2.1. *$F : (x, y) \to xy - x - y + 3$ has a multiplicative structure. But, $F : (x, y, z) = x^2yz - xy + z + 2$ does not have multiplicative structure as its first term x^2yz contains a higher power of x.*

Remark. Functions with additive or multiplicative structure cannot be self-loop functions. Proofs can be found in the Appendix (Lemma B.1 and Lemma B.2).

We now define an Induction Model. An Induction Model is identified by its base case and the associated generating function. Formally,

Definition 2.4 (Induction Model (I.M.))**.** A tuple $\langle B, S \rangle$ is said to be an Induction Model with base case B and generating function S if $B \subset \mathbb{N}$ and $S : \mathbb{N}^k \to \mathbb{Z}$

Remark. In particular, $\langle B_0, S_0 \rangle$ denotes the first principle of induction (Definition 1.1), where $B_0 = \{1\}$ and $S_0 : x \to x + 1$. Also, we will call this model to be the 'basic model of induction'.

In the next definition, we define the powers of a generating function acting on a set.

Definition 2.5 (Powers of S)**.** Let $S : \mathbb{N}^k \to \mathbb{Z}$ and $A \subseteq \mathbb{N}$. Let $S^0(A) = A$. Then, powers of S when applied on set A is defined as

$$S^i(A) := \left\{ S(x_1, x_2, \ldots, x_k) : x_1, x_2, \ldots x_k \in \bigcup_{j=0}^{i-1} S^j(A) \right\} \bigcap \mathbb{N}$$

Note that the x_is in the tuple $(x_1, x_2, \ldots, x_k)$ need not to be distinct. Also, notice that each power of S is obtained after intersecting with $\mathbb{N}$. For example, for $S : x \to x-1$ and $A = \{1, 2, 3\}$, we get $S(A) = \{0, 1, 2\}$. But after intersecting this set with $\mathbb{N}$, we get $\{1, 2\}$.

We also define the closure of an I.M. and the difference sets of powers of S.

Definition 2.6 (Closure of an I.M.)**.** Let $\langle B, S\rangle$ be an I.M. then we define the following.

$$Cl_n(\langle B, S\rangle) = \bigcup_{i=0}^{n} S^i(B)$$

In particular, we define $Cl(\langle B, S\rangle) = Cl_\infty(\langle B, S\rangle)$.

Definition 2.7 (Difference sets of powers of S)**.** Let $\langle B, S\rangle$ be an I.M. then we define

$$D_n(\langle B, S\rangle) = S^n(B) \setminus Cl_{n-1}(\langle B, S\rangle)$$

3 $\mathbb{N}$-Induction Models

Henkin [11] gave a definition for an I.M. which involved a base case containing an element 0 and a unary function S. We generalise this in Definition 3.1. It is not hard to see that this definition is equivalent to the condition $Cl(\langle B, S\rangle) = \mathbb{N}$. We prove this in Lemma 3.2.

Definition 3.1 ($\mathbb{N}$-Induction Model ($\mathbb{N}$-I.M.))**.** Let B be a non-empty subset of $\mathbb{N}$ and $S : \mathbb{N}^k \to \mathbb{Z}$. $\langle B, S\rangle$ is said to be an $\mathbb{N}$-Induction Model if the following holds: if $G \subseteq \mathbb{N}$ satisfies

1. $B \subseteq G$, and
2. if $x_1, x_2, \ldots, x_k \in G$ and $S(x_1, x_2, \ldots, x_k) \in \mathbb{N}$, then $S(x_1, x_2, \ldots, x_k) \in G$,

then $G = \mathbb{N}$.

Let us see if the first principle of induction $\langle B_0, S_0\rangle$ satisfies the above definition. Recall that $B_0 = \{1\}$ and $S_0 : x \to x + 1$. Suppose there exists a $G \subseteq \mathbb{N}$ which satisfies conditions 1) and 2) in Definition 3.1, but $G \neq \mathbb{N}$. Let $m \notin G$. Apply S_0 on $1 \in B_0$, $(m-1)$ times, to obtain m. So, $m \in G$, which is a contradiction. So, no such G exists.

Example 3.1. *Let us see an example of $\langle B, S\rangle$ which is not an $\mathbb{N}$-I.M. Consider $\langle \{2\}, S : x \to x + 1\rangle$. This is not an $\mathbb{N}$-I.M. as $G = \mathbb{N} \setminus \{1\}$ satisfies both conditions, but $G \neq \mathbb{N}$.*

For any $\mathbb{N}$-I.M., if S is repeatedly applied on elements of B and the new elements obtained in the previous steps, we should be able to obtain the entire set of natural numbers. We then would expect any $\langle B, S\rangle$ which satisfies Definition 3.1 to satisfy $Cl(\langle B, S\rangle) = \bigcup_{i=0}^{\infty} S^i(B) = \mathbb{N}$. In the next theorem, we prove the equivalence of both these definitions.

Lemma 3.2. *$\langle B, S\rangle$ satisfies Definition 3.1 $\iff$ $Cl(\langle B, S\rangle) = \mathbb{N}$.*

Proof. ($\Longrightarrow$) Suppose $\langle B, S\rangle$ satisfies Definition 3.1. Let $G = \bigcup_{i=0}^{\infty} S^i(B)$. We will show that G satisfies the conditions 1) & 2) in Definition 3.1, which will imply $G = \mathbb{N}$.

1. $B = S^0(B) \in G$.
2. Suppose $x_1, x_2, \ldots x_k \in G$ & $S(x_1, x_2, \ldots x_k) \in \mathbb{N}$. As $x_1, x_2, \ldots x_k \in G$, $x_1, x_2, \ldots x_k \in S^l(B)$ for some $l \geq 0$. As $S(x_1, x_2, \ldots x_k) \in \mathbb{N}$, $S(x_1, x_2, \ldots, x_k) \in S^{l+1}(B) \subseteq G$.

So, $G = \bigcup_{i=0}^{\infty} S^i(B) = \mathbb{N}$.

($\Longleftarrow$) We have $\bigcup_{i=0}^{\infty} S^i(B) = \mathbb{N}$. Suppose $G \subseteq \mathbb{N}$ such that

1. $B \subseteq \mathbb{N}$,
2. if $x_1, x_2, \ldots x_k \in G$ & $S(x_1, x_2, \ldots x_k) \in \mathbb{N}$

then $S(x_1, x_2, \ldots x_k) \in G$. It is enough to show that $\bigcup_{i=0}^{\infty} S^i(B) \subseteq G$.

From 1), $B = S^0(B) \subseteq G$. Suppose for some $m \in \mathbb{N}$, $S^m(B) \not\subseteq G$. For every k-tuple $(x_1, x_2, \ldots x_k) \in S^i(B)$, $S(x_1, x_2, \ldots x_k) \in G$ if $S(x_1, x_2, \ldots x_k) \in \mathbb{N}$. So $S^{i+1}(B) \subseteq G$. By applying S on B, m times, we get $S^m(B) \subseteq G$, which is a contradiction. So, $S^m(B) \subseteq G$ $\forall m \in \mathbb{N}$. Hence, $\bigcup_{i=0}^{\infty} S^i(B) = \mathbb{N} \subseteq G$. But, $G \subseteq \mathbb{N}$. So, $G = \mathbb{N}$. □

4 Characterisation of $\mathbb{N}$-Induction Models

In this section, we look at which $B \subset \mathbb{N}$ and $S : \mathbb{N}^k \to \mathbb{Z}$ combine to give an $\mathbb{N}$-I.M. $\langle B, S\rangle$. To start with, in subsection 4.1, we consider any general S, with no restrictions on its structure. Then in subsections 4.2 and 4.3, we look at S with 'additive' and 'multiplicative' structures respectively. We put these restrictions as the models which can be used practically tend to have generating functions with these type of structures.

We first describe a type of S which can never give us an $\mathbb{N}$-I.M. That is, $\langle B, S\rangle$ is not an $\mathbb{N}$-I.M. for any $B \subset \mathbb{N}$.

Lemma 4.1. *If $\langle B, S\rangle$ is an $\mathbb{N}$-I.M., S cannot be a self-loop function.*

Proof. Suppose S is a self-loop function. Consider $G = B$.

1. Clearly, $B \subseteq G$
2. For $x_1, x_2, \ldots x_k \in G(= B)$, $S(x_1, x_2, \ldots, x_k) \in \{x_1, x_2, \ldots x_k\}$. So, $S(x_1, x_2, \ldots, x_k) \in \mathbb{N}$. Clearly, $S(x_1, x_2, \ldots x_k) \in G$.

As $\langle B, S\rangle$ is an $\mathbb{N}$-I.M., we have $G = \mathbb{N}$, which is a contradiction. □

In the next sub-section, we look at the case where there are no restrictions put on the structure of S.

4.1 For any arbitrary S

We show in Lemma 4.2 that for every non-empty $B \subset \mathbb{N}$, there exists a non-self-loop function S such that $\langle B, S\rangle$ is an $\mathbb{N}$-I.M. In Lemma 4.4, we show that for every non-self-loop function S, there exists a $B \subset \mathbb{N}$ such that $\langle B, S\rangle$ is an $\mathbb{N}$-I.M.

Lemma 4.2. *For every non-empty $B \subset \mathbb{N}$, there exists a non-self-loop function S such that $\langle B, S\rangle$ is an $\mathbb{N}$-I.M.*

Proof. We have two cases: either B is a finite set or B is an infinite subset of $\mathbb{N}$.

Case 1: When B is finite.

If $1 \in B$, we can take $S : x \to x+1$. As $i \in S^{i-1}(B)$ for each $i \in \mathbb{N}$, $\mathbb{N} \subseteq \bigcup_{i=0}^{\infty} S^i(B)$. As $S^i(B) \subseteq \mathbb{N}$ for all $i \in \mathbb{N} \cup \{0\}$, $\bigcup_{i=0}^{\infty} S^i(B) = \mathbb{N}$. So, due to Theorem 3.2, $\langle B, S\rangle$ is an $\mathbb{N}$-I.M.

If $1 \notin B$, let $b = min(B)$. Consider

$$S(x) = \begin{cases} 1, & \text{if } x = b \\ b+1, & \text{if } x = b-1 \\ x+1, & \text{otherwise} \end{cases}$$

$S(b-1) = b+1$ is necessary. Without it, S will take $b-1$ to b and b is mapped to 1. So, we will not be able to generate elements greater than b.

Observe that $\{1, 2, \ldots, b+1\} \subset \bigcup_{i=0}^{b} S^i(B)$. Also, for each $i \geq b+2$, $i \in S^{i-1}(B)$. So, $\mathbb{N} \subseteq \bigcup_{i=0}^{\infty} S^i(B)$.

Case 2: When B is infinite.

Use $S : x \to x-1$. This is nothing but the backward induction. The detailed proof can be found in the Appendix (Lemma A.1). □

In the proof of the previous lemma, we used a unary S. We can extend it to say that for every k, such a k-ary S exists.

Lemma 4.3. *For every non-empty $B \subset \mathbb{N}$, there exists a k-ary non-self-loop function $S' : \mathbb{N}^k \to \mathbb{Z}$, for every k, such that $\langle B, S'\rangle$ is an $\mathbb{N}$-I.M.*

The proof for the above lemma can be found in the Appendix (section C).

Lemma 4.4. *For every non-self-loop function $S : \mathbb{N}^k \to \mathbb{Z}$, there exists a $B \subset \mathbb{N}$ such that $\langle B, S\rangle$ is an $\mathbb{N}$-I.M. So this holds for S with additive and multiplicative structure as well.*

Proof. As S is a non-self-loop function, $\exists\ (x_1, x_2, \ldots x_k) \in \mathbb{N}^k$ such that $S(x_1, x_2, \ldots x_k) \notin \{x_1, x_2, \ldots x_k\}$. Say $S(x_1, x_2, \ldots x_k) = a$. Take $B = \mathbb{N} \setminus \{a\}$. $x_1, x_2, \ldots x_k \in B$ as none of them is equal to a. So, $a \in S(B)$, which implies $B \cup S(B) \subseteq \mathbb{N}$. So, $\bigcup_{i=0}^{\infty} S^i(B) = \mathbb{N}$. □

In the proof of Lemma 4.2, in the case where B is finite and $1 \notin B$, we used the following generating function:

$$S(x) = \begin{cases} 1, & \text{if } x = b \\ b+1, & \text{if } x = b-1 \\ x+1, & \text{otherwise} \end{cases}$$

If we are trying to prove that a property $P(n)$ is true for all $n \in \mathbb{N}$, using induction, it is very unlikely that one would be able to show that $P(b) \implies P(1)$, $P(b-1) \implies P(b+1)$ and $P(x) \implies P(x+1)$ for all other x. While trying to prove properties/statements using induction, it could be useful to have some kind of a structure for S. In the following sub-sections, we look at S with 'additive' and 'multiplicative' structures.

4.2 S with Additive Structure

Let us see for which $B \subset \mathbb{N}$ and $S : \mathbb{N}^k \to \mathbb{Z}$, $\langle B, S\rangle$ is an $\mathbb{N}$-I.M. The results for a unary S and k-ary ($k \geq 2$) S are different. Let us look at the unary case to start with.

Lemma 4.5. *For a unary function $S : \mathbb{N} \to \mathbb{Z}$ with additive structure, $\langle B, S\rangle$ is an $\mathbb{N}$-I.M. iff B contains 1 or B is an infinite subset of $\mathbb{N}$.*

Proof. ($\implies$) Suppose $\langle B, S\rangle$ is an $\mathbb{N}$-I.M., where S is unary. A unary S with additive structure is of the form $S : x \to a_0 + a_1 x$. Observe that this function is monotonic i.e. it is either increasing or decreasing. If it is increasing, B should contain 1. If $1 \notin B$, 1 cannot be generated by an increasing function. If S is decreasing, then B has to be an infinite subset of $\mathbb{N}$. Otherwise, if B is finite, all elements greater than $max(B)$ cannot be generated.

($\impliedby$) If B contains 1, consider $S : x \to x + 1$. If B is an infinite subset of $\mathbb{N}$, $S : x \to x - 1$ would give us an $\mathbb{N}$-I.M. □

Let us now look at the k-ary ($k \geq 2$) case. In this case, no restrictions are required on B. For every non-empty B, we can find such an S.

Lemma 4.6. *For every non-empty $B \subset \mathbb{N}$, there exists a k-ary ($k \geq 2$) S with additive structure such that $\langle B, S\rangle$ is an $\mathbb{N}$-I.M.*

Proof. Say $q \in B$. Consider $S : (x, y) \to x - y + (q + 1)$. Take $y = q$ to get $S(x, q) = x + 1$. So, $\{q, q+1, q+2, \ldots\} \subseteq \bigcup_{i=0}^{\infty} S^i(B)$. Now we put $y = q + 2$, to get, $S(x, q + 2) = x - 1$. This implies $\{q - 1, q - 2, \ldots, 1\} \subseteq \bigcup_{i=3}^{q+1} S^i(B)$. So, $\mathbb{N} \subseteq \bigcup_{i=0}^{\infty} S^i(B)$. □

This lemma can be extended to show that such a k-ary S exists for every $k \geq 2$. One might think of using $S' : (x_1, x_2, \ldots, x_k) \to S(x_1, x_2)$, where S is the generating function used in Lemma 4.6 for proving this statement. But, for S', $a_i = 0$ for $i \geq 3$ and hence doesn't have an additive structure.

Lemma 4.7. *For every non-empty $B \subset \mathbb{N}$ and every $k \geq 2$, there exists a S with additive structure such that $\langle B, S\rangle$ is an $\mathbb{N}$-I.M.*

The proof for the above lemma can be found in the Appendix (section C).

Remark. We could also use the following generating function to give an alternate proof for the above lemma.

$$S : (x_1, x_2, \ldots, x_k) \to 2x_1 + x_2 + x_3 + \ldots + x_{k-1} - (k-1)x_k + 1$$

Put $x_2 = x$, $x_1 = x_3 = \ldots = x_k = q$ to get $S(q, x, q, \ldots, q) = x + 1$. Then, put $x_1 = q, x_2 = x, x_3 = x_4 = \ldots = x_k = (q + 1)$ to get $S(q, x, q + 1, q + 1, \ldots, q + 1) = x - 1$.

4.3 S with Multiplicative Structure

Consider this example which shows a generating function S having a 'multiplicative' structure.

Example 4.8. *Let $B = \mathbb{P} \cup \{1\}$ and $S : (x, y) \to xy$. We can use the fact that every natural number can be written as a product of primes to show that this is an $\mathbb{N}$-I.M. A detailed proof can be found in the Appendix (Lemma A.2).*

We will now show that for every $B \subset \mathbb{N}$ containing at least 2 elements, there exists an S with multiplicative structure such that $\langle B, S\rangle$ is an $\mathbb{N}$-I.M. Before that, we will prove a lemma which will be useful for proving this result.

Lemma 4.9. *For every $B \subset \mathbb{N}$ containing two consecutive natural numbers, there exists a non-self-loop function S with multiplicative structure such that $\langle B, S\rangle$ is an $\mathbb{N}$-I.M.*

Proof. Say $q - 1, q \in B$. Consider the following S:

$$S : (x, y) \to xy + y - yq + 1$$

Put $x = y = (q - 1)$ to get $S(q - 1, q - 1) = (q - 1)(q - 1) + (q - 1) - (q - 1)q + 1 = 1$. Now, put $x = q$ to get, $S(q, y) = y + 1$. As $1 \in S(B)$, $i \in S^i(B)\ \forall\ i \in \mathbb{N}$. □

We now prove the main lemma.

Lemma 4.10. *For every $B \subset \mathbb{N}$ containing at least two elements, there exists a non-self-loop function S with multiplicative structure such that $\langle B, S\rangle$ is an $\mathbb{N}$-I.M.*

Proof. Say $p, q \in B$, where $p < q$. Consider the same S as in Lemma 4.9. Put $x = q$ to get $S(q, y) = y + 1$. So, every $i > p$ can be generated, which implies $q - 1$ can also be generated. Now, we can use the same argument as in Lemma 4.9. In this case, $i \in S^{(q-p-1)+i}\ \forall\ i \in \mathbb{N}$. □

Like before, we can extend this lemma to say that for every $k \geq 2$, a k-ary S with multiplicative structure exists, which together with B, gives us an $\mathbb{N}$-I.M.

Lemma 4.11. *For every $B \subset \mathbb{N}$ containing at least two elements, there exists a k-ary S with multiplicative structure, for every k, such that $\langle B, S\rangle$ is an $\mathbb{N}$-I.M.*

The proof for the above lemma can be found in the appendix (section C).
The main results of this section are summarized in the following theorem.

Theorem 1.1.
1. *For every non-self loop function $S : \mathbb{N}^k \to \mathbb{Z}$, there exists a $B \subset \mathbb{N}$ such that $\langle B, S\rangle$ is an $\mathbb{N}$-I.M. So this is true for S with additive and multiplicative structures as well.*
2. *For any non-empty $B \subset \mathbb{N}$, there exists a function $S : \mathbb{N}^k \to \mathbb{Z}$ (for some k) such that $\langle B, S\rangle$ is an $\mathbb{N}$-I.M. We can find such an S with additive structure as well. If $|B| \geq 2$, this is also true for S with multiplicative structure.*

5 Reduction and Equivalence of Induction Models

In this section, we give a definition for reduction and equivalence between I.M.s (Subsection 5.1) and we prove a criterion which can be used to determine if one I.M. can be reduced to another or if they are equivalent (Subsection 5.2).

5.1 Reduction and Equivalence of Induction Models

Before defining reduction, we need to describe how to obtain an injective version of a generating function and its properties.

Definition 5.1 (Smallest power of S for x)**.** For an I.M. $\langle B, S\rangle$, we define

$$l(x, \langle B, S\rangle) = min\{i \geq 0 : x \in S^i(B)\}$$

Definition 5.2 (Injective version of S)**.** Consider the I.M. $\langle B, S\rangle$, where S is k-ary.

For every $x \in Cl(\langle B, S\rangle) \setminus B$, choose a tuple $\mathbf{n_x} = (n_1, n_2, \ldots, n_k) \in S^{l(x,\langle B,S\rangle)-1}$ such that $S(n_1, n_2, \ldots, n_k) = x$. Then the following is an injective version of S.

$$S_{inj}(\mathbf{n}) = \begin{cases} S(\mathbf{n}), & \text{if } \mathbf{n} = \mathbf{n_x}, \text{ for some x } \in Cl(\langle B, S\rangle) \setminus B \\ 0, & \text{otherwise} \end{cases}$$

Note that $S_{inj}(\mathbf{n}) = 0$ if $S(\mathbf{n}) \in B$ or $S(\mathbf{n}) \notin \mathbb{N}$.

Remark. We will use S_{inj} to denote the injective version of a generating function S.

Example 5.1. *Unary, additive $S : \mathbb{N} \to \mathbb{Z}$ are of the form $S(x) = a_0 + a_1 x$, where $a_0, a_1 \in \mathbb{Z}$. Let $S(x_1) = S(x_2)$. That means $a_0 + a_1 x_1 = a_0 + a_1 x_2$ or $x_1 = x_2$. So S is injective, which means*

$$S_{inj}(x) = \begin{cases} S(x), & \textit{when } x \in \mathbb{N} \\ 0, & \textit{otherwise} \end{cases}$$

Lemma 5.2. *Let $x \in Cl(\langle B, S\rangle) \setminus B$. Then, $l(x, \langle B, S\rangle) = m$ iff $x \in D_m(\langle B, S_{inj}\rangle)$.*

Proof. The proof can be found in the appendix (section D). □

Lemma 5.3. *Let $\langle B, S\rangle$ be an I.M. Then, ${S^i}_{inj}(B) = S^i(B) \setminus B$ for all $i \geq 1$.*

Proof. The proof can be found in the appendix (section D). □

Proposition 5.4. *For any I.M. $\langle B, S\rangle$, we have $Cl(\langle B, S\rangle) = Cl(\langle B, S_{inj}\rangle)$.*

Proof. By definition, $Cl(\langle B, S_{inj}\rangle) = \bigcup_{i=0}^{\infty} {S^i}_{inj}(B)$. As ${S^i}_{inj}(B) = S^i(B) \setminus B$ for all $i \geq 1$, $\bigcup_{i=0}^{\infty} {S^i}_{inj}(B) = \bigcup_{i=1}^{\infty} \left[S^i(B) \setminus B\right] \bigcup B = \bigcup_{i=0}^{\infty} S^i(B) = Cl(\langle B, S\rangle)$ □

Lemma 5.5. *If $\langle B, S\rangle$ is an $\mathbb{N}$-I.M., then $\langle B, S_{inj}\rangle$ is also an $\mathbb{N}$-I.M.*

Proof. It follows from Proposition 5.4 and Lemma 3.2. □

We now give a definition for reduction between Induction Models.

Definition 5.3. Let $\langle B_1, S_1\rangle$ and $\langle B_2, S_2\rangle$ be two I.M.s. $\langle B_1, S_1\rangle$ can be reduced to $\langle B_2, S_2\rangle$ if there exists a relation $R : Cl(\langle B_2, S_2\rangle) \to 2^{Cl(\langle B_1, S_1\rangle)}$ such that:

1. $\bigcup_{x \in Cl(\langle B_2, S_2\rangle)} R(x) = Cl(\langle B_1, S_1\rangle)$

2. $\bigcup_{x\in B_2} R(x) = B_1$
3. If $x \in Cl(\langle B_2, S_2\rangle) \setminus B_2$, we have $x = S_{2_{inj}}(n_1, n_2, \ldots, n_k)$ where $(n_1, n_2, \ldots, n_k) \in \mathbb{N}^k$. We define
$$R(x) = S_1(\bigcup_{i=1}^{k_2} R(n_i)) \cup \left[\bigcup_{i=1}^{k_2} R(n_i))\right]$$

An example that motivates this definition has been given in the appendix (Section E).

In the above definition, in (3), S_1 (a k_1-ary function) acts on the set $\bigcup_{i=1}^{k_2} R(n_i)$. This is defined even if this set contains less than k_1 elements. S_1 can act on a tuple $\mathbf{n} = (x_1, x_2, \ldots, x_{k_1})$ even if x_is are not all distinct (see Definition 2.5).

Remark. Let A and B be two sets. Then to denote $x \to B$ or $R(x) = B$ for each $x \in A$, we will use $A \to B$ or $R(A) = B$.

Example 5.6. *Consider the following $\mathbb{N}$-I.M.s: $\langle B_1, S_1\rangle = \langle \mathbb{P}, x \to x - 1\rangle$ and $\langle B_2, S_2\rangle = \langle \{1, 2, 3, 4, 5\}, x \to x + 5\rangle$. Recall that $\mathbb{P}$ denotes the set of primes. We will show that $\langle B_1, S_1\rangle$ can be reduced to $\langle B_2, S_2\rangle$. Notice that S_2 is injective. So, $S_{2_{inj}} = S_2$. Consider the following relation, R:*

$$\{1, 2, 3, 4, 5\} \to \mathbb{P}$$
$$\{5n + 1, 5n + 2, 5n + 3, 5n + 4, 5n + 5\} \to \{p - i : 1 \le i \le n, p \in \mathbb{P}\} \cap \mathbb{N}$$

Here, $Cl(\langle B_1, S_1\rangle) = Cl(\langle B_2, S_2\rangle) = \mathbb{N}$.

1. $\bigcup_{x\in Cl(\langle B_2,S_2\rangle)} R(x) = \bigcup_{x\in\mathbb{N}} \{p - i : 1 \le i \le x, p \in \mathbb{P}\} \cap \mathbb{N} = \mathbb{N}$
2. $\bigcup_{x\in\{1,2,3,4,5\}} R(x) = \mathbb{P}$
3. *Let $x \in \mathbb{N}\setminus B_2$. Then $x = 5a+b$, where $a > 0$ and $1 \le b \le 5$. We have $x = S_2(5(a-1)+b)$.*

$$\begin{aligned}
&S_1(R(5(a-1)+b)) \cup R(5(a-1)+b)\\
&= [S_1(\{p - i : 1 \le i \le (a-1), p \in \mathbb{P}\}) \cup \{p - i : 1 \le i \le (a-1), p \in \mathbb{P}\}] \cap \mathbb{N}\\
&= [\{p - i : 2 \le i \le a, p \in \mathbb{P}\} \cup \{p - i : 1 \le i \le (a-1) \in \mathbb{P}\}] \cap \mathbb{N}\\
&= [\{p - i : 1 \le i \le a, p \in \mathbb{P}\}] \cap \mathbb{N}\\
&= R(5a + b)
\end{aligned}$$

Example 5.7. *Suppose $\langle B_1, S_1\rangle$ can be reduced to $\langle B_2, S_2\rangle$. If $\langle B_2, S_2\rangle$ is an $\mathbb{N}$-I.M., then does it imply that $\langle B_1, S_1\rangle$ is also an $\mathbb{N}$-I.M.?*

The answer is no. Let $\langle B_1, S_1\rangle = \langle \{2\}, x \to x + 2\rangle$ and $\langle B_2, S_2\rangle = \langle \{1\}, x \to x + 1\rangle$. Notice that S_1 and S_2 are injective. Consider the following relation: $R(x) = \{2, 4, \ldots, 2(x - 1), 2x\}$. We get $Cl(\langle B_1, S_1\rangle) = \{2n : n \in \mathbb{N}\}$ and $Cl(\langle B_2, S_2\rangle) = \mathbb{N}$. Conditions 1 & 2 (in Definition 5.3) are clearly true. To see 3), suppose $x \neq 1$ and $x \in Cl(\langle B_2, S_2\rangle)$. We have $x = S_2(x - 1)$.

$$\begin{aligned}
S_1(R(x-1)) \cup R(x-1) &= S_1(\{2, 4, \ldots, 2(x-1)\}) \cup \{2, 4, \ldots, 2(x-1)\}\\
&= \{4, 6, \ldots, 2x\} \cup \{2, 4, \ldots, 2(x-1)\}\\
&= \{2, 4, \ldots, 2(x-1)\} = R(x)
\end{aligned}$$

So, $\langle B_1, S_1\rangle$ can be reduced to $\langle B_2, S_2\rangle$. Here, $\langle B_2, S_2\rangle$ is an $\mathbb{N}$-I.M., but $\langle B_1, S_1\rangle$ is not.

Definition 5.4. Two I.M.s $\langle B_1, S_1\rangle$ and $\langle B_2, S_2\rangle$ are said to be equivalent if:

1. $\langle B_1, S_1\rangle$ can be reduced to $\langle B_2, S_2\rangle$
2. $\langle B_2, S_2\rangle$ can be reduced to $\langle B_1, S_1\rangle$

Example 5.8. *In Example 5.6, we showed that $\langle B_1, S_1\rangle$ can be reduced to $\langle B_2, S_2\rangle$. We can also show that $\langle B_2, S_2\rangle$ can be reduced to $\langle B_1, S_1\rangle$ which implies that $\langle B_1, S_1\rangle$ and $\langle B_2, S_2\rangle$ are equivalent. (For details, see F).*

Example 5.9. *In Example 5.7, we can use $R(x) = \{x/2, x/2-1, \ldots, 1\}$ to show that $\langle B_2, S_2\rangle$ can be reduced to $\langle B_1, S_1\rangle$. So, $\langle\{2\}, x \to x+2\rangle$ and $\langle\{1\}, x \to x+1\rangle$ are equivalent.*

In the next example, we present an I.M. which can be reduced to $\langle B_0, S_0\rangle$, but $\langle B_0, S_0\rangle$ cannot be reduced to that I.M.

Example 5.10. *Let $B = \mathbb{N} \setminus \{2\}$.*

$$S(x) = \begin{cases} 10, & \text{when } x = 1 \text{ or } 5 \\ x-1, & \text{otherwise} \end{cases}$$

Consider the following relation, R:

$$x \to Cl_{x-1}(\langle B, S\rangle)$$

1. $\bigcup\limits_{x\in\mathbb{N}} R(x) = Cl_\infty(\langle B, S\rangle) = Cl(\langle B, S\rangle)$
   $S^0(B) = \mathbb{N} \setminus \{2\}$. $S(3) = 2$. *So,* $\{2\} \subseteq S(B)$ *which gives us* $\bigcup\limits_{x\in\mathbb{N}} R(x) = \mathbb{N}$.
2. $\bigcup\limits_{x\in\{1\}} R(x) = B$
3. S_0 *is injective. For* $x \in \mathbb{N} \setminus \{1\}$, $x = S(x-1)$.

$$\begin{aligned} S(R(x-1)) \cup R(x-1) &= S(Cl_{x-2}(\langle B, S\rangle)) \bigcup Cl_{x-2}(\langle B, S\rangle) \\ &= S^{x-1}(B) \bigcup Cl_{x-2}(\langle B, S\rangle) = Cl_{x-1}(\langle B, S\rangle) = R(x) \end{aligned}$$

So, $\langle B, S\rangle$ can be reduced to $\langle B_0, S_0\rangle$.

Let us now see if $\langle B_0, S_0\rangle$ can be reduced to $\langle B, S\rangle$. For a relation, R, satisfying Definition 5.3 to exist, we need $R(n) = 1$ for $n \in \mathbb{N} \setminus \{2\}$ (from the second condition) and $R(2) = \mathbb{N} \setminus \{1\}$ (from first condition). The S_{inj} is given by:

$$S_{inj} = \begin{cases} x-1, & \text{for } x = 3 \\ 0, & \text{otherwise} \end{cases}$$

From the third condition, as $2 = S_{inj}(3)$, we have $R(2) = S_0(R(3)) \cup R(3) = S_0(1) \cup \{1\} = \{1, 2\} \neq \mathbb{N} \setminus \{1\}$. So, such an R does not exist.

5.2 Checking Reducibility and Equivalence of Two Induction Models

In this section, we present a criterion to determine if one I.M. can be reduced to another (Theorem 1.2). It immediately follows from this theorem that every I.M. can be reduced to the basic model of induction. Now, we will give a few definitions and lemmas which will be useful in proving that result.

In Example 5.10, $B \cup S(B) = \mathbb{N}$. Whereas for the first principle of induction i.e. $\langle B_0, S_0\rangle = \langle\{1\}, x \to x+1\rangle$, S_0 needs to be applied infinitely on B_0 to obtain $\mathbb{N}$. We formally define this in the next definition.

Definition 5.5 (Number of Steps of an I.M.)**.** For an I.M. $\langle B, S\rangle$, we define

$$n(\langle B, S\rangle) = min\{i \geq 1 : D_i(\langle B, S\rangle) = \emptyset\}$$

Lemma 5.11. *Let $\langle B, S\rangle$ be an I.M. Then, $D_i(\langle B, S\rangle) = \emptyset \ \forall \ i \geq n(\langle B, S\rangle)$.*

Proof. The proof can be found in the appendix (Section D). □

Remark. Another way to look at $n(\langle B, S\rangle)$ is: $n(\langle B, S\rangle) = |\{i \geq 1 : D_i(\langle B, S\rangle) \neq \emptyset\}| + 1$.

Let $U = \{i \geq 1 : D_i(\langle B, S\rangle) \neq \emptyset\}$. If U is an infinite set, as $U \subseteq \mathbb{N}$, it has the same cardinality as $\mathbb{N}$. So, in cases where the minimum does not exist in Definition 5.5, we set $n(\langle B, S\rangle) = \aleph_0 + 1 = \aleph_0$.

Also, in fact, $U = \mathbb{N}$ when U is infinite. Let $n \in \mathbb{N}$. If $D_n(\langle B, S\rangle)$ is empty, then U is finite, which gives us a contradiction. So, it is non-empty. This implies that $n \in U$. As n is arbitrary, we have $\mathbb{N} \subseteq U$. But $U \subseteq \mathbb{N}$, which gives us $U = \mathbb{N}$.

Proposition 5.12. *Let $\langle B, S\rangle$ be an Induction Model. Then $Cl_{n(\langle B,S\rangle)-1}(\langle B, S\rangle) = Cl(\langle B, S\rangle)$.*

Proof. By definition, $\bigcup_{i=0}^{\infty} S^i(B) = Cl(\langle B, S\rangle)$. For $i \geq n(\langle B, S\rangle)$, we have $S^i(B) \setminus Cl_{n(\langle B,S\rangle)-1}(\langle B, S\rangle) = \bigcup_{j=n(\langle B,S\rangle)}^{i} S^j(B) \setminus Cl_{j-1}(\langle B, S\rangle)$, which is an empty set. So, $Cl_{n(\langle B,S\rangle)-1} = Cl(\langle B, S\rangle)$. □

Lemma 5.13. *Let $\langle B, S\rangle$ be an Induction Model. Then, $n(\langle B, S\rangle) = n(\langle B, S_{inj}\rangle)$.*

Proof. Suppose $n(\langle B, S_{inj}\rangle) < n(\langle B, S\rangle)$. From Lemma 5.12, we have $Cl_{n(\langle B,S\rangle)-1}(\langle B, S\rangle) = Cl(\langle B, S\rangle)$. This implies

$$\begin{aligned} Cl(\langle B, S\rangle) &= Cl(\langle B, S_{inj}\rangle) = Cl_{n(\langle B,S_{inj}\rangle)-1}(B, S_{inj}) \\ &\subseteq Cl_{n(\langle B,S_{inj}\rangle)-1}(\langle B, S\rangle) \qquad \text{(as } S^i{}_{inj}(B) = S^i(B) \setminus B \subseteq S^i(B)\text{)} \\ &\subseteq Cl(\langle B, S\rangle) \end{aligned}$$

This gives us $Cl_{n(\langle B,S_{inj}\rangle)-1}(\langle B, S\rangle) = Cl(\langle B, S\rangle)$. So, $D_i(\langle B, S\rangle) = \emptyset$ for $i = n(\langle B, S_{inj}\rangle) < n(\langle B, S\rangle)$, which is a contradiction. So, we have $n(\langle B, S_{inj}\rangle) \geq n(\langle B, S\rangle)$.

If $n(\langle B, S_{inj}\rangle) > n(\langle B, S\rangle)$, then $D_{n(\langle B,S\rangle)}(\langle B, S_{inj}\rangle) \neq \emptyset$.

$$D_{n(\langle B,S\rangle)}(\langle B, S_{inj}\rangle) = \left[S^{n(\langle B,S\rangle)}(B) \setminus B\right] \setminus \left[B \cup \bigcup_{i=1}^{n(\langle B,S\rangle)-1} (S^i(B) \setminus B)\right]$$

$$= \left[S^{n(\langle B,S\rangle)}(B) \setminus B\right] \setminus \bigcup_{i=0}^{n(\langle B,S\rangle)-1} S^i(B) = S^{n(\langle B,S\rangle)}(B) \setminus \bigcup_{i=0}^{n(\langle B,S\rangle)-1} S^i(B) = D_{n(\langle B,S\rangle)}(\langle B, S\rangle)$$

So, $D_{n(\langle B,S\rangle)}(\langle B, S\rangle) \neq \emptyset$, which is a contradiction. Therefore, $n(\langle B, S_{inj}\rangle) = n(\langle B, S\rangle)$. □

Proposition 5.14. *For $n \neq m$, $D_n(\langle B, S\rangle) \cap D_m(\langle B, S\rangle) = \emptyset$.*

Proof. Say $n > m$. $D_n(\langle B, S\rangle) = S^n(B) \setminus \bigcup_{i=0}^{n} S^i(B)$. So, $D_n(\langle B, S\rangle) \cap S^m(B) = \emptyset$, which implies $D_n(\langle B, S\rangle) \cap \left[S^m(B) \setminus \bigcup_{i=0}^{m-1} S^i(B)\right] = \emptyset$. Therefore, $D_n(\langle B, S\rangle) \cap D_m(\langle B, S\rangle) = \emptyset$. □

We now prove the criteria for reduction and equivalence.

Theorem 1.2. *Let $\langle B_1, S_1\rangle$ and $\langle B_2, S_2\rangle$ be Induction Models. Then, $\langle B_1, S_1\rangle$ can be reduced to $\langle B_2, S_2\rangle$ iff $n(\langle B_1, S_1\rangle) \leq n(\langle B_2, S_2\rangle)$. Moreover, $\langle B_1, S_1\rangle$ is equivalent to $\langle B_2, S_2\rangle$ iff $n(\langle B_1, S_1\rangle) = n(\langle B_2, S_2\rangle)$.*

Proof. ($\Longrightarrow$) Suppose $n(\langle B_1, S_1\rangle) \leq n(\langle B_2, S_2\rangle)$. Consider the following relation, R:

$$
\begin{gathered}
B_2 \to B_1 \\
D_1(\langle B_2, {S_2}_{inj}\rangle) \to Cl_1(\langle B_1, S_1\rangle) \\
D_2(\langle B_2, {S_2}_{inj}\rangle) \to Cl_2(\langle B_1, S_1\rangle) \\
\vdots \\
D_{n(\langle B_1,S_1\rangle)}(\langle B_2, {S_2}_{inj}\rangle) \to Cl_{n(\langle B_1,S_1\rangle)}(\langle B_1, S_1\rangle) \\
\vdots \\
D_{n(\langle B_2,S_2\rangle)}(\langle B_2, {S_2}_{inj}\rangle) \to Cl_{n(\langle B_2,S_2\rangle)}(\langle B_2, S_2\rangle)
\end{gathered}
$$

1. $\bigcup_{x\in\mathbb{N}} R(x) = \bigcup_{i=0}^{n(\langle B_2,S_2\rangle)} \bigcup_{x\in D_i(\langle B,S\rangle)} R(x) = \bigcup_{i=0}^{n(\langle B_2,S_2\rangle)} {S_1}^i(B_1) = \bigcup_{i=0}^{n(\langle B_1,S_1\rangle)} {S_1}^i(B_1) = Cl(\langle B_1, S_1\rangle)$

2. $\bigcup_{x\in B_2} R(x) = B_1$

3. Let $x \in \mathbb{N} \setminus B_2$. Say $x \in D(\langle B_2, {S_2}_{inj}\rangle, m)$. Then, from Lemma 5.2, $l(\langle B, S\rangle, x) = m$. Let $x = {S_2}_{inj}(n_1, n_2, \ldots, n_{k_2})$, where $n_i \in Cl_{m-1}(\langle B, S\rangle)$. But at least one of the n_is lies in $D_{m-1}(\langle B, S\rangle)$, otherwise $l(\langle B, S\rangle, x) < m$ which is a contradiction. So, $S_1(\bigcup_{i=1}^{k_2} R(n_i) \bigcup \left[\bigcup_{i=1}^{k_2} R(n_i)\right] = S_1(Cl_{m-1}(\langle B_1, S_1\rangle)) \cup [Cl_{m-1}(\langle B_1, S_1\rangle)] = {S_1}^m(B) \cup Cl_{m-1}(\langle B_1, S_1\rangle) = Cl_m(\langle B_1, S_1\rangle)$

($\Longleftarrow$) Suppose $\langle B_1, S_1\rangle$ can be reduced to $\langle B_2, S_2\rangle$. Let us assume that $n(\langle B_1, S_1\rangle) > n(\langle B_2, S_2\rangle)$ or $n(\langle B_2, S_2\rangle) < n(\langle B_1, S_1\rangle)$. As $\langle B_1, S_1\rangle$ can be reduced to $\langle B_2, S_2\rangle$, $\exists$ a relation R satisfying the conditions in Definition 5.3. We have $R(B_2) = B_1$ (from second condition). It follows from the third condition that $R({S_2}_{inj}(B_2)) \subseteq S_1(B_1) \cup B$.
Our claim is that $R(D_k(\langle B_2, {S_2}_{inj}\rangle) \subseteq Cl_k(\langle B_1, S_1\rangle)$ for $k \geq 1$. We will use induction to show

this. For $i = 1$, the statement is true. Assume it is true for $i < k$. If $k < n(\langle B_2, S_2\rangle)$:

$$\begin{aligned} R(D_k(\langle B_2, S_{2_{inj}}\rangle) &= \bigcup_{\substack{\mathbf{n}\in Cl_{k-1}(\langle B_2,S_{2_{inj}}\rangle)\\ S_{2_{inj}}(\mathbf{n})\notin Cl_{k-1}(\langle B_2,S_{2_{inj}}\rangle)}} S_1(\bigcup_{i=1}^{k_2} R(\mathbf{n}_i)) \bigcup \left[\bigcup_{i=1}^{k_2} R(\mathbf{n}_i)\right] \\ &\subseteq S_1(Cl_{k-1}(\langle B_1, S_1\rangle)) \bigcup Cl_{k-1}(\langle B_1, S_1\rangle) \\ &= {S_1}^k(B_1) \bigcup Cl_{k-1}(\langle B_1, S_1\rangle) \\ &= Cl_k(\langle B_1, S_1\rangle) \end{aligned}$$

If $k \geq n(\langle B_2, S_2\rangle)$: $R(D_k(\langle B_2, S_{2_{inj}}\rangle)) = \emptyset \subseteq Cl_k(\langle B_1, S_1\rangle)$ as $D_k(\langle B_2, S_{2_{inj}}\rangle) = \emptyset$ or in other words, $\nexists\ \mathbf{n} \in Cl_{k-1}(\langle B_2, S_{2_{inj}}\rangle)$ such that $S_{2_{inj}}(\mathbf{n}) \notin Cl_{k-1}(\langle B_2, S_{2_{inj}}\rangle)$. So we have,

$$\begin{aligned} R(Cl(\langle B_2, S_2\rangle)) &= R(Cl_{n(\langle B_2,S_2\rangle)-1}(\langle B_2, S_2\rangle)) \\ &= R\left(B_2 \bigcup \left[\bigcup_{i=1}^{n(\langle B_2,S_2\rangle)-1} D_i(\langle B_2, S_2\rangle)\right]\right) \subseteq B_1 \bigcup \left[\bigcup_{i=1}^{n(\langle B_2,S_2\rangle)-1} Cl_i(\langle B_1, S_1\rangle)\right] \\ &= Cl_{n(\langle B_2,S_2\rangle)-1}(\langle B_1, S_1\rangle) \neq Cl(\langle B_1, S_1\rangle) \qquad (\text{as } n(\langle B_1, S_1\rangle) > n(\langle B_2, S_2\rangle)) \end{aligned}$$

which is a contradiction. Therefore, $n(\langle B_1, S_1\rangle) \leq n(\langle B_2, S_2\rangle)$.

The criterion for equivalence follows immediately from the criterion for reduction. □

Corollary 5.15. *Let $\langle B, S\rangle$ be an I.M., where S is a k-ary function. Then it can be reduced to $\langle B_0, S_0\rangle$.*

Proof. $n(\langle B_0, S_0\rangle) = \aleph_0$. If $n(\langle B, S\rangle)$ is finite, we have $n(\langle B, S\rangle) \leq n(\langle B_0, S_0\rangle)$. If $n(\langle B, S\rangle) = \aleph_0$, then also we have $n(\langle B, S\rangle) \leq n(\langle B_0, S_0\rangle)$. It follows from Theorem 1.2 that $\langle B, S\rangle$ can be reduced to $\langle B_0, S_0\rangle$. □

In the next corollary, we show that reduction on Induction Models is a transitive property.

Corollary 5.16. *Let $\langle B_1, S_1\rangle$, $\langle B_2, S_2\rangle$ and $\langle B_3, S_3\rangle$ be I.M.s. If $\langle B_1, S_1\rangle$ can be reduced to $\langle B_2, S_2\rangle$ and $\langle B_2, S_2\rangle$ can be reduced to $\langle B_3, S_3\rangle$, then $\langle B_1, S_1\rangle$ can be reduced to $\langle B_3, S_3\rangle$. In other words, reduction on Induction Models is a transitive property.*

Proof. Follows from Theorem 1.2. □

6 Conclusion

In this paper, we generalize the notion of Induction Models introduced by Henkin [11]. We then characterize the existence of B for a given S and vice versa. Interestingly, we show that the existence of S with additive structure depends on $|B|$. Finally, we introduce the notion of reduction and equivalence among Induction Models.

Theorem 1.1 shows that for every non-empty B, there exists S with additive structure that $\langle B, S\rangle$ is an Induction Model but we could show existence of S with multiplicative structure only for $|B| \geq 2$. An open question would be to show existence of S with multiplicative structure for $|B| = 1$. Mathematical induction is a widely employed tool in mathematics and therefore while we have focused on Induction Models over $\mathbb{N}$, an interesting extension would be to seek logical foundations of definition and the notions of reduction and equivalence for induction over real numbers ([4],[8]), Induction over sets ([7]), structural and transfinite induction ([**?**]).

Acknowledgments

The authors owe their deepest gratitude to Parag Singla for hosting the first author at IIT Delhi. A. Dileep was partly supported through an IBM SUR award. This work was supported in part by National Research Foundation Singapore under its NRF Fellowship Programme [NRF-NRFFAI1-2019-0004], NUS ODPRT Grant [R-252-000-685-13], and Sung Kah Kay Assistant Professorship Endowment.

References

[1] Adel Bouhoula, Emmanuel Kounalis, and Michaël Rusinowitch. Automated mathematical induction. *Journal of Logic and Computation*, 5(5):631–668, 1995.

[2] Alan Bundy. The automation of proof by mathematical induction. Technical report, 1999.

[3] William Henry Bussey. The origin of mathematical induction. *The american mathematical monthly*, 24(5):199–207, 1917.

[4] Yuen Ren Chao. A note on "Continuous mathematical induction.". *Bull. Amer. Math. Soc.*, 26(1):17–18, 1919.

[5] Henk Doornbos, Roland Backhouse, and Jaap Van Der Woude. A calculational approach to mathematical induction. *Theoretical Computer Science*, 179(1-2):103–135, 1997.

[6] Ed Dubinsky. Teaching mathematical induction ii. *Journal of Mathematical Behavior*, 8(3):285–304, 1989.

[7] W. L. Duren, Jr. Mathematical induction in sets. *Amer. Math. Monthly*, 64(8, part II):19–22, 1957.

[8] L. R. Ford. Interval-additive propositions. *Amer. Math. Monthly*, 64:106–108, 1957.

[9] David S Gunderson. *Handbook of mathematical induction: Theory and applications*. Chapman and Hall/CRC, 2014.

[10] Guershon Harel. The development of mathematical induction as a proof scheme: A model for dnr-based instruction'23. *Learning and teaching number theory: Research in cognition and instruction*, 2:185, 2002.

[11] Leon Henkin. On mathematical induction. *Amer. Math. Monthly*, 67:323–338, 1960.

[12] Sorin Stratulat. A unified view of induction reasoning for first-order logic. 2012.

[13] Frank Van Harmelen, Vladimir Lifschitz, and Bruce Porter. *Handbook of knowledge representation*. Elsevier, 2008.

A Backward Induction and Prime Induction are $\mathbb{N}$-Induction Models

Lemma A.1. *The backward induction i.e. $\langle A, S : x \to x-1\rangle$, where A is an infinite subset of $\mathbb{N}$, is an $\mathbb{N}$-Induction Model.*

Proof. Suppose there exists a $G \subseteq \mathbb{N}$ such that:
1) $A \subseteq G$, and
2) if $x \in G$ and $S(x) \in \mathbb{N}$, then $S(x) \in G$,
but $G \neq \mathbb{N}$.

Say $m \notin G$. Pick the smallest element greater than m in A, say m'. Such an element exists as A is an infinite subset of $\mathbb{N}$. $m' \in G$ due to 1). Apply S on m', $m'-m$ times, to get m. Then, $m \in G$ due to 2), which is a contradiction. So, no such G exists, which implies, $G = \mathbb{N}$. □

Lemma A.2. *Let $B = \{p : p \text{ is a prime}\} \cup \{1\}$ and $S : (x, y) \to xy$. Then, $\langle B, S\rangle$ is an $\mathbb{N}$-Induction Model.*

Proof. Let $n \in \mathbb{N}$ be a composite number. Then, $n = p_1^{r_1} p_2^{r_2} \dots p_l^{r_l}$, where p_is are primes and $r_i \geq 1$. Let $r = max\{r_1, r_2, \dots, r_l\}$. Then, $p_i^{r_i} \in S^{r-1}(B)$ for $1 \leq i \leq l$. So, $p_1^{r_1} p_2^{r_2} \dots p_l^{r_l} \in S^{r-1+l-1} = S^{r+l-2}$. Note that $r + l - 2 \geq 0$ as $r \geq r_i \geq 1$ for all $1 \leq i \leq l$ and $l \geq 1$. This implies, every $n \in \mathbb{N}$ lies in some $S^i(B)$. So, $\mathbb{N} \subseteq \bigcup_{i=0}^{\infty} S^i(B)$. □

B Generating Functions with Additive and Multiplicative Structures are Non-self Loop Functions

Lemma B.1. *If $S : \mathbb{N}^k \to \mathbb{Z}$ has an additive structure, then S is a non-self-loop function.*

Proof. Let $S(x_1, x_2, \dots x_k) = a_0 + a_1 x_1 + \dots + a_k x_k$.

If $\sum_{i=0}^{k} a_i \neq 1$, we can take $x_1 = x_2 = \dots = x_k = 1$, to get, $S(1, 1, \dots, 1) = \sum_{i=0}^{k} a_i \notin \{1, 1, \dots, 1\}$.

If $\sum_{i=0}^{k} a_i = 1$, there are two cases. Either $a_0 = 0$ or $a_0 \neq 0$.

If $a_0 = 0$, for some $l \geq 1$, $a_l \neq 1$ (otherwise $\sum_{i=0}^{k} a_i = k$). As $l \geq 1$ and S is additive, $a_l \neq 0$ (see Definition 2.2).

If $a_0 \neq 0$, for some $l \geq 0$, $a_l \neq 1$ (otherwise $\sum_{i=0}^{k} a_i = k + 1$). $a_l \neq 0$ as $a_0 \neq 0$ and $a_i \neq 0$ for $i \geq 1$. So, we have $0 \leq l \leq k$ such that $a_l \notin \{0, 1\}$.

Take $x_l = 2$ and $x_i = 1$ for other i, to get,

$$\begin{aligned} S(1, \dots, 2, \dots, 1) &= a_0 + a_1 + \dots + 2a_l + \dots + a_k \\ &= \sum_{i=0}^{k} a_i + a_l \\ &= 1 + a_l \end{aligned}$$

As $a_l \notin \{0,1\}$, $1 + a_l \notin \{1,2\}$. So, $S(1,1,\ldots,2,\ldots,1) \notin \{1,2\}$. Hence, S is not a self-loop function.

□

Lemma B.2. *If $S : \mathbb{N}^k \to \mathbb{Z}$ has a multiplicative structure, then S is a non-self-loop function.*

Proof. Let $S(x_1, x_2, \ldots, x_k) = \sum_{\mathbf{i} \in 2^{[1,k]}} a_{\mathbf{i}} \cdot (\prod_{j \in \mathbf{i}} x_j)$. There are 3 cases: $a_\emptyset = 0$, $a_\emptyset = 1$ and $a_\emptyset \notin \{0,1\}$. Let us define

$$g(x) := \sum_{\substack{\mathbf{i} \in 2^{[1,k]} \\ |\mathbf{i}| \geq 1}} a_{\mathbf{i}} \cdot x^{|\mathbf{i}|-1}$$

If $a_\emptyset \notin \{0,1\}$: Consider a prime p such that $p \nmid a_\emptyset$. Take $x_1 = x_2 = \ldots = x_k = p$ to get,

$$S(p,p,\ldots,p) = a_\emptyset + p \cdot g(p)$$

So, $S(p,p,\ldots,p) \equiv a_\emptyset \pmod{p}$. As $p \nmid a_\emptyset$, $a_\emptyset \not\equiv 0 \pmod{p}$. So, $S(p,p,\ldots,p) \not\equiv a_\emptyset \pmod{p}$. This implies that $S(p,p,\ldots,p) \notin \{p\}$.

If $a_\emptyset = 1$: Put $x_1 = x_2 = \ldots = x_k = 2$, to get,

$$\begin{aligned} S(2,2,\ldots,2) &= a_\emptyset + 2 \cdot g(2) \\ &= 1 + 2 \cdot g(2) \end{aligned}$$

So, $S(2,2,\ldots,2) \equiv 1 \pmod{2}$ which implies $S(2,2,\ldots,2) \notin \{2\}$.

If $a_\emptyset = 0$: For some $n \in \mathbb{N}$, we have

$$S(n,n,\ldots,n) = n \cdot g(n)$$

Claim: $\exists\ m \in \mathbb{N}$ such that $g(m) \neq 1$.

Suppose $\forall\ n \in \mathbb{N}$, $g(n) = 1$.

Consider the following polynomial

$$\begin{aligned} f(x) &= g(x) - 1 \\ &= \left(\sum_{\substack{\mathbf{i} \in 2^{[1,k]} \\ |\mathbf{i}| \geq 1}} a_{\mathbf{i}} \cdot m^{|\mathbf{i}|-1} \right) - 1 \\ &= \left(\sum_{s=1}^{k} \left(\sum_{\substack{\mathbf{i} \in 2^{[1,k]} \\ |\mathbf{i}| = s}} a_{\mathbf{i}} \right) x^{s-1} \right) - 1 \end{aligned}$$

We have $f(n) = 0\ \forall\ n \in \mathbb{N}$ i.e. f has infinitely many roots. But f is a polynomial of degree $k-1$. So, it has exactly $k-1$ roots in $\mathbb{C}$, which is a contradiction. So, $\exists\ m \in \mathbb{N}$ such that $g(m) \neq 1$.

Take $x_1 = x_2 = \ldots = x_k = m$, to get,

$$\begin{aligned} S(m,m,\ldots,m) &= m \cdot g(m) \\ &\neq m \end{aligned}$$

□

Remark. The argument in the above proof cannot be used for proving Lemma B.1. If instead of the cases for $a_\emptyset$ in Lemma B.2, if we do the same with a_0, the method will work for $a_0 \notin \{0,1\}$. But for the $a_0 = 0$ case, we will have $S(n,n,\ldots,n) = n \sum_{\mathbf{i}\in 2^{[1,k]}} a_{\mathbf{i}}$. If $\sum_{\mathbf{i}\in 2^{[1,k]}} a_{\mathbf{i}} = 1$, it would not work.

C Proof of Lemmas 4.3, 4.7 and 4.11

Lemma 4.3. *For every non-empty $B \subset \mathbb{N}$, there exists a k-ary non-self-loop function $S' : \mathbb{N}^k \to \mathbb{Z}$, for every k, such that $\langle B, S'\rangle$ is an $\mathbb{N}$-I.M.*

Proof. Use $S'(x_1,x_2,\ldots,x_k) = S(min(x_1,x_2,\ldots,x_k))$, where S is the generating function in Lemma 4.2. Take $x_1 = x_2 = \ldots = x_k = x$ and use the same argument as in Lemma 4.2. □

Lemma 4.7. *For every non-empty $B \subset \mathbb{N}$ and every $k \geq 2$, there exists a S with additive structure such that $\langle B, S\rangle$ is an $\mathbb{N}$-I.M.*

Proof. Say $q \in B$. Consider the following S:

$$S : (x_1,x_1,\ldots,x_k) \to x_1 + x_2 + \ldots + x_{k-1} - (k-1)x_k + (q+1)$$

Take $x_1 = x,\ x_2 = x_3 = \ldots = x_k = q$ to get $S(x,q,\ldots,q) = x+1$. So, $\{q, q+1, q+2, \ldots\} \subseteq \bigcup_{i=0}^{\infty} S^i(B)$.

Now we put $x_1 = x,\ x_2 = x_3 = \ldots = x_k = q+2$, to get, $S(x, q+2, \ldots, q+2) = x-1$. This implies $\{q-1, q-2, \ldots, 1\} \subseteq \bigcup_{i=3}^{q+1} S^i(B)$. So, $\mathbb{N} \subseteq \bigcup_{i=0}^{\infty} S^i(B)$. □

Lemma 4.11. *For every $B \subset \mathbb{N}$ containing at least two elements, there exists a k-ary S with multiplicative structure, for every k, such that $\langle B, S\rangle$ is an $\mathbb{N}$-I.M.*

Proof. Say $p, q \in B$. Consider the following S:

$$S(x_1,x_2,\ldots,x_k) = x_1x_2\ldots x_k + (x_{n-1}x_n + x_n - x_nq + 1) - qx_2x_3\ldots x_k$$

Put $x_1 = q$, to get, $S(q,x_2,\ldots,x_n) = x_{n-1}x_n + x_n - x_nq + 1$. Now, use the same argument as in Lemma 4.10. □

D Proof of Lemmas 5.2, 5.3 and 5.11

Lemma 5.2. *Let $x \in Cl(\langle B, S\rangle) \setminus B$. Then, $l(x, \langle B, S\rangle) = m$ iff $x \in D_m(\langle B, S_{inj}\rangle)$.*

Proof. ($\Longrightarrow$) Let us use induction to prove this.

1. If $l(x, \langle B, S\rangle) = 1$, then for a tuple $\mathbf{n_x} \in B^k$, we have $S_{inj}(\mathbf{n_x}) = S(\mathbf{n_x}) = x$. So, $x \in S_{inj}(B)$. As $x \in Cl(\langle B, S\rangle) \setminus B$, $x \in D_1(\langle B, S_{inj}\rangle)$.

2. Suppose that if $l(x, \langle B, S\rangle) = m$, then $x \in D_m(\langle B, S_{inj}\rangle)$.

to show: if $l(x, \langle B, S\rangle) = m+1$, then $x \in D_{m+1}(\langle B, S_{inj}\rangle)$.

As, $l(x, \langle B, S\rangle) = m+1$, we have a tuple $\mathbf{n_x} \in \bigcup_{i=0}^{m} S^m(B)$ such that $S(\mathbf{n_x}) = x$. Let $\mathbf{n_x} = (y_1, y_2, \ldots, y_k)$. Then for at least one of the y_is, $l(y_i, \langle B, S\rangle) = m$, otherwise $l(x, \langle B, S\rangle) < m+1$. So, $y_i \in S^m_{inj}(B)$, which implies that $x \in S^{m+1}_{inj}(B)$.

($\Longleftarrow$) Suppose $x \in D_m(\langle B, S_{inj}\rangle)$. Then $x \in S^m(B)$, which implies $l(x, \langle B, S\rangle) \leq m$. If $l(x, \langle B, S\rangle) < m$, then $x \in S^l_{inj}(B)$ for some $l < m$. So, $x \notin D_m(\langle B, S_{inj}\rangle)$, which is a contradiction. So, $l(x, \langle B, S\rangle) = m$. □

Lemma 5.3. *Let $\langle B, S\rangle$ be an I.M. Then, ${S^i}_{inj}(B) = S^i(B) \setminus B$ for all $i \geq 1$.*

Proof. For any set $A \in \mathbb{N}^k$, as S_{inj} is a restricted version of S, $S_{inj}(A) \subseteq S(A)$. By repeatedly applying S_{inj} and this property, we get $S^i_{inj}(B) \subseteq S^i(B)$ for $i \geq 1$. Let us use induction now.
1) We have $S_{inj}(B) \subseteq S(B)$. Also, $S_{inj}(B) \cap B = \emptyset$ (follows from the definition of S_{inj}). So, $S_{inj}(B) = S_{inj}(B) \setminus B \subseteq S(B) \setminus B$. Let $x \in S(B) \setminus B$. Then, $l(x, \langle B, S\rangle) = 1$. So, from Lemma 5.2, we have $x \in S_{inj}(B)$, which implies that $S(B) \setminus B \subseteq S_{inj}(B)$.
2) Suppose $S^i_{inj}(B) = S^i(B) \setminus B \ \forall\ i \leq m$. We need to show that $S^{m+1}_{inj}(B) = S^{m+1}(B) \setminus B$.

$$\begin{aligned} S^{m+1}_{inj}(B) &= S_{inj}(\bigcup_{i=0}^{m} S^i_{inj}(B)) \\ &= S_{inj}(\bigcup_{i=1}^{m} [S^i(B) \setminus B] \cup B) \\ &= S_{inj}(\bigcup_{i=0}^{m} S^i(B)) \\ &\subseteq S(\bigcup_{i=0}^{m} S^i(B)) = S^{m+1}(B) \end{aligned}$$

But, $S^{m+1}_{inj}(B) \cap B = \emptyset$. So, $S^{m+1}_{inj}(B) = S^{m+1}_{inj}(B) \setminus B \subseteq S^{m+1}(B) \setminus B$. Let $x \in S^{m+1}(B) \setminus B$. Then, $l(x, \langle B, S\rangle) \leq m+1$. So, $x \in S^i_{inj}(B)$ for $1 \leq i \leq m+1$. But, as $S^i_{inj}(B) \subseteq S^{m+1}_{inj}(B) for 1 \leq i \leq m+1$, we have $x \in S^{m+1}_{inj}(B)$. So, $S^{m+1}(B) \setminus B \subseteq S^{m+1}_{inj}(B)$. Hence, from 1) & 2), ${S_{inj}}^i(B) = S^i(B) \setminus B$ for $i \geq 1$. □

Lemma 5.11. *Let $\langle B, S\rangle$ be an I.M. Then, $D_i(\langle B, S\rangle) = \emptyset\ \forall\ i \geq n(\langle B, S\rangle)$.*

Proof. We use induction to prove this.

1. $D_{n(\langle B,S\rangle)}(\langle B, S\rangle) = \emptyset$ (follows from the definition of $n(\langle B, S\rangle)$)
2. Suppose $D_k(\langle B, S\rangle) = \emptyset$ for some $k \geq n(\langle B, S\rangle)$. Either $S^k(B) = \emptyset$ or $S^k(B) \subseteq Cl_{k-1}(\langle B, S\rangle) = \emptyset$.

Case 1: If $S^k(B) = \emptyset$, then $S^i(B) = \emptyset$ for $1 \leq i \leq k-1$ (as $S^i(B) \subseteq S^k(B)$ for $1 \leq i \leq k-1$). So, we have $S^{k+1}(B) = S(Cl_k(\langle B, S\rangle)) = S(B) = \emptyset$. Similarly, $S^i(B) = \emptyset\ \forall\ i \geq k$. So, $Cl(\langle B, S\rangle) = B$, which is a contradiction as $\langle B, S\rangle$ is an $\mathbb{N}$-I.M.

Case 2: If $S^k(B) \subseteq Cl_{k-1}(\langle B, S\rangle)$, we have

$$S^{k+1}(B) = S(Cl_k(\langle B, S\rangle)) \subseteq S(Cl_{k-1}(\langle B, S\rangle)) = S^k(B).$$

So, $D_{k+1}(\langle B, S\rangle) = \emptyset$. By the principle of induction, $D_i(\langle B, S\rangle) = \emptyset\ \forall\ i \geq n(\langle B, S\rangle)$. □

E Motivation for Definition 5.3

Suppose we have a proof for the statement

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

that uses the first principle of induction i.e. $\langle B_0, S_0\rangle = \langle\{1\}, x \to x+1\rangle$. Now that we have this proof, can we construct a proof that uses the Prime Induction i.e. $\langle B, S\rangle = \langle\mathbb{P} \cup \{1\}, S : (x, y) \to xy\rangle$?

Let $\Omega(n)$ be the number of prime factors of n, counted with multiplicity. Consider the following relation $R : \mathbb{N} \to 2^{\mathbb{N}}$:

$$R(n) = \begin{cases} \{1\}, & \text{if } n = 1 \\ [1, \Omega(n)], & \text{otherwise} \end{cases}$$

We construct a new statement

$$Q(n) = \bigwedge_{x \in R(n)} P(x)$$

Now let us try to prove that $Q(n)$ is true for all $n \in \mathbb{N}$ using the Prime Induction Model.

Step 1 (Base Case): $Q(1) = \bigwedge_{x \in R(1)} P(x) = P(1)$. Also, for any prime p, $Q(p) = P(1)$. So, $Q(n)$ is true for $n = 1$ and $n \in \mathbb{P}$.

Step 2 (Induction Step): Suppose $Q(m)$ and $Q(n)$ are true $(m, n \neq 1)$. So, $\bigwedge_{x \in R(m)} P(x)$ and $\bigwedge_{x \in R(n)} P(x)$ i.e. $\bigwedge_{x \in [1,\Omega(m)]} P(x)$ and $\bigwedge_{x \in [1,\Omega(n)]} P(x)$ are true. As $P(x)$ is true implies $P(x+1)$ is true, we have that $\bigwedge_{x \in [1,\Omega(m)+\Omega(n)]} P(x)$ is true. But $\Omega(x) + \Omega(y) = \Omega(xy)$ for all $x, y \in \mathbb{N}$. So, $\bigwedge_{x \in [1,\Omega(mn)]} P(x)$ is true, which implies that $Q(mn)$ is true.

Step 3 (Conclusion): So, by the Prime Induction Model, $Q(n)$ is true for all $n \in \mathbb{N}$ i.e. $\bigwedge_{x \in [1,\Omega(n)} P(x)$ is true for all $n \in \mathbb{N}$. This implies that $P(n)$ is true for all n since $\bigcup_{n \in \mathbb{N}} [1, \Omega(n)] = \mathbb{N}$.

The key to this proof is the relation R and the new statement Q. We want the relation to satisfy three conditions essentially. First, that the base case of the first I.M. is mapped to the base case of the second one. This takes care of Step 1. Second, we need $\bigcup_{n \in \mathbb{N}} R(n) = \mathbb{N}$ for Step 3 to work. To take care of Step 2, we define $R(n)$ for $n \in S^i(B)$ using the values for $x \in \bigcup_{1 \leq j < i} S^j(B)$. We look at the tuple which generates n and we use the values of R for the components of this tuple to obtain the value of $R(n)$.

F Details for Example 5.8

In this example, we have $\langle B_1, S_1\rangle = \langle\mathbb{P}, x \to x-1\rangle$ and $\langle B_2, S_2\rangle = \langle\{1,2,3,4,5\}, x \to x+5\rangle$. We now show that $\langle B_2, S_2\rangle$ can be reduced to $\langle B_1, S_1\rangle$.

Consider the following relation, R:

$$\mathbb{P} \to \{1, 2, 3, 4, 5\}$$

For $x \in \mathbb{N} \setminus \mathbb{P}$, let p be the smallest prime greater than x. Then $R(x) = [1, 5(p - x + 1)]$

1. $\bigcup\limits_{x\in\mathbb{N}} R(x) = \left[\bigcup\limits_{x\in\mathbb{P}} R(x)\right] \bigcup \left[\bigcup\limits_{x\in\mathbb{N}\setminus\mathbb{P}} R(x)\right]$
   Let us see if there exists an $x \in \mathbb{N} \setminus \mathbb{P}$ such that $5n + b \in R(x) =$, where $n > 0$, $1 \leq b \leq 5$. Enough to check if $5(n + 1) \in R(x)$. Suppose such an x does not exist. Then the distance between every pair of primes is less than n, which is not true as we can construct arbitrarily long sequences of composite numbers of the form $m! + 2, m! + 3, \ldots, m! + m$. So, we have a contradiction. So, such an x exists. This gives us
   $$\bigcup_{x\in\mathbb{N}} R(x) = \{1, 2, 3, 4, 5\} \bigcup \left[\bigcup_{a=1}^{\infty} 5a + b\right] = \mathbb{N}$$
2. $\bigcup\limits_{x\in\mathbb{P}} R(x) = \{1, 2, 3, 4, 5\}$
3. For $x \in \mathbb{N} \setminus \mathbb{P}$, $x = S_1(x + 1)$. Let the first prime greater than or equal to x be p. If $x + 1$ is a prime, then $x + 1 = p$, then $R(x + 1) = \{1, 2, 3, 4, 5\} = [1, 5(p - x)]$. If $x + 1$ is composite, then p is the smallest prime $\geq x+1$. So, by definition, $R(x+1) = [1, 5(p-x)]$.
   $$\begin{aligned} S_2(R(x + 1)) \cup R(x + 1) &= S_2([1, 5(p - x)]) \cup [1, 5(p - x)] \\ &= [6, 5(p - x + 1)] \cup [1, 5(p - x)] \\ &= [1, 5(p - x + 1)] = R(x) \end{aligned}$$