The Non-Negative Integers

Jeffrey A. Barnett[1]
At Home

Year End Holiday Time, 2004

[1]jbb@notatt.com

Forward

I have read several descriptions of the axiomatizing of arithmetic, particular those based on Peano's postulates for the non-negative integers. Aspects of those descriptions that I've found particularly interesting are the development of theories of ordering and cardinality. My perception is that many arguments are based on counting and a concept of the finite available in the proof methodology. In other words, it seems that facts that should be derived from the axiom are already available. I'm reminded of an old joke: "'*I see*,' said the blind man."

This note is an attempt to see, for myself, how it all can be done within the model. I will raise a flag in places where I too fall from grace in this regard. There is no claim of innovation. I'm sure that the original works, whose descriptions I read, played the game fairly but the descriptions merely attempted to heuristically condense the reasoning chains.

The following is organized in three parts: (1) Arithmetic and Ordering, (2) Discussion, and (3) Cardinals. Arithmetic and Ordering starts with a reasonable facsimile of Peano's postulates for the non-negative integers, I, then defines two binary operations '$+$' and 'δ', where $\delta(x, y)$ is the absolute value of $x - y$. The ordering operator $<$ is defined as follows: $x < y$ means that $x \neq y$ and $y = x + \delta(x, y)$. The results on ordering include trichotomy, $x + 1$ is the immediate successor of x, and every non-empty subset of I has a minimum element. The first part concludes with definitions and theorems about multiply, divide, and remainder. Some of them rely on ordering to control (define uniquely) the remainder.

The second part, Discussion, begins with an analysis of the proof methodology used and notes that there might be a step missing between using the induction axiom and drawing conclusions in theorems. A theorem, the commutativity of addition, is examined in detail to show how the previous proofs could be prepared for an automated proof checker. This part concludes with a statement and proof of the pigeon hole theorem that is the bases of the cardinality results in Part 3. This proof probably needs either a new induction axiom or some explicit support from the logic system.

Part 3 develops theorems about the cardinals as regards subsets of I. The main results are transitivity of an ordering operator that compares cardinality and trichotomy. The proofs in this section are less formal than in the preceding material.

Contents

Part I

Arithmetic and Ordering

Chapter 1

The Model

1.1 Definitions

Definition 1 (Integer Model)**.** I is a set and $0 \in I$ is a constant. There are two unary functions, '$^+$' and '$^-$' that obey the following axioms:

Axiom 1.1 (Plus Type)**.** $\forall x \in I\ x^+ \in I$

Axiom 1.2 (Infinity)**.** $\forall x \in I\ x^+ \neq 0$

Axiom 1.3 (Minus Type)**.** $\forall x \in I\ x \neq 0 \to x^- \in I$

Axiom 1.4 (Linearity)**.** $\forall x \in I\ (x^+)^- = x$, $\forall x \in I\ x \neq 0 \to (x^-)^+ = x$

Axiom 1.5 (Induction)**.** $\forall S \subset I\ 0 \in S \wedge (\forall x \in S\ x^+ \in S) \to S = I$

1.2 Basic Theorems

Theorem 2. $\forall x \in I\ x \neq x^+ \wedge (x \neq 0 \to x \neq x^-)$.

Proof. Let $S = \{x \in I \mid x \neq x^+\}$. Clearly $0 \in S$ by the Infinity axiom. Assume $x^+ = x^{++}$ and $x \in S$. Since $x^+, x^{++} \neq 0$, $(x^+)^- = (x^{++})^-$ or $x = x^+$, a contradiction, so $x^+ \in S$. That $\forall x \in I\ x \neq 0 \to x \neq x^-$ follows immediately: assume $x = x^-$, then $(x)^+ = (x^-)^+$ and $x^+ = x$. □

Chapter 2

Addition and Subtraction

2.1 Definitions

Definition 3 (Addition)**.**

$$\forall x, y \in I \ +(x, y) = \begin{cases} y & x = 0 \\ +(x^-, y^+) & x \neq 0 \end{cases}$$

Definition 4 (Symmetric Difference)**.**

$$\forall x, y \in I \ \delta(x, y) = \begin{cases} y & x = 0 \\ x & y = 0 \\ \delta(x^-, y^-) & \text{otherwise} \end{cases}$$

Definition 5 (Unity)**.** $1 = 0^+$.

2.2 Addition Theorems

Theorem 6 (Add Type)**.** $\forall x, y \in I \ +(x, y) \in I$.

Proof. Let $S = \{x \in I \mid \forall y \in I \ +(x, y) \in I\}$. Now $\forall y \in I \ +(0, y) = y$ so $0 \in S$. Let $n \in S$ and $y \in I$. Now $+(n^+, y) = +(n, y^+) \in I$ so $n^+ \in S$. □

Theorem 7. $\forall x, y \in I \ +(x, y)^+ = +(x^+, y)$.

Proof. let $S = \{x \in I \mid +(x,y)^+ = +(x^+,y)\}$. Choose $y \in I$: $(0,y)^+ = y^+ = (0,y^+) = (0^+,y)$ so $0 \in S$. Assume $x \in S$ and $y \in I$. Now $+(x^+,y)^+ = +(x,y^+)^+ = +(x^+,y^+) = +(x^{++},y)$ so $x^+ \in S$. □

Theorem 8 (Right Identity)**.** $\forall x \in I\ x = +(x,0)$.

Proof. Let $S = \{x \in I \mid x = +(x,0)\}$. Since $0 = +(0,0)$, $0 \in S$. Let $x \in S$, then $x = +(x,0)$ or $x^+ = +(x,0)^+ = +(x^+,0)$ so $x^+ \in S$. □

Theorem 9 (Add Commutative)**.** $\forall x,y \in I\ +(x,y) = +(y,x)$.

Proof. Let $S = \{x \in I \mid \forall y \in I\ +(x,y) = +(y,x)\}$. Surely $0 \in S$. Assume that $n \in S$ and $y \in I$. Since $n \in S$, $+(n,y^+) = +(y^+,n)$. So $+(n^+,y) = +(n,y^+) = +(y^+,n) = +(y,n^+)$. So $n^+ \in S$. □

Theorem 10. $\forall x \in I\ +(1,x) = +(x,1) = x^+$.

Proof. From the definition of '+' and '1' and commutativity. □

Theorem 11. $\forall x,y,z \in I\ +(x,y) = +(x,z) \to y = z$.

Proof. Let $S = \{x \in I \mid \forall y,z \in I\ +(x,y) = +(x,z) \to y = z\}$. Since $+(0,y) = y$ and $+(0,z) = z$, $+(0,y) = +(0,z) \to y = z$ so $0 \in S$. Let $x \in S$ and $y,z \in I$, then

$$\begin{aligned} +(x^+,y) &= +(x^+,z) \\ +(x,y^+) &= +(x,z^+) \\ y^+ &= z^+ \\ y &= z \end{aligned}$$

so $x^+ \in S$. □

Corollary 12. $\forall x,z \in I\ x = +(x,z) \to z = 0$.

Proof. $+(x,0) = x = +(x,z)$ so $z = 0$. □

Theorem 13. $\forall x,y \in I\ +(x,y) = 0 \to x = y = 0$.

Proof. If $x \neq 0$ then $0 = +(x,y) = +(x^-,y)^+$. But 0 isn't the successor of any number (Infinity Axiom). So $x = 0$ and similarly for y. □

Theorem 14 (Add Associative)**.** $\forall x,y,z \in I\ +(x,+(y,z)) = +(+(x,y),z)$.

Proof. Let $S = \{x \in I \mid \forall y, z \in I \ +(x, +(y, z)) = +(+(x, y), z)\}$. Choose $y, z \in I$: $+(0, +(y, z)) = +(y, z) = +(+(0, y), z)$ so $0 \in S$. Assume $x \in S$ and $y, z \in I$. Now $+(x^+, +(y, z)) = +(x, +(y, z)^+) = +(x, +(y^+, z)) = +(+(x, y^+), z) = +(+(x^+, y), z)$ so $x^+ \in S$. □

Theorem 15. $\forall x, y, z \in I \ y = +(x, z) \wedge x = +(y, z) \to z = 0$.

Proof. Let $S = \{x \in I \mid \forall y, z \in I \ y = +(x, z) \wedge x = +(y, z) \to z = 0\}$. Let $y, z \in I$ and assume $y = +(0, z) = z$ and $0 = +(y, z) = +(z, z)$. If $z \neq 0$, then $0 = +(z^-, z)^+$ but that is impossible so $0 \in S$. Now let $x \in S$ and $y, z \in I$. If y or z is 0, the result follows by the above argument. So assume $y = +(x^+, z)$ and $x^+ = +(y, z)$. From the first assumption, $y^- = +(x, z)$ and from the second $x = +(y^-, z)$. So $z = 0$ by the inductive assumption and $x^+ \in S$. □

2.3 Difference Theorems

Theorem 16 (Sub Type)**.** $\forall x, y \in I \ \delta(x, y) \in I$.

Proof. Let $S = \{x \in I \mid \forall y \in I \ \delta(x, y) \in I\}$. Let $y \in I$, then $\delta(0, y) = y \in I$ so $0 \in S$. Let $x \in S$ and $y \in I$. If $y = 0$, then $\delta(x^+, y) = x^+ \in I$, otherwise $\delta(x^+, y) = \delta(x, y^-) \in I$ by the inductive assumption. □

Theorem 17. $\forall x, y \in I \ \delta(x, y) = 0 \leftrightarrow x = y$.

Proof. Let $S = \{x \in I \mid \delta(x, x) = 0\}$. Clearly, $0 \in S$. Let $x \in S$. Now $\delta(x^+, x^+) = \delta(x, x) = 0$ by the inductive assumption since $x^+ \neq 0$. So $x^+ \in S$. It remains to show that $\delta(x, y) = 0 \to x = y$. In this case, let $S = \{x \in I \mid \forall y \in I \ \delta(x, y) = 0 \to x = y\}$. Since $0 = \delta(0, y) = y$, $0 \in S$. Let $x \in S$ and pick $y \in I$ such that $\delta(x^+, y) = 0$. If $y = 0$, then $\delta(x^+, y) = x^+ \neq 0$. If $y \neq 0$, then $\delta(x^+, y) = \delta(x, y^-) \to x = y^-$, i.e., $x^+ = y$, so $x^+ \in S$. □

Theorem 18 (Sub Commutative)**.** $\forall x, y \in I \ \delta(x, y) = \delta(y, x)$.

Proof. Let $S = \{x \in I \mid \forall y \in I \ \delta(x, y) = \delta(y, x)\}$. Choose $y \in I$: $\delta(0, y) = y = \delta(y, 0)$ so $0 \in S$. Let $x \in S$ and $y \in I$: If $y = 0$ then $\delta(x^+, y) = x^+ = \delta(y, x^+)$. If $y \neq 0$, then $\delta(x^+, y) = \delta(x, y^-) = \delta(y^-, x) = \delta(y, x^+)$ by the inductive assumption, so $x^+ \in S$. □

Theorem 19. $\forall x \in I \ x \neq 0 \to \delta(x, 1) = \delta(1, x) = x^-$.

Proof. If $x \neq 0$, then $\delta(x, 1) = \delta(x^-, 0) = x^-$. The rest follows from commutativity of δ. □

Theorem 20 (Cancellation)**.** $\forall x, y, z \in I \ \ \delta(+(x, y), +(x, z)) = \delta(y, z)$.

Proof. Let $S = \{x \in I \mid \forall y, z \in I \ \ \delta(+(x, y), +(x, z)) = \delta(y, z)\}$. Now $\forall y, z \in I \ \ \delta(+(0, y), +(0, z)) = \delta(y, z)$ so $0 \in S$. Let $x \in S$ and $y, z \in I$, then $\delta(+(x^+, y), +(x^+, z)) = \delta(+(x, y)^+, +(x, z)^+) = \delta(+(x, y), +(x, z)) = \delta(y, z)$ by the inductive assumption, so $x^+ \in S$. □

Corollary 21. $\forall x, y \in I \ \ \delta(+(x, y), x) = y$.

Proof. Use the above theorem with $z = 0$ and note that $+(x, z) = x$ and that $\delta(y, z) = y$. □

Theorem 22. $\forall x, y \in I \ y = +(x, \delta(x, y)) \vee x = (y, \delta(x, y))$.

Proof. Let $S = \{x \in I \mid \forall y \in I \ y = +(x, \delta(x, y)) \vee x = (y, \delta(x, y))\}$. Select any $y \in I$ and note that $+(0, \delta(0, y)) = \delta(0, y) = y$ so $0 \in S$. Now let $x \in S$ and $y \in I$. If $y = 0$, then $x^+ = +(y, \delta(x^+, y))$, otherwise

$$\begin{array}{rcr} x = +(y^-, \delta(x, y^-)) & \vee & y^- = +(x, \delta(x, y^-)) \\ x^+ = +(y^-, \delta(x, y^-))^+ & \vee & y = +(x, \delta(x, y^-))^+ \\ x^+ = +(y, \delta(x, y^-)) & \vee & y = +(x^+, \delta(x, y^-)) \\ x^+ = +(y, \delta(x^+, y)) & \vee & y = +(x^+, \delta(x^+, y)) \end{array}$$

so $x^+ \in S$. □

Corollary 23. $\forall x, y \in I \ y = +(x, \delta(x, y)) \wedge x = (y, \delta(x, y)) \leftrightarrow x = y$.

Proof. A direct consequence of the above and Theorem 15. □

Chapter 3

Ordering

3.1 Definitions

Definition 24 (Ordering)**.** $\forall x, y \in I\ x < y \equiv x \neq y \wedge y = +(x, \delta(x, y))$.

3.2 Ordering Theorems

Theorem 25 (Successor Order)**.** $\forall x \in I\ x < x^+$.

Proof. Let $S = \{x \in I \mid x < x^+\}$. Since $0 \neq 0^+$ and $+(0, \delta(0, 0^+)) = +(0, 0^+) = 0^+$, $0 \in S$. If $x \in S$, $+(x^+, \delta(x^+, x^{++})) = +(x, \delta(x^+, x^{++}))^+ = +(x, \delta(x, x^+))^+ = x^{++}$ by the inductive assumption so $x^+ \in S$. □

Theorem 26 (Trichotomy)**.** *For all $x, y \in I$ exactly one of $x = y$, $x < y$, or $y < x$ is true.*

Proof. Follows immediately from Theorem 22 and its Corollary 23. □

Theorem 27 (Transitivity)**.** $\forall x, y, z \in I\ x < y \wedge y < z \rightarrow x < z$.

Proof. The assumption, $x < y$ entails that $x \neq y$. If $z = x$, then $y < x$ and trichotomy is violated. If $z < x$, then

$$y = +(x, \delta(x, y)) \qquad z = +(y, \delta(y, z)) \qquad x = +(z, \delta(x, z)).$$

Combine them using the commutativity and associativity of '+' to show

$$+(x, +(y, z)) = +(+(x, +(y, z)), +(\delta(x, y), +(\delta(y, z), \delta(x, z))))$$

Now by Corollary 12, $+(\delta(x,y),+(\delta(y,z),\delta(x,z)))=0$, and an application of Theorem 13 shows that $\delta(x,y)=0$, hence $x=y$ by Theorem 17, a contradiction. So $x<z$ from trichotomy. □

Theorem 28 (Minimum Element)**.** $\forall x\in I\ 0=x\vee 0<x$.

Proof. Since $\forall x\in I\ x=+(0,\delta(x,0))$, either $0=x$ or $0<x$. □

Theorem 29 (Successor)**.** $\forall x,y\in I\ \neg(x<y<x^+)$.

Proof. Let $S=\{x\in I\mid \forall y\in I\ \neg(x<y<x^+\})$. Assume $y\in I$ such that $0<y<0^+$. Then since $y=0$ is impossible,

$$\begin{aligned} 0^+ &= +(y,\delta(0^+,y))\\ 0^+ &= +(y,\delta(0,y^-))\\ 0 &= +(y^-,\delta(0,y^-))\\ y^- &< 0 \end{aligned}$$

That is impossible so $0\in S$. Now let $x\in S$ and $y\in I$ and assume that $x^+<y<x^{++}$ and note that $y\neq 0$. Now,

$$\begin{aligned} x^+ &< y & \qquad y &< x^{++}\\ y &= +(x^+,\delta(y,x^+)) & \qquad x^{++} &= +(y,\delta(y,x^{++}))\\ y^- &= +(x,\delta(y^-,x)) & \qquad x^+ &= +(y^-,\delta(y^-,x^+))\\ x &< y^- & \qquad y^- &< x^+ \end{aligned}$$

or $x<y^-<x^+$ which violates the inductive assumption so $x^+\in S$. □

Theorem 30 (Set Minimum)**.** *If $T\subset I\wedge T\neq\emptyset$ then T contains a minimum element, i.e., $\exists m\in T\ \forall x\in T\ m=x\vee m<x$.*

Proof. Let $S=\{x\in I\mid \forall T\subset I\ x\in T\vee(\exists y\in T\ y<x)\to\exists m\in T\ \forall y\in T\ m=y\vee m<y\}$. If $T\subset I$ and $0\in T$, then 0 is the minimum element so $0\in S$. Let $T\subset I$ and $x\in S$. If there is a $y\in T$ where $y<x^+$, then $y=x$ or $y<x$ so T has a minimum element by the inductive assumption. The other possibility, when $x^+\in T$, is that $\forall y\in T\ x^+=y\vee x^+<y$ in which case x^+ is the minimum element of T. □

Theorem 31 (Count Down)**.** $\forall x,y\in I\ x<y\wedge x\neq 0\to\delta(x,y)<y$.

Proof. From $x < y$ we have $y = +(x, \delta(x, y))$. From the cancellation theorem we have $x = \delta(\delta(x, y), +(x, \delta(x, y)))$. Substitute the latter in the former to show that $y = +(\delta(\delta(x, y), +(x, \delta(x, y))), \delta(x, y))$. Now substitute y for $+(x, \delta(x, y))$ to obtain $y = +(\delta(\delta(x, y), y), \delta(x, y))$ to show that $\delta(x, y) = y$ or $\delta(x, y) < y$. But the former possibility entails that $x = 0$ (since $y = +(x, \delta(x, y)) = +(x, y)$ would follow). □

Theorem 32 (Count Up)**.** $\forall x, y \in I\ x < +(x, y) \vee y = 0$.

Proof. Since $+(x, y) = +(x, \delta(x, +(x, y)))$, either $x < +(x, y)$ or $x = +(x, y)$. In the latter case, $y = 0$. □

Chapter 4

Multiplication and Division

4.1 Definitions

Definition 33 (Multiplication)**.**

$$\forall x, y \in I \ *(x, y) = \begin{cases} 0 & x = 0 \\ +(*(x^-, y), y) & \text{otherwise} \end{cases}$$

Definition 34 (Division)**.**

$$\forall x, y \in I \ \div(x, y) = \begin{cases} 0 & x < y \\ \div(\delta(x, y), y)^+ & \text{otherwise} \end{cases}$$

Definition 35 (Remainder)**.** $\forall x, y \in I \ \mathrm{mod}(x, y) = \delta(x, *(\div(x, y), y))$.

4.2 Multiplication Theorems

Theorem 36 (Mul Type)**.** $\forall x, y \in I \ *(x, y) \in I$.

Proof. Let $S = \{x \in I \mid \forall y \in I \ *(x, y) \in I\}$. $\forall y \in I \ *(0, y) = 0 \in I$, so $0 \in S$. Let $x \in S$ and $y \in I$, then $*(x^+, y) = +(*(x, y), y) \in I$ because $*(x, y) \in I$ by the inductive assumption. So $x^+ \in S$. □

Theorem 37. $\forall x \in I \ *(1, x) = *(x, 1) = x$.

Proof. $\forall x \in I \ *(1, x) = *(0^+, x) = +(*(0, x), x) = +(0, x) = x$. Let $S = \{x \in I \mid *(x, 1) = x\}$. Clearly, $0 \in S$. If $x \in S$, then $*(x^+, 1) = +(*(x, 1), 1) = +(x, 1) = x^+$ so $x^+ \in S$. □

Theorem 38 (Distribution)**.** $\forall x, y, z \in I \ *(x, +(y, z)) = +(*(x, y), *(x, z))$.

Proof. Let $S = \{x \in I \mid \forall y, z \in I \ *(x, +(y, z)) = +(*(x, y), *(x, z))\}$. Now $\forall y, z \in I \ *(0, +(y, z)) = 0 = +(0, 0) = +(*(0, y), *(0, z))$ so $0 \in S$. Let $x \in S$ and $x, y \in I$, then

$$\begin{aligned} *(x^+, +(y, z)) &= +(*(x, +(y, z)), +(y, z)) \\ &= +(+(*(x, y), *(x, z)), +(y, z)) \end{aligned}$$

because $x \in S$. Then use associatvity and communtativity of '+'

$$\begin{aligned} &= +(+(*(x, y), y), +(*(x, z), z)) \\ &= +(*(x^+, y), *(x^+, z)) \end{aligned}$$

so $x^+ \in S$. □

Corollary 39. $\forall x, y, z \in I \ \delta(*(x, y), *(x, z)) = *(x, \delta(y, z))$.

Proof. From Theorem 22 $y = +(z, \delta(y, z))$ or $z = +(y, \delta(y, z))$. Assume the latter. Then

$$\begin{aligned} \delta(*(*x, y), *(x, z)) &= \delta(*(x, y), *(x, +(y, \delta(y, z)))) \\ &= \delta(*(x, y), +(*(x, y), *(x, \delta(y, z)))) \\ &= *(x, \delta(y, z)). \end{aligned}$$

The case were $y = +(z, \delta(y, z))$ is virtually identical. □

Theorem 40 (Mul Commutative)**.** $\forall x, y \in I \ *(x, y) = *(y, x)$.

Proof. $\forall x \in I \ *(0, x) = 0$. Let $S = \{x \in I \mid *(x, 0) = 0\}$. Clearly $0 \in S$. If $x \in S$, then $*(x^+, 0) = +(*(x, 0), 0) = +(0, 0) = 0 = *(0, x+)$.

Now let $S = \{x \in I \mid \forall y \in I \ *(x, y) = *(y, x)\}$. By the above argument, $0 \in S$. Now let $x \in S$ and $y \in I$. If $y = 0$, $*(x^+, y) = *(y, x^+)$. If $y \neq 0$, then

$$\begin{aligned} *(y, x^+) &= *(y, +(x, 1)) \\ &= +(*(y, x), *(y, 1)) \\ &= +(*(y, x), y) \\ &= +(*(x, y), y) \\ &= *(x^+, y) \end{aligned}$$

so $x^+ \in S$. □

Theorem 41 (Mul Associative)**.** $\forall x, y, z \in I \ *(x, *(y, z)) = *(*(x, y), z)$.

Proof. Let $S = \{x \in I \mid \forall y, z \in I \ *(x, *(y, z)) = *(*(x, y), z)\}$. Now $*(0, *(y, z)) = *(*(0, y), z) = 0$, so $0 \in S$. Let $x \in S$ and $y, z \in I$, then

$$*(x^+, *(y, z)) = +(*(x, *(y, z)), *(y, z))$$

because $x^+ = +(x, 1)$ and the distributive law

$$= +(*(*(x, y), z), *(y, z))$$

by the inductive assumption

$$= *(+(*(x, y), y), z)$$

using the distributive law

$$= *(*(x^+, y), z)$$

from the definition of '*', so $x^+ \in S$. □

Theorem 42. $\forall x, y \in I \ y \neq 0 \to \exists q, r \in I \ x = +(*(q, y), r) \wedge r < y$.

Proof. Let $S = \{x \in I \mid \forall y \in I \ y \neq 0 \to \exists q, r \in I \ x = +(*(q, y), r) \wedge r < y\}$. If $y \in I$ and $y \neq 0$, then $+(*(0, y), 0) = 0$ and $0 < y$ so $0 \in S$. Let $x \in S$ and $y \in I$, where $y \neq 0$, then $+(*(q, y), r) = x$ has a solution for q and r where $r < y$. If $r^+ < y$, then $+(*(q, y), r^+) = +(*(q, y), r)^+ = x^+$ is a solution for x^+. If $r^+ = y$, then

$$\begin{aligned} +(*(q^+, y), 0) &= *(q^+, y) \\ &= +(*(q, y), y) \\ &= +(*(q, y), r^+) \\ &= +(*(q, y), r)^+ \\ &= x^+ \end{aligned}$$

by the inductive assumption, so $q' = q^+$ and $r' = 0$ are solutions for x^+, hence, $x^+ \in S$. □

4.3 Division Theorems

Theorem 43 (Div Type)**.** $\forall x \in I \ \div(x,0) \notin I$ *and* $\forall x,y \in I \ y \neq 0 \rightarrow \div(x,y) \in I$.

Proof. By definition of '$\div$' and the fact that $x < 0$ is never true, $\div(x,0) = \div(\delta(x,0),0)^+ = \div(x,0)^+$. But for no $a \in I$ is $a = a^+$ possible. Therefore, $\div(x,0) \notin I$.

Let $S = \{x \in I \mid \forall n,y, \in I \ (n < x \vee n = x) \wedge y \neq 0 \rightarrow \div(n,y) \in I\}$. Clearly, $0 \in S$. Now let $x \in S$ and $y \in I$, where $y \neq 0$. If $x^+ < y$ then $\div(x^+,y) = 0 \in I$. Now assume that $x^+ < y$ is false so $\div(x^+,y) = \div(\delta(x^+,y),y)^+$. Then the fact that $y \neq 0$ and the Countdown Theorem entail that $\delta(x^+,y) < x^+$ and this proof is finished by the inductive assumption. □

Theorem 44. $\forall x,y,z \in I \ y \neq 0 \wedge z < y \rightarrow \div(+(*(x,y),z),y) = x$.

Proof. Let $S = \{x \in I \mid \forall y,z \in I \ y \neq 0 \wedge z < y \rightarrow \div(+(*(x,y),z),y) = x\}$. Let $y,z \in I$, where $y \neq 0 \wedge z < y$. Now $\div(+(*(0,y),z),y) = \div(+(0,z),y) = \div(z,y) = 0$ so $0 \in S$ since $z < y$. Let $x \in S$ and $y,z \in I$ where $y \neq 0$ and $z < y$. Then

$$\begin{aligned}\div(+(*(x^+,y),z),y) &= \div(+(+(*(x,y),y),z),y)\\ &= \div(+(+(*(x,y),z),y),y)\end{aligned}$$

Since $y < +(+(*(x,y),z),y)$ or the quantities are equal,

$$\begin{aligned}&= \div(\delta(+(+(*(x,y),z),y),y),y)^+\\ &= \div(+(*(x,y),z),y)^+\\ &= x^+\end{aligned}$$

by the inductive assumption, so $x^+ \in S$. □

Corollary 45. $\forall x,y \in I \ y \neq 0 \rightarrow \div(*(x,y),y) = x$.

Theorem 46. *If* $x,y \in I$*, where* $y \neq 0$*, and* $x = +(*(q,y),r)$*, where* $q,r \in I$ *and* $r < y$*, then* q *and* r *are unique.*

Proof. Assume $+(*(q_1,y),r_1) = +(*(q_2,y),r_2) = x$, where $q_1,q_2,r_1,r_2 \in I$ and $r_1,r_2 < y$, then

$$\div(+(*(q_1,y),r_1),y) = \div(+(*(q_2,y),r_2),y)$$

$$q_1 = q_2$$

and, therefore,

$$\begin{aligned} +(*(q_1, y), r_1) &= +(*(q_1, y), r_2) \\ \delta(+(*(q_1, y), r_1), *(q_1, y)) &= \delta(+(*(q_1, y), r_2), *(q_1, y)) \\ r_1 &= r_2, \end{aligned}$$

so q and r are unique. □

4.4 Remainder Theorems

Theorem 47 (Rem Type)**.** $\forall x, y \in I\ y \neq 0 \rightarrow \mathrm{mod}(x, y) \in I$.

Proof. If $y \neq 0$, the results of all of the defining operators are in I. □

Theorem 48. $\forall x, y \in I\ y \neq 0 \rightarrow \mathrm{mod}(x, y) < y$.

Proof. There are unique q and $r < y$, in I, such that $x = +(*(q, y), r)$, where $\div(x, y) = q$. So

$$\mathrm{mod}(x, y) = \delta(x, *(\div(x, y), y)) = \delta(+(*(q, y), r), *(q, y))) = r < y$$

and the theorem follows. □

Corollary 49. $\forall x, y \in I\ y \neq 0 \rightarrow x = +(*(\div(x, y), y), \mathrm{mod}(x, y))$.

Corollary 50. $\forall x, y \in I\ y \neq 0 \rightarrow \delta(x, *(\div(x, y), y)) < y$.

Theorem 51. $\forall x, y \in I\ y \neq 0 \rightarrow \mathrm{mod}(*(x, y), y) = 0$.

Proof. If $x, y \in I$, where $y \neq 0$, then

$$\mathrm{mod}(*(x, y), y) = \delta(*(x, y), *(\div(*(x, y), y), y) = \delta(*(x, y), *(x, y)) = 0$$

which proves the theorem. □

Theorem 52. *If* $\mathrm{mod}(x, y) = \mathrm{mod}(z, y)$ *then* $\mathrm{mod}(\delta(x, z), y) = 0$.

Proof. There are unique $q_x, r_x, q_z.r_z \in I$, where $r_x, r_z < y$, such that $x = +(*(q_x, y), r_x)$ and $z = +(*(q_z, y), r_z)$. So

$$\delta(x, y) = \delta(+(*(q_x, y), r_x), +(*(q_z, y), r_z)) = \delta(*(q_x, y), *(q_z, y))$$

since $r_x = r_z$ by hypothesis. But $\delta(*(q_x, y), *(q_z, y)) = *(y, \delta(q_x, q_z))$ so $\mathrm{mod}(\delta(x, z), y) = \mathrm{mod}(*(y, \delta(q_x, q_z)), y) = 0$. □

Part II

Discussion

Chapter 5

Remarks

While the nature of the above proofs is what has often been referred to by some mathematicians as "boring axiomatics," I found them interesting. The power and necessity of the induction axiom was somewhat unexpected. That axiom appeared to serve two purposes: The first was to somehow bar the intrusion of pests into the model. The second was to provide a proof mechanism within the model.

There is a hidden proof obligation that I did not address above. Consider an example, the trichotomy theorem: $\forall x, y \in I\ x = y \vee x < y \vee y < x$. This was proved by defining a set $S = \{x \in I \mid \forall y \in I\ x = y \vee x < y \vee y < x\}$, showing $0 \in S$, then showing $x \in S \rightarrow x^+ \in S$ so $S = I$. I'm not sure exactly how to go from that conclusion to the stated theorem in a formal manner. Perhaps an inference scheme such as the following, where U is the universe of discussion, is needed but here we have quantification over predicates:

$$\forall S \subset U\ \forall n \in I\ \forall p\colon S^{n+1} \rightarrow 2$$
$$\{\forall x_0 \in S \mid \forall x_1, \ldots, x_n \in S\ p(x_0, \ldots, x_n)\} = S \rightarrow$$
$$\forall x_0, \ldots, x_n \in S\ p(x_0, \ldots, x_n).$$

Note that the idea of forming a powerset using elements of I as the powers is totally beyond anything that can be handled by the mechanisms introduced so for. The 2 above denotes any two-element set; $\{\text{true}, \text{false}\}$ is an excellent choice. Section 6 describes the underlying proof methods as used.

The definition $x < y \equiv x \neq y \wedge y = +(x, \delta(x, y))$ allowed the ordering theorems to be derived arithmetically, a goal of this venture. However, more is necessary, for example, the proof of properties such as the pigeon hole

theorem. I'm not clear whether additional mechanisms are needed to state and prove such propositions. Section 7 further discusses this point.

Perhaps Theorem 30 and its proof are the shakiest of the above. In order to apply it, one is given a set that is claimed nonempty. If x is an element of that set, then it's easy to see that the theorem and proof show that either x or some smaller element is the minimum. What is not clear is how to apply the theorem if an element of the nonempty set isn't specified. So the *application* of the theorem may need some weak form of the choice axiom while the *proof* itself appears fine without it.

The proof of Theorem 30 might be clearer if the following presentation were used: Start with the definitions

$$\begin{aligned} S &= \{x \in I \mid \forall T \subset I \; x \in T \to \min(T) \in T\} \\ S' &= \{x \in I \mid \forall y \in I \; y = x \vee y < x \to y \in S\} \\ S'' &= S \cap S', \end{aligned}$$

where '$\min(T) \in I$' is shorthand for 'there is an element in T that is not larger than any element of T'. The proof outline now goes: $0 \in S$ and $0 \in S'$ so $0 \in S''$; let $x \in S''$ so that $x \in S$ and $x \in S'$; show that $x^+ \in S$ and $x^+ \in S'$ so $x^+ \in S''$. In other words, $S = S' = S'' = I$. $\square$.

The theorems on multiplication and division (actually the truncation operator) were added to round out the basic results for the non-negative integers. However, I'm not sure whether more proof power would be needed to state and prove results such as the fundamental theorem of arithmetic (unique factorization). It seems that at least a notion of ordered pairs or relations is needed but that would drag in a fairly large chunk of naive set theory and that would not be in the spirit of this minimalist activity.

Chapter 6

Detailed Proof Methodology

While the proofs in this note were not 100% complete, the aim was to provide enough material to convince one that an automated proof checker could fill in the blanks. This is as close to boring axiomatics as I care to venture. Figure 6.1 is an elaboration of the proof of Theorem 9 which shows that '+' is commutative. It is meant to illustrate the next, but certainly not the ultimate level of rigor.

There are three columns and seventeen rows. The first column gives a line number in the form Li for each proof step. The middle column is a mathematical formula justified by the reasons in the third column. The reasons notations are as follows: Li—see line Li, Di—see definition i in the main text, Ti—see theorem i in the main text, Ai—see axiom i in the main text, '('—open a quantification scope, ')'—close a quantification scope. Justifications such as substitute equals for equals, the transitivity of '=', and general unification operations are not included.

$\forall x, y\ +(x, y) = +(y, x)$		
L1	$S = \{x \in I \mid \forall y \in I\ +(x, y) = +(y, x)\}$	Def
L2	$\forall y \in I\ +(0, y) = y$	D3
L3	$\forall y \in I\ +(y, 0) = y$	T8
L4	$\forall y \in I\ +(0, y) = +(y, 0)$	L2–3
L5	$0 \in S$	L4
L6	$\forall x \in S$	(
L7	$\forall y \in I$	(
L8	$+(x, y^+) = +(y^+, x)$	L1,6–7
L9	$y^+ \neq 0$	A1.2
L10	$+(y^+, x) = +(y, x^+)$	D3, L9
L11	$+(x, y^+) = (y^+, x)$	L8
L12	$+(y^+, x) = +(y, x^+)$	D3, L9
L13	$+(x^+, y) = +(y, x^+)$	L10–12
L14	$x^+ \in S$	L1,6,7,13
L15		L7)
L16		L6)
L17	$S = I$	A1.5, L5–16

Figure 6.1: Step-by-step proof of a theorem.

Chapter 7

A Different Type of Proof

In this section, I investigate the proof structure of a more complicated theorem. The example used is pigeon hole. The statement of the theorem needs a definition of a summation operator:

Definition 53 (Summation)**.** Let $f\colon I \to I$, then

$$\forall x \in I \ \sigma(f,x) = \begin{cases} 0 & x = 0 \\ +(f(x^-), \sigma(f,x^-)) & x \neq 0 \end{cases}$$

Note that this definition supposes a function, f, defined on the integers but is meant to apply to any such function. Now the theorem can be stated and the proof sketched.

Theorem 54 (Pigeon Hole)**.** $\forall f\colon I \to I \ \forall x \in I \ x < \sigma(f,x) \to \exists y \in I \ y < x \wedge 1 < f(y)$.

Proof. Let $f\colon I \to I$ and $S = \{x \in I \mid x < \sigma(f,x) \to \exists y \in I \ y < x \wedge 1 < f(y)\}$. Since $\sigma(f,0) = 0$ and, thus, $0 \not< \sigma(f,0)$, it follows that $0 \in S$. Now let $x \in S$ and note that $\sigma(f,x^+) = +(f(x), \sigma(f,x))$. Assume that $x^+ < \sigma(f,x^+)$ but that $\forall y \in I \ y < x^+ \to 1 \not< f(y)$ so $f(y)$ is 0 or 1. In particular, $f(x) = 0$ or $f(x) = 1$. Therefore,

$$x^+ < \sigma(f,x^+) = +(f(x), \sigma(f,x)) = \begin{cases} \sigma(f,x) \\ \sigma(f,x)^+ \end{cases} \quad \text{or}$$

In either case, $x < \sigma(f,x)$ is entailed and that violates the inductive assumption. Thus, $x^+ \in S$. □

The added complications in this example are the definition of an operator 'σ' with a function as an argument and quantification over functions. The validity of these mechanisms in general mathematics is certainly not in doubt. The issue here is what must be added to the existing proof toolkit to legitimize these proofs. Consider the above proof restructured so that it starts with the definition $S = \{\forall f{:}\, I \to I \ \mid \forall x \in I \text{ etc.}\}$. What would one use, as an induction axiom, to show that S was the set of all (total) integer functions? Another minor issue is that $\sigma(f, x) \in I$ should be proved.

A corollary/alternative form of the theorem will be used in Part III is the following:

Corollary 55. $\forall f{:}\, I \to I\ \forall m, n \in I\ m < n \wedge (\forall x \in I\ x < n \wedge f(x) < m) \to \exists x, y \in I\ x < y \wedge y < n \wedge f(x) = f(y)$.

Proof. Define a function, $g(c)$, that depends on f and n using the σ operator, that counts the number of $x < n$ where $f(x) = c$. Then an application of the above theorem gives the desired result. □

At this point, we have enough mechanisms to state and prove a theorem such as the following:

Theorem 56. $\forall f{:}\, I \to I\ \forall x \in I\ 0 < x \to \exists n, m \in I\ (m < n) \wedge (n < x \vee n = x) \to \mathrm{mod}(\delta(\sigma(f, n), \sigma(f, m)), x) = 0$.

The proof is omitted. What this says is that every x-element sequence contains a consecutive non-null subsequence where the sum of its elements is divisible by x. Of course, the pigeon hole theorem is implicated in this proof. The harder version of this homework problem (which shares the same proof) omits the word "consecutive" from the problem statement. I don't think the machinery discussed so far comes close to being able to state and prove this harder version.

Part III

The Cardinals

Chapter 8

Cardinality

8.1 Definitions

Note, definitions 57–59 define three 2-place relations: $\pi(\cdot) \preceq \pi(\cdot)$, $\pi(\cdot) \doteq \pi(\cdot)$, and $\pi(\cdot) \prec \pi(\cdot)$, they do not define π directly.

Definition 57. $\forall S, T \subset I \;\; \pi(S) \preceq \pi(T) \equiv \exists f : S \to T \;\forall x, y \in S \;\; x = y \vee f(x) \neq f(y)$.

Definition 58. $\forall S, T \subset I \;\; \pi(S) \doteq \pi(T) \equiv \pi(S) \preceq \pi(T) \wedge \pi(T) \preceq \pi(S)$.

Definition 59. $\forall S, T \subset I \;\; \pi(S) \prec \pi(T) \equiv \pi(S) \preceq \pi(T) \wedge \neg(\pi(T) \preceq \pi(S))$.

Definition 60 (Finite Powers)**.** $\forall n \in I \; I_n = \{x \in I \mid x < n\}$.

Definition 61 (Cardinals)**.** $\forall S \subset I \;\; \text{Card}(S) = \{T \subset I \mid \pi(T) \doteq \pi(S)\}$.

8.2 Partition

Theorem 62. *The set of cardinals partitions* 2^I.

Proof. In other words, "$\doteq$" must be shown to be an equivalence relation, i.e., we must prove that it is

reflexive $\forall S \subset I \;\; \pi(S) \doteq \pi(S)$

symmetric $\forall S, T \subset I \;\; \pi(S) \doteq \pi(T) \to \pi(T) \doteq \pi(S)$

transitive $\forall S, T, U \subset I \ \pi(S) \doteq \pi(T) \wedge \pi(T) \doteq \pi(U) \rightarrow \pi(S) \doteq \pi(U)$

That "$\doteq$" is reflexive, consider the identity map of S onto itself. That it is symmetric follows immediately from the definition. The antecedents of transitivity entail the existence of four one-to-one functions: $f_{ST}: S \rightarrow T$, $f_{TS}: T \rightarrow S$, $f_{TU}: T \rightarrow U$, and $f_{UT}: U \rightarrow T$. The two one-to-one functions, $f_{SU}: S \rightarrow U$ and $f_{US}: U \rightarrow S$, defined by $\forall s \in S \ f_{SU}(s) = f_{TU}(f_{ST}(s))$ and $\forall u \in U \ f_{US}(s) = f_{TS}(f_{UT}(u))$ suffice to show that $\pi(S) \doteq \pi(U)$. □

8.3 Comparison

Theorem 63. $\forall S \subset T \subset I \ \pi(S) \preceq \pi(T)$.

Proof. Let $f: S \rightarrow T$, where $\forall s \in S \ f(s) = s$. □

Corollary 64. $\forall S \subset I \ \pi(S) \preceq \pi(I)$.

Corollary 65. $\forall A, B \subset I \ \pi(A) \preceq \pi(A \cup B)$.

Corollary 66. $\forall A, B \subset I \ \pi(A \cap B) \preceq \pi(A)$.

Corollary 67. $\forall m, n \in I \ m < n \rightarrow \pi(I_m) \prec \pi(I_n)$.

Proof. Clearly, $\pi(I_m) \preceq \pi(I_n)$ because $I_m \subset I_n \subset I$. The rest is a corollary of the pigeon hole theorem. □

Theorem 68. $\forall n \in I \ \pi(I_n) \prec \pi(I)$.

Proof. Clearly, $\pi(I_n) \preceq \pi(I)$ because $I_n \subset I$. Now assume an $f: I \rightarrow I_n$, one-to-one. Let $f^*: I_{n^+} \rightarrow I_n$ be defined as $\forall x \in I_{n^+} \ f^*(x) = f(x)$. Clearly f^* is not one-to-one by the previous corollary so neither is f. Therefore, $\pi(I_n) \prec \pi(I)$. □

Theorem 69. $\forall A, B \subset I \ \pi(A) \doteq \pi(I) \rightarrow \pi(A \cup B) \doteq \pi(I)$.

Proof. Since $A \cup B \subset I$, $\pi(A \cup B) \preceq \pi(I)$. Since $\pi(A) \doteq \pi(I)$ there is a $f: I \rightarrow A$, one-to-one. The same f is one-to-one into $A \cup B$ so $\pi(I) \preceq \pi(A \cup B)$. □

8.4 Transitivity

Theorem 70 (Weak Transitivity)**.** $\forall S, T, U \in I \;\; \pi(S) \preceq \pi(T) \wedge \pi(T) \preceq \pi(U) \rightarrow \pi(S) \preceq \pi(U)$.

Proof. From the given conditions, there exist $f\colon S \rightarrow T$ and $g\colon T \rightarrow U$, where f and g are one-to-one. Let $h\colon S \rightarrow U$ be defines as $\forall s \in S \; h(s) = g(f(s))$, then h is one-to-one. □

Theorem 71 (Strong Transitivity)**.** $\forall A, B, C \subset I$

1. $\pi(A) \prec \pi(B) \wedge \pi(B) \preceq \pi(C) \rightarrow \pi(A) \prec \pi(C)$.
2. $\pi(A) \preceq \pi(B) \wedge \pi(B) \prec \pi(C) \rightarrow \pi(A) \prec \pi(C)$.
3. $\pi(A) \prec \pi(B) \wedge \pi(B) \prec \pi(C) \rightarrow \pi(A) \prec \pi(C)$.

Proof. First note that

a. $\pi(A) \prec \pi(B) \rightarrow \pi(A) \preceq \pi(B)$ and

b. $\pi(B) \prec \pi(C) \rightarrow \pi(B) \preceq \pi(C)$.

Therefore, 1 (or 2) and a (or b) entail 3. Furthermore, a and b and Weak Transitivity entail that $\pi(A) \preceq \pi(C)$ in 1–3.

Consider case 1: If $\pi(A) \doteq \pi(C)$, there is a one-to-one $f\colon C \rightarrow A$ and a one-to-one $g\colon B \rightarrow C$. So $h\colon B \rightarrow A$ defined by $\forall b \in B \; h(b) = f(g(b))$ is one-to-one and this contradicts $\pi(A) \prec \pi(B)$.

Case 2 succumbs to a similar demonstration. □

8.5 Cardinal Trichotomy

Theorem 72. $\forall S \subset I \; S = \emptyset \rightarrow \pi(S) \doteq \pi(I_0)$

Theorem 73. $\forall S \subset I \;\; \max(S) \in I \rightarrow \exists n \in I \;\; \pi(S) \preceq \pi(I_n)$.

Proof. Let $m \in S$ be the maximum element of S and let $n = m^+$. Then Clearly $\pi(S) \preceq \pi(I_n)$ because $S \subset I_n$. □

Theorem 74. $\forall S \subset I \; S = \emptyset \vee \max(S) \in I \vee \pi(S) \doteq \pi(I)$.

Proof. Clearly $\pi(S) \preceq \pi(I)$ because $S \subset I$. Assuming $S \neq \emptyset$ and $\max(S) \notin I$, it remains to find an $f: I \to S$ that is one-to-one. Let

$$g(n,T) = \begin{cases} \min(T) & n = 0 \\ g(n^-, T \setminus \min(T)) & n \neq 0, \end{cases}$$

where $n \in I$ and $T \subset I$. Now define $f: I \to S$ as $\forall n \in I \ f(n) = g(n,S)$ and note that f is one-to-one and is well defined because S is non-empty (it has an element) and the fact that S has no maximum entails T in the above definition of g is never empty. Finally, ever non-empty $T \subset I$ has a minimum element. □

Theorem 75. $\forall A \subset I \ \max(A) \in I \to \exists n \in I \ \pi(A) = \pi(I_n)$.

Proof. Let $S = \{x \in I \mid \pi(A) \preceq \pi(I_x)\}$ and note that $S \neq \emptyset$ by Theorem 73. Let $n = \min(S)$, justified by Theorem 30. Claim: $\pi(A) = \pi(I_n)$. Since $\pi(A) \preceq \pi(I_n)$, there exists a one-to-one $f: A \to I_n$. If f is also onto I_n, then the one-to-one function $f^{-1}: I_n \to A$, along with f, would certify $\pi(A) \doteq \pi(I_n)$. Assume that f is not onto, i.e., there is an $x \in I_n$ such that $\forall y \in A \ f(y) \neq x$. Then consider the one-to-one function $g: A \to I_{n^-}$, where $\forall a \in A$,

$$g(a) = \begin{cases} f(a) & f(a) \leq x \\ f(a)^- & f(a) \not\leq x \end{cases}$$

which shows that $\pi(A) \preceq \pi(I_{n^-})$ and contradicts the fact that $n = \min(S)$. □

Theorem 76 (Trichotomy of Cardinals)**.** $\forall A, B \subset I$ *exactly one of the three* $\pi(A) \prec \pi(B)$, $\pi(A) \doteq \pi(B)$, *or* $\pi(B) \prec \pi(A)$ *is true.*

Proof. That at most one of the three possibilities holds follows from the definitions. To show that one possibility must hold, select $A, B \subset I$, note whether either is empty and whether either has a maximum element. If A is empty or has a maximum element, there is an $a \in I$ such that $\pi(A) \doteq \pi(I_a)$. (If A is empty, $a = 0$.) Similarly, if B is empty or has a maximum element there is a $b \in I$ such that $\pi(B) \doteq \pi(I_b)$. In these four cases, $\pi(A) \prec \pi(B)$, $\pi(A) \doteq \pi(B)$, or $\pi(B) \prec \pi(A)$ as, respectively, $a < b$, $a = b$, or $b < a$. If A is not empty and has no maximum element but B is empty or has a maximum element, then $\pi(B) \prec \pi(A)$. If A and B switch descriptions, then

$\pi(A) \prec \pi(B)$. The remaining case is where A and B are both non-empty but have no maximum element so $\pi(A) \doteq \pi(I) \doteq \pi(B)$. This analysis is supported by Theorems 67, 68, and 75. $\square$