# Truth and Consequences

Jeffrey Clark
Elon University
email: clarkj@elon.edu
web: http://frodo.elon.edu

March 26, 2004

# 1. Introduction

It can be fun to play around with axioms; it can also be very tedious. A lot of the proofs of the immediate consequences of axioms are mechanical, easy for someone with experience and mystifying for the newcomer.

# 1. Introduction

It can be fun to play around with axioms; it can also be very tedious. A lot of the proofs of the immediate consequences of axioms are mechanical, easy for someone with experience and mystifying for the newcomer.

In this talk I will show the mechanical nature of a few of the proofs involving arithmetic on the natural numbers. Along the way I will demonstrate the use of a mathlet, *Simplification*, that I have created for finding the consequences of algebraic axioms using *Term Rewriting Systems*.

# 2. Term Rewriting Systems

*Terms* are either variables or operators applied to terms. It will be easier to work with rewriting systems if we use prefix notation, where all operators are written in front. Here are some terms, written in prefix notation with their normal (infix) equivalents on the right.

| | |
|---|---|
| $a$ | $a$ |
| $+\ a\ b$ | $a + b$ |
| $*\ +\ a\ b\ +\ c\ b$ | $(a + b) * (c + b)$ |

A *rewrite rule* is a rule describing how to replace a term by an equivalent but simpler term. The following are examples of rewrite rules, where we view addition as a simpler operation to end on than multiplication.

- $* \; a \; 1 \longrightarrow a$
- $+ \; a \; 0 \longrightarrow a$
- $* \; a + b \; c \longrightarrow + * a \; b * a \; c$

A *term rewriting system* consists of a specification of variables, operators, and rewrite rules. The mathlet *Simplification*, when it converges, takes a set of axioms and produces a term rewriting system that can take any term and in a finite number of steps produce a unique simplest equivalent form for that term. Checking equality between two terms reduces to applying rewrite rules to both terms and seeing if the resulting simplest forms are the same.

# 3. Simplification

I wrote *Simplification* to facilitate computations involving rewrite rules. It prompts the user for variables, operators, and axioms, and then attempts to create a complete rewriting system such that if a term can be written in a simpler form according to the axioms, the rewrite rules can be used to find that simpler form. The system will also find the unique simplest form for the term in a finite number of steps. The procedure used to search for the rewrite rules does not necessarily converge, so there is a user-set upper bound on how long the program runs.

*Simplification* is written mostly in *Python*, with a *Java* graphical user interface. The program and its source code are freely available from my web site.

Demonstration: let $m$ be a multiplication operator, $i$ an inversion operator, $e$ be the multiplicative identity, and $a$, $b$, $c$ be variables. We will start with the associative, left identity, and left inverse identities:

- $m\ m\ a\ b\ c = m\ a\ m\ b\ c$
- $m\ e\ a = a$
- $m\ i\ a\ a = e$

# 4. Natural Numbers

My main example will be the natural numbers $\mathbb{N}$, defined by the following axioms:

- $0 \in \mathbb{N}$
- $S\colon \mathbb{N} \longrightarrow \mathbb{N}$ is injective.
- $0 \notin S(\mathbb{N})$
- If $M \subseteq \mathbb{N}$, $0 \in M$, and $S(M) \subseteq M$, then $M = \mathbb{N}$.

We can work with a term algebra with the following operators and properties:

- 0 is a nullary operator
- $S$ (successor) is a unary operator
- $P$ (predecessor) is a unary operator such that $P\ S\ a = a$ (which ensures that $S$ is injective)

It is hard to encode that 0 is not the successor of any other natural number; most of what follows will apply to more general number systems than the natural numbers because of that.

It is hard to encode that 0 is not the successor of any other natural number; most of what follows will apply to more general number systems than the natural numbers because of that.

The last Peano axiom specifies that mathematical induction is valid; we will use it repeatedly in the proofs that follow as a method of proof and not as an axiom.

It is hard to encode that 0 is not the successor of any other natural number; most of what follows will apply to more general number systems than the natural numbers because of that.

The last Peano axiom specifies that mathematical induction is valid; we will use it repeatedly in the proofs that follow as a method of proof and not as an axiom.

If we run *Simplification* on this term algebra with only one axiom $P\ S\ a = a$, we get only one rewrite rule:

1. $P\ S\ a \rightarrow a$

# 5. Addition

We can define addition recursively on the second input:

1. $P\ S\ a = a$
2. $+\ a\ 0 = a$
3. $+\ a\ S\ b = S + a\ b$

# 5. Addition

We can define addition recursively on the second input:

1. $P\ S\ a = a$
2. $+\ a\ 0 = a$
3. $+\ a\ S\ b = S + a\ b$

If we run *Simplification* on this term algebra, we get three rewrite rules:

1. $+\ a\ 0 \longrightarrow a$
2. $P\ S\ a \longrightarrow a$
3. $+\ a\ S\ b \longrightarrow S + a\ b$

0 is also a left additive identity: $+\,0\;a = a$ for all $a$. We can prove this by induction on $a$.

0 is also a left additive identity: $+\,0\;a = a$ for all $a$. We can prove this by induction on $a$.

Base case: $a = 0$. We seek to show that $+\,0\;0 = 0$.

$$+\,0\;0 \longrightarrow 0 \qquad \text{Rule \#1: } +\,a\;0 \longrightarrow a$$

Inductive step: assume that $+0\ a = a$ and try to show that $+0\ S\ a = S\ a$. When we perform this step we are temporarily fixing $a$ as a constant. We therefore append our inductive hypothesis as an axiom after declaring $a$ to be a constant. We re-label the variables in the other axioms accordingly.

1. $P\ S\ b = b$
2. $+\ b\ 0 = b$
3. $+\ b\ S\ c = S + b\ c$
4. $+\ 0\ a = a$

We have the following rewrite system from these axioms:

1. $+\, 0\; a \to a$
2. $+\, b\; 0 \to b$
3. $P\; S\; b \to b$
4. $+\, b\; S\; c \to S + b\; c$

We have the following rewrite system from these axioms:

1. $+\,0\;a \rightarrow a$
2. $+\,b\;0 \rightarrow b$
3. $P\;S\;b \rightarrow b$
4. $+\,b\;S\;c \rightarrow S\,+\,b\;c$

Then we can apply these rules to prove that $+\,0\;S\;a = S\;a$.

$$\begin{aligned} +\,0\;S\;a &\rightarrow S\,+\,0\;a \qquad \text{(Rule \#4)} \\ &\rightarrow S\;a \qquad \text{(Rule \#1)} \end{aligned}$$

The recursive formula for addition is also symmetric: $+\,S\ a\ b = S + a\ b$. We can prove this by induction on $b$.

We start with the following axioms:

1. $P\ S\ a = a$
2. $+\ a\ 0 = a$
3. $+\ a\ S\ b = S + a\ b$
4. $+\ 0\ a = a$

We start with the following axioms:

1. $P\ S\ a = a$
2. $+\ a\ 0 = a$
3. $+\ a\ S\ b = S + a\ b$
4. $+\ 0\ a = a$

We get the following rewrite system:

1. $+\ 0\ a \longrightarrow a$
2. $+\ a\ 0 \longrightarrow a$
3. $P\ S\ a \longrightarrow a$
4. $+\ a\ S\ b \longrightarrow S + a\ b$

Base case: $b = 0$.

$$+\ S\ a\ 0 \longrightarrow S\ a \qquad \text{Rule \#2: } +\ a\ 0 \longrightarrow a$$
$$S + a\ 0 \longrightarrow S\ a \qquad \text{Rule \#2: } +\ a\ 0 \longrightarrow a$$

Inductive step: assume true for $b$, where $b$ is a constant term. We start with the following axioms:

1. $P\ S\ a = a$
2. $+\ a\ 0 = a$
3. $+\ a\ S\ c = S + a\ c$
4. $+\ 0\ a = a$
5. $+\ S\ a\ b = S + a\ b$

We end up with the following rewrite system:

1. $+ \, 0 \; a \longrightarrow a$
2. $+ \, a \; 0 \longrightarrow a$
3. $P \; S \; a \longrightarrow a$
4. $+ \, S \; a \; b \longrightarrow S + a \; b$
5. $+ \, a \; S \; c \longrightarrow S + a \; c$

We end up with the following rewrite system:

1. $+ 0\ a \longrightarrow a$
2. $+ a\ 0 \longrightarrow a$
3. $P\ S\ a \longrightarrow a$
4. $+ S\ a\ b \longrightarrow S + a\ b$
5. $+ a\ S\ c \longrightarrow S + a\ c$

Then for our inductive step:

$$\begin{aligned} +S\ a\ S\ b &\longrightarrow S + S\ a\ b && \text{Rule \#5: } + a\ S\ c \longrightarrow S + a\ c \\ &\longrightarrow S\ S + a\ b && \text{Rule \#4: } + S\ a\ b \longrightarrow S + a\ b \\ S + a\ S\ b &\longrightarrow S\ S + a\ b && \text{Rule \#5: } + a\ S\ c \longrightarrow S + a\ c \end{aligned}$$

Addition is associative. We will prove

$$+ \; + \, a \; b \; c = \; + \, a + b \; c$$

by induction on $a$.

Addition is associative. We will prove

$$+ \; + a \; b \; c = \; + a + b \; c$$

by induction on $a$.

Our axioms are now:

1. $P \; S \; a = a$
2. $+ \; a \; 0 = a$
3. $+ \; a \; S \; b = S + a \; b$
4. $+ \; 0 \; a = a$
5. $+ \; S \; a \; b = S + a \; b$

If we run *Simplification* on these axioms, we get five rewrite rules:

1. $+\,0\;a \longrightarrow a$
2. $+\,a\;0 \longrightarrow a$
3. $P\;S\;a \longrightarrow a$
4. $+\,a\;S\;b \longrightarrow S+a\;b$
5. $+\,S\;a\;b \longrightarrow S+a\;b$

Base case: $a = 0$. We seek to show that $+\ +0\ b\ c = +0 + b\ c$.

$$+\ +0\ b\ c \rightarrow\ +b\ c \qquad \text{Rule \#1:}\ +0\ a \rightarrow a$$
$$+0 + b\ c \rightarrow\ +b\ c \qquad \text{Rule \#1:}\ +0\ a \rightarrow a$$

Base case: $a = 0$. We seek to show that $+ \; + 0 \; b \; c =$ $+ 0 + b \; c$.

$$+ \; + 0 \; b \; c \longrightarrow \; + b \; c \qquad \text{Rule \#1:} \; + 0 \; a \longrightarrow a$$
$$+ 0 + b \; c \longrightarrow \; + b \; c \qquad \text{Rule \#1:} \; + 0 \; a \longrightarrow a$$

Inductive step: assume that $+ + a \; b \; c = \; + a + b \; c$ and try to show that $+ + a \; b \; c = \; + a + b \; c$. When we perform this step we are temporarily fixing $a$ as a constant. We therefore append our inductive hypothesis as an axiom after declaring $a$ to be a constant.

1. $P \; S \; b = b$
2. $+ \; b \; 0 = b$
3. $+ \; b \; S \; c = S + b \; c$
4. $+ \; 0 \; b = b$
5. $+ \; S \; b \; c = S + b \; c$
6. $+ \; + a \; b \; c = \; + a + b \; c$

If we run *Simplification* on these axioms, we get six rewrite rules:

1. $+\,0\,b \rightarrow b$
2. $+\,b\,0 \rightarrow b$
3. $P\,S\,b \rightarrow b$
4. $+\,b\,S\,c \rightarrow S + b\,c$
5. $+\,S\,b\,c \rightarrow S + b\,c$
6. $+\,+\,a\,b\,c \rightarrow\,+\,a + b\,c$

$$\begin{aligned} +\,+\,S\,a\,b\,c &\rightarrow\,+\,S + a\,b\,c && \text{Rule \#5} \\ &\rightarrow S +\,+\,a\,b\,c && \text{Rule \#5} \\ &\rightarrow S + a + b\,c && \text{Rule \#6} \\ +\,S\,a + b\,c &\rightarrow S + a + b\,c && \text{Rule \#5} \end{aligned}$$

If we run *Simplification* on these axioms, we get six rewrite rules:

1. $+\,0\;b \longrightarrow b$
2. $+\,b\;0 \longrightarrow b$
3. $P\;S\;b \longrightarrow b$
4. $+\,b\;S\;c \longrightarrow S+b\;c$
5. $+\,S\;b\;c \longrightarrow S+b\;c$
6. $+\;+a\;b\;c \longrightarrow\;+a+b\;c$

$$\begin{aligned} +\;+S\;a\;b\;c &\longrightarrow\;+S+a\;b\;c && \text{Rule \#5}\\ &\longrightarrow S+\;+a\;b\;c && \text{Rule \#5}\\ &\longrightarrow S+a+b\;c && \text{Rule \#6}\\ +S\;a+b\;c &\longrightarrow S+a+b\;c && \text{Rule \#5} \end{aligned}$$

*Simplification* would not converge in the proof for associativity if we had not shown first that $+S\;a\;b = S{+}a\;b$.

Rewrite systems can't handle commutativity. If we work with $+ a\ b = + b\ a$, which side is simpler than the other?

# 6. Conclusion

The proofs of some of the elementary properties of arithmetic are essentially mechanical in nature. Using rewrite systems, we can verify these algebraic identities by reducing each side and verifying that the two sides simplify to the same canonical form.

# 6. Conclusion

The proofs of some of the elementary properties of arithmetic are essentially mechanical in nature. Using rewrite systems, we can verify these algebraic identities by reducing each side and verifying that the two sides simplify to the same canonical form.

In using mathematical induction, the base case was straight-forward. For the inductive step, we added a new constant term and the inductive hypothesis as a new axiom to our system.

# 6. Conclusion

The proofs of some of the elementary properties of arithmetic are essentially mechanical in nature. Using rewrite systems, we can verify these algebraic identities by reducing each side and verifying that the two sides simplify to the same canonical form.

In using mathematical induction, the base case was straight-forward. For the inductive step, we added a new constant term and the inductive hypothesis as a new axiom to our system.

There were no significant simplifications in converting the axioms to a rewrite system; each equation became a rewrite rule.

# 6. Conclusion

The proofs of some of the elementary properties of arithmetic are essentially mechanical in nature. Using rewrite systems, we can verify these algebraic identities by reducing each side and verifying that the two sides simplify to the same canonical form.

In using mathematical induction, the base case was straight-forward. For the inductive step, we added a new constant term and the inductive hypothesis as a new axiom to our system.

There were no significant simplifications in converting the axioms to a rewrite system; each equation became a rewrite rule.

Neither the fact that $S$ was injective nor the fact that 0 was not in the image of $S$ was relevant. The only things that we needed were mathematical induction and the recursive definition of addition.

# 7. References

This talk and the related software can be found at `http://frodo.elon.edu` under the link "Simplification".


1. Franz Baader and Tobias Nipkow. *Term Rewriting and All That*. Cambridge University Press, 1998.
2. Donald E. Knuth and P.B. Bendix. Simple word problems in universal algebra. In J. Leech, editor, *Computational Problems in Abstract Algebra*, pages 263–297. Pergamon Press, 1970.
3. Enno Ohlebusch. *Advanced Topics in Term Rewriting*. Springer-Verlag, 2002.
4. All things *Python* can be found starting at `http://www.python.org`.
5. All things *Jython* (using *Python* to create *Java* bytecode) can be found starting at `http://www.jython.org`.