

Introduction to Logic

Equality

Michael Genesereth
Computer Science Department
Stanford University

Isomorphic Representation

People

michael $\leftrightarrow$ 
maureen $\leftrightarrow$ 

Arithmetic

0 $\leftrightarrow$ 0
s(0) $\leftrightarrow$ 1
s(*s*(0)) $\leftrightarrow$ 2
s(*s*(*s*(0))) $\leftrightarrow$ 3

In this course, we have so far assumed that there is a one-to-one relationship between ground terms in our language and objects in the application area we are trying to describe. For example, we assumed a unique name for each person. In Arithmetic, we assumed a unique term for each number. This is often called an isomorphic representation because there is a one to one relationship from the ground terms in our language onto objects in the world. This makes things conceptually simple, and it is a reasonable way to go in many circumstances. But not always.

Homomorphic Representation

People (Nicknames):

michael $\leftrightarrow$ 
mike $\leftrightarrow$ 

Arithmetic:

plus(*s*(0), *s*(0)) $\leftrightarrow$
times(*s*(*s*(0)), *s*(0)) $\leftrightarrow$ 2
s(*s*(0)) $\leftrightarrow$

In real life, we often find it convenient to use more than one term refer to the same real world object. For example, we sometimes have nicknames for the same person - Michael, Mike. And, in Elementary Arithmetic, we frequently use different terms to refer to the same number - $1+2$, $2*1$, and $s(s(0))$. This contradicts our assumption about isomorphic representation. However, we can deal with this in the context of Herbrand Logic.

Two Approaches

Approach 1 - Equality:
mike = michael
father(michael) = william

Equivalence of terms in Herbrand universe

Approach 2 - Evaluable Terms (nicknames):
s(0) + s(0) --> s(s(0))
s(s(0)) * s(0) --> s(s(0))

Add new terms (terms not in the Herbrand universe)
that "evaluate" to terms in Herbrand universe

Equality

Partitioning the Herbrand Universe

People:

michael mike	maureen	katherine kathy kate	...
-----------------	---------	----------------------------	-----

Arithmetic:

...	plus(s(0), s(0)) times(s(s(0)), s(0)) s(s(0))	...
-----	---	-----

Equality

Co-referential terms:

$plus(s(0), s(0))$
 $times(s(s(0)), s(0))$
 $s(s(0))$

Equality:

$equal(plus(s(0), s(0)), s(s(0)))$
 $equal(times(s(s(0)), s(0)), s(s(0)))$

Syntactic Sugar

Formal Syntax:

$equal(plus(s(0), s(0)), s(s(0)))$
 $equal(times(s(s(0)), s(0)), s(s(0)))$

Syntactic Sugar:

$s(0) + s(0) = s(s(0))$
 $s(s(0)) * s(0) = s(s(0))$

What is Needed

(1) Axioms that define properties of equality.

$michael = mike$
 $mike = michael$

(2) Axioms that ensure that any true sentence that mentions a given term is also true of the sentence in which that term is replaced by an equivalent term.

$older(michael, maureen) \Leftrightarrow older(mike, maureen)$

In real life, we often find it convenient to use more than one term refer to the same real world object. For example, we sometimes have nicknames for the same person - Michael, Mike. And, in Elementary Arithmetic, we frequently use different terms to refer to the same number - $2+2$, $2*2$, and $s(s(s(s(0))))$. This contradicts our assumption about isomorphic representation. However, we can deal with this in the context of Herbrand Logic.

Equality Axioms

Reflexivity

$$\forall x.(x=x)$$

Symmetry

$$\forall x.\forall y.(x=y \Rightarrow y=x)$$

Transitivity

$$\forall x.\forall y.\forall z.(x=y \wedge y=z \Rightarrow x=z)$$

Equality Proof

- | | | |
|----|--|---------|
| 1. | $b = a$ | Premise |
| 2. | $b = c$ | Premise |
| 3. | $\forall x.(x = x)$ | Premise |
| 4. | $\forall x.\forall y.(x = y \Rightarrow y = x)$ | Premise |
| 5. | $\forall x.\forall y.\forall z.(x = y \wedge y = z \Rightarrow x = z)$ | Premise |

Equality Proof

- | | | |
|----|--|-----------|
| 1. | $b = a$ | Premise |
| 2. | $b = c$ | Premise |
| 3. | $\forall x.(x = x)$ | Premise |
| 4. | $\forall x.\forall y.(x = y \Rightarrow y = x)$ | Premise |
| 5. | $\forall x.\forall y.\forall z.(x = y \wedge y = z \Rightarrow x = z)$ | Premise |
| 6. | $b = a \Rightarrow a = b$ | 2 x UE: 4 |
| 7. | $a = b$ | IE: 6, 1 |

Equality Proof

- | | | |
|----|--|-----------|
| 1. | $b = a$ | Premise |
| 2. | $b = c$ | Premise |
| 3. | $\forall x.(x = x)$ | Premise |
| 4. | $\forall x.\forall y.(x = y \Rightarrow y = x)$ | Premise |
| 5. | $\forall x.\forall y.\forall z.(x = y \wedge y = z \Rightarrow x = z)$ | Premise |
| 6. | $b = a \Rightarrow a = b$ | 2 x UE: 4 |
| 7. | $a = b$ | IE: 6, 1 |
| 8. | $a = b \wedge b = c \Rightarrow a = c$ | 3 x UE: 5 |

Equality Proof

- | | | |
|-----|--|-----------|
| 1. | $b = a$ | Premise |
| 2. | $b = c$ | Premise |
| 3. | $\forall x.(x = x)$ | Premise |
| 4. | $\forall x.\forall y.(x = y \Rightarrow y = x)$ | Premise |
| 5. | $\forall x.\forall y.\forall z.(x = y \wedge y = z \Rightarrow x = z)$ | Premise |
| 6. | $b = a \Rightarrow a = b$ | 2 x UE: 4 |
| 7. | $a = b$ | IE: 6, 1 |
| 8. | $a = b \wedge b = c \Rightarrow a = c$ | 3 x UE: 5 |
| 9. | $a = b \wedge b = c$ | AI: 7, 2 |
| 10. | $a = c$ | IE: 8, 9 |

Substitution Problems

Given:

$$f(a) = b$$

$$f(b) = a$$

Prove:

$$f(f(a)) = a$$

Given:

$$\forall x.\text{older}(\text{father}(x), x)$$

$$\text{father}(\text{bob}) = \text{art}$$

Prove:

$$\text{older}(\text{art}, \text{bob})$$

Substitution Axioms

Unary Relations

$$\forall x. \forall y. (p(x) \wedge x=y \Rightarrow p(y))$$

Binary Relations

$$\forall u. \forall v. \forall x. \forall y. (q(u,v) \wedge u=x \wedge v=y \Rightarrow q(x,y))$$

Unary Functions

$$\forall x. \forall y. \forall z. (f(x)=z \wedge x=y \Rightarrow f(y)=z)$$

Binary Functions

$$\forall u. \forall v. \forall x. \forall y. \forall z. (g(u,v)=z \wedge u=x \wedge v=y \Rightarrow g(x,y)=z)$$

Substitution Proof

1.	$f(a) = b$	Premise
2.	$f(b) = a$	Premise
3.	$\forall x.(x = x)$	Premise
4.	$\forall x. \forall y.(x = y \Rightarrow y = x)$	Premise
5.	$\forall x. \forall y. \forall z.(x = y \wedge y = z \Rightarrow x = z)$	Premise
6.	$\forall x. \forall y. \forall z.(f(x)=z \wedge x=y \Rightarrow f(y)=z)$	Premise

Substitution Proof

1.	$f(a) = b$	Premise
2.	$f(b) = a$	Premise
3.	$\forall x.(x = x)$	Premise
4.	$\forall x. \forall y.(x = y \Rightarrow y = x)$	Premise
5.	$\forall x. \forall y. \forall z.(x = y \wedge y = z \Rightarrow x = z)$	Premise
6.	$\forall x. \forall y. \forall z.(f(x)=z \wedge x=y \Rightarrow f(y)=z)$	Premise
7.	$f(b)=a \wedge b=f(a) \Rightarrow f(f(a))=a$	3 x UE: 6
8.	$f(a)=b \Rightarrow b=f(a)$	2 x UE: 4
9.	$b=f(a)$	IE: 8, 1

Substitution Proof

1. $f(a) = b$	Premise
2. $f(b) = a$	Premise
3. $\forall x.(x = x)$	Premise
4. $\forall x.\forall y.(x = y \Rightarrow y = x)$	Premise
5. $\forall x.\forall y.\forall z.(x = y \wedge y = z \Rightarrow x = z)$	Premise
6. $\forall x.\forall y.\forall z.(f(x)=z \wedge x=y \Rightarrow f(y)=z)$	Premise
7. $f(b)=a \wedge b=f(a) \Rightarrow f(f(a))=a$	3 x UE: 6
8. $f(a)=b \Rightarrow b=f(a)$	2 x UE: 4
9. $b=f(a)$	IE: 8, 1
10. $f(b) = a \wedge b=f(a)$	AI: 2, 9
11. $f(f(a))=a$	IE: 7, 10

Too tedious. Too long.

Rules of Inference

Equality Introduction (QI):

$$\frac{}{\tau = \tau}$$

where τ is a ground term

Equality Elimination (QE) - also called *paramodulation*:

$$\frac{\begin{array}{c} \phi \\ \sigma = \tau \end{array}}{\phi_{\sigma \leftarrow \tau}}$$

where σ and τ are ground terms

NB: $\phi_{\sigma \leftarrow \tau}$ is a copy of ϕ with *0 or more* occurrences of σ replaced by τ .

NB: Works using the equality in the opposite direction as well.

Substitution Proof

1. $f(a) = b$	Premise
2. $f(b) = a$	Premise
3. $f(f(a)) = a$	QE: 2, 1

Substitution Proof

1. $\forall x. \text{older}(\text{father}(x), x)$

2. $\text{father}(\text{bob}) = \text{art}$

3. $\text{older}(\text{father}(\text{bob}), \text{bob})$

4. $\text{older}(\text{art}, \text{bob})$
- Premise

Premise

UE: 1

QE: 3, 2

Fitch				
Undo Copy Paste Load Save Library Help				
		Objects:		
		Functions:		
☐	Select All			
☐	1.	$f(a)=b$	Premise	
☐	2.	$f(b)=a$	Premise	
☐	3.	$f(f(a))=a$	Equality Elimination: 1, 2	
Premise	Negation Introduction	Assumption	Universal Introduction	Domain Closure
Reiteration	Negation Elimination	Implication Introduction	Universal Elimination	Induction
Truthable	And Introduction	Implication Elimination	Existential Introduction	Equality Introduction
Shortcut	And Elimination	Biconditional Introduction	Existential Elimination	Equality Elimination
Replace	Or Introduction	Biconditional Elimination		Rational Equation
Coalesce	Or Elimination			Rational Induction
Delete				

Fitch				
Undo Copy Paste Load Save Library Help				
+ -	Objects:			
+ -	Functions:			
☐	Select All			
☐	1.	AX:older(father(X),X)	Premise	
☐	2.	father(bob)=art	Premise	
☐	3.	older(father(bob),bob)	Universal Elimination: 1	
☐	4.	older(art,bob)	Equality Elimination: 2,3	
Premise	Negation Introduction	Assumption	Universal Introduction	Domain Closure
Reiteration	Negation Elimination		Universal Elimination	Induction
Truthable	And Introduction	Implication Elimination	Existential Introduction	Equality Introduction
Shortcut	And Elimination	Biconditional Introduction	Existential Elimination	Equality Elimination
Replace	Or Introduction	Biconditional Elimination		Rational Equation
Coalesce	Or Elimination			Rational Induction
Delete				

Evaluable Terms

Signature

Object Constant: 0, ...

Unary Function Constant: s

Evaluable Function Constants: $+$, $\times$

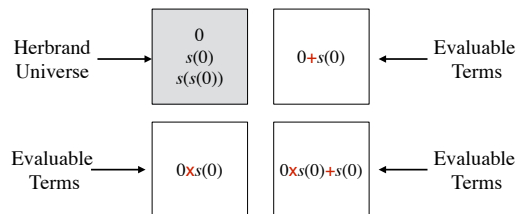
Binary Relation Constant: $=$

*Evaluable functions do **not** expand Herbrand universe.*

*Evaluable terms **refer** to terms in Herbrand universe.*

*Evaluable functions **defined** in terms of other concepts.*

Different Types of Terms



Significance

For induction to work, we must show that a property holds of **all terms in the Herbrand Universe** (Herbrand terms).

When some objects or functions are defined in terms of others, it is not necessary to show that a property holds of **evaluable terms** (since all sentences involving those terms necessarily have the same truth values as sentences with equivalent **Herbrand terms**).

Upshot: Need to do induction only on objects and functions comprising the Herbrand universe.

Binary Function Example

Object Constant: 0, ...

Unary Function Constant: s

Binary Evaluable Function Constant: $+$

Binary Relation Constant: $=$

Binary Function Problem

Axioms for $+$:

$$\begin{aligned} &\forall y.(y + 0 = y) \\ &\forall x.\forall y.(x + s(y) = s(x + y)) \end{aligned}$$

Problem: Prove that 0 is a left identity for $+$.

$$\forall y.(0 + y = y)$$

Inductive Proof

- | | | |
|----|---|---------|
| 1 | $\forall x. (x + 0 = x)$ | Premise |
| 2. | $\forall x. \forall y. (x + s(y) = s(x + y))$ | Premise |

Inductive Proof

- | | | |
|----|---|---------|
| 1 | $\forall x. (x + 0 = x)$ | Premise |
| 2. | $\forall x. \forall y. (x + s(y) = s(x + y))$ | Premise |
| 3. | $0 + 0 = 0$ | UE: 1 |

Inductive Proof

- | | | |
|----|---|------------|
| 1 | $\forall x. (x + 0 = x)$ | Premise |
| 2. | $\forall x. \forall y. (x + s(y) = s(x + y))$ | Premise |
| 3. | $0 + 0 = 0$ | UE: 1 |
| 4. | $ 0 + c = c$ | Assumption |

Inductive Proof

- | | | |
|---|---|------------|
| 1 | $\forall x. (x + 0 = x)$ | Premise |
| 2 | $\forall x. \forall y. (x + s(y) = s(x + y))$ | Premise |
| 3 | $0 + 0 = 0$ | UE: 1 |
| 4 | $\left 0 + c = c \right.$ | Assumption |
| 5 | $\left \forall y. (0 + s(y) = s(0 + y)) \right.$ | UE: 2 |

Inductive Proof

- | | | |
|---|---|------------|
| 1 | $\forall x. (x + 0 = x)$ | Premise |
| 2 | $\forall x. \forall y. (x + s(y) = s(x + y))$ | Premise |
| 3 | $0 + 0 = 0$ | UE: 1 |
| 4 | $\left 0 + c = c \right.$ | Assumption |
| 5 | $\left \forall y. (0 + s(y) = s(0 + y)) \right.$ | UE: 2 |
| 6 | $\left 0 + s(c) = s(0 + c) \right.$ | UE: 5 |

Inductive Proof

- | | | |
|---|---|------------|
| 1 | $\forall x. (x + 0 = x)$ | Premise |
| 2 | $\forall x. \forall y. (x + s(y) = s(x + y))$ | Premise |
| 3 | $0 + 0 = 0$ | UE: 1 |
| 4 | $\left 0 + c = c \right.$ | Assumption |
| 5 | $\left \forall y. (0 + s(y) = s(0 + y)) \right.$ | UE: 2 |
| 6 | $\left 0 + s(c) = s(0 + c) \right.$ | UE: 5 |
| 7 | $\left 0 + s(c) = s(c) \right.$ | QE: 6, 4 |

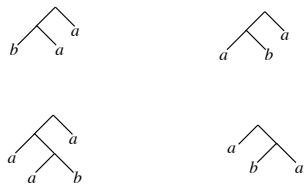
Inductive Proof

- | | | |
|----|---|------------|
| 1. | $\forall x. (x + 0 = x)$ | Premise |
| 2. | $\forall x. \forall y. (x + s(y) = s(x + y))$ | Premise |
| 3. | $0 + 0 = 0$ | UE: 1 |
| 4. | $0 + c = c$ | Assumption |
| 5. | $\forall y. (0 + s(y) = s(0 + y))$ | UE: 2 |
| 6. | $0 + s(c) = s(0 + c)$ | UE: 5 |
| 7. | $0 + s(c) = s(c)$ | QE: 6, 4 |
| 8. | $0 + c = c \Rightarrow 0 + s(c) = s(c)$ | II: 4, 7 |

Inductive Proof

- | | | |
|-----|--|------------|
| 1. | $\forall x. (x + 0 = x)$ | Premise |
| 2. | $\forall x. \forall y. (x + s(y) = s(x + y))$ | Premise |
| 3. | $0 + 0 = 0$ | UE: 1 |
| 4. | $0 + c = c$ | Assumption |
| 5. | $\forall y. (0 + s(y) = s(0 + y))$ | UE: 2 |
| 6. | $0 + s(c) = s(0 + c)$ | UE: 5 |
| 7. | $0 + s(c) = s(c)$ | QE: 6, 4 |
| 8. | $0 + c = c \Rightarrow 0 + s(c) = s(c)$ | II: 4, 7 |
| 9. | $\forall y. (0 + y = y \Rightarrow 0 + s(y) = s(y))$ | UI: 8 |
| 10. | $\forall y. (0 + y = y)$ | Ind: 3, 9 |

Trees

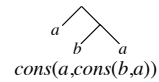
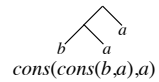


Trees have many properties - e.g. symmetry, uniformity. Also many relationships - e.g. congruence.

Tree Vocabulary

Object constants: a, b

Binary function constant: $cons$

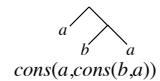
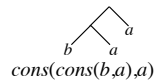


Binary relation constant: $equal$

Tree Vocabulary

Object constants: a, b

Binary function constant: $cons$



Unary evaluable function: rev

Binary relation constant: $equal$

Reversing Trees



Reversing Atomic Trees:

$$\begin{aligned} rev(a) &= a \\ rev(b) &= b \end{aligned}$$

Reversing Compound Trees:

$$\forall x. (rev(cons(x, y)) = cons(rev(y), rev(x)))$$

Problem

Reverse is its own inverse. (In other words, the result of reversing a list twice is equal to the original list.)

$\forall x. rev(rev(x)) = x$

Let's prove it using induction.

Hint: *rev* is defined in terms of *cons* so we just need to do induction on *cons*.

Before we leave our discussion of Peano arithmetic, it is worthwhile to look at the concept of Diophantine equations. A polynomial equation is an algebraic expression composed using only addition, multiplication, and exponentiation with fixed exponents (that is numbers not variables). For example, $3x^2 + 2y = 2z^3$ is a polynomial equation. A natural Diophantine equation is a polynomial equation in which the variables are restricted to the natural numbers. For example, the polynomial equation here is also a Diophantine equation and happens to have a solution in the natural numbers, viz. $X=2$ and $y=2$ and $z=2$.

Proof By Induction

1. $rev(a) = a$	Premise
2. $rev(b) = b$	Premise
3. $\forall x. \forall y. (rev(cons(x, y)) = cons(rev(y), rev(x)))$	Premise
4. $rev(rev(a)) = a$	QE: 1, 1
5. $rev(rev(b)) = b$	QE: 2, 2

Proof By Induction

1. $rev(a) = a$	Premise
2. $rev(b) = b$	Premise
3. $\forall x. \forall y. (rev(cons(x, y)) = cons(rev(y), rev(x)))$	Premise
4. $rev(rev(a)) = a$	QE: 1, 1
5. $rev(rev(b)) = b$	QE: 2, 2
6. $\mid rev(rev(c)) = c \wedge rev(rev(d)) = d$	Assumption

Proof By Induction

1.	$rev(a) = a$	Premise
2.	$rev(b) = b$	Premise
3.	$\forall x. \forall y. (rev(cons(x, y)) = cons(rev(y), rev(x)))$	Premise
4.	$rev(rev(a)) = a$	QE: 1, 1
5.	$rev(rev(b)) = b$	QE: 2, 2
6.	$rev(rev(c)) = c \wedge rev(rev(d)) = d$	Assumption
7.	$rev(rev(cons(c, d))) = rev(rev(cons(c, d)))$	QI

Proof By Induction

1.	$rev(a) = a$	Premise
2.	$rev(b) = b$	Premise
3.	$\forall x. \forall y. (rev(cons(x, y)) = cons(rev(y), rev(x)))$	Premise
4.	$rev(rev(a)) = a$	QE: 1, 1
5.	$rev(rev(b)) = b$	QE: 2, 2
6.	$rev(rev(c)) = c \wedge rev(rev(d)) = d$	Assumption
7.	$rev(rev(cons(c, d))) = rev(rev(cons(c, d)))$	QI
8.	$rev(rev(cons(c, d))) = rev(cons(rev(d), rev(c)))$	UE QE: 7, 3

Proof By Induction

1.	$rev(a) = a$	Premise
2.	$rev(b) = b$	Premise
3.	$\forall x. \forall y. (rev(cons(x, y)) = cons(rev(y), rev(x)))$	Premise
4.	$rev(rev(a)) = a$	QE: 1, 1
5.	$rev(rev(b)) = b$	QE: 2, 2
6.	$rev(rev(c)) = c \wedge rev(rev(d)) = d$	Assumption
7.	$rev(rev(cons(c, d))) = rev(rev(cons(c, d)))$	QI
8.	$rev(rev(cons(c, d))) = rev(cons(rev(d), rev(c)))$	UE QE: 7, 3
9.	$rev(rev(cons(c, d))) = cons(rev(rev(c)), rev(rev(d)))$	UE QE: 8, 3

Proof By Induction

1.	$rev(a) = a$	Premise
2.	$rev(b) = b$	Premise
3.	$\forall x. \forall y. (rev(cons(x, y)) = cons(rev(y), rev(x)))$	Premise
4.	$rev(rev(a)) = a$	QE: 1, 1
5.	$rev(rev(b)) = b$	QE: 2, 2
6.	$rev(rev(c)) = c \wedge rev(rev(d)) = d$	Assumption
7.	$rev(rev(cons(c, d))) = rev(rev(cons(c, d)))$	QI
8.	$rev(rev(cons(c, d))) = rev(cons(rev(d), rev(c)))$	UE QE: 7, 3
9.	$rev(rev(cons(c, d))) = cons(rev(rev(c)), rev(rev(d)))$	UE QE: 8, 3
10.	$rev(rev(cons(c, d))) = cons(c, d)$	2 x QE: 9, 6

Proof By Induction

1.	$rev(a) = a$	Premise
2.	$rev(b) = b$	Premise
3.	$\forall x. \forall y. (rev(cons(x, y)) = cons(rev(y), rev(x)))$	Premise
4.	$rev(rev(a)) = a$	QE: 1, 1
5.	$rev(rev(b)) = b$	QE: 2, 2
6.	$rev(rev(c)) = c \wedge rev(rev(d)) = d$	Assumption
7.	$rev(rev(cons(c, d))) = rev(rev(cons(c, d)))$	QI
8.	$rev(rev(cons(c, d))) = rev(cons(rev(d), rev(c)))$	UE QE: 7, 3
9.	$rev(rev(cons(c, d))) = cons(rev(rev(c)), rev(rev(d)))$	UE QE: 8, 3
10.	$rev(rev(cons(c, d))) = cons(c, d)$	2 x QE: 9, 6
11.	$rev(rev(c)) = c \wedge rev(rev(d)) = d \implies rev(rev(cons(c, d))) = cons(c, d)$	II: 6, 10

Proof By Induction

1.	$rev(a) = a$	Premise
2.	$rev(b) = b$	Premise
3.	$\forall x. \forall y. (rev(cons(x, y)) = cons(rev(y), rev(x)))$	Premise
4.	$rev(rev(a)) = a$	QE: 1, 1
5.	$rev(rev(b)) = b$	QE: 2, 2
6.	$rev(rev(c)) = c \wedge rev(rev(d)) = d$	Assumption
7.	$rev(rev(cons(c, d))) = rev(rev(cons(c, d)))$	QI
8.	$rev(rev(cons(c, d))) = rev(cons(rev(d), rev(c)))$	UE QE: 7, 3
9.	$rev(rev(cons(c, d))) = cons(rev(rev(c)), rev(rev(d)))$	UE QE: 8, 3
10.	$rev(rev(cons(c, d))) = cons(c, d)$	2 x QE: 9, 6
11.	$rev(rev(c)) = c \wedge rev(rev(d)) = d \implies rev(rev(cons(c, d))) = cons(c, d)$	II: 6, 10
12.	$\forall x. \forall y. (rev(rev(x)) = x \wedge rev(rev(y)) = y \implies rev(rev(cons(x, y))) = cons(x, y))$	2 x UI: 11

Proof By Induction

1.	$rev(a) = a$	Premise
2.	$rev(b) = b$	Premise
3.	$\forall x. \forall y. (rev(cons(x, y)) = cons(rev(y), rev(x)))$	Premise
4.	$rev(rev(a)) = a$	QE: 1, 1
5.	$rev(rev(b)) = b$	QE: 2, 2
6.	$rev(rev(c)) = c \wedge rev(rev(d)) = d$	Assumption
7.	$rev(rev(cons(c, d))) = rev(rev(cons(c, d)))$	QI
8.	$rev(rev(cons(c, d))) = rev(cons(rev(d), rev(c)))$	UE QE: 7, 3
9.	$rev(rev(cons(c, d))) = cons(rev(rev(c)), rev(rev(d)))$	UE QE: 8, 3
10.	$rev(rev(cons(c, d))) = cons(c, d)$	2 x QE: 9, 6
11.	$rev(rev(c)) = c \wedge rev(rev(d)) = d \implies rev(rev(cons(c, d))) = cons(c, d)$	II: 6, 10
12.	$\forall x. \forall y. (rev(rev(x)) = x \wedge rev(rev(y)) = y \implies rev(rev(cons(x, y))) = cons(x, y))$	2 x UI: 11
13.	$\forall x. (rev(rev(x)) = x)$	Ind: 4, 5, 12

Polynomial Arithmetic

Signature for Arithmetic

- Object Constant: 0
- Unary Function Constant: *s*
- Binary Evaluable Function Constants:
 - plus* - addition
 - times* - multiplication
- Binary Relation Constant: =

More Syntactic Sugar

Formal Syntax:

$equal(plus(s(0), s(0)), s(s(0)))$
 $equal(times(s(s(0)), s(0)), s(s(0)))$

Syntactic Sugar:

$1 + 1 = 2$
 $2 \times 1 = 2$

Definitions of Evaluable Arithmetic Functions

Addition:

$\forall x.(x + 0 = x)$
 $\forall x.\forall y.(x + (y + 1) = (x + y) + 1)$

Multiplication:

$\forall y.(0 \times y = 0)$
 $\forall x.\forall y.((x + 1) \times y = (x \times y) + y)$

Once we have the same relation, we can define the other relations in our arithmetic. The axioms shown here define the plus relation in terms of 0, s, and same. Adding 0 to any number results in that number. If adding a number x to a number y produces a number z, then adding the successor of x to y produces the successor of z. Finally, using same, we write a functionality axiom for plus.

Equality Proof

- | | | |
|----|--|---------|
| 1. | $b = a$ | Premise |
| 2. | $b = c$ | Premise |
| 3. | $\forall x.(x = x)$ | Premise |
| 4. | $\forall x.\forall y.(x = y \Rightarrow y = x)$ | Premise |
| 5. | $\forall x.\forall y.\forall z.(x = y \wedge y = z \Rightarrow x = z)$ | Premise |

Long Messy Proofs

1.	$f(a) = b$	Premise
2.	$f(b) = a$	Premise
3.	$\forall x.(x = x)$	Premise
4.	$\forall x.\forall y.(x = y \Rightarrow y = x)$	Premise
5.	$\forall x.\forall y.\forall z.(x = y \wedge y = z \Rightarrow x = z)$	Premise
6.	$\forall x.\forall y.\forall z.(f(x)=z \wedge x=y \Rightarrow f(y)=z)$	Premise
7.	$f(b)=a \wedge b=f(a) \Rightarrow f(f(a))=a$	3 x UE: 6
8.	$f(a)=b \Rightarrow b=f(a)$	2 x UE: 4
9.	$b=f(a)$	IE: 8, 1
10.	$f(b) = a \wedge b=f(a)$	AI: 2, 9
11.	$f(f(a))=a$	IE: 7, 10

Rational Equation

Rule of Inference (Rational Equation):

$$\frac{}{\sigma = \tau}$$

where σ and τ are **equivalent** polynomials

Example:

$$\frac{}{(c+1)^*(c+1) = c*c+2*c+1}$$

Rational Induction

+ definable in terms of s , so we need only do induction on s .

$$\frac{\begin{array}{l} \phi[0] \\ \forall x.(\phi[x] \Rightarrow \phi[s(x)]) \end{array}}{\forall x.\phi[x]}$$

Rational Induction (since $x + 1 = s(x)$)

$$\frac{\begin{array}{l} \phi[0] \\ \forall x.(\phi[x] \Rightarrow \phi[x + 1]) \end{array}}{\forall x.\phi[x]}$$

Problem

Consider the following function.

$$\begin{aligned} f(0) &= 0 \\ \forall z. (f(z+1) &= f(z) + (z+1) + (z+1)) \end{aligned}$$

$f(z)$ is 2 x the sum of numbers from 0 through z .

Problem

Function definition:

$$\begin{aligned} f(0) &= 0 \\ \forall z. (f(z+1) &= f(z) + (z+1) + (z+1)) \end{aligned}$$

Claim: f can be defined *non-recursively* in terms of $+$ and $\times$.

$$\forall z. (f(z) = z \times (z + 1))$$

Let's prove it, using induction.

Problem

- | | | |
|----|--|---------|
| 1 | $f(0) = 0$ | Premise |
| 2. | $\forall z. (f(z+1) = f(z) + (z+1) + (z+1))$ | Premise |

Problem	
1. $f(0) = 0$	Premise
2. $\forall z.(f(z+1) = f(z) + (z+1) + (z+1))$	Premise
3. $0 \times (0 + 1) = 0$	Equation

Problem	
1. $f(0) = 0$	Premise
2. $\forall z.(f(z+1) = f(z) + (z+1) + (z+1))$	Premise
3. $0 = 0 \times (0 + 1)$	Equation
4. $f(0) = 0 \times (0 + 1)$	QE: 3, 1
Base Case for : $\forall z.(f(z) = z \times (z + 1))$	

Problem	
1. $f(0) = 0$	Premise
2. $\forall z.(f(z+1) = f(z) + (z+1) + (z+1))$	Premise
3. $0 \times (0 + 1) = 0$	Equation
4. $f(0) = 0 \times (0 + 1)$	QE: 3, 1
5. $\downarrow f(c) = c \times (c+1)$	Assumption
We want to prove: $\forall z.(f(z) = z \times (z + 1) \Rightarrow f(z+1) = (z + 1) \times ((z + 1) + 1))$ To do that, we need to prove: $f(c) = c \times (c + 1) \Rightarrow f(c+1) = (c + 1) \times ((c + 1) + 1)$ To do that, we assume $f(c) = c \times (c + 1)$ and prove $f(c+1) = (c + 1) \times ((c + 1) + 1)$	

Problem		
1	$f(0) = 0$	Premise
2.	$\forall z.(f(z+1) = f(z) + (z+1) + (z+1))$	Premise
3.	$0 \times (0 + 1) = 0$	Equation
4.	$f(0) = 0 \times (0 + 1)$	QE: 3, 1
5.	$\downarrow f(c) = c \times (c+1)$	Assumption
6.	$\downarrow f(c+1) = f(c) + (c+1) + (c+1)$	UE: 2

Problem		
1	$f(0) = 0$	Premise
2.	$\forall z.(f(z+1) = f(z) + (z+1) + (z+1))$	Premise
3.	$0 \times (0 + 1) = 0$	Equation
4.	$f(0) = 0 \times (0 + 1)$	QE: 3, 1
5.	$\downarrow f(c) = c \times (c+1)$	Assumption
6.	$\downarrow f(c+1) = f(c) + (c+1) + (c+1)$	UE: 2
7.	$\downarrow f(c+1) = c \times (c+1) + (c+1) + (c+1)$	QE: 5, 6

Problem		
1	$f(0) = 0$	Premise
2.	$\forall z.(f(z+1) = f(z) + (z+1) + (z+1))$	Premise
3.	$0 \times (0 + 1) = 0$	Equation
4.	$f(0) = 0 \times (0 + 1)$	QE: 3, 1
5.	$\downarrow f(c) = c \times (c+1)$	Assumption
6.	$\downarrow f(c+1) = f(c) + (c+1) + (c+1)$	UE: 2
7.	$\downarrow f(c+1) = c \times (c+1) + (c+1) + (c+1)$	QE: 5, 6
8.	$\downarrow c \times (c+1) + (c+1) + (c+1) = (c+1) \times ((c+1) + 1)$	Equation

Problem		
1	$f(0) = 0$	Premise
2	$\forall z.(f(z+1) = f(z) + (z+1) + (z+1))$	Premise
3	$0 \times (0 + 1) = 0$	Equation
4	$f(0) = 0 \times (0 + 1)$	QE: 3, 1
5	$f(c) = c \times (c+1)$	Assumption
6	$f(c+1) = f(c) + (c+1) + (c+1)$	UE: 2
7	$f(c+1) = c \times (c+1) + (c+1) + (c+1)$	QE: 5, 6
8	$c \times (c+1) + (c+1) + (c+1) = (c+1) \times ((c+1) + 1)$	Equation
9	$f(c+1) = (c+1) \times ((c+1) + 1)$	QE: 8, 7

Problem		
1	$f(0) = 0$	Premise
2	$\forall z.(f(z+1) = f(z) + (z+1) + (z+1))$	Premise
3	$0 \times (0 + 1) = 0$	Equation
4	$f(0) = 0 \times (0 + 1)$	QE: 3, 1
5	$f(c) = c \times (c+1)$	Assumption
6	$f(c+1) = f(c) + (c+1) + (c+1)$	UE: 2
7	$f(c+1) = c \times (c+1) + (c+1) + (c+1)$	QE: 5, 6
8	$c \times (c+1) + (c+1) + (c+1) = (c+1) \times ((c+1) + 1)$	Equation
9	$f(c+1) = (c+1) \times ((c+1) + 1)$	QE: 8, 7
10	$f(c) = c \times (c+1) \Rightarrow f(c+1) = (c+1) \times ((c+1) + 1)$	II: 5, 9

Problem		
1	$f(0) = 0$	Premise
2	$\forall z.(f(z+1) = f(z) + (z+1) + (z+1))$	Premise
3	$0 \times (0 + 1) = 0$	Equation
4	$f(0) = 0 \times (0 + 1)$	QE: 3, 1
5	$f(c) = c \times (c+1)$	Assumption
6	$f(c+1) = f(c) + (c+1) + (c+1)$	UE: 2
7	$f(c+1) = c \times (c+1) + (c+1) + (c+1)$	QE: 5, 6
8	$c \times (c+1) + (c+1) + (c+1) = (c+1) \times ((c+1) + 1)$	Equation
9	$f(c+1) = (c+1) \times ((c+1) + 1)$	QE: 8, 7
10	$f(c) = c \times (c+1) \Rightarrow f(c+1) = (c+1) \times ((c+1) + 1)$	II: 5, 9
11	$\forall z.(f(z) = z \times (z+1) \Rightarrow f(z+1) = (z+1) \times ((z+1) + 1))$	UI: 10

Problem

- 1

$f(0) = 0$

Premise
- 2

$\forall z.(f(z+1) = f(z) + (z+1) + (z+1))$

Premise
- 3

$0 \times (0 + 1) = 0$

Equation
- 4

$f(0) = 0 \times (0 + 1)$

QE: 3, 1
- 5

$f(c) = c \times (c+1)$

Assumption
- 6

$f(c+1) = f(c) + (c+1) + (c+1)$

UE: 2
- 7

$f(c+1) = c \times (c+1) + (c+1) + (c+1)$

QE: 5, 6
- 8

$c \times (c+1) + (c+1) + (c+1) = (c+1) \times ((c+1) + 1)$

Equation
- 9

$f(c+1) = (c+1) \times ((c+1) + 1)$

QE: 8, 7
- 10

$f(c) = c \times (c+1) \Rightarrow f(c+1) = (c+1) \times ((c+1) + 1)$

II: 5, 9
- 11

$\forall z.(f(z) = z \times (z+1) \Rightarrow f(z+1) = (z+1) \times ((z+1) + 1))$

UI: 10
- 12

$\forall z.(f(z) = z \times (z+1))$

Ratind: 4, 11

Fitch		
Undo Copy Paste Load Save Help		
⌋	Objects:	
⌋	Functions:	
Select All		
1.	$f(0)=0$	Premise
2.	$AZ:f(Z+1)=f(Z)+(Z+1)+(Z+1)$	Premise
3.	$0*(0+1)=0$	Equation
4.	$f(0)=0*(0+1)$	Equality Elimination: 3, 1
5.	$f(c)=c*(c+1)$	Assumption
6.	$f(c+1)=f(c)+(c+1)+(c+1)$	Universal Elimination: 2
7.	$f(c+1)=c*(c+1)+(c+1)+(c+1)$	Equality Elimination: 5, 6
8.	$c*(c+1)+(c+1)+(c+1)=(c+1)*((c+1)+1)$	Equation
9.	$f(c+1)=(c+1)*((c+1)+1)$	Equality Elimination: 8, 7
10.	$f(c)=c*(c+1) \Rightarrow f(c+1)=(c+1)*((c+1)+1)$	Implication Introduction: 5, 9
11.	$AZ:f(Z)=Z*(Z+1) \Rightarrow f(Z+1)=(Z+1)*((Z+1)+1)$	Universal Introduction: 10
12.	$AZ:f(Z)=Z*(Z+1)$	Rational Induction
Goal	$AZ:f(Z)=Z*(Z+1)$	Complete

Yet Another Problem

Recursive Function:

$g(0) = 0$

$g(z + 1) = g(z) + (2 \times z + 1)$

z	$g(z)$
0	0
1	1
2	4
3	9

Non-recursive definition in terms of z :

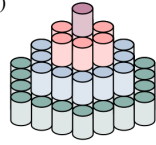
$g(z) = z \times z$

And Another

Number of cans per layer (starting at 1)

$$h(1) = 1$$

$$h(z + 1) = h(z) + 6 \times z$$



Non-recursive definition in terms of + and $\times$:

$$h(z+1) = 3 \times z \times (z + 1) + 1$$

