CS208 (Semester 1) Week 9 : Equality and Arithmetic

Dr. Robert Atkey

Computer & Information Sciences

Equality and Arithmetic, Part 1

Rules for Equality

What is Equality?

$$t_1 = t_2$$

What is Equality?

Some properties:

1. *Reflexivity:* for all x, $x = x$
2. *Symmetry:* for all x and y, if $x = y$ then $y = x$
3. *Transitivity:* for all x, y and z, if $x = y$ and $y = z$, then $x = z$

What is Equality?

Some properties:

1. *Reflexivity:* for all x, $x = x$
2. *Symmetry:* for all x and y, if $x = y$ then $y = x$
3. *Transitivity:* for all x, y and z, if $x = y$ and $y = z$, then $x = z$

Any binary relation that satisfies these properties is called an *equivalence relation.*

What is Equality?

The **special** property of equality is the following:

If $s = t$, then everything that is true about s is true about t.

What is Equality?

The **special** property of equality is the following:

If $s = t$, then everything that is true about s is true about t.

(and vice versa. but do we need to say this?)

What is Equality?

The **special** property of equality is the following:

If $s = t$, then everything that is true about s is true about t.

(and vice versa. but do we need to say this?)

Gottfried Leibniz (co-inventor of Calculus) took this as the *definition* of equality.

What is Equality?

With more symbols:

$$\text{If } t_1 = t_2\text{, then for all } P\text{, if } P[x \mapsto t_1] \text{ then } P[x \mapsto t_2]$$

What is Equality?

All we will need is:

1. Reflexivity: for every term t, $t = t$
2. Substitution: $t_1 = t_2$ and $P[x \mapsto t_1]$ implies $P[x \mapsto t_2]$

Amazingly, this is enough!

Symmetry

To prove that $x = y$ implies $y = x$:

1. We know that $x = x$ by reflexivity
2. So we use our assumption to replace the first x by y to get $y = x$.

Transitivity

To prove that $x = y$ and $y = z$ implies $x = z$:

1. Substitute the second assumption in the first to get $x = z$.

Rules for Equality: Introduction

$$\frac{}{\Gamma \vdash t = t}\ \textsc{Reflexivity}$$

Every term is equal to itself.

Rules for Equality: Elimination

$$\frac{\Gamma \vdash P[x \mapsto t_2]}{\Gamma\ [t_1 = t_2] \vdash P[x \mapsto t_1]}\ \textsc{Subst}$$

If we know that $t_1 = t_2$ then we can replace t_1 with t_2 in the goal. This is substitution backwards: if we know $P[x \mapsto t_2]$ and $t_1 = t_2$, then we know $P[x \mapsto t_1]$.

Example: Symmetry

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{x, y, x = y \vdash y = y}\ \textsc{Reflexivity}}{x, y, x = y\ [x = y] \vdash y = x}\ \textsc{Subst}}{x, y, x = y \vdash y = x}\ \textsc{Use}}{x, y \vdash x = y \to y = x}\ \textsc{Introduce}}{x \vdash \forall y. x = y \to y = x}\ \textsc{Introduce}}{\vdash \forall x. \forall y. x = y \to y = x}\ \textsc{Introduce}
$$

Example: Transitivity

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{x, y, z, x = y, y = z \; [y = z] \vdash y = z}\textsc{Done}}{x, y, z, x = y, y = z \vdash y = z}\textsc{Use}}{x, y, z, x = y, y = z \; [x = y] \vdash x = z}\textsc{Subst}}{x, y, z, x = y, y = z \vdash x = z}\textsc{Use}}{x, y, z, x = y \vdash y = z \to x = z}\textsc{Introduce}}{x, y, z \vdash x = y \to y = z \to x = z}\textsc{Introduce}}{x, y \vdash \forall z. x = y \to y = z \to x = z}\textsc{Introduce}}{x \vdash \forall y. \forall z. x = y \to y = z \to x = z}\textsc{Introduce}}{\vdash \forall x. \forall y. \forall z. x = y \to y = z \to x = z}\textsc{Introduce}
$$

Rewriting

1. Subst can be quite tricky to use because we have to give a formula P such that $P[x \mapsto t_1]$ is the one we start with, and $P[x \mapsto t_2]$ is the one we end up with.
2. Usually, we want to replace *every* occurrence of t_1 with t_2. We write this as:

$$P\{t_1 \mapsto t_2\}$$

Rewriting

$$\frac{\Gamma \vdash P\{t_1 \mapsto t_2\}}{\Gamma\ [t_1 = t_2] \vdash P}\ \textsc{Rewrite}{\rightarrow}$$

If we have $t_1 = t_2$ then we can replace t_1 with t_2 everywhere.

Rewriting

For convenience:

$$\frac{\Gamma \vdash P\{t_2 \mapsto t_1\}}{\Gamma\ [t_1 = t_2] \vdash P}\ \textsc{Rewrite}{\leftarrow}$$

If we have $t_1 = t_2$ then we can replace t_1 with t_2 everywhere.

Summary

Equality is characterised by two principles:

1. Everything is equal to itself (*reflexivity*)
2. If $s = t$, then everything that is true about s is true about t.

Equality and Arithmetic, Part 2

Arithmetic and Induction

Arithmetic

One thing we might want to do with Predicate Logic is reason about numbers:

- $\forall x. \forall y.\ x + y = y + x$
- $\forall x. \forall y. \forall z.\ x + (y + z) = (x + y) + z$
- $\forall x. \forall y. \forall z.\ x \times (y + z) = (x \times y) + (x \times z)$
- $\forall n.\ n > 2 \to \neg(\exists x. \exists y. \exists z.\ x^n + y^n = z^n)$

Representation of Numbers

To make thing easier, we use a *unary* representation of numbers:

A number is either:

1. 0 or
2. $S(n)$, where n is a number.

For example, 5 is represented as $S(S(S(S(S(0)))))$.

This is *massively* inefficient, but makes reasoning easier.

Axioms

We can now write down some plausible axioms for arithmetic.

Axiom 1

$$\forall x. \neg(0 = S(x))$$

0 is not the successor of any number.

Axiom 2

$$\forall x.\forall y.S(x) = S(y) \to x = y$$

If two successors are equal, the things they are successors of must be equal.

This is a way of saying "successor goes on forever". If we had a loop such that $S(x)$ was equal to some number y less than x, then this axiom would not hold.

Axioms 3 and 4

$$\forall x.\ \mathrm{add}(0, x) = x$$
$$\forall x.\forall y.\ \mathrm{add}(S(x), y) = S(\mathrm{add}(x, y))$$

1. Adding 0 to x gives x, i.e., $0 + x = x$
2. $(1 + x) + y = 1 + (x + y)$.

These axioms define addition.

Axioms 5 and 6

$$\forall x.\, \mathrm{mul}(0, x) = 0$$
$$\forall x.\forall y.\, \mathrm{mul}(S(x), y) = \mathrm{add}(y, \mathrm{mul}(x, y))$$

1. $0 \times x = 0$
2. $(1 + x) \times y = y + (x \times y)$

These axioms define multiplication.

Peano's Axioms (not all of them)

1. $\forall x.\ \neg(0 = S(x))$
2. $\forall x.\forall y.\ S(x) = S(y) \to x = y$
3. $\forall x.\ \mathrm{add}(0, x) = x$
4. $\forall x.\forall y.\ \mathrm{add}(S(x), y) = S(\mathrm{add}(x, y))$
5. $\forall x.\ \mathrm{mul}(0, x) = 0$
6. $\forall x.\forall y.\ \mathrm{mul}(S(x), y) = \mathrm{add}(y, \mathrm{mul}(x, y))$

(named after Guiseppe Peano)

What can we prove?

Can do computation:

$$\mathrm{add}(S(S(0)), S(S(S(0)))) = S(S(S(S(S(0)))))$$

(2+3=5)

But can't prove anything for all numbers:

$$\forall x. \forall y. x + y = y + x$$

is not provable yet.

Induction

To prove things for all numbers, we use the principle of *induction*:

To prove for all x, $P(x)$, we must:

- Prove $P(0)$
- For all n, prove that $P(n)$ implies $P(S(n))$

(this is the main reason we use the unary representation)

The assumption $P(n)$ in part 2 is called the *induction hypothesis*.

Example (informal)

To prove $\mathrm{add}(x, 0) = x$ by induction on x:

1. Need to prove that $\mathrm{add}(0, 0) = 0$, which is axiom 3.
2. Need to prove if $\mathrm{add}(n, 0) = n$, then $\mathrm{add}(S(n), 0) = S(n)$:
   2.1 We have $\mathrm{add}(S(n), 0) = S(\mathrm{add}(n, 0))$ by axiom 4; and
   2.2 so $S(\mathrm{add}(n, 0)) = S(n)$ by the induction hypothesis

Induction as a Rule

$$\frac{\Gamma \vdash P[x \mapsto 0] \qquad \Gamma, x_1, P[x \mapsto x_1] \vdash P[x \mapsto S(x_1)]}{\Gamma \vdash P}\ \textsc{Induction}$$

where x is declared in Γ.

Peano's Axioms

1. $\forall x.\, \neg(0 = S(x))$
2. $\forall x.\forall y.\, S(x) = S(y) \to x = y$
3. $\forall x.\, \mathrm{add}(0, x) = x$
4. $\forall x.\forall y.\, \mathrm{add}(S(x), y) = S(\mathrm{add}(x, y))$
5. $\forall x.\, \mathrm{mul}(0, x) = 0$
6. $\forall x.\forall y.\, \mathrm{mul}(S(x), y) = \mathrm{add}(y, \mathrm{mul}(x, y))$

$+$ induction

Summary

We can reason about arithmetic using Peano's Axioms.

- 6 axioms defining 0, S, $\mathtt{add}$ and $\mathtt{mul}$
- and induction

This system is surprisingly powerful.

Summary

We can reason about arithmetic using Peano's Axioms.

- 6 axioms defining 0, S, $\mathtt{add}$ and $\mathtt{mul}$
- and induction

This system is surprisingly powerful.

In fact, it is *too* powerful, as we shall see next week.