Warm-Up Problem

Recall EQ2:

For each formula α and variable z,

$$\Big(\forall x \ \Big(\forall y \ \Big((x = y) \to \Big(\alpha[x/z] \to \alpha[y/z] \Big) \Big) \Big) \Big)$$

is an axiom.

Suppose in a ND$=$ proof you had the statements $(a = c)$ and $(P(a) \to P(b))$. If you wanted to prove $(P(c) \to P(b))$, what could a choice for α be?

Predicate Logic: Peano Arithmetic

Carmen Bruni

Lecture 15

Based on slides by Jonathan Buss, Lila Kari, Anna Lubiw and Steve Wolfman with thanks to B. Bonakdarpour, A. Gao, D. Maftuleac, C. Roberts, R. Trefler, and P. Van Beek

Last Time

- Natural Deduction with Equality.

Learning Goals

- Peano Arithmetic
- State Peano's axioms.
- Be able to use these axioms to solve problems.

Recall: Axioms

Definition: An *axiom* is a formula that is assumed as a premise in any proof. An *axiom schema* is a set of axioms, defined by a pattern or rule.

Axioms often behave like additional “inference rules”.

Example: Axioms for equality

Recall the axioms of equality:

EQ1: $(\forall x\ (x = x))$ is an axiom.

EQ2: For each formula α and variable z,

$$\Big(\forall x\ \Big(\forall y\ \Big((x = y) \to \Big(\alpha[x/z] \to \alpha[y/z]\Big)\Big)\Big)\Big)$$

is an axiom.

We shall keep these, and add new ones.

Notation: in place of writing

k.	$(\forall x\,(x = x))$	Axiom EQ1
$k{+}1$.	$(t = t)$	$\forall$e[term t]: k

we shall simply write

k.	$(t = t)$	EQ1+$\forall$e

and similarly for other axioms.

Derived Proof Rules for Equality

Equality satisfies the following derived rules.

EQsymm: $\emptyset \vdash_{ND=} \Big(\forall x\,(\forall y\,((x = y) \rightarrow (y = x)))\Big)$.

EQtrans(k): $$\frac{(t_1 = t_2) \quad (t_2 = t_3) \quad \cdots \quad (t_k = t_{k+1})}{(t_1 = t_{k+1})}$$

for any t_1, ..., t_{k+1}.

EQsubs(r): $$\frac{(t_1 = t_2)}{(r[t_1/z] = r[t_2/z])}$$

for any variable z and terms r, t_1 and t_2.

In what follows, we will describe the work of Italian Mathematician Giuseppe Peano (1858-1932) who building on the work of Dedekind and Grassman suggested the following axioms defining arithmetic over the natural numbers.

Natural Numbers

Fix the domain as $\mathbb{N}$, the natural numbers. Interpret the constant symbol 0 as zero and the unary function symbol s as successor.

Thus each number in $\mathbb{N}$ has a term: 0, $s(0)$, $s(s(0))$, $s(s(s(0)))$, ...

Zero and successor satisfy the following axioms.

Natural Numbers

Fix the domain as $\mathbb{N}$, the natural numbers. Interpret the constant symbol 0 as zero and the unary function symbol s as successor.

Thus each number in $\mathbb{N}$ has a term: 0, $s(0)$, $s(s(0))$, $s(s(s(0)))$, ...

Zero and successor satisfy the following axioms.

PA1: $\big(\forall x\,(\neg(s(x) = 0))\big)$.
"Zero is not a successor."

PA2: $\Big(\forall x\,(\forall y\,((s(x) = s(y)) \rightarrow (x = y)))\Big)$.
"Nothing has two predecessors."

("PA" stands for Peano Axioms)

Addition and Multiplication

Further axioms characterize + (addition) and × (multiplication).

PA3: $(\forall x\,((x+0)=x))$.
Adding zero to any number yields the same number.

PA4: $\Big(\forall x\,(\forall y\,((x+s(y))=s((x+y))))\Big)$.
Adding a successor yields the successor of adding the number.

PA5: $(\forall x\,((x\times 0)=0))$.
Multiplying by zero yields zero.

PA6: $\Big(\forall x\,\Big(\forall y\,((x\times s(y))=((x\times y)+x))\Big)\Big)$.
Multiplication by a successor.

Induction in Peano Arithmetic

The six axioms above define $+$ and $\times$ for any particular numbers.
They do not, however, allow us to reason adequately about all numbers.
For that, we use an additional axiom: induction.

PA7: For each formula φ and variable v,

$$\Big(\varphi[0/v] \to \Big(\big(\forall v\,(\varphi \to \varphi[s(v)/v])\big) \to (\forall v\ \varphi)\Big)\Big)$$

is an axiom.

The formula φ represents the "property" to be proved.

To prove φ for every x, we can prove the base case $\varphi[0/x]$
and the inductive case $\big(\forall x\,(\varphi \to \varphi[s(x)/x])\big)$.

Axioms on One Slide and Equality

- PA1: $\big(\forall x\,(\neg(s(x)=0))\big)$
- PA2: $\Big(\forall x\,\big(\forall y\,((s(x)=s(y))\to(x=y))\big)\Big)$
- PA3: $\big(\forall x\,((x+0)=x)\big)$
- PA4: $\Big(\forall x\,\big(\forall y\,((x+s(y))=s((x+y)))\big)\Big)$
- PA5: $\big(\forall x\,((x\times 0)=0)\big)$
- PA6: $\Big(\forall x\,\Big(\forall y\,((x\times s(y))=((x\times y)+x))\Big)\Big)$
- PA7: $\Big(\varphi[0/v]\to\Big((\forall v\,(\varphi\to\varphi[s(v)/v]))\to(\forall v\;\varphi)\Big)\Big)$
- EQsymm: $\Big(\forall x\,\big(\forall y\,((x=y)\to(y=x))\big)\Big)$
- EQtrans(k): $$\frac{(t_1=t_2)\quad(t_2=t_3)\quad\cdots\quad(t_k=t_{k+1})}{(t_1=t_{k+1})}$$
- EQsubs(r): $$\frac{(t_1=t_2)}{(r[t_1/z]=r[t_2/z])}$$

With Great Power...

- We will use these axioms to prove some familiar results for the Natural numbers like Associativity and Commutativity
- This seems fantastic as we have axiomatized the natural numbers.
- Do we lose anything with this new found power?

With Great Power...

- We will use these axioms to prove some familiar results for the Natural numbers like Associativity and Commutativity
- This seems fantastic as we have axiomatized the natural numbers.
- Do we lose anything with this new found power?
- Yes! In what follows, Peano's Axioms will mean the aforementioned axioms with Natural Deduction and equality rules.
- Gödel in 1931 proved the following:

Theorem (Gödel's Imcompletness Theorem)

If Peano Axioms are consistent (that is, they do not derive a contradiction) then the proof system is incomplete.

So in other words, our proof theory of PA is either...

- Inconsistent (that is, there is no model that satisfies all the axioms)
- Incomplete (that is, for every model of PA, there are true statements that cannot be proven)

Since the natural numbers form a model of PA (and we believe these numbers exist!) there must be true statements about the natural numbers that cannot be proven in PA.

Let's try to prove associativity and commutativity in PA.

Properties from the Peano Axioms

These axioms imply all of the familiar properties of the natural numbers.

For example, addition is associative.

Theorem: Addition in Peano Arithmetic is associative; that is,

$$\emptyset \vdash_{PA} \Big(\forall x \left(\forall y \left(\forall z \left(((x+y)+z) = (x+(y+z))\right)\right)\right)\Big) \, .$$

(Notation "$\vdash_{PA}$" means "provable [in *ND*] using the EQ and PA axioms".)

How can we find such a proof?

We must use induction (Axiom PA7). The key first step: choose a good formula φ for the induction property.

Setting Up the Induction

Recall Axiom PA7: $\Big(\varphi[0/z] \to \big((\forall z\,(\varphi \to \varphi[s(z)/z])) \to (\forall z\ \varphi)\big)\Big)$.

Choosing φ to be $(((x+y)+z) = (x+(y+z)))$ yields the instance

$$(((x+y)+0) = (x+(y+0))) \to$$
$$\Big((\forall z\,(((x+y)+z) = (x+(y+z)) \to ((x+y)+s(z)) = (x+(y+s(z)))))$$
$$\to (\forall z\ ((x+y)+z) = (x+(y+z)))\Big)$$

Thus we must prove the base case $(((x+y)+0) = (x+(y+0)))$
and the inductive case

$$(\forall z\,(((x+y)+z) = (x+(y+z)) \to ((x+y)+s(z)) = (x+(y+s(z)))))$$

Then two uses of $\to$e yield the desired formula

$$(\forall z\ ((x+y)+z) = (x+(y+z)))\ .$$

The Base Case for Associativity

To prove: $(((x + y) + 0) = (x + (y + 0)))$.

How?

The Base Case for Associativity

To prove: $(((x + y) + 0) = (x + (y + 0)))$.

How?

The axioms tell us how to add zero: $\big(\forall u\, ((u + 0) = u)\big)$.

We can apply this to $(x + y)$ and also to y.

The rules for equality then give us what we want.

3.	$(((x + y) + 0) = (x + y))$	PA3 $+ \forall$e
4.	$((y + 0) = y)$	PA3 $+ \forall$e
5.	$(x + (y + 0)) = (x + y)$	EQsubs$((x + \cdot))$: 4
6.	$(((x + y) + 0) = (x + (y + 0)))$	EQTrans: 3, 5

The inductive step shows that associativity with z implies associativity with $s(z)$:

$$\left(\forall z\left(((x+y)+z)=(x+(y+z))\rightarrow((x+y)+s(z))=(x+(y+s(z)))\right)\right)$$

Axiom PA4 — $\left(\forall u\left(\forall v\left(u+s(v)=s(u+v)\right)\right)\right)$ — gives addition of successors.

We will need it three times: once for $(y+s(z))$, once for $((x+y)+s(z))$, and once for $(x+s((y+z)))$.

To get the $\forall$ quantifier, we select a fresh variable z', in place of z.

Details on the next page....

Proof of the Inductive Case

8.	z' fresh	
9.	$(((x+y)+z') = (x+(y+z')))$	Assumption
10.	$\big(s((x+(y+z'))) = s(((x+y)+z'))\big)$	EQsubs($s(\cdot)$): 9
11.	$\big(((x+y)+s(z')) = s(((x+y)+z'))\big)$	PA4 + $\forall$e
12.	$\big((y+s(z')) = s((y+z'))\big)$	PA4 + $\forall$e
13.	$\big((x+(y+s(z'))) = (x+s((y+z')))\big)$	EQsubs($(x+\cdot)$): 12
14.	$\big((x+s((y+z'))) = s((x+(y+z')))\big)$	PA4 + $\forall$e
15.	$\big(((x+y)+s(z')) = (x+(y+s(z')))\big)$	EqTrans: 13, 14, 10, 11
16.	$\big(A(x,y,z') \to A(x,y,s(z'))\big)$	$\to$i: 9–15
17.	$\Big(\forall z\,\Big(\big(A(x,y,z) \to A(x,y,s(z))\big)\Big)\Big)$	$\forall$i: 8–16

(*Note:* $A(a,b,c)$ *abbreviates* $(((a+b)+c) = (a+(b+c)))$.)

Completing the Proof

Now that we have the base case and the inductive case, we must

- Combine them and complete the induction, and
- Add the quantifiers onto x and y.

The full proof appears next.

1.	x, y fresh	
2.	$\Big((A(x,y,0)) \to \Big((\forall z\,(A(x,y,z) \to A(x,y,s(z)))) \to (\forall z\ A(x,y,z))\Big)\Big)$	PA7
3.	$(((x+y)+0) = (x+y))$	PA3 + $\forall$e
4.	$((y+0) = y)$	PA3 + $\forall$e
5.	$((x+(y+0)) = (x+y))$	EQsubs($((x+\cdot))$): 4
6.	$((x+(y+0)) = ((x+y)+0))$	EqTrans: 3, 5
7.	$\Big((\forall z\,(A(x,y,z) \to A(x,y,s(z)))) \to (\forall z\ A(x,y,z))\Big)$	$\to$e: 6, 2
8.	z fresh	
9.	$(((x+y)+z) = (x+(y+z)))$	Assumption
10.	$(s((x+(y+z))) = s(((x+y)+z)))$	EQsubs($s(\cdot)$): 9
11.	$(((x+y)+s(z)) = s(((x+y)+z)))$	PA4 + $\forall$e
12.	$((y+s(z)) = s((y+z)))$	PA4 + $\forall$e
13.	$((x+(y+s(z))) = (x+s((y+z))))$	EqSubs: 12
14.	$((x+s((y+z))) = s((x+(y+z))))$	PA4 + $\forall$e
15.	$(((x+y)+s(z)) = (x+(y+s(z))))$	EqTrans: 13, 14, 10, 11
16.	$((((x+y)+z) = (x+(y+z))) \to (((x+y)+s(z)) = (x+(y+s(z)))))$	$\to$i: 9–15
17.	$\forall z\,(((((x+y)+z) = (x+(y+z))) \to (((x+y)+s(z)) = (x+(y+s(z))))))$	$\forall$i: 8–16
18.	$(\forall z\,(((x+y)+z) = (x+(y+z))))$	$\to$e: 7, 17
19.	$\Big(\forall x\,\Big(\forall y\,(\forall z\,(((x+y)+z) = (x+(y+z)))))\Big)\Big)$	$\forall$i $(\times 2)$: 1–18

Recapitulation

The formula to be proven had three universal quantifiers: on x, y, and z.

Q: Why did we do induction on only one?

A: We only needed one. Rule ∀i worked fine for the other two.

Q: Did it matter which variable we chose for the induction?

A: Yes!
Consider what would happen in an induction on x. The base would be to derive

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

But that's not easy—Axiom PA3 has $(u + 0)$, not $(0 + u)$.

Next, let's consider commutativity.

Commutativity of Addition

Theorem: Addition in Peano Arithmetic is commutative; that is, there is a proof

$$\emptyset \vdash_{PA} \left(\forall x \left(\forall y \left((x+y) = (y+x)\right)\right)\right) \ .$$

To do the proof, we will need to use induction both on x and on y.

I have chosen to do x first. Thus I let φ be the formula $\left(\forall y \left((x+y) = (y+x)\right)\right)$.

Setting Up the Induction

For $\varphi = (\forall y\,((x+y) = (y+x)))$, the instance of PA7 is

$$(\forall y\,((0+y) = (y+0))) \rightarrow$$
$$\Big(\Big(\forall x\,\big((\forall y\,((x+y)=(y+x))) \rightarrow (\forall y\,((s(x)+y)=(y+s(x))))\big)\Big) \rightarrow$$
$$\Big(\forall x\,(\forall y\,((x+y)=(y+x)))\Big)\Big)$$

The base case: $(\forall y\,((0+y) = (y+0)))$.

The inductive case:

$$\Big(\forall x\,\big((\forall y\,((x+y)=(y+x))) \rightarrow (\forall y\,((s(x)+y)=(y+s(x))))\big)\Big) .$$

The Base Case for Commutativity

To prove: $\big(\forall y\,((0+y)=(y+0))\big)$.

How?

The Base Case for Commutativity

To prove: $\big(\forall y\,((0+y)=(y+0))\big)$.

How?

We must use induction on y, in order to prove the base case for x.

Let's make it a lemma:

Lemma
Peano Arithmetic has a proof of $\big(\forall y\,((0+y)=(y+0))\big)$.

Plan, to prove lemma: induction (PA7) with $((0+y)=(y+0))$ for φ.

Basis: Prove $((0+0)=(0+0))$. Immediate from EQ1.

Basis Lemma, continued

Inductive step sketch: Prove
$\Big(\forall y \left(((0+y) = (y+0)) \rightarrow ((0+s(y)) = (s(y)+0))\right)\Big)$.

Pick y' fresh. Then assume $((0+y') = (y'+0))$ [start a subproof].

$$\begin{aligned}(0+s(y')) &= s((0+y')) && \text{PA4}\\ &= s((y'+0)) && \text{assumption} + \text{EQsubs}(s(\cdot))\\ &= (s(y')+0) && \text{PA3} \ .\end{aligned}$$

Applying $\rightarrow$i and generalization ($\forall$i) yield the required formula.

Using PA7 and $\rightarrow$e (twice) completes the proof of the lemma.

The full proof of the lemma (the base case for commutativity) appears on the next page.

1.	$((0+0)=(0+0))$	EQ1 $+ \forall$e
2.	y' fresh	
3.	$((0+y')=(y'+0))$	Assumption
4.	$((0+s(y'))=s((0+y')))$	PA4 $+ \forall$e
5.	$(s((0+y'))=s((y'+0)))$	EQsubs($s(\cdot)$): 3
6.	$((y'+0)=y')$	PA3 $+ \forall$e
7.	$(s((y'+0))=s(y'))$	EQsubs($s(\cdot)$): 6
8.	$((s(y')+0)=s(y'))$	PA3 $+ \forall$e
9.	$((0+s(y'))=(s(y')+0))$	EqTrans(3): 4, 5, 7, 8
10.	$(((0+y')=(y'+0)) \to ((0+s(y'))=(s(y')+0)))$	$\to$i: 3–9
11.	$\left(\forall y\,((0+y)=(y+0) \to (0+s(y))=(s(y)+0))\right)$	$\forall$i: 10
12.	$(\forall y\,((0+y)=(y+0)))$	PA7 $+ \to$e $(\times 2)$: 1, 11

Inductive Case for Commutativity

Lemma. $(\forall y\,((x+y)=(y+x))) \vdash_{PA} (\forall y\,((s(x)+y)=(y+s(x))))$.
(*"If x commutes with everything, then $s(x)$ also does."*)

Plan of proof: induction on variable y, for formula $((s(x)+y)=(y+s(x)))$.

Basis: $((s(x)+0)=(0+s(x)))$. Already proven (the previous lemma).

Ind. step: for a fresh variable y', we need to show

$$\left(((s(x)+y')=(y'+s(x))) \to ((s(x)+s(y'))=(s(y')+s(x)))\right)\ .$$

Note that the premise of the Lemma implies both

$$((x+y')=(y'+x)) \quad \text{and} \quad ((x+s(y'))=(s(y')+x))\ .$$

That is, we use $\forall$e on the premise *twice*, with different terms.

Inductive Case, continued

We calculate the sums in our goal:

$$\begin{aligned}(s(x) + s(y')) &= s\big((s(x) + y')\big) && \text{PA4}\\ &= s\big((y' + s(x))\big) && \text{assumption} + \text{EQsubs}(s(\cdot))\\ &= s\big(s((y' + x))\big) && \text{PA4} + \text{EQsubs}(s(\cdot))\end{aligned}$$

and

$$\begin{aligned}(s(y') + s(x)) &= s\big((s(y') + x)\big) && \text{PA4}\\ &= s\big((x + s(y'))\big) && \text{premise} + \text{EQsubs}(s(\cdot))\\ &= s\big(s((x + y'))\big) && \text{PA4} + \text{EQsubs}(s(\cdot)) \enspace .\end{aligned}$$

Recall we have $((x + y') = (y' + x))$; thus EQsubs($s(s(\cdot))$) yields the required

$$((s(x) + s(y')) = (s(y') + s(x))) \enspace .$$

12.	$(\forall y\,((x+y)=(y+x)))$	Premise
13.	$((s(x)+0)=(0+s(x)))$	$\forall$e: 12
14.	y' fresh	
15.	$((x+y')=(y'+x))$	$\forall$e: 12
16.	$((x+s(y'))=(s(y')+x))$	$\forall$e: 12
17.	$((s(x)+y')=(y'+s(x)))$	Assumption
18.	*(Uses of PA4 omitted)*	
22.	*(Uses of EqSubs on 17–21 omitted)*	
27.	$((s(x)+s(y'))=(s(y')+s(x)))$	EqTrans $(\times 6)$: 17–26
28.	$(((s(x)+y')=(y'+s(x)))\rightarrow$ $((s(x)+s(y'))=(s(y')+s(x))))$	$\rightarrow$i: 17–27
29.	$(\forall y\,((((s(x)+y)=(y+s(x))))\rightarrow$ $((s(x)+s(y))=(s(y)+s(x)))))$	$\forall$i: 14–28

Putting It All Together

1.	$((0+0) = 0)$	PA3 + $\forall$e
2.	*Lemma, p. 25*	
12.	$(\forall y\,((0+y) = (y+0)))$	PA7 + $\to$e $(\times 2)$: 1, 11
13.	$(\forall y\,((x+y) = (y+x)))$	Assumption
	Lemma, p. 28	
30.	$\big(\forall y\,((x+y) = (y+x))\big) \to \big(\forall y\,((s(x)+y) = (y+s(x)))\big)$	$\to$i: 13–29
31.	$(\forall x\,(\forall y\,((x+y) = (y+x))))$	PA7 + $\to$e $(\times 2)$: 12, 30

The other familiar properties of addition and multiplication have similar proofs. One can continue: divisibility, primeness, etc.

Let formula φ have free variables x_1, ..., x_k.

Given an interpretation $\mathcal{I}$, a formula φ *defines* the k-ary relation of tuples that make φ true — that is, the relation

$$R_\varphi = \left\{ \langle \mathsf{a}_1, \ldots, \mathsf{a}_k \rangle \in dom(I)^k \mid \varphi^{(\mathcal{I}, E[x_1 \mapsto \mathsf{a}_1] \cdots [x_k \mapsto \mathsf{a}_k])} = \mathtt{T} \right\} .$$

A relation R is *definable (in $\mathcal{I}$)* iff $R = R_\varphi$ for some formula φ.

Example: in Peano Arithmetic, the relation $\leq$ is defined by the formula

$$(\exists z \, ((x_1 + z) = x_2)) .$$

Properties of Defined Relations

The PA axioms allow one to show that the defined relation $\leq$ has the expected properties.

- $(x \leq y)$ and $(y \leq z)$ imply $(x \leq z)$ (transitivity).
- If $(x \leq y)$ and $(y \leq x)$ then $(x = y)$.

We can also define further relations using $\leq$; e.g.,

$$(x < y) \quad \text{iff} \quad ((x \leq y) \wedge (x \neq y)) \ .$$

Transitivity of Less-or-Equal

To show: $\{x \leq y, \, y \leq z\} \vdash x \leq z$.

1.	$\exists w\,(x + w = y)$	Premise
2.	$\exists w\,(y + w = z)$	Premise
3.	$x + u = y$, u fresh	Assumption
4.	$y + v = z$, v fresh	Assumption
5.	$x + (u + v) = (x + u) + v$	Associativity of $+$
6.	$(x + u) + v = y + v$	EQsubs($\cdot + v$): 3
7.	$x + (u + v) = z$	EqTrans(2): 5, 6, 4
8.	$\exists w\,(x + w = z)$	$\exists$i: 7
9.	$\exists w\,(x + w = z)$	$\exists$e: 2, 4–8
10.	$\exists w\,(x + w = z)$	$\exists$e: 1, 3–9

Defining Functions

To define a k-ary function, use its $(k+1)$-ary relation.

Example: Let $\mathscr{R}_{sq}$ ("square-of") be defined by $x_1 \times x_1 = x_2$.
Then we can get the effect of having the squaring function:

> if φ contains a free variable x, but u is fresh, then the formula
>
> $$\exists u \, (\mathscr{R}_{sq}(t, u) \land \varphi[u/x])$$
>
> expresses "the square of t satisfies φ."

We must, however, ensure that $\mathscr{R}_{sq}$ really does define a function; that is, that every number has exactly one square:

$$\forall x \left((\exists y \; \mathscr{R}_{sq}(x, y)) \land \forall y \; \forall z \left((\mathscr{R}_{sq}(x, y) \land \mathscr{R}_{sq}(x, z)) \rightarrow y = z \right) \right) \; .$$

We leave this proof as an exercise.