Plan for today

Formal Proofs In FOPC

- What new rules are we adding?
- How do we use them?
- Examples
- Equality

Proofs in FOPC

We're really not changing a whole lot.
In fact all of the old proofs still apply.
Really, we're just adding four new rules.

Proof rules

$$\dfrac{A \land B}{A}\,\land E1 \qquad \dfrac{A \land B}{B}\,\land E2 \qquad \dfrac{A \qquad B}{A \land B}\,\land I$$

$$\dfrac{A}{A \lor B}\,\lor I1 \qquad \dfrac{B}{A \lor B}\,\lor I2 \qquad \dfrac{A \lor B \qquad A \to C \qquad B \to C}{C}\,\lor E$$

$$\dfrac{[A] \qquad \begin{array}{c}[A]\\ \vdots\\ B\end{array}}{A \to B} \to I \qquad \dfrac{A \qquad A \to B}{B} \to E$$

$$\dfrac{A \to \bot}{\neg A}\,\neg I \qquad \dfrac{A \qquad \neg A}{\bot}\,\neg E$$

$$\dfrac{}{\top}\,\top I \qquad \dfrac{\bot}{A}\,\bot E \qquad \dfrac{}{A \lor \neg A}\,LEM$$

Proof rules

$$\frac{\forall x.A(x)}{A(c)}\,\forall E \qquad\qquad \frac{A(c)}{\exists x.A(x)}\,\exists I$$

$$\frac{[x] \qquad \begin{array}{c}[x]\\ \vdots\\ A(x)\end{array}}{\forall x.A(x)}\,\forall I \qquad\qquad \frac{\exists x.A(x) \qquad A(c) \to B}{B}\,\exists E$$

$$\frac{\forall x.P(x)}{\forall z.P(z)}\,\forall[x \mapsto z] \qquad\qquad \frac{\exists x.P(x)}{\exists z.P(z)}\,\exists[x \mapsto z]$$

Example: tree proofs

Prove: $\forall x.P(x) \vdash \forall z.P(z)$

$$\dfrac{[z] \qquad \dfrac{\forall x.P(x)}{P(z)}\,\forall E}{\forall z.P(z)}\,\forall I$$

Example: 3-column proofs

Prove: $\forall x.P(x) \vdash \forall z.P(z)$

1	$\forall x.P(x)$	premise
2	$\mid\quad [z]$	assumption
3	$\mid\quad P(z)$	$\forall E$ 1
4	$\forall z.P(z)$	$\forall I$ 2-3

Example: tree proofs

Prove: $\exists x.P(x) \vdash \exists z.P(z)$

$$\dfrac{\exists x.P(x) \qquad \dfrac{[P(c)] \qquad \dfrac{[P(c)]}{\exists z.P(z)}\,\exists I}{P(c) \to \exists z.P(z)}\,\to I}{\exists z.P(z)}\,\exists E$$

Example: 3-column proofs

Prove: $\exists x.P(x) \vdash \exists z.P(z)$

1	$\exists x.P(x)$	premise
2	$[P(c)]$	assumption
3	$\exists z.P(z)$	$\exists I$ 2
4	$P(c) \rightarrow \exists z.P(z)$	$\rightarrow I$ 2-3
5	$\exists z.P(z)$	$\exists E$ 1,4

Example: tree proofs

Prove: $\exists x.\exists y.P(x,y) \vdash \exists y.\exists x.P(x,y)$

$$
\dfrac{\exists x.\exists y.P(x,y) \qquad \dfrac{[\exists y.P(u,y)] \qquad \dfrac{[\exists y.P(u,y)] \qquad \dfrac{[P(u,v)] \qquad \dfrac{\dfrac{[P(u,v)]}{\exists x.P(x,v)}\,\exists I}{\exists y.\exists x.P(x,y)}\,\exists I}{P(u,v) \to \exists y.\exists x.P(x,y)}\,\to I}{\exists y.\exists x.P(x,y)}\,\exists E}{\exists y.P(u,y) \to \exists y.\exists x.P(x,y)}\,\to I}{\exists y.\exists x.P(x,y)}\,\exists E
$$

Example: 3-column proofs

Prove: $\exists x.\exists y.P(x,y) \vdash \exists y.\exists x.P(x,y)$

1	$\exists x.\exists y.P(x,y)$	premise
2	$\mid\ [\exists y.P(u,y)]$	assumption
3	$\mid\ \mid\ [P(u,v)]$	assumption
4	$\mid\ \mid\ \exists x.P(x,v)$	$\exists I$ 3
5	$\mid\ \mid\ \exists y.\exists x.P(x,y)$	$\exists I$ 4
6	$\mid\ P(u,v) \rightarrow \exists y.\exists x.P(x,y)$	$\rightarrow I$ 3-5
7	$\mid\ \exists y.\exists x.P(x,y)$	$\exists E$ 2,6
8	$\exists y.P(u,y) \rightarrow \exists y.\exists x.P(x,y)$	$\rightarrow I$ 2-7
9	$\exists y.\exists x.P(x,y)$	$\exists E$ 1,8

Example: tree proofs

Prove: $\exists x.\forall y.P(x,y) \vdash \forall y.\exists x.P(x,y)$

$$\dfrac{\exists x.\forall y.P(x,y) \qquad \dfrac{[\forall y.P(u,y)] \qquad \dfrac{[v] \qquad \dfrac{\dfrac{[\forall y.P(u,y)]}{P(u,v)}\,\forall E}{\exists x.P(x,v)}\,\exists I}{\forall y.\exists x.P(x,y)}\,\forall I}{\forall y.P(u,y) \rightarrow \forall y.\exists x.P(x,y)}\,\rightarrow I}{\forall y.\exists x.P(x,y)}\,\exists E$$

Example: 3-column proofs

Prove: $\exists x.\forall y.P(x,y) \vdash \forall y.\exists x.P(x,y)$

1	$\exists x.\forall y.P(x,y)$	premise
2	$\mid\ [\forall y.P(u,y)]$	assumption
3	$\mid\ \mid\ [v]$	assumption
4	$\mid\ \mid\ P(u,v)$	$\forall E$ 2
5	$\mid\ \mid\ \exists x.P(x,v)$	$\exists I$ 4
6	$\mid\ \forall y.\exists x.P(x,y)$	$\forall I$ 3-5
7	$\forall y.P(u,y) \rightarrow \forall y.\exists x.P(x,y)$	$\rightarrow I$ 2-6
8	$\forall y.\exists x.P(x,y)$	$\exists E$ 1,7

Equality Proofs

$=$ is just a predicate, so we should be able to prove things about it right?

Try this

Prove: $2 + 2 = 4$

This should be easy, but we don't really know anything about $=$

Proofs involving some form of $=$ are very common.

We should have a way to talk about them.

Equality Proof rules

$$\frac{\forall x.A(x)}{A(c)}\,\forall E \qquad\qquad \frac{A(c)}{\exists x.A(x)}\,\exists I$$

$$\frac{[x] \qquad \begin{array}{c}[x]\\ \vdots \\ A(x)\end{array}}{\forall x.A(x)}\,\forall I \qquad\qquad \frac{\exists x.A(x) \qquad A(c) \to B}{B}\,\exists E$$

$$\frac{\forall x.P(x)}{\forall z.P(z)}\,\forall[x \mapsto z] \qquad\qquad \frac{\exists x.P(x)}{\exists z.P(z)}\,\exists[x \mapsto z]$$

$$\frac{}{x = x}\,\mathit{Refl}$$

$$\frac{a = b \qquad P(a)}{P(b)} = E1$$

$$\frac{a = b \qquad P(b)}{P(a)} = E2$$

Equality Proofs

Ok, let's try this again!
First, lets define a few things about numbers.
We need to know what these symbols mean $2, 3, 4$

We'll say $2 = 1 + 1$, $3 = 1 + 2$, and $4 = 1 + 3$

Next we need a fact about addition.
Namely that it's associative.

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

This is not obvious, and it's not easy to prove.
But we can assume its true for now.

Equality Proofs

prove: $2 = 1 + 1,\ 3 = 1 + 2,\ 4 = 1 + 3,$
$\forall xyz.(x + y) + z = x + (y + z) \vdash 2 + 2 = 4$

$$\dfrac{4 = 1 + 3 \qquad \dfrac{3 = 1 + 2 \qquad \dfrac{\dfrac{2 = 1 + 1 \qquad \dfrac{}{2 + 2 = 2 + 2}\,\mathit{Refl}}{2 + 2 = (1 + 1) + 2}\,{=}\,E1 \qquad \dfrac{\forall xyz.(x + y) + z = x + (y + z)}{(1 + 1) + 2 = 1 + (1 + 2)}\,\forall E}{2 + 2 = 1 + (1 + 2)}\,{=}\,E1}{2 + 2 = 1 + 3}\,{=}\,E2}{2 + 2 = 4}\,{=}\,E2$$

Equality Proofs

prove: $2 = 1 + 1$, $3 = 1 + 2$, $4 = 1 + 3$,
$\forall xyz.(x + y) + z = x + (y + z) \vdash 2 + 2 = 4$

1	$4 = 1 + 3$	premise
2	$3 = 1 + 2$	premise
3	$2 = 1 + 1$	premise
4	$2 + 2 = 2 + 2$	Refl
5	$2 + 2 = (1 + 1) + 2$	$= E1$ 3,4
6	$\forall xyz.(x + y) + z = x + (y + z)$	premise
7	$(1 + 1) + 2 = 1 + (1 + 2)$	$\forall E$ 6
8	$2 + 2 = 1 + (1 + 2)$	$= E1$ 7,5
9	$2 + 2 = 1 + 3$	$= E2$ 2,8
10	$2 + 2 = 4$	$= E2$ 1,9

Equality proofs

Equality proofs can become very long very fast.
Although they're really just showing two things are equal.

This is one of the only times I'm going to recommend using 3-column proofs.
tree proofs tend to fall off of the side

If you still want to use tree proof, try to structure them vertically.

Equality Proofs: hard mode

There's a common idea that once you've proved something, you understand it.

So, in vector calculus there are a few theroems

Curl-grad theorem
$\forall f : \mathbb{R}^2 \to \mathbb{R}. \nabla \times \nabla f = \mathbf{0}$

0 vector
$\forall \mathbf{v} \in \mathbb{R}^3 . \mathbf{0} \cdot \mathbf{v} = 0$

0 integral
$\iint_S 0 dS = 0$

Stoke's Theorem
$\forall \mathbf{f} : \mathbb{R}^2 \to \mathbb{R}^3 . \oint_{\partial \mathbf{S}} \mathbf{f} \cdot T ds = \iint_S \nabla \times \mathbf{f} \cdot \mathbf{N} dS$

Equality Proofs: hard mode

I want to prove the divergence theorem:
$\forall f : \mathbb{R}^2 \to \mathbb{R}. \nabla \times \nabla f = \mathbf{0}$,
$\forall \mathbf{v} \in \mathbb{R}^3. \mathbf{0} \cdot \mathbf{v} = 0$,
$\iint_S 0 dS = 0$,
$\forall \mathbf{f} : \mathbb{R}^2 \to \mathbb{R}^3. \oint_{\partial \mathbf{S}} \mathbf{f} \cdot T ds = \iint_S \nabla \times \mathbf{f} \cdot \mathbf{N} dS$,
$\vdash \oint_{\partial \mathbf{S}} \nabla f \cdot T ds = 0$

Let's do this!

Equality Proofs: hard mode

1	$\forall f : \mathbb{R}^2 \to \mathbb{R}. \nabla \times \nabla f = \mathbf{0}$	premise
2	$\forall \mathbf{v} \in \mathbb{R}^3 . \mathbf{0} \cdot \mathbf{v} = 0$	premise
3	$\iint_S 0 dS = 0$	premise
4	$\forall \mathbf{f} : \mathbb{R}^2 \to \mathbb{R}^3 . \oint_{\partial \mathbf{S}} \mathbf{f} \cdot T ds = \iint_S \nabla \times \mathbf{f} \cdot \mathbf{N} dS$	premise
5	$\oint_{\partial \mathbf{S}} \nabla f \cdot T ds = \iint_S \nabla \times \nabla f \cdot \mathbf{N} dS$	$\forall E$, 4
6	$\nabla \times \nabla f = \mathbf{0}$	$\forall E$, 1
7	$\oint_{\partial \mathbf{S}} \nabla f \cdot T ds = \iint_S \mathbf{0} \cdot \mathbf{N} dS$	$= E$1, 5, 6
8	$\mathbf{0} \cdot \mathbf{N} = 0$	$\forall E$, 2
9	$\oint_{\partial \mathbf{S}} \nabla f \cdot T ds = \iint_S 0 dS$	$= E$1, 7, 8
10	$\oint_{\partial \mathbf{S}} \nabla f \cdot T ds = 0$	$= E$1, 3, 9

Soundness and completeness

Just like last time, we can ask if first order logic is sound and complete.

Unlike last time, this is really hard.
So, we won't be proving either of these.
But we can at least statement.

Soundness:
if $p_1, p_2 \ldots p_n \vdash p$,
then $p_1 \wedge p_2 \ldots p_n \rightarrow p$ is valid for all models.

Completeness:
if $p_1 \wedge p_2 \ldots p_n \rightarrow p$ is valid for all models,
then $p_1, p_2 \ldots p_n \vdash p$.

Recap

- Forall and Exists rules require us to make up a variable
- These proofs aren't any different than the ones before
- The only thing we know about equality is $a = a$