Worth quoting from previous lecture-PDF that we saw earlier:

0.0.1 Theorem. *If* $\Gamma \vdash X \equiv Y$*, then also* $\Gamma \vdash (\forall \mathbf{x})X \equiv (\forall \mathbf{x})Y$*,* as long as Γ *does not contain wff with* $\mathbf{x}$ *free.*

0.0.2 Theorem. *If* $\vdash A \equiv B$*, then* $\vdash (\forall \mathbf{x})A \equiv (\forall \mathbf{x})B$*.*

0.0.3 Metatheorem. (Weak (1st-order) Leibniz —Acronym "WL")
If $\vdash A \equiv B$*, then also* $\vdash C[\mathbf{p} \setminus A] \equiv C[\mathbf{p} \setminus B]$*.*

Proof. This generalises 0.0.2 repeated above, being a part of the previous "lectures-PDF" that we saw.

The metatheorem is proved by *Induction on the wff* C.

Basis. Atomic case:

(1) C is $\mathbf{p}$. The metatheorem boils down to "if $\vdash A \equiv B$, then $\vdash A \equiv B$", which trivially holds!

(2) C is *NOT* $\mathbf{p}$ —that is, it is $\mathbf{q}$ (other than $\mathbf{p}$), or is $\perp$ or $\top$, or is $t = s$, or it is $\phi(t_1, \ldots, t_n)$.

Then our Metatheorem statement becomes "*if* $\vdash A \equiv B$*, then* $\vdash C \equiv C$".

Given that $\vdash C \equiv C$ is correct by axiom 1, the "if" part is irrelevant. Done.

The complex cases.

(i) C is $\neg D$. From the I.H. we have $\vdash D[\mathbf{p} \setminus A] \equiv D[\mathbf{p} \setminus B]$,

hence $\vdash \neg D[\mathbf{p} \setminus A] \equiv \neg D[\mathbf{p} \setminus B]$ by Post and thus

$$\vdash \overbrace{(\neg D)}^{C}[\mathbf{p} \setminus A] \equiv \overbrace{(\neg D)}^{C}[\mathbf{p} \setminus B]$$

since

$$(\neg D)[\mathbf{p} \setminus A] \text{ is the same wff as } \neg D[\mathbf{p} \setminus A]$$

(ii) C is $D \circ E$, where $\circ \in \{\wedge, \vee, \rightarrow, \equiv\}$.

The I.H. yields $\vdash D[\mathbf{p} \setminus A] \equiv D[\mathbf{p} \setminus B]$ and $\vdash E[\mathbf{p} \setminus A] \equiv E[\mathbf{p} \setminus B]$ hence $\vdash D[\mathbf{p} \setminus A] \circ E[\mathbf{p} \setminus A] \equiv D[\mathbf{p} \setminus B] \circ E[\mathbf{p} \setminus B]$ by Post.

Thus

$$\vdash \overbrace{(D \circ E)}^{C}[\mathbf{p} \setminus A] \equiv \overbrace{(D \circ E)}^{C}[\mathbf{p} \setminus B]$$

due to the way substitution works, namely,

$$(D \circ E)[\mathbf{p} \setminus A] \text{ is the same wff as } D[\mathbf{p} \setminus A] \circ E[\mathbf{p} \setminus A]$$

(iii) C is $(\forall \mathbf{x})D$. This is the "*interesting case*".

From the I.H. follows $\vdash D[\mathbf{p} \setminus A] \equiv D[\mathbf{p} \setminus B]$.

From 0.0.2 we get $\vdash (\forall \mathbf{x})D[\mathbf{p} \setminus A] \equiv (\forall \mathbf{x})D[\mathbf{p} \setminus B]$, also written as

$$\vdash \overbrace{\big((\forall \mathbf{x})D\big)}^{C}[\mathbf{p} \setminus A] \equiv \overbrace{\big((\forall \mathbf{x})D\big)}^{C}[\mathbf{p} \setminus B]$$

since

$$\big((\forall \mathbf{x})D\big)[\mathbf{p} \setminus A] \text{ is the same wff as } (\forall \mathbf{x})D[\mathbf{p} \setminus A]$$

$\square$

WL is the only "Leibniz" we will need (practically) in our use of 1st-order logic.

Why "weak"? Because of the restriction on the Rule's Hypothesis: $A \equiv B$ must be an absolute theorem. (Recall that the Boolean Leibniz was not so restricted).

Why not IGNORE the restriction and "adopt" the strong rule (i) below?

Well, in logic you do *NOT* arbitrarily "*adopt*" derived rules; you prove them.

BUT, CAN I prove (i) *below* then?

NO, our logic does not allow it; here is why: If I can prove (i) then I can also prove STRONG generalisation (ii) from (i).

$$A \equiv B \vdash C[\mathbf{p} \setminus A] \equiv C[\mathbf{p} \setminus B] \tag{i}$$

$$\text{strong generalisation: } A \vdash (\forall \mathbf{x})A \tag{ii}$$

Here is why $(i) \Rightarrow (ii)$*:*

So, assume I have "Rule" (i). THEN

(1)	A	$\langle \text{hyp} \rangle$
(2)	$A \equiv \top$	$\langle (1) + \text{Post} \rangle$
(3)	$(\forall \mathbf{x})A \equiv (\forall \mathbf{x})\top$	$\langle (2) + (i); \text{ "Denom:" } (\forall \mathbf{x})\mathbf{p} \rangle$
(4)	$(\forall \mathbf{x})A \equiv \top$	$\langle (3) + \vdash (\forall \mathbf{x})\top \equiv \top + \text{Post} \rangle$
(5)	$(\forall \mathbf{x})A$	$\langle (4) + \text{Post} \rangle$

So if I have (i) I have (ii) too.

Question: Why is it $\vdash (\forall \mathbf{x})\top \equiv \top$? **Answer**: Ping-Pong, Plus

$$\overbrace{(\forall \mathbf{x})\top \rightarrow \top}^{\mathbf{Ax2}} \text{ and } \overbrace{\top \rightarrow (\forall \mathbf{x})\top}^{\mathbf{Ax3}}$$

BUT: Here is *an informal reason* I cannot have (ii).

It is a provable fact —this is ***1st-order Soundness***[†]— that all absolute theorems of 1st-order logic are true *in every informal interpretation I build for them*.

So *IF I have (ii)*, then by the DThm I also have

$$\vdash A \to (\forall \mathbf{x})A \tag{1}$$

Interpret the above over the natural numbers as

$$\vdash x = 0 \to (\forall x)x = 0 \tag{2}$$

By 1st-order Soundness, IF I have (1), *then (2) is true for all values of (the free) x*.

Well, try $x = 0$. We get $0 = 0 \to (\forall x)x = 0$. The lhs of "$\to$" is true but the rhs is false.

So I cannot have (ii) —nor (i), which implies it!

[†]For a proof wait until the near-end of the course

We *CAN* have a MODIFIED (i) where the substitution into $\mathbf{p}$ is restricted.

0.0.4 Metatheorem. (Strong Leibniz —Acronym "SL") $A \equiv B \vdash C[\mathbf{p} := A] \equiv C[\mathbf{p} := B]$

Goes without saying that if the rhs of $\vdash$ *is NOT* defined, then there is nothing to prove since the expresion "$C[\mathbf{p} := A] \equiv C[\mathbf{p} := B]$" represents no wff.

Remember this comment during the proof!

Proof. As we did for WL, the proof is an induction on the definition/formation of C.

Basis. C is atomic:

subcases

- C is $\mathbf{p}$. We need to prove $A \equiv B \vdash A \equiv B$, which is the familiar $X \vdash X$.
- C is not $\mathbf{p}$. The metatheorem now claims $A \equiv B \vdash C \equiv C$ which is correct since $C \equiv C$ is an axiom.

The complex cases.

(i) C is $\neg D$. By the I.H. we have $A \equiv B \vdash D[\mathbf{p} := A] \equiv D[\mathbf{p} := B]$, thus, $A \equiv B \vdash \neg D[\mathbf{p} := A] \equiv \neg D[\mathbf{p} := B]$ by Post.

We can rewrite the above as $A \equiv B \vdash (\neg D)[\mathbf{p} := A] \equiv (\neg D)[\mathbf{p} := B]$ since when substitution is allowed

$$\overbrace{(\neg D)}^{C}[\mathbf{p} := A] \text{ is the same as } \neg D[\mathbf{p} := A], \text{ etc.}$$

(ii) C is $D \circ E$. By the I.H. we get $A \equiv B \vdash D[\mathbf{p} := A] \equiv D[\mathbf{p} := B]$

and

$A \equiv B \vdash E[\mathbf{p} := A] \equiv E[\mathbf{p} := B]$.

Thus, by Post,

$$A \equiv B \vdash D[\mathbf{p} := A] \circ E[\mathbf{p} := A] \equiv D[\mathbf{p} := B] \circ E[\mathbf{p} := B]$$

The way substitution works (when defined), the above says

$$A \equiv B \vdash \overbrace{(D \circ E)}^{C}[\mathbf{p} := A] \equiv \overbrace{(D \circ E)}^{C}[\mathbf{p} := B]$$

(iii) *C is* $(\forall \mathbf{x})D$. This is the "interesting case".
From the I.H. we get

$$A \equiv B \vdash D[\mathbf{p} := A] \equiv D[\mathbf{p} := B]$$

Now, since the expressions $C[\mathbf{p} := A]$ and $C[\mathbf{p} := B]$ *ARE* defined —else we wouldn't be doing all this— the definition of *conditional* (restricted) substitution implies that neither A nor B have any free occurrences of $\mathbf{x}$.

Then $\mathbf{x}$ *does not occur free in* $A \equiv B$ *either.*

From 0.0.1 we get

$$A \equiv B \vdash (\forall \mathbf{x})D[\mathbf{p} := A] \equiv (\forall \mathbf{x})D[\mathbf{p} := B]$$

which —the way substitution works— *is the same as*

$$A \equiv B \vdash \overbrace{\big((\forall \mathbf{x})D\big)}^{C}[\mathbf{p} := A] \equiv \overbrace{\big((\forall \mathbf{x})D\big)}^{C}[\mathbf{p} := B]$$

$\square$

0.1. More Useful Tools

Since

$$A_1 \equiv A_2, A_2 \equiv A_3, \ldots, A_{n-1} \equiv A_n \models_{taut} A_1 \equiv A_n$$

holds in 1st-order logic, we also have by Post

$$A_1 \equiv A_2, A_2 \equiv A_3, \ldots, A_{n-1} \equiv A_n \vdash A_1 \equiv A_n \tag{1}$$

As we know, (1) enables Equational proofs, including the fundamental metatheorem for such proofs

0.1.1 Metatheorem. *If each "$A_i \equiv A_{i+1}$" in (1) is a Γ-theorem, then we have $\Gamma \vdash A_1 \equiv A_n$ (this just repeats (1)) and $\Gamma \vdash A_1$ iff $\Gamma \vdash A_n$.*

Trivially, we also have

$$A_1 \rightarrow \text{ or } \equiv A_2, A_2 \rightarrow \text{ or } \equiv A_3, \ldots, A_{n-1} \rightarrow \text{ or } \equiv A_n \models_{taut} A_1 \rightarrow A_n$$

and thus, by Post,

$$A_1 \rightarrow \text{ or } \equiv A_2, A_2 \rightarrow \text{ or } \equiv A_3, \ldots, A_{n-1} \rightarrow \text{ or } \equiv A_n \vdash A_1 \rightarrow A_n \tag{2}$$

The fundamental metatheorem for (2) is:

0.1.2 Metatheorem. *If each "$A_i \rightarrow$ or $\equiv A_{i+1}$" in (2) is a Γ-theorem, then we have $\Gamma \vdash A_1 \rightarrow A_n$ (this just repeats (2)) and IF $\Gamma \vdash A_1$ THEN $\Gamma \vdash A_n$.*

This last metatheorem extends *Equational proofs* so they can have a mix of $\rightarrow$ and $\equiv$, BUT

- ALL $\rightarrow$ go in the same direction

  and

- ALL $\rightarrow$ are replaced by the *conjunctional implication* $\Rightarrow$.

  That is, unlike $A \rightarrow B \rightarrow C$ that means $A \rightarrow (B \rightarrow C)$ or $A \wedge B \rightarrow C$, *$A \Rightarrow B \Rightarrow C$ means $A \rightarrow B$ AND $B \rightarrow C$.*

The thus Extended Equational Proofs are called *Calculational Proofs* ([DS90, GS94, Tou08]) and have the following layout:

$$
\begin{aligned}
& A_1 \\
\circ\ & \langle \text{annotation} \rangle \\
& A_2 \\
\circ\ & \langle \text{annotation} \rangle \\
& \vdots \\
& A_{n-1} \\
\circ\ & \langle \text{annotation} \rangle \\
& A_n \\
\circ\ & \langle \text{annotation} \rangle \\
& A_{n+1}
\end{aligned}
$$

where "$\circ$" here —in each line where it occurs— is one of $\Leftrightarrow$ or $\Rightarrow$.

More Examples and "Techniques".

0.1.3 Theorem. $\vdash (\forall \mathbf{x})(A \to B) \equiv (A \to (\forall \mathbf{x})B)$, as long as $\mathbf{x}$ has no free occurrences in A.

Proof.
Ping-Pong using DThm.

$(\to)$ I want

$$\vdash (\forall \mathbf{x})(A \to B) \to (A \to (\forall \mathbf{x})B)$$

Better still, let me do (DThm)

$$(\forall \mathbf{x})(A \to B) \vdash A \to (\forall \mathbf{x})B$$

and, even better, (DThm!) I will do

$$(\forall \mathbf{x})(A \to B), A \vdash (\forall \mathbf{x})B$$

(1)	$(\forall \mathbf{x})(A \to B)$	$\langle$hyp$\rangle$
(2)	A	$\langle$hyp$\rangle$
(3)	$A \to B$	$\langle$(1) + spec$\rangle$
(4)	B	$\langle$(2, 3) + MP$\rangle$
(5)	$(\forall \mathbf{x})B$	$\langle$(4) + gen; OK: no free $\mathbf{x}$ in (1) or (2)$\rangle$

($\leftarrow$) I want

$$\vdash (A \to (\forall \mathbf{x})B) \to (\forall \mathbf{x})(A \to B)$$

or better still (DThm)

$$A \to (\forall \mathbf{x})B \vdash (\forall \mathbf{x})(A \to B) \tag{1}$$

Seeing that $A \to (\forall \mathbf{x})B$ has no free $\mathbf{x}$, I can prove the even easier

$$A \to (\forall \mathbf{x})B \vdash A \to B \tag{2}$$

and after the proof is done I can apply gen to $A \to B$ to get $(\forall \mathbf{x})(A \to B)$.

OK! By DThm I can prove the even simpler than (2)

$$A \to (\forall \mathbf{x})B, A \vdash B \tag{3}$$

Here it is:

(1)	$A \to (\forall \mathbf{x})B$	$\langle$hyp$\rangle$
(2)	A	$\langle$hyp$\rangle$
(3)	$(\forall \mathbf{x})B$	$\langle$(1, 2) + MP$\rangle$
(4)	B	$\langle$(3) + spec $\rangle$

$\square$

As a curiosity, here is a Calculational proof of the $\rightarrow$ Direction:

$(\rightarrow)$

$$
\begin{aligned}
& (\forall \mathbf{x})(A \rightarrow B) \\
\Rightarrow\ & \langle \mathbf{Ax4} \rangle \\
& (\forall \mathbf{x})A \rightarrow (\forall \mathbf{x})B \\
\Rightarrow\ & \langle \mathbf{Ax3} + \text{Post} \rangle \\
& A \rightarrow (\forall \mathbf{x})B
\end{aligned}
$$

Do you buy the second step?

Think of A as p and $(\forall \mathbf{x})A$ as q. Axiom 3 says "$p \rightarrow q$" and I say

$$p \rightarrow q \models_{taut} (q \rightarrow (\forall \mathbf{x})B) \rightarrow (p \rightarrow (\forall \mathbf{x})B)$$

Do you believe this? *Exercise*!

Lecture # 17. Nov.13

0.1.4 Corollary. $\vdash (\forall \mathbf{x})(A \lor B) \equiv A \lor (\forall \mathbf{x})B$, as long as $\mathbf{x}$ does not occur free in A.

Proof.

$$
\begin{aligned}
& (\forall \mathbf{x})(A \lor B) \\
\Leftrightarrow\ & \langle \text{WL} + \neg\lor\ (\,=\text{axiom!});\ \text{“Denom:”}\ \ (\forall \mathbf{x})\mathbf{p} \rangle \\
& (\forall \mathbf{x})(\neg A \to B) \\
\Leftrightarrow\ & \langle \text{“forall vs arrow”}\ \ (0.1.3) \rangle \\
& \neg A \to (\forall \mathbf{x})B \\
\Leftrightarrow\ & \langle \text{tautoloy, hence axiom} \rangle \\
& A \lor (\forall \mathbf{x})B
\end{aligned}
$$

□

Most of the statements we prove in what follows have *Dual* counterparts obtained by swapping $\forall$ and $\exists$ and $\vee$ and $\wedge$.

Let us give a theorem version of the definition of $\exists$. This is useful in Equational/Calculational proofs.

Definition (Recall):

$$(\exists \mathbf{x})A \text{ is short for } \neg(\forall \mathbf{x})\neg A \tag{1}$$

Next consider the axiom

$$\neg(\forall \mathbf{x})\neg A \equiv \neg(\forall \mathbf{x})\neg A \tag{2}$$

Let me use the *ABBREVIATION* (1) ONLY on *ONE* side of "$\equiv$" in (2). I get the theorem

$$(\exists \mathbf{x})A \equiv \neg(\forall \mathbf{x})\neg A$$

So I can write the theorem without words:

$$\vdash (\exists \mathbf{x})A \equiv \neg(\forall \mathbf{x})\neg A \tag{3}$$

I can apply (3) in Equational proofs —via WL— easily!

I will refer to (3) in proofs as "Def of E".

Here's something useful AND good practise too!

0.1.5 Corollary. $\vdash (\exists \mathbf{x})(A \wedge B) \equiv A \wedge (\exists \mathbf{x})B$, as long as $\mathbf{x}$ does not occur free in A.

In annotaton we may call the above the "$\exists\wedge$ theorem".

Proof.

$$
\begin{aligned}
& (\exists \mathbf{x})(A \wedge B) \\
\Leftrightarrow\ & \langle \text{Def of E} \rangle \\
& \neg(\forall \mathbf{x})\neg(A \wedge B) \\
\Leftrightarrow\ & \langle \text{WL + axiom (deM); "Denom:" } \neg(\forall \mathbf{x})\mathbf{p} \rangle \\
& \neg(\forall \mathbf{x})(\neg A \vee \neg B) \\
\Leftrightarrow\ & \langle \text{WL + forall over or (0.1.4) —no free } \mathbf{x} \text{ in } \neg A\text{; "Denom:" } \neg\mathbf{p} \rangle \\
& \neg(\neg A \vee (\forall \mathbf{x})\neg B) \\
\Leftrightarrow\ & \langle \mathbf{Ax1} \rangle \\
& A \wedge \neg(\forall \mathbf{x})\neg B \\
\Leftrightarrow\ & \langle \text{WL + Def of E; "Denom:" } A \wedge \mathbf{p} \rangle \\
& A \wedge (\exists \mathbf{x})B
\end{aligned}
$$

□

Bibliography

[DS90] Edsger W. Dijkstra and Carel S. Scholten, *Predicate Calculus and Program Semantics*, Springer-Verlag, New York, 1990.

[GS94] David Gries and Fred B. Schneider, *A Logical Approach to Discrete Math*, Springer-Verlag, New York, 1994.

[Tou08] G. Tourlakis, *Mathematical Logic*, John Wiley & Sons, Hoboken, NJ, 2008.