CSE 311: Foundations of Computing I

Axioms & Inference Rules

Propositional Logic

Modus Ponens

$$\begin{array}{ll} & A \quad A \to B \\ \hline \therefore & B \end{array}$$

Direct Proof

$$\begin{array}{ll} & A \Rightarrow B \\ \hline \therefore & A \to B \end{array}$$

Elim $\wedge$

$$\begin{array}{ll} & A \wedge B \\ \hline \therefore & A \qquad B \end{array}$$

Intro $\wedge$

$$\begin{array}{ll} & A \qquad B \\ \hline \therefore & A \wedge B \end{array}$$

Proof By Cases

$$\begin{array}{ll} & A \vee B \quad A \to C \quad B \to C \\ \hline \therefore & C \end{array}$$

Intro $\vee$

$$\begin{array}{ll} & A \\ \hline \therefore & A \vee B \qquad B \vee A \end{array}$$

Principium Contradictionis

$$\begin{array}{ll} & \neg A \quad A \\ \hline \therefore & \bot \end{array}$$

Reductio Ad Absurdum

$$\begin{array}{ll} & A \Rightarrow \bot \\ \hline \therefore & \neg A \end{array}$$

Ex Falso Quodlibet

$$\begin{array}{ll} & \bot \\ \hline \therefore & A \end{array}$$

Ad Litteram Verum

$$\begin{array}{ll} & \\ \hline \therefore & \top \end{array}$$

Tautology

$$\begin{array}{ll} & A \equiv \top \\ \hline \therefore & A \end{array}$$

Equivalent

$$\begin{array}{ll} & A \equiv B \quad B \\ \hline \therefore & A \end{array}$$

Predicate Logic

Elim $\forall$
$\dfrac{\forall x, P(x)}{\therefore\ P(a) \text{ for } \textit{any} \text{ object } a}$

Intro $\forall$
$\dfrac{\text{Let } a \text{ be arbitrary} \Rightarrow P(a)}{\therefore \quad \forall x, P(x)}$

Elim $\exists$
$\dfrac{\exists x, P(x)}{\therefore\ P(c) \text{ for a } \textit{new} \text{ name } c}$

Intro $\exists$
$\dfrac{P(c) \text{ for some } c}{\therefore \quad \exists x, P(x)}$

Theorems

The following rules demonstrate Cite and Apply for a theorem T of the form "$\forall x, P(x) \rightarrow Q(x)$".

Cite T
$\dfrac{}{\therefore\ \forall x, P(x) \rightarrow Q(x)}$

Apply T
$\dfrac{P(c) \text{ for some } c}{\therefore \quad Q(c)}$

These same rules work for any other known theorem. The statement of a theorem can start with any positive number of "$\forall$" quantifiers and can use "$\leftrightarrow$" instead of "$\rightarrow$".

Definitions

The following rules demonstrate Def of and Undef for a definition f of the form "$f(x) ::= \exists, y, x = g(y)$". The premise "$P$" should include the expression "$f(c)$" for some c in at least one place.

The expression "$P[u/v]$" means the result of replacing all instances of the expression "u" in P with "v". Hence, Def of replaces "$f(c)$" with "$\exists y, c = g(y)$", while Undef replaces "$\exists y, c = g(y)$" with "$f(c)$".

Def of f
$\dfrac{P}{\therefore\ P[f(c) \,/\, (\exists y, c = g(y))]}$

Undef f
$\dfrac{P[f(c) \,/\, (\exists y, c = g(y))]}{\therefore \quad P}$

These same rules work for any other known definition. The definition can use any positive number of variables.

Equations

The equality predicate "$=$" holds special status in our logic, so we provide a special rule that allows one side of an equation to be replaced with the other side since we know they have the same value.

Substitute

$$\begin{array}{ll} & x = y \qquad P \\ \hline \therefore & P[x/y] \quad P[y/x] \end{array}$$

This rule works with "x" and "y" replaced by arbitrary expressions.

Number Theory

The following rule demonstrates ALGEBRA for inferring $x = 2$ from the equations $2x + 3y = 7$ and $x + 2y = 4$. Twice the first equation minus three times the second equation gives $2(2x + 3y) - 3(x + 2y) = 2 \cdot 7 - 3 \cdot 4$, which simplifies to $x = 2$, showing that these equations imply $x = 2$.

Algebra

$$\begin{array}{ll} & 2x + 3y = 7 \qquad x + 2y = 4 \\ \hline \therefore & x = 2 \end{array}$$

These same rules work for any number of equations (even zero) provided that the concluding equation can be proved by multiplying the premise equations by constants, adding them together, and then simplifying.

Set Theory

The DEF OF and UNDEF rules can also be applied to sets. The following rules show how they would be used for the set $E ::= \{n \in \mathbb{Z} \mid \exists\, m, n = 2m\}$. This definition tells us that "$n \in E ::= \exists\, m, n = 2m$", so we can use these rules to between "$n \in E$" and "$\exists\, m, n = 2m$"'.

Def of E

$$\begin{array}{ll} & P \\ \hline \therefore & P[n \in E \,/\, (\exists\, m, n = 2m)] \end{array}$$

Undef E

$$\begin{array}{ll} & P[n \in E \,/\, (\exists\, m, n = 2m)] \\ \hline \therefore & P \end{array}$$

These rules work for any known set with a set-builder definition.

Since we can define the set operations (complement, union, intersection, and difference) using set-builder notation, their definitions can also be used. For example, here are the rules for intersection:

Def of $A \cap B$

$$\begin{array}{ll} & P \\ \hline \therefore & P[x \in A \cap B \,/\, (x \in A \wedge x \in B)] \end{array}$$

Undef $A \cap B$

$$\begin{array}{ll} & P[x \in A \cap B \,/\, (x \in A \wedge x \in B)] \\ \hline \therefore & P \end{array}$$

These rules (and those for the other set operations) work with "A" and "B" replaced by arbitrary expressions.