MAT 320W
9/6/2017

Inference rules

Theorems and proofs in a formal system:
We fix a universe $\mathcal{U}$ and a collection $\mathbb{A}$ of *axioms*, $\mathbb{A} = P_1 \wedge \ldots \wedge P_n$. A *theorem* is then a proposition R such that $\mathbb{A} \Rightarrow R$ is a tautology. A *proof* of a proposition R is a sequence of propositions, ending with R, which conforms to the following *inference rules*.

1. Premise: The premise $P_1 \wedge \ldots \wedge P_n$ may be included in the proof.
2. Tautology: Any tautology may be included in the proof.
3. Equivalence: If S has appeared in the proof, and S is equivalent to T, then T may be included in the proof.
4. Detachment: If P and $P \Rightarrow Q$ have appeared in the proof, then Q may be included in the proof.
5. Adjunction: If P and Q have appeared in the proof, then $P \wedge Q$ may be included in the proof.
6. Disjunction: If $P \vee Q$ and $\sim P$ have appeared in the proof, then Q may be included in the proof.
7. Existential Generalization: If y is a member of $\mathcal{U}$ and $P(y)$ has appeared in the proof, then $(\exists x)P(x)$ may appear in the proof.
8. Existential specialization: If $(\exists x)P(x)$ has appeared in the proof, then $P(y)$ may be included in the proof, where y is a fixed but not general member of $\mathcal{U}$.
9. Universal specialization: If $(\forall x)P(x)$ has appeared in the proof, and y is a member of $\mathcal{U}$, then $P(y)$ may be included in the proof.
10. Universal generalization: If $P(y)$ has appeared in the proof, where y is a fixed, general member of $\mathcal{U}$, then $(\forall x)P(x)$ may be included in the proof.

In rules 8 and 10, a "general member of $\mathcal{U}$" is a member of $\mathcal{U}$ that has no properties not shared by every member of $\mathcal{U}$.

Any proposition for which there exists a proof is a theorem - that is, if there is a proof whose last line is R, then $\mathbb{A} \Rightarrow R$ is a tautology. (In the mid-'30's Kurt Gödel showed that there are theorems in axiomatic set theory (actually, in multiplicative number theory) that do not have proofs, and there's no way to fix the axiom system to remedy the situation.)

Methods of proof:

- Conditional (direct) proof: To construct a proof of $P \Rightarrow Q$, adopt P as a temporary premise, and construct a proof of Q. This method of proof is an application of the tautology
$$((\mathbb{A} \wedge P) \Rightarrow Q) \Rightarrow ((\mathbb{A} \Rightarrow (P \Rightarrow Q))\,.$$
- Indirect proof (or proof by contraposition): To construct a proof of $P \Rightarrow Q$, adopt $\sim Q$ as a temporary premise and construct a proof of $\sim P$. This method of proof is an application of the tautology
$$((\mathbb{A} \wedge \sim Q) \Rightarrow \sim P) \Rightarrow (\mathbb{A} \Rightarrow (P \Rightarrow Q))\,.$$
- Proof by contradiction: To construct a proof of P, adopt $\sim P$ as a temporary premise and construct a proof of $Q \wedge \sim Q$, for some other statement Q. This method of proof is an application of the tautology
$$((\mathbb{A} \wedge \sim P) \Rightarrow (Q \wedge \sim Q)) \Rightarrow (\mathbb{A} \Rightarrow P).$$