

590N: Logical Methods in Information Security Lecture 11

Ninghui Li

February 6, 2008

One Example Hilbert Style System

► Axioms

1. $\phi \rightarrow (\psi \rightarrow \phi)$
2. $\phi \rightarrow (\psi \rightarrow \xi) \rightarrow ((\phi \rightarrow \psi) \rightarrow (\phi \rightarrow \xi))$
3. $(\neg\phi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \phi)$

One Example Hilbert Style System

► Axioms

1. $\phi \rightarrow (\psi \rightarrow \phi)$
2. $\phi \rightarrow (\psi \rightarrow \xi) \rightarrow ((\phi \rightarrow \psi) \rightarrow (\phi \rightarrow \xi))$
3. $(\neg\phi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \phi)$

► Rules

Modus Ponens (MP): from ϕ and $\phi \rightarrow \phi'$, deduce ϕ' , for all ϕ, ϕ'

An Example Using the System

Prove: $\vdash \phi \rightarrow \phi$

1. $(\phi \rightarrow ((\phi \rightarrow \phi) \rightarrow \phi)) \rightarrow ((\phi \rightarrow (\phi \rightarrow \phi)) \rightarrow (\phi \rightarrow \phi))$

An Example Using the System

Prove: $\vdash \phi \rightarrow \phi$

1. $(\phi \rightarrow ((\phi \rightarrow \phi) \rightarrow \phi)) \rightarrow ((\phi \rightarrow (\phi \rightarrow \phi)) \rightarrow (\phi \rightarrow \phi))$
2. $\phi \rightarrow ((\phi \rightarrow \phi) \rightarrow \phi)$

An Example Using the System

Prove: $\vdash \phi \rightarrow \phi$

1. $(\phi \rightarrow ((\phi \rightarrow \phi) \rightarrow \phi)) \rightarrow ((\phi \rightarrow (\phi \rightarrow \phi)) \rightarrow (\phi \rightarrow \phi))$
2. $\phi \rightarrow ((\phi \rightarrow \phi) \rightarrow \phi)$
3. $((\phi \rightarrow (\phi \rightarrow \phi)) \rightarrow (\phi \rightarrow \phi))$

An Example Using the System

Prove: $\vdash \phi \rightarrow \phi$

1. $(\phi \rightarrow ((\phi \rightarrow \phi) \rightarrow \phi)) \rightarrow ((\phi \rightarrow (\phi \rightarrow \phi)) \rightarrow (\phi \rightarrow \phi))$
2. $\phi \rightarrow ((\phi \rightarrow \phi) \rightarrow \phi)$
3. $((\phi \rightarrow (\phi \rightarrow \phi)) \rightarrow (\phi \rightarrow \phi))$
4. $((\phi \rightarrow (\phi \rightarrow \phi))$

An Example Using the System

Prove: $\vdash \phi \rightarrow \phi$

1. $(\phi \rightarrow ((\phi \rightarrow \phi) \rightarrow \phi)) \rightarrow ((\phi \rightarrow (\phi \rightarrow \phi)) \rightarrow (\phi \rightarrow \phi))$
2. $\phi \rightarrow ((\phi \rightarrow \phi) \rightarrow \phi)$
3. $((\phi \rightarrow (\phi \rightarrow \phi)) \rightarrow (\phi \rightarrow \phi))$
4. $((\phi \rightarrow (\phi \rightarrow \phi))$
5. $\phi \rightarrow \phi$

Another Example Hilbert Style System

► Axioms

1. $\phi \vee \phi \rightarrow \phi$ for every formula ϕ
2. $\phi \rightarrow \psi \vee \phi$ for all formulas ϕ, ψ
3. $(\phi \rightarrow \phi_1) \rightarrow (\phi \vee \phi_2 \rightarrow \phi_1 \vee \phi_2)$ for all ϕ, ϕ_1, ϕ_2

► Rules

Modus Ponens (MP): from ϕ and $\phi \rightarrow \psi$, deduce ψ , for all ϕ, ψ