CS250: Draft Crib Sheet for Second Test F2016

Tarski's Definition of Truth

$G \models t_1 = t_2$ iff $t_1^G = t_2^G$

$G \models P(t_1, \ldots, t_a)$ iff $(t_1^G, \ldots, t_a^G) \in P^G$

$G \models \sim\alpha$ iff $G \not\models \alpha$

$G \models \alpha \wedge \beta$ iff $G \models \alpha$ **and** $G \models \beta$

$G \models \alpha \vee \beta$ iff $G \models \alpha$ **or** $G \models \beta$

$G \models \forall x(\alpha)$ iff **for all** $a \in |G|$ $G[a/x] \models \alpha$

$G \models \exists x(\alpha)$ iff **exists** $a \in |G|$ $G[a/x] \models \alpha$

Logical Equivalences and Abbreviatons

$p \to q \equiv \sim p \vee q$

$\sim(p \wedge q) \equiv \sim p \vee \sim q$

$\sim\forall x\, \varphi \equiv \exists x\ \sim\varphi$

$\sim(p \vee q) \equiv \sim p \wedge \sim q$

$\sim\exists x\, \varphi \equiv \forall x\ \sim\varphi$

p only if q $\equiv$ $p \to q$

p if q $\equiv$ $q \to p$

p iff q $\equiv$ $p \leftrightarrow q$

p is necessary for q $\equiv$ $q \to p$

p is sufficient for q $\equiv$ $p \to q$

p unless q $\equiv$ $\sim q \to p$

$t_1 \neq t_2 \equiv \sim(t_1 = t_2)$

$(\forall x\,.\,\alpha)\beta \equiv \forall x(\alpha \to \beta)$

$(\exists x\,.\,\alpha)\beta \equiv \exists x(\alpha \wedge \beta)$

$\exists! x(\alpha(x)) \equiv \exists x \forall y(\alpha(x) \wedge (\alpha(y) \to y = x))$

$x|y \equiv \exists z\ (x \cdot z = y)$

$a \equiv b \pmod m \equiv m|(a-b)$

$\text{prime}(x) \equiv 1 < x \wedge \forall y\ (1 < y \wedge y|x \to y = x)$

Natural Deduction Rules

Proviso for $\forall$-i and $\exists$-e: x_0 is a "new" variable, i.e., it does not appear in φ, ψ, or Γ.

	introduction	elimination
$\wedge$	$\dfrac{\alpha \quad \beta}{\alpha \wedge \beta}$	$\dfrac{\alpha \wedge \beta}{\alpha}$ $\dfrac{\alpha \wedge \beta}{\beta}$
$\vee$	$\dfrac{\alpha}{\alpha \vee \beta}$ $\dfrac{\beta}{\alpha \vee \beta}$	$\dfrac{\alpha \vee \beta \quad \alpha \vdash \psi \quad \beta \vdash \psi}{\psi}$
$\to$	$\dfrac{\alpha \vdash \beta}{\alpha \to \beta}$	$\dfrac{\alpha \to \beta \quad \alpha}{\beta}$ $\dfrac{\alpha \to \beta \quad \sim\beta}{\sim\alpha}$
F	$\dfrac{\alpha \quad \sim\alpha}{\mathbf{F}}$	$\dfrac{\alpha \vdash \mathbf{F}}{\sim\alpha}$ $\dfrac{\sim\alpha \vdash \mathbf{F}}{\alpha}$
$\sim\sim$	$\dfrac{\alpha}{\sim\sim\alpha}$	$\dfrac{\sim\sim\alpha}{\alpha}$
$=$	$\dfrac{}{t = t}$	$\dfrac{t_1 = t_2 \quad \varphi[t_1/x]}{\varphi[t_2/x]}$
$\forall$	$\dfrac{\Gamma \vdash \varphi[x_0/x]}{\Gamma \vdash \forall x\, \varphi}$	$\dfrac{\forall x\, \varphi}{\varphi[t/x]}$
$\exists$	$\dfrac{\varphi[t/x]}{\exists x\, \varphi}$	$\dfrac{\Gamma \vdash \exists x\, \varphi \quad \Gamma, \varphi[x_0/x] \vdash \psi}{\Gamma \vdash \psi}$

Truth Game: literal: **D** wins iff $W \models \varphi$

$\wedge, \forall$: **G** chooses $\vee, \exists$: **D** chooses

Euclid's Algorithm $\gcd(a,b) = ax + by$.

If $\gcd(a,b) = 1$ then $a^{-1} \text{mod}\ b = (x\%b)$.

$\varphi(m) = |\mathbf{Z}_m^*| = |\{a \in \mathbf{Z}/m\mathbf{Z} \mid \gcd(a,m) = 1\}|$

$a|(bc) \wedge \gcd(a,b) = 1 \to a|c$