Patrik Jansson

## Prop

**Book section 2.1**

$\wedge, \vee, \Rightarrow, \neg, F, T$

Name Nam

## FOL

**Book section 2.2**

Same core logic

+ predicates (over some domain)

+ quantifiers $(\forall, \exists)$

Two extensions

from Prop → FOL

FOL = First Order Logic

Patrik Jansson

## Prop

$\land, \lor, \Rightarrow, \neg, F, T$

Name Nam $\longmapsto$

## FOL(Dom)

Same

String

Pred Nam [Dom]

| Domain | Predicates |
|---|---|
| Numbers | Prime(n), $\overbrace{\text{Less}(a,b)}^{a<b}$, Divides(a,b) |
| Family | ChildOf(c,p), Male(x) |
| ⋮ | |

Prop

$\wedge, \vee, \Rightarrow, \neg, F, T$

FOL(Dom)

Patrik Jansson

Same ...

+ quantifiers $(\forall, \exists)$

$fol_1 = \forall x. \exists y. ChildOf(x, y)$

Dom = Family

quantifier examples

$fol_2 = \forall n. Prime(n) \Rightarrow \exists s. (n < s) \& Prime(s)$

Dom = Numbers

**Book section 2.2.2**

DSL → δσλ

DSLsofMath

# FOL (Dom)

## Quantifiers $(\forall, \exists)$ + predicates

$$\forall x.\ \exists y.\ \underbrace{ChildOf(x, y)}_{FOL}$$

$$\boxed{Dom = Family}$$

$$ChildOf : Dom \to Dom \to FOL$$

---

$$\forall n.\ Prime(n) \Rightarrow \exists s.\ \overbrace{(n < s)}^{FOL} \,\&\, Prime(s)$$

$$Dom = Numbers$$

$$Prime : Dom \to FOL$$

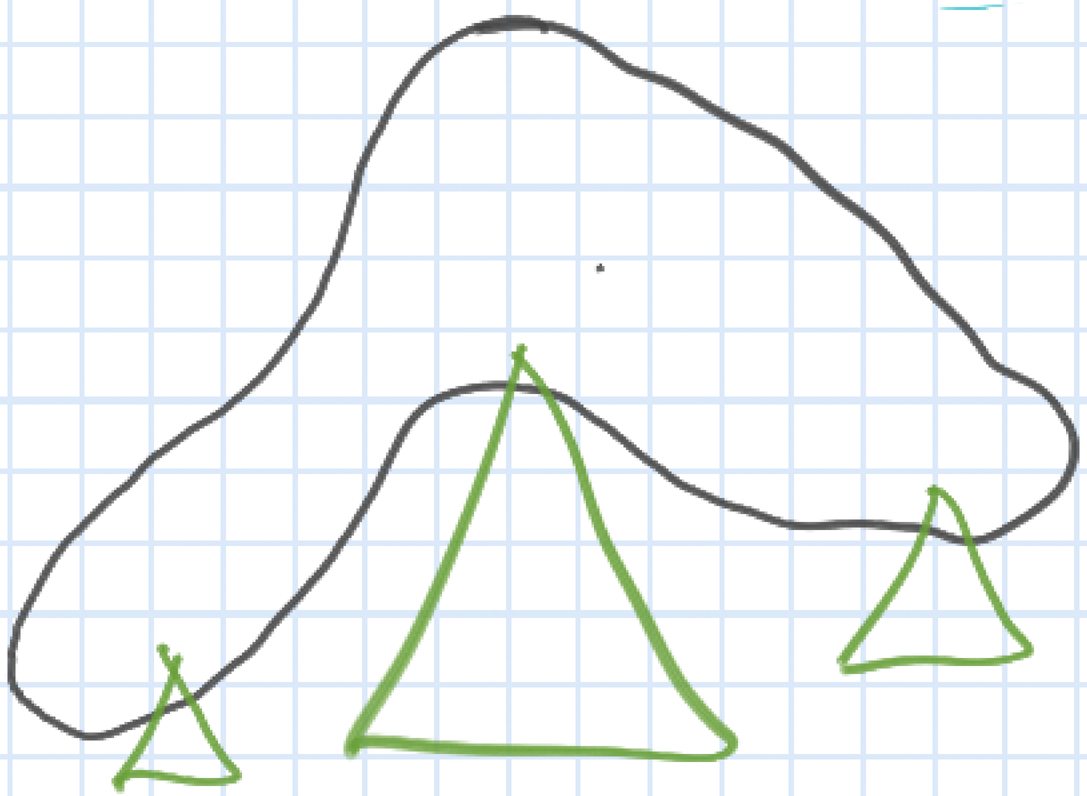
$$(<) : Dom \to Dom \to FOL$$

# FOL (Dom) | Prop + quantifiers ($\forall, \exists$) + predicates

```
data FOL where
  And :: FOL -> FOL -> FOL
  ⋮
  Not :: FOL -> FOL
  Forall :: DVar -> FOL -> FOL
  Exists :: DVar -> FOL -> FOL
  Pred :: Nam -> [Dom] -> FOL
```

"Domain-variables"

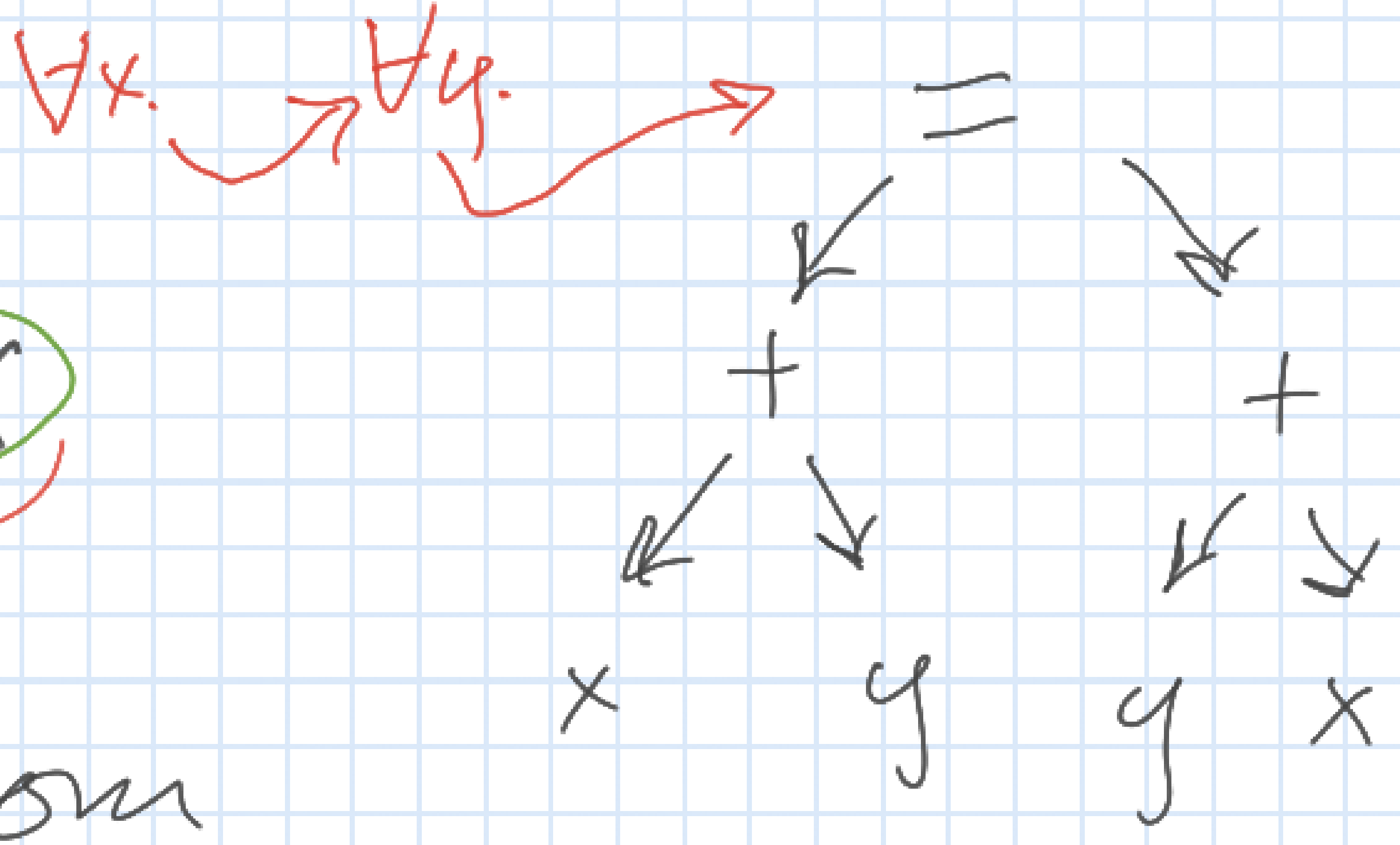
DVar = String



```
data Dom where  -- Numbers
  Var :: DVar -> Dom
  Add :: Dom -> Dom -> Dom
  Mul :: Dom -> Dom -> Dom
  Con :: ℕ -> Dom
```

# Interpret FOL-syntax

$$\forall x.\ \forall y.\ \underbrace{x+y = y+x}_{FOL}$$




$$(+) : Dom \to Dom \to Dom$$

$$(=) : Dom \to Dom \to FOL$$

```
Pred "=" [Add x y, Add y x]
  where x = Var "x" ; y = Var "y"
```

# Typed quantifiers

"syntactic sugar" = can be translated away

$$\forall x{:}A.\ B(x) \equiv \forall x.\ A(x) \Rightarrow B(x)$$

**Book section 2.2.4**

$\forall x.\ P$

$$\exists x{:}A.\ B(x) \equiv \exists x.\ A(x) \land B(x)$$

Dom = Numbers $\boxed{x : N}$ $N(x) = x \geq 0$

$$\forall x{:}N.\ Prime(x) \equiv \forall x.\ x \geq 0 \Rightarrow Prime(x)$$

# Negation & quantifiers

"de Morgan"

$$\neg(\forall x.\, P) \equiv \exists x.\, \neg P$$

$$\neg(A \wedge B) \equiv (\neg A) \vee (\neg B)$$

$$\neg(\underbrace{\exists x.\, Q}) \equiv \forall x.\, \neg Q$$

$$\underbrace{\neg(A \vee B) \equiv (\neg A) \wedge (\neg B)}$$

$$Q[x=a_0] \vee Q[x=a_1] \vee Q[x=a_2] \vee \dots$$

where $a_0, a_1, a_2 \dots \in \mathrm{Dom}$

predicate

$$x : A \equiv x \in A \equiv A(x)$$

type      set

Exercise: $\neg(\forall x{:}A.\, B(x))$

$\neg(\exists x{:}A.\, B(x))$

# Proof by contradiction

**Book section 2.4.1**

Variants:

$$\frac{\neg P \Rightarrow \bot}{P}$$

$$\frac{\neg\neg P}{P}$$

$$\boxed{\frac{\neg P \Rightarrow (Q \land \neg Q)}{P}}$$

free choice of Q

For example $P = \neg R(r) =$ "r is irrational"

so that $\neg P = \neg\neg R(r) = R(r)$

$$\boxed{\frac{R(r) \Rightarrow (Q \land \neg Q)}{\neg R(r)}}$$

"Assume r is rational. Prove both Q and $\neg Q$ as consequences. This is impossible, thus r is irrational"

"$\sqrt{2}$ is irrational"

**Book section 2.4.2**

$Dom = \mathbb{R}^+$

$x = \frac{t}{n}$

greatest common divisor of $t$ & $n$

$(r = \sqrt{2}) \equiv (r^2 = 2)$

$R(x) \equiv \exists t{:}\mathbb{Z}.\, \exists n{:}\mathbb{N}^+.\ \underbrace{t = x \cdot n}\ \wedge\ \underbrace{\gcd(t,n) = 1}_{Q}$

Prove: $\boxed{\neg R(r)}$. Assume $R(r)$.

We know $t = r \cdot n$, thus $t^2 = r^2 \cdot n^2 = 2 \cdot n^2$ $\quad \exists k{:}\mathbb{Z}.\, t = 2 \cdot k$

$2^2 \cdot k^2 = 2 \cdot n^2 \quad \Rightarrow \quad 2 \cdot k^2 = n^2$

$\exists l{:}\mathbb{Z}.\ n = 2 \cdot l$

$t = 2 \cdot k$ & $n = 2 \cdot l$

$\gcd(t,n) = \gcd(2k, 2l) \geq 2 \neq 1$

$\boxed{Q \wedge \neg Q}$

QED!

# Proof by cases

$$\boxed{\frac{A \vee B \qquad A \Rightarrow C \qquad B \Rightarrow C}{C}}$$

special case: $B = \neg A$ $\qquad A \vee \neg A$

$$\boxed{\frac{A \Rightarrow C \qquad \neg A \Rightarrow C}{C}}$$

# Proof by cases

$$\frac{A \Rightarrow C \qquad \neg A \Rightarrow C}{C}$$

$$\boxed{(a^b)^c = a^{b \cdot c}}$$

**Claim**

"There are two irrational numbers $x$ & $y$ such that $x^y$ is rational"

$$(2^3)^2 = (2 \cdot 2 \cdot 2)^2 = (\underbrace{2 \cdot 2 \cdot 2}) \cdot (\underbrace{2 \cdot 2 \cdot 2}) = 2^6 = 2^{3 \cdot 2}$$

$$C = \boxed{\exists p. \exists q. \neg R(p) \land \neg R(q) \land R(p^q)}$$

$r^2 = 2$

let $p = r = q$

$p = r = \sqrt{2}$

$$? \; R(p^q) \equiv R(r^r) = \underbrace{R(\sqrt{2}^{\sqrt{2}})}_{A}$$

Case 1: $A \Rightarrow C$ Yes. trivial

# Proof by cases

$$\frac{A \Rightarrow C \qquad \neg A \Rightarrow C}{C}$$

$$\boxed{(a^b)^c = a^{b\cdot c}}$$

Claim

"There are two irrational numbers x & y such that $x^y$ is rational"

$$C = \boxed{\exists p. \exists q. \neg R(p) \wedge \neg R(q) \wedge R(p^q)}$$

let $p = r = q$

$p = r = \sqrt{2}$

? $R(p^q) \equiv R(r^r) = \underbrace{R(\sqrt{2}^{\sqrt{2}})}_{A}$

Case 1: $A \Rightarrow C$

Case 2: $\neg A \Rightarrow C$

let $x = r^r$ try $p = x$, $q = r$

$r^2 = 2$

$p^q = x^r = (r^r)^r = r^{r\cdot r} = r^2 = 2$

QED!