Introduction to Higher-Order Logic and Sequent Calculus

In order to formally reason about mathematical objects, or programs, a formal language is needed. For this purpose, PVS uses higher-order logic.

the following logical constructs are used:

$\neg$	not ...
$\wedge$	... and ...
$\vee$	... or ...
$\rightarrow$	if ... then ...
$\leftrightarrow$	... if-and-only-if ...
$\forall x\colon X\ p(x)$	for all x of type X, $p(x)$
$\exists x\colon X\ p(x)$	there exists at least one x of type X, s.t. $p(x)$
$=$	$\cdots$ is equal to $\cdots$
$p(t_1, \ldots, t_n)$	$t_1, \ldots, t_n$ stand in relation p to each other.

(Formulas of form $p(t_1, \ldots, t_n)$ or $t_1 = t_2$ are called atoms)

Examples

The atoms $p(t_1, \ldots, t_n)$ can have form

$3 < 4$, $1 < 1 + 1$, even(4), odd(5),

substring($"cde", "abcdefgh"$).

Examples of formulas are

$\forall x, y{:}\,\mathrm{Nat}\ x < y \leftrightarrow x + 1 < y + 1$

$\forall x, y{:}\,\mathrm{Nat}\ x \leq y \rightarrow x < y + 1$

$\forall p{:}\,\mathrm{Nat}\ \mathrm{prime(p)} \leftrightarrow \neg\exists x{:}\,\mathrm{Nat}\ 1 < x \wedge x < p \wedge \mathrm{divides}(x, p)$

$\forall x, y{:}\,\mathrm{Real}\ \ \mathrm{square}(x + y) = \mathrm{square}(x) + \mathrm{square}(y) + 2 * x * y$

Higher-order, classical logic, What is an order?

- Predicates that speak about domain objects are of 1-st order.
- Predicates that speak about objects of at most i-th order, are by themselves of $(i+1)$-th order.
- Functions that take and return domain objects are of 1-st order.
- Functions that take and return objects of at most i-th order, are by themselves of $(i+1)$-th order.

For example, the induction principle is 2-nd order:
$\forall P{:}\,\mathrm{Nat} \rightarrow \mathrm{Bool}\ P(0) \wedge (\forall n{:}\,\mathrm{Nat}\ P(n) \rightarrow P(n+1)\ ) \rightarrow \forall n{:}\,\mathrm{Nat}\ P(n)$.
For the moment, we consider only first-order logic.

Higher-order, classical logic, what is classical?

When reasoning about physical objects, the following principles are considered valid: $A \vee \neg A$, and $\neg\neg A \to A$. (law of excluded middle and law of double negation).

Either there are WMD's in Irak or there are no WMD's in Irak

When speaking about complicated mathematical objects, the law of excluded middle is not generally accepted.

If one drops excluded middle, one obtains intuitionistic or constructive logic. If one proves a formula of form $\exists x{:}\, X\, p(x)$ in intuitionistic logic, then one can always find a witness t, s.t. $p(t)$ holds.

Sequent Calculus for First-Order Logic

The most important types of deduction systems are:

- Natural Deduction: Natural Deduction models the natural style of reasoning, as it can be found in mathematical textbooks. Most of the proof consists of forward reasoning, i.e. deriving conslusions, deriving new conclusions from these conclusions, etc. Occassionally hypotheses are introduced or dropped.
- Sequent Calculus: In sequent calculus, conclusions and premisses are treated in the same way. The proof constructs judgements, rather than conclusions. This is different from the style found in textbooks, but the resulting calculus is easier.

PVS is based on higher-order sequent calculus for classical logic.

COQ is based on higher-order, intuitionistic logic with inductive types.

Sequent Calculus for Classical Logic

A multiset is a set that can distinguish how often an element occurs in it, (or alternatively it is a list that cannot see the order of its elements).

Examples:

$$A \vee B,\ A \wedge B,\ A \wedge B,$$

$$A \vee B,\ A \wedge B,\ C \rightarrow D,$$

$$A \wedge B,\ A \vee B,\ A \wedge B.$$

The first and the last multiset are equal.

A sequent is an object of form

$$\Gamma \vdash \Delta.$$

Here both Γ and Δ are multisets of formulas.

The meaning is: Whenever all of the Γ are true, then at least one of the Δ is true.

Propositional Rules:

$$\text{(axiom)} \ \frac{}{\Gamma, A \vdash \Delta, A}$$

$$\text{(cut)} \ \frac{\Gamma, A \vdash \Delta \qquad \Gamma \vdash \Delta, A}{\Gamma \vdash \Delta}$$

Structural Rules:

$$\text{(weakening left)} \ \frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta} \qquad \text{(weakening right)} \ \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, A}$$

$$\text{(contraction left)} \ \frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta} \qquad \text{(contraction right)} \ \frac{\Gamma \vdash \Delta, A, A}{\Gamma \vdash \Delta, A}$$

Rules for the constants:

$$(\top\text{-left}\ )\ \frac{\Gamma \vdash \Delta}{\Gamma, \top \vdash \Delta} \qquad (\top\text{-right}\ )\ \frac{}{\Gamma \vdash \Delta, \top}$$

$$(\bot\text{-left}\ )\ \frac{}{\Gamma, \bot \vdash \Delta} \qquad (\bot\text{-right}\ )\ \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, \bot}$$

Rules for $\neg$:

$$(\neg\text{-left}\ )\ \frac{\Gamma \vdash \Delta, A}{\Gamma, \neg A \vdash \Delta} \qquad (\neg\text{-right}\ )\ \frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \Delta, \neg A}$$

Rules for $\wedge$ and $\vee$:

$$(\wedge\text{-left }) \ \frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta} \qquad (\wedge\text{-right }) \ \frac{\Gamma \vdash \Delta, A \qquad \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \wedge B}$$

$$(\vee\text{-left }) \ \frac{\Gamma, A \vdash \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta} \qquad (\vee\text{-right }) \ \frac{\Gamma \vdash \Delta, A, B}{\Gamma \vdash \Delta, A \vee B}$$

(one can see from this, that premisses and conclusions are treated in completely the same way)

Rules for $\to$ and $\leftrightarrow$:

$$(\to\text{-left})\ \frac{\Gamma \vdash \Delta, A \qquad \Gamma, B \vdash \Delta}{\Gamma, A \to B \vdash \Delta} \qquad\qquad (\to\text{-right})\ \frac{\Gamma, A \vdash \Delta, B}{\Gamma \vdash \Delta, A \to B}$$

$$(\leftrightarrow\text{-left})\ \frac{\Gamma, A \to B,\ B \to A \vdash \Delta}{\Gamma, A \leftrightarrow B \vdash \Delta}$$

$$(\leftrightarrow\text{-right})\ \frac{\Gamma \vdash \Delta, A \to B \qquad \Gamma \vdash \Delta, B \to A}{\Gamma \vdash \Delta, A \leftrightarrow B}$$

Rules for the quantifiers:

$$(\forall\text{-left }) \ \frac{\Gamma, P[x := t] \vdash \Delta}{\Gamma, \forall x{:}\, X \ \ P(x) \vdash \Delta} \qquad (\forall\text{-right }) \ \frac{\Gamma \vdash \Delta, P[x := y]}{\Gamma \vdash \Delta, \forall x{:}\, X \ \ P(x)}$$

$$(\exists\text{-left }) \ \frac{\Gamma, P[x := y] \vdash \Delta}{\Gamma, \exists x{:}\, X \ \ P(x) \vdash \Delta} \qquad (\exists\text{-right }) \ \frac{\Gamma \vdash \Delta, P[x := t]}{\Gamma \vdash \Delta, \exists x{:}\, X \ \ P(x)}$$

The t is an arbitrary term of type X. The y is a variable of type X, which is not free in Γ, Δ.

rules for equality:

$$\text{(refl)}\ \frac{}{\Gamma \vdash \Delta,\ t = t}$$

$$\text{(repl)}\ \frac{t_1 = t_2,\ \Gamma[t_2] \vdash \Delta[t_2]}{t_1 = t_2, \Gamma[t_1] \vdash \Delta[t_1]}$$

The last rule means: If $t_1 = t_2$ appears among the premisses, then arbitrary occurrences of t_2 in other formulas can be replaced by t_1.

rules for IF

PVS has an IF-operator. $\mathrm{IF}(A, B, C)$ is defined as $(A \wedge B) \vee (\neg A \wedge C)$

$$\text{(IF-left)}\ \frac{\Gamma, A, B \vdash \Delta \qquad \Gamma, \neg A, C \vdash \Delta}{\Gamma, \mathrm{IF}(A, B, C) \vdash \Delta}$$

$$\text{(IF-right)}\ \frac{\Gamma, A \vdash \Delta, B \qquad \Gamma, \neg A \vdash \Delta, C}{\Gamma \vdash \Delta, \mathrm{IF}(A, B, C)}$$