Formal Specification and Verification of Object-Oriented Programs

First-Order Calculus

TECHNISCHE UNIVERSITÄT DARMSTADT

Reasoning by Syntactic Transformation

TECHNISCHE UNIVERSITÄT DARMSTADT

Prove validity of ϕ by syntactic transformation of ϕ

Logic Calculus: Sequent Calculus based on notion of sequent:

$$\underbrace{\psi_1, \ldots, \psi_m}_{\text{Antecedent}} \quad \Rightarrow \quad \underbrace{\phi_1, \ldots, \phi_n}_{\text{Succedent}}$$

has same meaning as

$$(\psi_1 \wedge \cdots \wedge \psi_m) \quad \rightarrow \quad (\phi_1 \vee \cdots \vee \phi_n)$$

Notation for Sequents

TECHNISCHE UNIVERSITÄT DARMSTADT

$$\psi_1, \ldots, \psi_m \quad \Rightarrow \quad \phi_1, \ldots, \phi_n$$

Consider antecedent/succedent as sets of formulas, may be empty

Schema Variables, Schematic Sequents

$\phi_i, \psi_j, \ldots$ match formulas; $\Gamma, \Delta, \ldots$ match sets of formulas
Characterize infinitely many sequents with a single schematic sequent

$$\Gamma \quad \Rightarrow \quad \phi \wedge \psi, \Delta$$

Matches sequents with top-level occurrence of conjunction in succedent

Call $\phi \wedge \psi$ main formula and Γ, Δ side formulas of sequent

Any sequent of the form $\Gamma, \phi \Rightarrow \phi, \Delta$ is logically valid: axiom

Sequent Calculus Rules

Write syntactic transformation schema for sequents that precisely reflects semantics of connectives

$$\text{RuleName}\ \frac{\overbrace{\Gamma_1 \Rightarrow \Delta_1 \quad \cdots \quad \Gamma_r \Rightarrow \Delta_r}^{\text{Premisses}}}{\underbrace{\Gamma \Rightarrow \Delta}_{\text{Conclusion}}}$$

Meaning: to prove the conclusion, it suffices to prove all premisses

Example

$$\text{andRight}\ \frac{\Gamma \Rightarrow \phi, \Delta \qquad \Gamma \Rightarrow \psi, \Delta}{\Gamma \Rightarrow \phi \wedge \psi, \Delta}$$

Admissible to have no premisses (iff conclusion is valid, e.g., axiom)

Sequent Calculus Rules: Soundness (Correctness)

TECHNISCHE UNIVERSITÄT DARMSTADT

$$\text{RuleName}\ \frac{\overbrace{\Gamma_1 \Rightarrow \Delta_1 \quad \cdots \quad \Gamma_r \Rightarrow \Delta_r}^{\text{Premisses}}}{\underbrace{\Gamma \Rightarrow \Delta}_{\text{Conclusion}}}$$

Meaning: to prove the conclusion, it suffices to prove all premisses

Definition (Sound Sequent Rule)

A rule is sound (correct) iff the validity of its premisses implies the validity of its conclusion.

Example

$$\text{andRight}\ \frac{\Gamma \Rightarrow \phi, \Delta \qquad \Gamma \Rightarrow \psi, \Delta}{\Gamma \Rightarrow \phi \wedge \psi, \Delta}$$

"Propositional" Sequent Calculus Rules

TECHNISCHE UNIVERSITÄT DARMSTADT

main	left side (antecedent)	right side (succedent)
not	$\dfrac{\Gamma \Rightarrow \phi, \Delta}{\Gamma, \neg\phi \Rightarrow \Delta}$	$\dfrac{\Gamma, \phi \Rightarrow \Delta}{\Gamma \Rightarrow \neg\phi, \Delta}$
and	$\dfrac{\Gamma, \phi, \psi \Rightarrow \Delta}{\Gamma, \phi \wedge \psi \Rightarrow \Delta}$	$\dfrac{\Gamma \Rightarrow \phi, \Delta \qquad \Gamma \Rightarrow \psi, \Delta}{\Gamma \Rightarrow \phi \wedge \psi, \Delta}$
or	$\dfrac{\Gamma, \phi \Rightarrow \Delta \qquad \Gamma, \psi \Rightarrow \Delta}{\Gamma, \phi \vee \psi \Rightarrow \Delta}$	$\dfrac{\Gamma \Rightarrow \phi, \psi, \Delta}{\Gamma \Rightarrow \phi \vee \psi, \Delta}$
imp	$\dfrac{\Gamma \Rightarrow \phi, \Delta \qquad \Gamma, \psi \Rightarrow \Delta}{\Gamma, \phi \rightarrow \psi \Rightarrow \Delta}$	$\dfrac{\Gamma, \phi \Rightarrow \psi, \Delta}{\Gamma \Rightarrow \phi \rightarrow \psi, \Delta}$

close $\dfrac{}{\Gamma, \phi \Rightarrow \phi, \Delta}$ true $\dfrac{}{\Gamma \Rightarrow \text{true}, \Delta}$ false $\dfrac{}{\Gamma, \text{false} \Rightarrow \Delta}$

Sequent Calculus Proofs

Goal to prove: $\mathcal{G} = \quad \psi_1, \dots, \psi_m \ \Rightarrow \ \phi_1, \dots, \phi_n$

- find rule $\mathcal{R}$ whose conclusion matches $\mathcal{G}$
- instantiate $\mathcal{R}$ such that conclusion identical to $\mathcal{G}$
- recursively find proofs for resulting premisses $\mathcal{G}_1, \dots, \mathcal{G}_r$
- tree structure with goal as root
- close proof branch when rule without premiss encountered

Goal-directed proof search

In KeY tool proof displayed as JAVA Swing tree

A Simple Proof

$$
\dfrac{\dfrac{\dfrac{\textsc{Close}\;\dfrac{*}{p \Rightarrow q,\, p} \qquad \dfrac{*}{p,\, q \Rightarrow q}\;\textsc{Close}}{p,\, (p \rightarrow q) \Rightarrow q}}{p \wedge (p \rightarrow q) \Rightarrow q}}{\Rightarrow (p \wedge (p \rightarrow q)) \rightarrow q}
$$

A proof is closed iff all its branches are closed

Demo

`prop.key`

Soundness and Completeness

Definition (Soundness of Sequent Calculus)

A sequent calculus is sound iff a closed proof implies the validity of the formula corresponding to its root sequent.

Definition (Completeness of Sequent Calculus)

A sequent calculus is complete iff for any valid formula ϕ a closed proof with root sequent $\Rightarrow \phi$ exists.

Theorem (Soundness, Completeness)

The sequent calculus as introduced in this lecture is sound and complete.

Proving Validity of First-Order Formulas

TECHNISCHE UNIVERSITÄT DARMSTADT

Proving a universally quantified formula

Claim: $\forall \tau\ x;\ \phi$ is true

How is such a claim proved in mathematics?

All even numbers are divisible by 2	$\forall$ **int** x; (even(x) $\rightarrow$ divByTwo(x))
Let c be an arbitrary number	Declare "unused" constant `int c`
The even number c is divisible by 2	prove even(c) $\rightarrow$ divByTwo(c)

Sequent rule $\forall$-right

$$\text{allRight}\ \frac{\Gamma \Rightarrow [x/c]\ \phi, \Delta}{\Gamma \Rightarrow \forall \tau\ x;\ \phi, \Delta}$$

- $[x/c]\ \phi$ is result of replacing each occurrence of x in ϕ with c
- c new constant of type τ, not occurring anywhere in ϕ, Γ, Δ

Proving Validity of First-Order Formulas Cont'd

TECHNISCHE UNIVERSITÄT DARMSTADT

Proving an existentially quantified formula

Claim: $\exists\,\tau\ x;\ \phi$ is true

How is such a claim proved in mathematics?

There is at least one prime number	$\exists$ **int** x; prime(x)
Provide any "witness", say, 7	Use variable-free term $\mathtt{int}\ \ 7$
7 is a prime number	prime(7)

Sequent rule $\exists$-right

$$\text{exRight}\ \frac{\Gamma \Rightarrow \left[x/t\right]\phi,\ \exists\,\tau\ x;\ \phi, \Delta}{\Gamma \Rightarrow \exists\,\tau\ x;\ \phi, \Delta}$$

- t any variable-free term of type τ
- Proof might not work with t! Need to keep $\exists\,\tau\ x;\ \phi$ in premise

Proving Validity of First-Order Formulas Cont'd

TECHNISCHE UNIVERSITÄT DARMSTADT

Using a universally quantified formula

We assume $\forall \tau\, x; \phi$ is true

How is such a fact used in a mathematical proof?

We know: all primes $>$ 2 are odd	$\forall\, \mathbf{int}\, x; (\mathrm{prime}(x) \land x > 2 \rightarrow \mathrm{odd}(x))$
In particular, this holds for 17	Use variable-free term $\mathtt{int}\ 17$
We know: if 17 is prime it is odd	$\mathrm{prime}(17) \land 17 > 2 \rightarrow \mathrm{odd}(17)$

Sequent rule $\forall$-left

$$\text{allLeft}\ \frac{\Gamma, \forall \tau\, x; \phi, \left[x/t'\right] \phi \Rightarrow \Delta}{\Gamma, \forall \tau\, x; \phi \Rightarrow \Delta}$$

- t' any variable-free term of type τ
- Might need other instances besides t'! Keep $\forall \tau\, x; \phi$ in premise

Proving Validity of First-Order Formulas Cont'd

TECHNISCHE UNIVERSITÄT DARMSTADT

Using an existentially quantified formula

We assume $\exists \tau\, x; \phi$ is true

How is such a fact used in a mathematical proof?

We know such an element exists, but we don't know which it is
Let's give it a new name for future reference

Sequent rule $\exists$-left

$$\text{exLeft}\ \frac{\Gamma, [x/c]\,\phi \Rightarrow \Delta}{\Gamma, \exists \tau\, x; \phi \Rightarrow \Delta}$$

- c new constant of type τ, not occurring anywhere in ϕ, Γ, Δ
- Now, we can refer to the c, for which we know that $[x/c]\,\phi$ holds

Example (A simple theorem about binary relations)

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{p(c,d),\ \forall\, y;\ p(c,y) \Rightarrow p(c,d),\ \exists\, x;\ p(x,y)}}{p(c,d),\ \forall\, y;\ p(c,y) \Rightarrow \exists\, x;\ p(x,d)}}{\forall\, y;\ p(c,y) \Rightarrow \exists\, x;\ p(x,d)}}{\forall\, y;\ p(c,y) \Rightarrow \forall\, y;\ \exists\, x;\ p(x,y)}}{\exists\, x;\ \forall\, y;\ p(x,y) \Rightarrow \forall\, y;\ \exists\, x;\ p(x,y)}$$

Untyped logic: let type of x and y be `any`

$\exists$-left: substitute new constant c of type `any` for x

$\forall$-right: substitute new constant d of type `any` for y

$\forall$-left: free to substitute any term of type `any` for y, choose d

$\exists$-right: free to substitute any term of type `any` for x, choose c

Proving Validity of First-Order Formulas: Equality

TECHNISCHE UNIVERSITÄT DARMSTADT

Using an equation between terms

We assume $t \doteq t'$ is true

How is such a fact used in a mathematical proof?

Use $x \doteq y - 1$ to simplify $(x+1)/y$ $\quad\quad$ $x \doteq y-1 \Rightarrow 1 \doteq (x+1)/y$

Replace x in conclusion with right-hand side of equation

We know: $(x+1)/y$ equal to $(y-1+1)/y$ $\quad\quad$ $x \doteq y-1 \Rightarrow 1 \doteq (y-1+1)/y$

Sequent rule $\doteq$-left

$$\text{applyEqL}\ \frac{\Gamma, t \doteq t', [t/t']\,\phi \Rightarrow \Delta}{\Gamma, t \doteq t', \phi \Rightarrow \Delta} \qquad \text{applyEqR}\ \frac{\Gamma, t \doteq t' \Rightarrow [t/t']\,\phi, \Delta}{\Gamma, t \doteq t' \Rightarrow \phi, \Delta}$$

- Always replace left- with right-hand side (use eqSymm if necessary)
- t, t' variable-free terms of the same type

Proving Validity of First-Order Formulas: Example

TECHNISCHE UNIVERSITÄT DARMSTADT

Using an existentially quantified formula and an equation

Let x, y denote arbitrary integer constants, x is not zero

We know further that x divides y

Show: $(y/x) * x \doteq y$

($'/'$ is integer division: existential premise needed, e.g., $x = 2, y = 1$)

Proof: We know x divides y, i.e., there exists a k such that $k * x \doteq y$

Let now c denote such a k

Hence we can replace y by $c * x$ on the right side

Arithmetic simplification (using $\neg(x \doteq 0)$) $\square$

$$\dfrac{\dfrac{\dfrac{\dfrac{*}{\neg(x \doteq 0),\ c * x \doteq y \Rightarrow c * x \doteq y}}{\neg(x \doteq 0),\ c * x \doteq y \Rightarrow ((c * x)/x) * x \doteq y}}{\neg(x \doteq 0),\ c * x \doteq y \Rightarrow (y/x) * x \doteq y}}{\neg(x \doteq 0),\ \exists\,\mathbf{int}\ k;\ k * x \doteq y \Rightarrow (y/x) * x \doteq y}$$

Demo

`divide.key`

Proving Validity of First-Order Formulas Cont'd

Closing a subgoal in a proof is possible when:

- We derived a sequent that is obviously valid

$$\text{close}\ \frac{}{\Gamma, \phi \Rightarrow \phi, \Delta} \qquad \text{true}\ \frac{}{\Gamma \Rightarrow \text{true}, \Delta} \qquad \text{false}\ \frac{}{\Gamma, \text{false} \Rightarrow \Delta}$$

- We derived an equation that is obviously valid

$$\text{eqClose}\ \frac{}{\Gamma \Rightarrow t \doteq t, \Delta}$$

Sequent Calculus for FOL at One Glance

	left side, antecedent	right side, succedent
$\forall$	$\dfrac{\Gamma, \forall \tau\, x;\ \phi,\ [x/t']\,\phi \Rightarrow \Delta}{\Gamma, \forall \tau\, x;\ \phi \Rightarrow \Delta}$	$\dfrac{\Gamma \Rightarrow [x/c]\,\phi, \Delta}{\Gamma \Rightarrow \forall \tau\, x;\ \phi, \Delta}$
$\exists$	$\dfrac{\Gamma, [x/c]\,\phi \Rightarrow \Delta}{\Gamma, \exists \tau\, x;\ \phi \Rightarrow \Delta}$	$\dfrac{\Gamma \Rightarrow [x/t']\,\phi,\ \exists \tau\, x;\ \phi, \Delta}{\Gamma \Rightarrow \exists \tau\, x;\ \phi, \Delta}$
$\doteq$	$\dfrac{\Gamma, t \doteq t' \Rightarrow [t/t']\,\phi, \Delta}{\Gamma, t \doteq t' \Rightarrow \phi, \Delta}$ (+ application rule on left side)	$\dfrac{}{\Gamma \Rightarrow t \doteq t, \Delta}$

- $[t/t']\,\phi$ is result of replacing each occurrence of t in ϕ with t'
- t, t' arbitrary variable-free terms of type τ
- c new constant of type τ (occurs not on current proof branch)
- Equations can be reversed by symmetry

Recap: “Propositional” Sequent Calculus Rules

TECHNISCHE UNIVERSITÄT DARMSTADT

main	left side (antecedent)	right side (succedent)
not	$\dfrac{\Gamma \Rightarrow \phi, \Delta}{\Gamma, \neg\phi \Rightarrow \Delta}$	$\dfrac{\Gamma, \phi \Rightarrow \Delta}{\Gamma \Rightarrow \neg\phi, \Delta}$
and	$\dfrac{\Gamma, \phi, \psi \Rightarrow \Delta}{\Gamma, \phi \wedge \psi \Rightarrow \Delta}$	$\dfrac{\Gamma \Rightarrow \phi, \Delta \qquad \Gamma \Rightarrow \psi, \Delta}{\Gamma \Rightarrow \phi \wedge \psi, \Delta}$
or	$\dfrac{\Gamma, \phi \Rightarrow \Delta \qquad \Gamma, \psi \Rightarrow \Delta}{\Gamma, \phi \vee \psi \Rightarrow \Delta}$	$\dfrac{\Gamma \Rightarrow \phi, \psi, \Delta}{\Gamma \Rightarrow \phi \vee \psi, \Delta}$
imp	$\dfrac{\Gamma \Rightarrow \phi, \Delta \qquad \Gamma, \psi \Rightarrow \Delta}{\Gamma, \phi \to \psi \Rightarrow \Delta}$	$\dfrac{\Gamma, \phi \Rightarrow \psi, \Delta}{\Gamma \Rightarrow \phi \to \psi, \Delta}$

close $\dfrac{}{\Gamma, \phi \Rightarrow \phi, \Delta}$ true $\dfrac{}{\Gamma \Rightarrow \text{true}, \Delta}$ false $\dfrac{}{\Gamma, \text{false} \Rightarrow \Delta}$