Some Calculus Rules in KeY

http://www.key-project.org

by Christoph Gladisch

(R1) notLeft $\frac{\Rightarrow \mathrm{A}}{\neg A \Rightarrow}$	(R7) notRight $\frac{A \Rightarrow}{\Rightarrow \neg A}$	(R2) left $\frac{A, B \Rightarrow}{A \wedge B \Rightarrow}$	(R8) andRight $\frac{\Rightarrow A \quad \Rightarrow B}{\Rightarrow A \wedge B}$	(R3) orLeft $\frac{A \Rightarrow \quad B \Rightarrow}{A \vee B \Rightarrow}$	(R9) orRight $\frac{\Rightarrow A, B}{\Rightarrow A \vee B}$
(R4) impLeft $\frac{\Rightarrow A \quad B \Rightarrow}{A \rightarrow B \Rightarrow}$	(R10) impRight $\frac{A \Rightarrow B}{\Rightarrow A \rightarrow B}$	(R11a) close $\frac{\Rightarrow}{A \Rightarrow A}$	(R11b) close $\frac{\Rightarrow}{\Rightarrow \text{true}}$	(R11c) close $\frac{\Rightarrow}{\text{false} \Rightarrow}$	
(R6) hide_left $\frac{\Rightarrow}{A \Rightarrow}$	(R12) hide_right $\frac{\Rightarrow}{\Rightarrow A}$	(R11d) replace_known_left $\frac{A \Rightarrow \text{true}}{A \Rightarrow A}$	(R11d) replace_known_right $\frac{\text{false} \Rightarrow A}{A \Rightarrow A}$	(R5) cut $\frac{A \Rightarrow \quad \Rightarrow A}{\Rightarrow}$ Click on „==>“ Case distinction	

Table 1. Propositional Inference Rules

Generalisation of rules:

If $\frac{A_0 \Rightarrow B_0 \;\; \ldots \;\; A_n \Rightarrow B_n}{A \Rightarrow B}$ is a rule, than also $\frac{\Gamma, A_0 \Rightarrow B_0, \Delta \;\; \ldots \;\; \Gamma, A_n \Rightarrow B_n, \Delta}{\Gamma, A \Rightarrow B, \Delta}$ is a rule.

(R13) allLeft $\frac{A(t), \forall x\, A(x) \Rightarrow}{\forall x\, A(x) \Rightarrow}$ Instantiate quntifier by Drag'n'Drop of t	(R17) allRight $\frac{\Rightarrow A(x\_0)}{\Rightarrow \forall x\, A(x)}$ Skolmize x. Replace by constant x_0.
(R14) exLeft $\frac{A(x\_0) \Rightarrow}{\exists x\, A(x) \Rightarrow}$ Skolmize x. Replace by constant x_0.	(R18) exRight $\frac{\Rightarrow A(x), \exists x\, A(x0}{\Rightarrow \exists x\, A(x)}$ Instantiate quntifier by Drag'n'Drop of t
(R15) int_induction $\frac{\Rightarrow \mathrm{IH}(0) \quad i \geqslant 0, \mathrm{IH}(i) \Rightarrow \mathrm{IH}(i+1) \quad \forall n\, \mathrm{IH}(n) \Rightarrow \Phi}{\Rightarrow \Phi}$ Click on „==>“. IH is Induction Hypothesis	

Table 2. First-Order Inference Rules.

(R19) eqClose $\frac{\Rightarrow \text{true}}{\Rightarrow t \doteq t}$	(R20) eqSymm $\frac{\Rightarrow b \doteq a}{\Rightarrow a \doteq b}$	(R21) make_insert_eq $\frac{a \doteq b \Rightarrow F[a/b]}{a \doteq b \Rightarrow F}$ Generate substitution $[a/b]$	(R22) applyEq or insert_eq $\frac{\Rightarrow F_b}{\Rightarrow F_a[a/b]}$ Apply substitution $[a/b]$

Table 3. First-Order with Equality. These rules are mostly symetric with respect to the sequent symbol.

(R30) polySimp_addComm0 switch_params $\boldsymbol{a+b \rightsquigarrow b+a}$	(R31) polySimp_mulComm0 mul_comm $\boldsymbol{a*b \rightsquigarrow b*a}$	(R32) polySimp_elimSub $\boldsymbol{a-b \rightsquigarrow a+b*-1}$	(R33) multiply_distribute (only with plus!) $\boldsymbol{(a+b)*c \rightsquigarrow a*c+b*c}$
(R34) switch_brackets $\boldsymbol{(a \circ b) \circ c \rightsquigarrow a \circ (b \circ c)}$	(R35) rotate_params $\boldsymbol{a \circ (b \circ c) \rightsquigarrow b \circ (a \circ c)}$	(R36) add_literals $\boldsymbol{4+19 \rightsquigarrow 23}$	(R37) polySimp_pullOutFactor $\boldsymbol{a+a \rightsquigarrow 2*a}$
(R38) add_equations $\boldsymbol{\dfrac{\Rightarrow a+c=b+d}{a=b \Rightarrow c=d}}$	(R39) add_eq $\boldsymbol{a=b \rightsquigarrow a+x=b+x}$	(R40) divide_equation $\boldsymbol{a=b \rightsquigarrow {''}a/x=b/x{''}}$	(R41) multipy_eq $\boldsymbol{a=b \rightsquigarrow a*x=b*x}$
(R42) polySimp_homoEq eq_sides $\boldsymbol{a=t \rightsquigarrow a-t=0}$	(R43) polySimp_SepPosMonomial $\boldsymbol{a+t=0 \rightsquigarrow a=-t}$ inEqSimp_SepPosMonomial $\boldsymbol{a+t \leqslant 0 \rightsquigarrow a \leqslant -t}$	(R44) inEqSimp_ltToLeq $\boldsymbol{a<t \rightsquigarrow a-t-1 \leqslant 0}$	(R45) inEqSimp_ContradIn $\boldsymbol{\dfrac{x>0 \rightarrow t_2 \leqslant t_1 \Rightarrow}{a \leqslant t_1, a \geqslant t_2 \Rightarrow}}$

Table 4. Some arithmetic rules for First-Order Logic with Integers. These rules are applicable on subformulas.

How to solve equations:

Apply *polySimp_homoEq* (R42) to obtain equations of the "normal form" **term = 0**. In order to group function symbols together (note that a, b, c... are function symbols with arity 0) apply rules like rule (R30) to (R37) manualy on **term** or right click on **term** and choose "Apply rules automatically here" (e.g. $\boldsymbol{2a}+(3b-\boldsymbol{a}) \rightsquigarrow \boldsymbol{a}+3b$). Then apply e.g. *polySimp_SepPosMonomial* (R43) in order to solve the equation for one function symbol (e.g. $\boldsymbol{a}+3b=0 \rightsquigarrow \boldsymbol{a}=-3b$). Use the rules (R38) ... (R41) only if abolutely needed. Use the rules *eqSymm* (R20), *make_inserte_eq* (R21), and *applyEq* or *insert_eq* (R22) to replace the function symbol $\boldsymbol{a}$ in other formulas.

How to solve inequations:

The idea is to move the inequation to the antecedent (left sides of the sequent symbol $\Rightarrow$), then to combine the inequations, and then to show a contradiction for the combined inequation in the antecedent.

In order to combine the inequations first use the rule *inEqSimp_ltToLeq* (R44) in order to obtain inequations of the "normal form" **term** $\boldsymbol{\leqslant 0}$. "Solve" the inequations for a common function symbol using rules (R30)... (R37) and then the rule *inEqSimp_SepPosMonomial* (R43). The antecedent should contain something like, e.g., $\boldsymbol{a}*x \leqslant t_1, \boldsymbol{a}*y \geqslant t_2 \Rightarrow$. Now combine the inequations using rule *inEqSimp_ContradIn* R45 which restults in something like $x>0 \wedge y>0 \rightarrow \boldsymbol{t_2*x \leqslant t_1*y}$. Try to derive *false* from the resulting inequation.

Generalization of Program rules:

(R46) $\langle\rangle$ generalisation $\dfrac{A \Rightarrow B}{\langle\alpha\rangle A \Rightarrow \langle\alpha\rangle B}$	(R47) [] generalisation $\dfrac{A \Rightarrow B}{[\alpha]A \Rightarrow [\alpha]B}$

Table 5. Global inference rules

If $\dfrac{A_0 \Rightarrow B_0 \quad \ldots \quad A_n \Rightarrow B_n}{A \Rightarrow B}$ is a rule, than also $\dfrac{\{U\}A_0 \Rightarrow \{U\}B_0 \quad \ldots \quad \{U\}A_n \Rightarrow \{U\}B_n}{\{U\}A \Rightarrow \{U\}B}$ is a rule, where $\{U\}$ is an update.