Discrete Mathematics with Applications I

COMPSCI&SFWRENG 2DM3

McMaster University, Fall 2019

Wolfram Kahl

2019-11-19

Given: $x \leq z \quad \equiv \quad x \leq 5$

What do you know about z? Why? (Prove it!)

Given: $X \subseteq A \rightarrowtriangle B \quad \equiv \quad X \cap A \subseteq B$

Calculate the **relative pseudocomplement** $A \rightarrowtriangle B$!

Given, for $R : A \leftrightarrow B$ and $S : A \leftrightarrow C$: $\quad X \subseteq R \backslash S \quad \equiv \quad R \fatsemi X \subseteq S$

Calculate the **right residual** (“left division”) $R \backslash S$!

$$\begin{tikzcd} A \arrow[rr, "S"] \arrow[dr, "R"'] & & C \\ & B \arrow[ur, "R \backslash S"'] & \end{tikzcd}$$

$R \backslash S$ is the largest solution $X : B \leftrightarrow C$ for $R \fatsemi X \subseteq S$.

Same idea as for “$\rightarrowtriangle$”:
Using extensionality, calculate $\quad b \llparenthesis R \backslash S \rrparenthesis c \quad \equiv \quad b \llparenthesis \,?\, \rrparenthesis c$

Given, for $R : A \leftrightarrow B$ and $S : A \leftrightarrow C$: $\quad X \subseteq R \backslash S \quad \equiv \quad R \fatsemi X \subseteq S$

Calculate the **right residual** (“left division”) $R \backslash S$!

$$\begin{tikzcd} A \arrow[rr, "S"] \arrow[dr, "R"'] & & C \\ & B \arrow[ur, "R \backslash S"'] & \end{tikzcd}$$

$$\begin{aligned} & b \llparenthesis R \backslash S \rrparenthesis c \\ = \; & \langle \text{ Similar to the calculation for relative pseudocomplement } \rangle \\ & (\forall a \mid a \llparenthesis R \rrparenthesis b \bullet a \llparenthesis S \rrparenthesis c) \\ = \; & \langle \text{ Generalised De Morgan, Relation conversions } \rangle \\ & b \llparenthesis \sim (R^{\smile} \fatsemi \sim S) \rrparenthesis c \end{aligned}$$

Therefore: $\quad R \backslash S = \sim (R^{\smile} \fatsemi \sim S)$

— monotonic in second argument; antitonic in first argument

Formalisations Using Residuals

"Aos called only brothers of Jun."

"Everybody called by Aos is a brother of Jun."

$$\begin{array}{ll} & (\forall p \mid Aos \,(\!|\, C \,|\!)\, p \;\bullet\; p \,(\!|\, B \,|\!)\, Jun) \\ \equiv & \langle \text{(14.18) Relation converse} \rangle \\ & (\forall p \mid p \,(\!|\, C^{\smile} \,|\!)\, Aos \;\bullet\; p \,(\!|\, B \,|\!)\, Jun) \\ \equiv & \langle \text{Right residual} \rangle \\ & Aos \,(\!|\, C^{\smile} \backslash B \,|\!)\, Jun \end{array}$$

Relationship via $\backslash$:

$$\begin{array}{ll} & b \,(\!|\, R \backslash S \,|\!)\, c \\ \equiv & (\forall a \mid a \,(\!|\, R \,|\!)\, b \bullet a \,(\!|\, S \,|\!)\, c) \end{array}$$

"Aos called every brother of Jun."

"Every brother of Jun has been called by Aos."

$$\begin{array}{ll} & (\forall p \mid p \,(\!|\, B \,|\!)\, Jun \;\bullet\; Aos \,(\!|\, C \,|\!)\, p) \\ \equiv & \langle \text{(14.18) Relation converse} \rangle \\ & (\forall p \mid p \,(\!|\, B \,|\!)\, Jun \;\bullet\; p \,(\!|\, C^{\smile} \,|\!)\, Aos) \\ \equiv & \langle \text{Right residual} \rangle \\ & Jun \,(\!|\, B \backslash C^{\smile} \,|\!)\, Aos \end{array}$$

Plan for Today

- Relations
  - **Relation Algebraic Proofs**
  - **Properties of Homogeneous Relations**
- Side notes on "`with`" — nothing new...

Translating between Relation Algebra and Predicate Logic

$$\begin{array}{rcl}
R = S & \equiv & (\forall x,y \bullet x \,(\!|\, R \,|\!)\, y \equiv x \,(\!|\, S \,|\!)\, y) \\
R \subseteq S & \equiv & (\forall x,y \bullet x \,(\!|\, R \,|\!)\, y \Rightarrow x \,(\!|\, S \,|\!)\, y) \\
u \,(\!|\, \{\} \,|\!)\, v & \equiv & \mathit{false} \\
u \,(\!|\, A \times B \,|\!)\, v & \equiv & u \in A \wedge v \in B \\
u \,(\!|\, \sim S \,|\!)\, v & \equiv & \neg(u \,(\!|\, S \,|\!)\, v) \\
u \,(\!|\, S \cup T \,|\!)\, v & \equiv & u \,(\!|\, S \,|\!)\, v \vee u \,(\!|\, T \,|\!)\, v \\
u \,(\!|\, S \cap T \,|\!)\, v & \equiv & u \,(\!|\, S \,|\!)\, v \wedge u \,(\!|\, T \,|\!)\, v \\
u \,(\!|\, S - T \,|\!)\, v & \equiv & u \,(\!|\, S \,|\!)\, v \wedge \neg(u \,(\!|\, T \,|\!)\, v) \\
u \,(\!|\, S \rightarrow T \,|\!)\, v & \equiv & u \,(\!|\, S \,|\!)\, v \Rightarrow u \,(\!|\, T \,|\!)\, v \\
u \,(\!|\, \mathbb{I}\, A \,|\!)\, v & \equiv & u = v \in A \\
u \,(\!|\, \mathrm{Id} \,|\!)\, v & \equiv & u = v \\
u \,(\!|\, R^{\smile} \,|\!)\, v & \equiv & v \,(\!|\, R \,|\!)\, u \\
u \,(\!|\, R \,;\, S \,|\!)\, v & \equiv & (\exists x \bullet u \,(\!|\, R \,|\!)\, x \,(\!|\, S \,|\!)\, v) \\
u \,(\!|\, R \backslash S \,|\!)\, v & \equiv & (\forall x \mid x \,(\!|\, R \,|\!)\, u \bullet x \,(\!|\, S \,|\!)\, v) \\
u \,(\!|\, S / R \,|\!)\, v & \equiv & (\forall x \mid v \,(\!|\, R \,|\!)\, x \bullet u \,(\!|\, S \,|\!)\, x)
\end{array}$$

Translating between Relation Algebra and Predicate Logic

$$
\begin{array}{rcl}
R = S & \equiv & (\forall\, x, y \bullet x \llparenthesis R \rrparenthesis y \equiv x \llparenthesis S \rrparenthesis y) \\
R \subseteq S & \equiv & (\forall\, x, y \bullet x \llparenthesis R \rrparenthesis y \Rightarrow x \llparenthesis S \rrparenthesis y) \\
u \llparenthesis \{\} \rrparenthesis v & \equiv & \mathit{false} \\
u \llparenthesis A \times B \rrparenthesis v & \equiv & u \in A \wedge v \in B \\
u \llparenthesis \sim S \rrparenthesis v & \equiv & \neg(u \llparenthesis S \rrparenthesis v) \\
u \llparenthesis S \cup T \rrparenthesis v & \equiv & u \llparenthesis S \rrparenthesis v \vee u \llparenthesis T \rrparenthesis v \\
u \llparenthesis S \cap T \rrparenthesis v & \equiv & u \llparenthesis S \rrparenthesis v \wedge u \llparenthesis T \rrparenthesis v \\
u \llparenthesis S - T \rrparenthesis v & \equiv & u \llparenthesis S \rrparenthesis v \wedge \neg(u \llparenthesis T \rrparenthesis v) \\
u \llparenthesis S \rightarrowtriangle T \rrparenthesis v & \equiv & u \llparenthesis S \rrparenthesis v \Rightarrow u \llparenthesis T \rrparenthesis v \\
u \llparenthesis \mathbb{I}\, A \rrparenthesis v & \equiv & u = v \in A \\
u \llparenthesis \mathrm{Id} \rrparenthesis v & \equiv & u = v \\
u \llparenthesis R^{\smile} \rrparenthesis v & \equiv & v \llparenthesis R \rrparenthesis u \\
u \llparenthesis R \fatsemi S \rrparenthesis v & \equiv & (\exists\, x \mid u \llparenthesis R \rrparenthesis x \bullet x \llparenthesis S \rrparenthesis v) \\
u \llparenthesis R \backslash S \rrparenthesis v & \equiv & (\forall\, x \mid x \llparenthesis R \rrparenthesis u \bullet x \llparenthesis S \rrparenthesis v) \\
u \llparenthesis S / R \rrparenthesis v & \equiv & (\forall\, x \mid v \llparenthesis R \rrparenthesis x \bullet u \llparenthesis S \rrparenthesis x)
\end{array}
$$

Translating between Relation Algebra and Predicate Logic

$$
\begin{array}{rcl}
R = S & \equiv & (\forall\, x, y \bullet x \llparenthesis R \rrparenthesis y \equiv x \llparenthesis S \rrparenthesis y) \\
R \subseteq S & \equiv & (\forall\, x, y \bullet x \llparenthesis R \rrparenthesis y \Rightarrow x \llparenthesis S \rrparenthesis y) \\
u \llparenthesis \{\} \rrparenthesis v & \equiv & \mathit{false} \\
u \llparenthesis A \times B \rrparenthesis v & \equiv & u \in A \wedge v \in B \\
u \llparenthesis \sim S \rrparenthesis v & \equiv & \neg(u \llparenthesis S \rrparenthesis v) \\
u \llparenthesis S \cup T \rrparenthesis v & \equiv & u \llparenthesis S \rrparenthesis v \vee u \llparenthesis T \rrparenthesis v \\
u \llparenthesis S \cap T \rrparenthesis v & \equiv & u \llparenthesis S \rrparenthesis v \wedge u \llparenthesis T \rrparenthesis v \\
u \llparenthesis S - T \rrparenthesis v & \equiv & u \llparenthesis S \rrparenthesis v \wedge \neg(u \llparenthesis T \rrparenthesis v) \\
u \llparenthesis S \rightarrowtriangle T \rrparenthesis v & \equiv & u \llparenthesis S \rrparenthesis v \Rightarrow u \llparenthesis T \rrparenthesis v \\
u \llparenthesis \mathbb{I}\, A \rrparenthesis v & \equiv & u = v \in A \\
u \llparenthesis \mathrm{Id} \rrparenthesis v & \equiv & u = v \\
u \llparenthesis R^{\smile} \rrparenthesis v & \equiv & v \llparenthesis R \rrparenthesis u \\
u \llparenthesis R \fatsemi S \rrparenthesis v & \equiv & (\exists\, x \bullet u \llparenthesis R \rrparenthesis x \wedge x \llparenthesis S \rrparenthesis v) \\
u \llparenthesis R \backslash S \rrparenthesis v & \equiv & (\forall\, x \bullet x \llparenthesis R \rrparenthesis u \Rightarrow x \llparenthesis S \rrparenthesis v) \\
u \llparenthesis S / R \rrparenthesis v & \equiv & (\forall\, x \bullet v \llparenthesis R \rrparenthesis x \Rightarrow u \llparenthesis S \rrparenthesis x)
\end{array}
$$

Relation-Algebraic Proof of Sub-Distributivity

Use set-algebraic properties and

Monotonicity of $\fatsemi$: $Q \subseteq R \quad \Rightarrow \quad P \fatsemi Q \subseteq P \fatsemi R$

to prove:

Subdistributivity of $\fatsemi$ over $\cap$: $Q \fatsemi (R \cap S) \;\subseteq\; (Q \fatsemi R) \cap (Q \fatsemi S)$

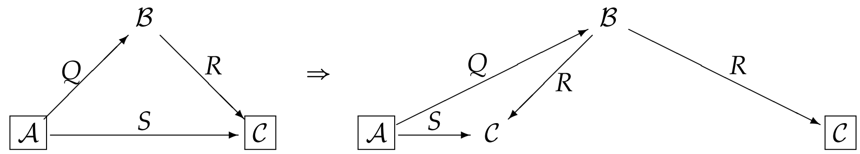
$$
\begin{array}{cl}
 & Q \fatsemi (R \cap S) \\
= & \langle \text{ Idempotence of } \cap \text{ (11.35) } \rangle \\
 & (Q \fatsemi (R \cap S)) \cap (Q \fatsemi (R \cap S)) \\
\subseteq & \langle \text{ Mon. of } \cap \text{ with Mon. of } \fatsemi \text{ with Weakening } X \cap Y \subseteq X \ \rangle \\
 & (Q \fatsemi (R \cap S)) \cap (Q \fatsemi S) \\
\subseteq & \langle \text{ Mon. of } \cap \text{ with Mon. of } \fatsemi \text{ with Weakening } X \cap Y \subseteq X \ \rangle \\
 & (Q \fatsemi R) \cap (Q \fatsemi S)
\end{array}
$$

Recall: Modal Rules & Dedekind Rule— Converse as Over-Approximation of Inverse

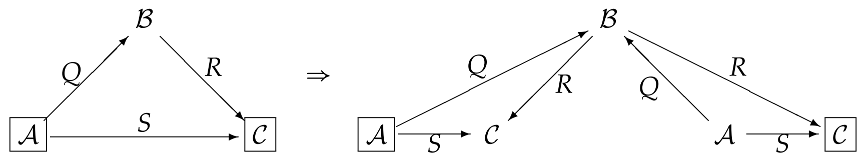
Modal rules: For $Q : \mathcal{A} \leftrightarrow \mathcal{B}$, $R : \mathcal{B} \leftrightarrow \mathcal{C}$, and $S : \mathcal{A} \leftrightarrow \mathcal{C}$:

$$Q ; R \cap S \subseteq Q ; (R \cap Q^{\smile} ; S)$$
$$Q ; R \cap S \subseteq (Q \cap S ; R^{\smile}) ; R$$

In constraint diagrams:



Equivalent: **Dedekind:** $Q ; R \cap S \subseteq (Q \cap S ; R^{\smile}) ; (R \cap Q^{\smile} ; S)$



Useful to "make information available locally" ($Q \longrightarrow Q \cap S ; R^{\smile}$) for use in further proof steps.

Proving the Modal Rules from the Dedekind Rule

Dedekind: $Q ; R \cap S \subseteq (Q \cap S ; R^{\smile}) ; (R \cap Q^{\smile} ; S)$

Modal rule: $Q ; R \cap S \subseteq Q ; (R \cap Q^{\smile} ; S)$

$$
\begin{aligned}
& Q ; R \cap S \\
\subseteq\ & \langle \text{ Dedekind } \rangle \\
& (Q \cap S ; R^{\smile}) ; (R \cap Q^{\smile} ; S) \\
\subseteq\ & \langle \text{ Mon. of } ; \text{ with (11.38) Weakening } S \cap T \subseteq S \ \rangle \\
& Q ; (R \cap Q^{\smile} ; S)
\end{aligned}
$$

Modal rule: $Q ; R \cap S \subseteq (Q \cap S ; R^{\smile}) ; R$

$$
\begin{aligned}
& Q ; R \cap S \\
\subseteq\ & \langle \text{ Dedekind } \rangle \\
& (Q \cap S ; R^{\smile}) ; (R \cap Q^{\smile} ; S) \\
\subseteq\ & \langle \text{ Mon. of } ; \text{ with (11.38) Weakening } S \cap T \subseteq S \ \rangle \\
& (Q \cap S ; R^{\smile}) ; R
\end{aligned}
$$

Proving the Dedekind Rule from the Modal Rules

Modal rules:

$$Q ; R \cap S \subseteq Q ; (R \cap Q^{\smile} ; S)$$
$$Q ; R \cap S \subseteq (Q \cap S ; R^{\smile}) ; R$$

Dedekind: $Q ; R \cap S \subseteq (Q \cap S ; R^{\smile}) ; (R \cap Q^{\smile} ; S)$

$$
\begin{aligned}
& Q ; R \cap S \\
=\ & \langle \text{ (11.35) Idempotency of } \cap \ \rangle \\
& Q ; R \cap S \cap S \\
\subseteq\ & \langle \text{ Mon. of } \cap \text{ with Modal rule } \rangle \\
& (Q \cap S ; R^{\smile}) ; R \cap S \\
\subseteq\ & \langle \text{ Modal rule } \rangle \\
& (Q \cap S ; R^{\smile}) ; (R \cap (Q \cap S ; R^{\smile})^{\smile} ; S) \\
\subseteq\ & \langle \text{ Mon. of } ; \text{ with Mon. of } \cap \text{ with Mon. of } ; \text{ with Mon. of } {}^{\smile} \text{ with Weakening } \rangle \\
& (Q \cap S ; R^{\smile}) ; (R \cap Q^{\smile} ; S)
\end{aligned}
$$

Modal Rules and Dedekind Rule: Sharp Versions

For all $Q : \mathcal{A} \leftrightarrow \mathcal{B}$, $R : \mathcal{B} \leftrightarrow \mathcal{C}$, and $S : \mathcal{A} \leftrightarrow \mathcal{C}$:

Modal rules:
$$Q ⨾ R \cap S \subseteq Q ⨾ (R \cap Q^\smile ⨾ S)$$
$$Q ⨾ R \cap S \subseteq (Q \cap S ⨾ R^\smile) ⨾ R$$

Modal rules (sharp versions):
$$Q ⨾ R \cap S \;=\; Q ⨾ (R \cap Q^\smile ⨾ S) \cap S$$
$$Q ⨾ R \cap S \;=\; (Q \cap S ⨾ R^\smile) ⨾ R \cap S$$

Dedekind:
$$Q ⨾ R \cap S \subseteq (Q \cap S ⨾ R^\smile) ⨾ (R \cap Q^\smile ⨾ S)$$

Dedekind (sharp version):
$$Q ⨾ R \cap S \;=\; (Q \cap S ⨾ R^\smile) ⨾ (R \cap Q^\smile ⨾ S) \cap S$$

Proofs: Exercise!

Relation Algebra

- For any two sets B and C, on the set $B \leftrightarrow C$ of **relations between B and C** we have the ordering $\subseteq$ with:
  - binary minima $\_\cap\_$ and maxima $\_\cup\_$ (which are monotonic)
  - least relation $\{\}$ and largest ("universal") relation $B \times C$
  - complement operation $\sim\_$ such that $R \cap \sim R = \{\}$ and $R \cup \sim R = B \times C$
  - relative pseudo-complement $R \mathrel{-\!\triangleright} S \;=\; \sim R \cup S$
- The composition operation $\_ ⨾ \_$
  - is defined on any two relations $R : B \leftrightarrow C_1$ and $S : C_2 \leftrightarrow D$ iff $C_1 = C_2$
  - is associative, monotonic, and has identities Id
  - distributes over union: $Q ⨾ (R \cup S) = Q ⨾ R \cup Q ⨾ S$
- The converse operation $\_^\smile$
  - maps relation $R : B \leftrightarrow C$ to $R^\smile : C \leftrightarrow B$
  - is self-inverse ($R^{\smile\smile} = R$) and monotonic
  - is contravariant wrt. composition: $(R ⨾ S)^\smile = S^\smile ⨾ R^\smile$
- The Dedekind rule holds: $Q ⨾ R \cap S \subseteq (Q \cap S ⨾ R^\smile) ⨾ (R \cap Q^\smile ⨾ S)$
- The Schröder equivalences hold:
  $$Q ⨾ R \subseteq S \;\equiv\; Q^\smile ⨾ \sim S \subseteq \sim R \qquad \text{and} \qquad Q ⨾ R \subseteq S \;\equiv\; \sim S ⨾ R^\smile \subseteq \sim Q$$
- $⨾$ has left-residuals $S \,/\, R = \sim(\sim S ⨾ R^\smile)$ and right-residuals $Q \setminus S = \sim(Q^\smile ⨾ \sim S)$

Properties of Homogeneous Relations

reflexive	$\mathrm{Id} \subseteq R$	$(\forall\, b : B \bullet b \,(R)\, b)$
irreflexive	$\mathrm{Id} \cap R = \{\}$	$(\forall\, b : B \bullet \neg(b \,(R)\, b))$
symmetric	$R^\smile = R$	$(\forall\, b, c : B \bullet b \,(R)\, c \equiv c \,(R)\, b)$
antisymmetric	$R \cap R^\smile \subseteq \mathrm{Id}$	$(\forall\, b, c \bullet b \,(R)\, c \wedge c \,(R)\, b \Rightarrow b = c)$
asymmetric	$R \cap R^\smile = \{\}$	$(\forall\, b, c : B \bullet b \,(R)\, c \Rightarrow \neg(c \,(R)\, b))$
transitive	$R ⨾ R \subseteq R$	$(\forall b, c, d \bullet b \,(R)\, c \wedge c \,(R)\, d \Rightarrow b \,(R)\, d)$

R is an **equivalence (relation) on** B iff it is reflexive, transitive, and symmetric.

R is a **(partial) order on** B iff it is reflexive, transitive, and antisymmetric. (E.g., $\leq$, $\geq$, $\subseteq$, $\supseteq$, *divides*)

R is a **strict-order on** B iff it is irreflexive, transitive, and asymmetric. (E.g., $<$, $>$, $\subset$, $\supset$)

Most Homogeneous Rel. Properties are Preserved by Intersection

reflexive	$\mathrm{Id} \subseteq R$
irreflexive	$\mathrm{Id} \cap R = \{\}$
transitive	$R ; R \subseteq R$
idempotent	$R ; R = R$

symmetric	$R^{\smallsmile} = R$
antisymmetric	$R \cap R^{\smallsmile} \subseteq \mathrm{Id}$
asymmetric	$R \cap R^{\smallsmile} = \{\}$

Theorem: If $R, S : B \leftrightarrow B$ are reflexive/irreflexive/symmetric/antisymmetric/asymmetric/transitive, then $R \cap S$ has that property, too.

Proof: Reflexivity:

$$
\begin{aligned}
& \mathrm{Id} \\
=\ & \langle \text{ Idempotence of } \cap \rangle \\
& \mathrm{Id} \cap \mathrm{Id} \\
\subseteq\ & \langle \text{ Mon. of } \cap \text{ with Reflexivity of } R \rangle \\
& R \cap \mathrm{Id} \\
\subseteq\ & \langle \text{ Mon. of } \cap \text{ with Reflexivity of } S \rangle \\
& R \cap S
\end{aligned}
$$

Transitivity:

$$
\begin{aligned}
& (R \cap S) ; (R \cap S) \\
\subseteq\ & \langle \text{ Sub-distributivity of } ; \text{ over } \cap \rangle \\
& (R ; R) \cap (R ; S) \cap (S ; R) \cap (S ; S) \\
\subseteq\ & \langle \text{ Weakening } X \cap Y \subseteq X \rangle \\
& (R ; R) \cap (S ; S) \\
\subseteq\ & \langle \text{ Mon. } \cap \text{ with transitivity of } R \text{ and } S \rangle \\
& R \cap S
\end{aligned}
$$

<u>Some</u> Homogeneous Rel. Properties are Preserved by Union

reflexive	$\mathrm{Id} \subseteq R$
irreflexive	$\mathrm{Id} \cap R = \{\}$
transitive	$R ; R \subseteq R$
idempotent	$R ; R = R$

symmetric	$R^{\smallsmile} = R$
antisymmetric	$R \cap R^{\smallsmile} \subseteq \mathrm{Id}$
asymmetric	$R \cap R^{\smallsmile} = \{\}$

Theorem: If $R, S : B \leftrightarrow B$ are reflexive/irreflexive/symmetric, then $R \cup S$ has that property, too.

Proof:

Reflexivity:

$$
\begin{aligned}
& \mathrm{Id} \\
\subseteq\ & \langle \text{ Reflexivity of } R \rangle \\
& R \\
\subseteq\ & \langle \text{ Weakening } X \subseteq X \cup Y \rangle \\
& R \cup S
\end{aligned}
$$

Irreflexivity:

$$
\begin{aligned}
& \mathrm{Id} \cap (R \cup S) \\
=\ & \langle \text{ Distributivity of } \cap \text{ over } \cup \rangle \\
& (\mathrm{Id} \cap R) \cup (\mathrm{Id} \cap S) \\
=\ & \langle \text{ Mon. of } \cup \text{ with Irreflexivity of } R \text{ and } S \rangle \\
& \{\} \cup \{\} \\
=\ & \langle \text{ Idempotence of } \cup \rangle \\
& \{\}
\end{aligned}
$$

Weaker Formulation of Symmetry

reflexive	$\mathrm{Id} \subseteq R$
irreflexive	$\mathrm{Id} \cap R = \{\}$
transitive	$R ; R \subseteq R$
idempotent	$R ; R = R$

symmetric	$R^{\smallsmile} = R$
antisymmetric	$R \cap R^{\smallsmile} \subseteq \mathrm{Id}$
asymmetric	$R \cap R^{\smallsmile} = \{\}$

For proving symmetry of $R, S : B \leftrightarrow B$, it is sufficient to prove $R^{\smallsmile} \subseteq R$.

In other words:

Theorem: If $R^{\smallsmile} \subseteq R$, then $R^{\smallsmile} = R$.

Proof: By mutual inclusion, we only need to show $R \subseteq R^{\smallsmile}$:

$$
\begin{aligned}
& R \\
=\ & \langle \text{ Self-inverse of converse } \rangle \\
& (R^{\smallsmile})^{\smallsmile} \\
\subseteq\ & \langle \text{ Mon. of } {}^{\smallsmile} \text{ with Assumption } R^{\smallsmile} \subseteq R \rangle \\
& R^{\smallsmile}
\end{aligned}
$$

`with` — Overview

CalcCheck currently knows three kinds of “`with`”:

- “$\texttt{with}_0$”: For explicit substitutions: **“Identity of +”** with ‘$x := 2$‘
- “$\texttt{with}_1$”: *ThmA* `with` *ThmB*
  - If *ThmB* gives rise to an equality/equivalence $L = R$:
    Rewrite *ThmA* with $L \mapsto R$ to *ThmA*′,
    and use *ThmA*′ for rewriting the goal.
- “$\texttt{with}_2$”: *ThmA* `with` *ThmB* and *ThmB*$_2$ ...
  - If *ThmA* gives rise to an implication $A_1 \Rightarrow A_2 \Rightarrow \ldots (L = R)$:
    Perform **conditional rewriting**, rigidly applying $L\sigma \mapsto R\sigma$
    if using *ThmB* and *ThmB*$_2$ ... to prove $A_1\sigma, A_2\sigma, \ldots$ succeeds

Using hi_1: sp_1 sp_2	is essentially syntactic sugar for:	By hi_1 with sp_1 and sp_2

$\texttt{with}_1$: Rewriting Theorems before Rewriting

ThmA `with` *ThmB*

- If *ThmB* gives rise to an equality/equivalence $L = R$:
  Rewrite *ThmA* with $L \mapsto R$
- E.g.: “Instantiation” with (3.60)

  $(\forall\, x \bullet P) \Rightarrow P[x := E]$ rewrites via $q \Rightarrow r \;\mapsto\; q \equiv q \wedge r$

  to: $(\forall\, x \bullet P) \;\equiv\; (\forall\, x \bullet P) \wedge P[x := E]$

  which can be used as: $(\forall\, x \bullet P) \;\mapsto\; (\forall\, x \bullet P) \wedge P[x := E]$

```
  ∃ b • a ( Q ) b ∧ b ( S ) c
⇒⟨ “Body monotonicity of ∃” with “Monotonicity of ∧”
   with assumption `Q ⊆ R` with “Relation inclusion” ⟩
  ∃ b • a ( R ) b ∧ b ( S ) c
```

$\texttt{with}_2$: Conditional Rewriting

ThmA `with` *ThmB* and *ThmB*$_2$ ...

- If *ThmA* gives rise to an implication $A_1 \Rightarrow A_2 \Rightarrow \ldots (L = R)$:
  - Find substitution σ such that $L\sigma$ matches goal
  - Resolve $A_1\sigma, A_2\sigma, \ldots$ using *ThmB* and *ThmB*$_2$ ...
  - Rewrite goal applying $L\sigma \mapsto R\sigma$ rigidly.
- E.g.: “Cancellation of $\cdot$” with Assumption ‘$m + n \neq 0$‘
  when trying to prove $(m + n) \cdot (n + 2) = (m + n) \cdot 5 \cdot k$:
  - “Cancellation of $\cdot$” is: $c \neq 0 \Rightarrow (c \cdot a = c \cdot b \equiv a = b)$
  - We try to use: $c \cdot a = c \cdot b \mapsto a = b$, so L is $c \cdot a = c \cdot b$
  - Matching L against goal produces $\sigma = [a, b, c := (n + 2), (5 \cdot k), (m + n)]$
  - $(c \neq 0)\sigma$ is $(m + n) \neq 0$ and can be proven by “Assumption ‘$m + n \neq 0$‘”
  - The goal is rewritten to $(a = b)\sigma$, that is, $(n + 2) = 5 \cdot k$.

```
  ∃ b • a ( Q ) b ∧ b ( S ) c
⇒⟨ “Body monotonicity of ∃” with “Monotonicity of ∧”
   with “Relation inclusion” with assumption `Q ⊆ R` ⟩
  ∃ b • a ( R ) b ∧ b ( S ) c
```

$\texttt{with}_1$ and $\texttt{with}_2$: Example

```
  ∃ b • a ⦇ Q ⦈ b ∧ b ⦇ S ⦈ c
⇒⟨ “Body monotonicity of ∃” with “Monotonicity of ∧”
     with assumption `Q ⊆ R` with “Relation inclusion” ⟩
  ∃ b • a ⦇ R ⦈ b ∧ b ⦇ S ⦈ c
```

- assumption ‘$Q \subseteq R$‘ gives you $Q \subseteq R$
- assumption ‘$Q \subseteq R$‘ with “Relation inclusion”

  gives you via $\texttt{with}_1$: $\forall x \bullet \forall y \bullet x ⦇ Q ⦈ y \Rightarrow x ⦇ R ⦈ y$

  and then via implicit “Instantiation” triggered by the next $\texttt{with}_2$:

  $a ⦇ Q ⦈ b \quad \Rightarrow \quad a ⦇ R ⦈ b$
- “Monotonicity of $\wedge$” with

  assumption ‘$Q \subseteq R$‘ with “Relation inclusion”

  gives you via $\texttt{with}_2$: $a ⦇ Q ⦈ b \wedge b ⦇ S ⦈ c \quad \Rightarrow \quad a ⦇ R ⦈ b \wedge b ⦇ S ⦈ c$
- “Body monotonicity of $\exists$” with “Monotonicity of $\wedge$” with

  assumption ‘$Q \subseteq R$‘ with “Relation inclusion”

  gives you via $\texttt{with}_2$:

  $$(\exists b \bullet a ⦇ Q ⦈ b \wedge b ⦇ S ⦈ c) \quad \Rightarrow \quad (\exists b \bullet a ⦇ R ⦈ b \wedge b ⦇ S ⦈ c)$$