Discrete Mathematics with Applications I

COMPSCI&SFWRENG 2DM3

McMaster University, Fall 2019

Wolfram Kahl

2019-11-13

Let c be defined by: $\qquad x \leq c \quad \equiv \quad x \leq 5$

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

A Set Theory Exercise

Let A, B : **set** t be two sets of the same type.

The **relative pseudocomplement** $A \twoheadrightarrow B$ of A with respect to B is defined by:

$$X \subseteq (A \twoheadrightarrow B) \quad \equiv \quad X \cap A \subseteq B$$

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

Using extensionality, that is:

Calculate $\quad x \in A \twoheadrightarrow B \quad \equiv \quad x \in$ **?**

Let c be defined by: $\qquad x \leq c \quad \equiv \quad x \leq 5$

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

Note: x is implicitly univerally quantified!

Proving $5 \leq c$**:**

$$\begin{array}{ll} & 5 \leq c \\ \equiv & \langle \text{ The given equivalence, with } x := 5 \ \rangle \\ & 5 \leq 5 \quad \text{— This is Reflexivity of } \leq \end{array}$$

Proving $c \leq 5$**:**

$$\begin{array}{ll} & c \leq 5 \\ \equiv & \langle \text{ Given equivalence, with } x := c \ \rangle \\ & c \leq c \quad \text{— This is Reflexivity of } \leq \end{array}$$

With antisymmetry of $\leq$ (that is, $a \leq b \wedge b \leq a \Rightarrow a = b$),we obtain $z = 5$ — this is:

(15.47) **Indirect equality:** $\quad a = b \quad \equiv \quad (\forall z \bullet z \leq a \quad \equiv \quad z \leq b)$

Characterisation of relative pseudocomplement of sets: $X \subseteq (A \twoheadrightarrow B) \quad \equiv \quad X \cap A \subseteq B$

$$
\begin{array}{ll}
 & x \in A \twoheadrightarrow B \\
\equiv & \langle\, e \in S \equiv \{e\} \subseteq S \quad \text{— Exercise!} \,\rangle \\
 & \{x\} \subseteq A \twoheadrightarrow B \\
\equiv & \langle\, \text{Def. } \twoheadrightarrow \text{, with } X := \{x\} \,\rangle \\
 & \{x\} \cap A \subseteq B \\
\equiv & \langle\, \text{(11.13) Subset} \,\rangle \\
 & (\forall y \mid y \in \{x\} \cap A \bullet y \in B) \\
\equiv & \langle\, \text{(11.21) Intersection} \,\rangle \\
 & (\forall y \mid y \in \{x\} \land y \in A \bullet y \in B) \\
\equiv & \langle\, y \in \{x\} \equiv y = x \quad \text{— Exercise!} \,\rangle \\
 & (\forall y \mid y = x \land y \in A \bullet y \in B) \\
\equiv & \langle\, \text{(9.4b) Trading for } \forall \text{, Def. } \notin \,\rangle \\
 & (\forall y \mid y = x \bullet y \notin A \lor y \in B) \\
\equiv & \langle\, \text{(8.14) One-point rule} \,\rangle \\
 & x \notin A \lor x \in B \\
\equiv & \langle\, \text{(11.17) Set complement, (11.20) Union} \,\rangle \\
 & x \in {\sim}A \cup B
\end{array}
$$

Theorem: $A \twoheadrightarrow B \quad = \quad {\sim}A \cup B$

Characterisation of relative pseudocomplement of sets: $X \subseteq A \twoheadrightarrow B \quad \equiv \quad X \cap A \subseteq B$

Theorem "Pseudocomplement via $\cup$": $A \twoheadrightarrow B \quad = \quad {\sim}A \cup B$

Calculation:

$$
\begin{array}{ll}
 & x \in A \twoheadrightarrow B \\
\equiv & \langle\, \text{Pseudocomplement via } \cup \,\rangle \\
 & x \in {\sim}A \cup B \\
\equiv & \langle\, \text{(11.17) Set complement, (11.20) Union} \,\rangle \\
 & \neg(x \in A) \lor x \in B \\
\equiv & \langle\, \text{(3.59) Definition of } \Rightarrow \,\rangle \\
 & x \in A \Rightarrow x \in B
\end{array}
$$

Corollary "Membership in pseudocomplement": $x \in A \twoheadrightarrow B \quad \equiv \quad x \in A \Rightarrow x \in B$

Easy to see: On sets, relative pseudocomplement wrt. $\{\}$ is complement: $A \twoheadrightarrow \{\} \;=\; {\sim}A$

Plan for Today: Relations, Relation Properties

- Theorems about relation composition $⨾$
- Properties of relations: Definitions via predicate logic and via relation algebra
- First relation-algebraic proofs

Operations on Relations

- Set operations $\sim$, $\cup$, $\cap$, $-$, $\rightharpoondown$ are all available.

- If $R : B \leftrightarrow C$, $\quad B \xrightarrow{R} C$
  then its **converse** $R^{\smile} : C \leftrightarrow B$
  (in the textbook called "inverse" and written: R^{-1})
  stands for "going R backwards": $\quad c \,(\!|\, R^{\smile} \,|\!)\, b \quad \equiv \quad b \,(\!|\, R \,|\!)\, c$

- If $R : B \leftrightarrow C$ and $S : C \leftrightarrow D$, $\quad B \xrightarrow{R} C \xrightarrow{S} D$
  then their **composition** $R \fatsemi S$
  (in the textbook written: $R \circ S$)
  is a relation in $B \leftrightarrow D$, and stands for
  "going first a step via R, and then a step via S":
  $$b \,(\!|\, R \fatsemi S \,|\!)\, d \quad \equiv \quad (\exists c : C \bullet b \,(\!|\, R \,|\!)\, c \,(\!|\, S \,|\!)\, d)$$

The resulting **relation algebra**

- allows concise formalisations **without quantifications**,
- enables simple calculational proofs.

$$\begin{array}{lcll} P & := & \text{type of persons} & \\ C & : & P \leftrightarrow P & \text{— "called"} \\ B & : & P \leftrightarrow P & \text{— "brother of"} \\ Aos : P & & & \\ Jun : P & & & \end{array}$$

Convert into English (via predicate logic):

$$Aos \,(\!|\, C \,|\!)\, Jun$$
$$Aos \,(\!|\, C \fatsemi B \,|\!)\, Jun$$
$$Aos \,(\!|\, \sim (C \fatsemi \sim B) \,|\!)\, Jun$$
$$Aos \,(\!|\, \sim (\sim C \fatsemi B) \,|\!)\, Jun$$
$$Aos \,(\!|\, \sim ((C \cap \sim (B \fatsemi C^{\smile})) \fatsemi \sim B) \,|\!)\, Jun$$
$$(B \fatsemi (\{Jun\} \times \llcorner P \lrcorner)) \cap (C \fatsemi C^{\smile}) \quad \subseteq \quad \mathbb{I}\, \llcorner P \lrcorner$$

$$\begin{array}{lcll} P & := & \text{type of persons} & \\ C & : & P \leftrightarrow P & \text{— "called"} \\ B & : & P \leftrightarrow P & \text{— "brother of"} \\ Aos : P & & & \\ Jun : P & & & \end{array}$$

Convert into English (via predicate logic):

$$\begin{array}{ll} & Aos \,(\!|\, C \fatsemi B \,|\!)\, Jun \\ = & \langle \text{(14.20) Relation composition} \rangle \\ & (\exists\, b \bullet Aos \,(\!|\, C \,|\!)\, b \,(\!|\, B \,|\!)\, Jun) \end{array}$$

"Aos called some brother of Jun."

"Aos called a brother of Jun."

$$\begin{array}{ll}
& Aos \,(\!|\, \sim(C \mathbin{;} \sim B) \,|\!)\, Jun \\
= & \langle \text{ (11.17r) Relation complement } \rangle \\
& \neg(Aos \,(\!|\, C \mathbin{;} \sim B \,|\!)\, Jun) \\
= & \langle \text{ (14.20) Relation composition } \rangle \\
& \neg(\exists\, p \bullet Aos \,(\!|\, C \,|\!)\, p \,(\!|\, \sim B \,|\!)\, Jun) \\
= & \langle \text{ (11.17r) Relation complement } \rangle \\
& \neg(\exists\, p \bullet Aos \,(\!|\, C \,|\!)\, p \wedge \neg(p \,(\!|\, B \,|\!)\, Jun)) \\
= & \langle \text{ (9.18b) Generalised De Morgan } \rangle \\
& (\forall\, p \bullet \neg(Aos \,(\!|\, C \,|\!)\, p \wedge \neg(p \,(\!|\, B \,|\!)\, Jun))) \\
= & \langle \text{ (3.47) De Morgan, (3.12) Double negation } \rangle \\
& (\forall\, p \bullet \neg(Aos \,(\!|\, C \,|\!)\, p) \vee p \,(\!|\, B \,|\!)\, Jun) \\
= & \langle \text{ (9.3a) Trading for } \forall \rangle \\
& (\forall\, p \mid Aos \,(\!|\, C \,|\!)\, p \bullet p \,(\!|\, B \,|\!)\, Jun)
\end{array}$$

"Everybody Aos called is a brother of Jun."

"Aos called only brothers of Jun."

Formalise Without Quantifiers! (2)

$$\begin{array}{lcl}
P & := & \text{type of persons} \\
C & : & P \leftrightarrow P \\
p \,(\!|\, C \,|\!)\, q & :\equiv & p \text{ called } q
\end{array}$$

1. Helen called somebody who called her.

   $$Helen \in Dom\,(C \cap C^{\smile})$$

2. For arbitrary people x, z, if x called z, then there is sombody whom x called, and who was called by somebody who also called z.

   $$C \quad \subseteq \quad C \mathbin{;} C^{\smile} \mathbin{;} C$$

3. For arbitrary people x, y, z, if x called y, and y was called by somebody who also called z, then x called z.

   $$C \mathbin{;} C^{\smile} \mathbin{;} C \quad \subseteq \quad C$$

4. Obama called everybody directly, or indirectly via at most two intermediaries.

   $$\{Obama\} \times \llcorner P \lrcorner \quad \subseteq \quad C \cup C \mathbin{;} C \cup C \mathbin{;} C \mathbin{;} C$$

Translating between Relation Algebra and Predicate Logic

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

Properties of Composition

If $R : B \leftrightarrow C$ and $S : C \leftrightarrow D$, then their **composition** $R \fatsemi S : B \leftrightarrow D$ is defined by:

(14.20) $b \llparenthesis R \fatsemi S \rrparenthesis d \;\equiv\; (\exists c : C \bullet b \llparenthesis R \rrparenthesis c \wedge c \llparenthesis S \rrparenthesis d)$ (for $b : B, d : D$)

(14.22) **Associativity of $\fatsemi$:** $Q \fatsemi (R \fatsemi S) \;=\; (Q \fatsemi R) \fatsemi S$

Left- and Right-identities of $\fatsemi$: If $R : B \leftrightarrow C$, then:

$$\mathbb{I}\llcorner B \lrcorner \fatsemi R \;=\; R \;=\; R \fatsemi \mathbb{I}\llcorner C \lrcorner$$

We define another abbreviation: $\mathrm{Id} \;=\; \mathbb{I}\,\mathbf{U}$

Relationship via Id: $x \llparenthesis \mathrm{Id} \rrparenthesis y \;\equiv\; x = y$

Then Id is "the" identity of composition:

Identity of $\fatsemi$: $\mathrm{Id} \fatsemi R \;=\; R \;=\; R \fatsemi \mathrm{Id}$

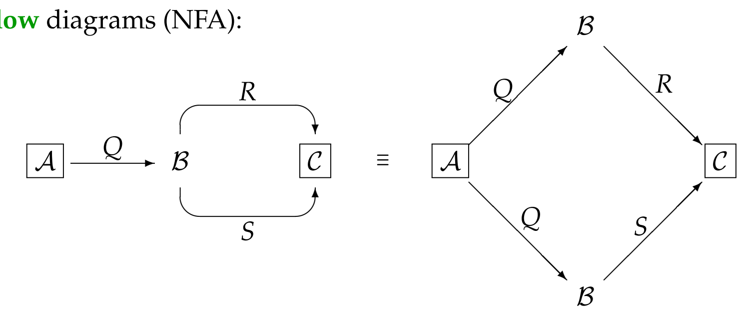
Contravariance: $(R \fatsemi S)^{\smile} \;=\; S^{\smile} \fatsemi R^{\smile}$

Distributivity of Relation Composition over Union

Composition distributes over **union** from both sides:

(14.23)
$$Q \fatsemi (R \cup S) \;=\; Q \fatsemi R \cup Q \fatsemi S$$
$$(P \cup Q) \fatsemi R \;=\; P \fatsemi R \cup Q \fatsemi R$$

In **control flow** diagrams (NFA):



Q := walk $\quad$ R := take bus $\quad$ S := take train

$$\forall\, a : A, c : C \bullet \quad (\exists\, b : B \bullet a \llparenthesis Q \rrparenthesis b \llparenthesis R \cup S \rrparenthesis c) \;\equiv\; (\exists\, b_1, b_2 : B \bullet a \llparenthesis Q \rrparenthesis b_1 \llparenthesis R \rrparenthesis c \;\vee\; a \llparenthesis Q \rrparenthesis b_2 \llparenthesis S \rrparenthesis c)$$

Monotonicity of Relation Composition

Relation composition is monotonic in both arguments:

$$Q \subseteq R \;\Rightarrow\; Q \fatsemi S \subseteq R \fatsemi S$$
$$Q \subseteq R \;\Rightarrow\; P \fatsemi Q \subseteq P \fatsemi R$$

We could prove this via **"Relation inclusion"** *and* **"For any"**, *but we don't need to:*

Assume $Q \subseteq R$, which by (11.45) is equivalent to $Q \cup R = R$:

Proving $Q \fatsemi S \subseteq R \fatsemi S$:

$R \fatsemi S$

$=$ ⟨ Assumption $Q \cup R = R$ ⟩

$(Q \cup R) \fatsemi S$

$=$ ⟨ (14.23) Distributivity of $\fatsemi$ over $\cup$ ⟩

$Q \fatsemi S \cup R \fatsemi S$

$\supseteq$ ⟨ (11.31) Strengthening $S \subseteq S \cup T$ ⟩

$Q \fatsemi S$

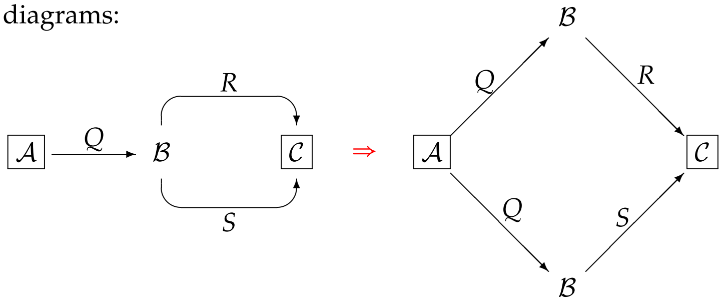
Sub-Distributivity of Composition over Intersection

Composition **sub-**distributes over **intersection** from both sides:

(14.24) $\quad Q ⨾ (R \cap S) \subseteq Q ⨾ R \cap Q ⨾ S$

$\qquad\qquad (P \cap Q) ⨾ R \subseteq P ⨾ R \cap Q ⨾ R$

In **constraint** diagrams:



Q := neighbour of $\qquad R$:= brother of $\qquad S$:= parent of

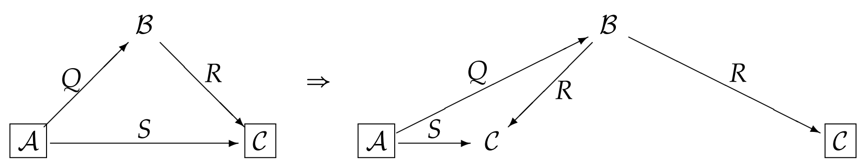
$$\forall\, a : A, c : C \bullet \quad (\exists\, b : B \bullet a \,(\!|Q|\!)\, b \,(\!|R \cap S|\!)\, c) \;\Rightarrow\; (\,\exists\, b_1, b_2 : B \bullet a \,(\!|Q|\!)\, b_1 \,(\!|R|\!)\, c \;\wedge\; a \,(\!|Q|\!)\, b_2 \,(\!|S|\!)\, c\,)$$

Modal Rules and Dedekind Rule— Converse as Over-Approximation of Inverse

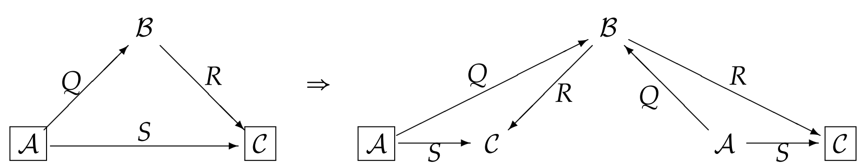
Modal rules: For $Q : \mathcal{A} \leftrightarrow \mathcal{B}$, $R : \mathcal{B} \leftrightarrow \mathcal{C}$, and $S : \mathcal{A} \leftrightarrow \mathcal{C}$: $\quad Q ⨾ R \cap S \subseteq Q ⨾ (R \cap Q^{\smile} ⨾ S)$

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

In **constraint** diagrams:



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



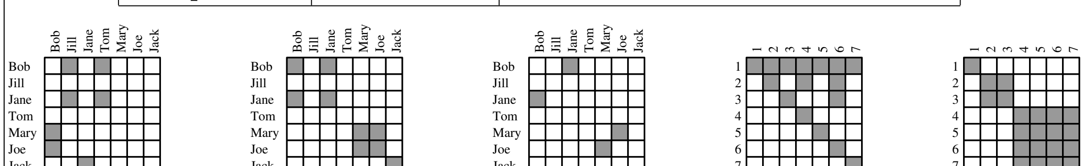
Useful to "**make information available locally**" $\quad (Q \longrightarrow Q \cap S ⨾ R^{\smile})$ for use in further proof steps.

Properties of Homogeneous Relations (Table 14.1)

A relation $R : B \leftrightarrow C$ is called **homogeneous** iff $B = C$.

A (homogeneous) relation $R : B \leftrightarrow B$ is called:

reflexive	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	$R \cap R^{\smile}$	$\subseteq$	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	$(\forall b, c, d \bullet b \,(\!|R|\!)\, c \,(\!|R|\!)\, d \Rightarrow b \,(\!|R|\!)\, d)$
idempotent	$R ⨾ R$	$=$	R	



Properties of Homogeneous Relations (ctd.)

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., $<$, $>$, $\subset$, $\supset$)

Homogeneous Relation Properties are Preserved by Converse

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	$R ⨾ R \subseteq R$	$(\forall b, c, d \bullet b \,(R)\, c \,(R)\, d \;\Rightarrow\; b \,(R)\, d)$
idempotent	$R ⨾ R = R$	

Theorem: If $R : B \leftrightarrow B$ is reflexive/irreflexive/symmetric/antisymmetric/asymmetric/transitive/idempotent, then $R^{\smile}$ has that property, too.

Proof: Reflexivity:

Id

$=$ ⟨ Symmetry of $\mathbb{I}$ ⟩

$\mathrm{Id}^{\smile}$

$\subseteq$ ⟨ Mon. $^{\smile}$ with Reflexivity of R ⟩

$R^{\smile}$

Transitivity:

$R^{\smile} ⨾ R^{\smile}$

$=$ ⟨ Converse of $⨾$ ⟩

$(R ⨾ R)^{\smile}$

$\subseteq$ ⟨ Mon. $^{\smile}$ with Transitivity of R ⟩

$R^{\smile}$

Reflexive and Transitive Implies Idempotent

reflexive	$\mathrm{Id} \subseteq R$	$(\forall\, b : B \bullet b \,(R)\, b)$
transitive	$R ⨾ R \subseteq R$	$(\forall b, c, d \bullet b \,(R)\, c \,(R)\, d \;\Rightarrow\; b \,(R)\, d)$
idempotent	$R ⨾ R = R$	

Theorem: If $R : B \leftrightarrow B$ is reflexive and transitive, then it is also idempotent.
Proof: By mutual inclusion and transitivity of R, we only need to show $R \subseteq R ⨾ R$:

R

$=$ ⟨ Identity of $⨾$ ⟩

$R ⨾ \mathrm{Id}$

$\subseteq$ ⟨ Mon. $⨾$ with Reflexivity of R ⟩

$R ⨾ R$

Symmetric and Transitive Implies Idempotent

symmetric	$R^{\smile}$	$=$	R	$(\forall\, b, c : B \bullet b \,(\!\|\, R \,\|\!)\, c \equiv c \,(\!\|\, R \,\|\!)\, b)$
transitive	$R \fatsemi R$	$\subseteq$	R	$(\forall b, c, d \bullet b \,(\!\|\, R \,\|\!)\, c \,(\!\|\, R \,\|\!)\, d \Rightarrow b \,(\!\|\, R \,\|\!)\, d)$
idempotent	$R \fatsemi R$	$=$	R	

Theorem: A symmetric and transitive $R : B \leftrightarrow B$ is also idempotent.

Proof: By mutual inclusion and transitivity of R, we only need to show $R \subseteq R \fatsemi R$:

$$
\begin{array}{ll}
 & R \\
= & \langle \text{ Idempotence of } \cap\text{, Identity of } \fatsemi \ \rangle \\
 & R \fatsemi \mathrm{Id} \ \cap \ R \\
\subseteq & \langle \text{ Modal rule } \quad Q \fatsemi R \cap S \quad \subseteq \quad Q \fatsemi (R \cap Q^{\smile} \fatsemi S) \ \rangle \\
 & R \fatsemi (\mathrm{Id} \ \cap \ R^{\smile} \fatsemi R) \\
\subseteq & \langle \text{ Mon. } \fatsemi \text{ with Weakening } X \cap Y \subseteq X \ \rangle \\
 & R \fatsemi R^{\smile} \fatsemi R \\
= & \langle \text{ Symmetry of } R \ \rangle \\
 & R \fatsemi R \fatsemi R \\
\subseteq & \langle \text{ Mon. } \fatsemi \text{ with Transitivity of } R \ \rangle \\
 & R \fatsemi R
\end{array}
$$