Discrete Mathematics with Applications I

COMPSCI&SFWRENG 2DM3

McMaster University, Fall 2019

Wolfram Kahl

2019-11-15

How can you simplify if you know $P_1 \Rightarrow P_2$?

$$\begin{array}{ll} & \vdots \\ \equiv & \langle \ldots \rangle \\ & \ldots \lor P_1 \lor P2 \lor \ldots \\ \equiv & \langle \quad ? \quad \rangle \\ & ? \end{array}$$

$$\begin{array}{ll} & \vdots \\ \equiv & \langle \ldots \rangle \\ & \ldots \land P_1 \land P2 \land \ldots \\ \equiv & \langle \quad ? \quad \rangle \\ & ? \end{array}$$

Plan for Today

- Relations
  - Properties of relations: Definitions via predicate logic and via relation algebra
  - First relation-algebraic proofs
- **Command Correctness**
  - While loops

Properties of Homogeneous Relations

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

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	$\mathsf{Id} \subseteq R$	$(\forall\, b : B \bullet b \llparenthesis R \rrparenthesis b)$
irreflexive	$\mathsf{Id} \cap R = \{\}$	$(\forall\, b : B \bullet \neg(b \llparenthesis R \rrparenthesis b))$
symmetric	$R^{\smile} = R$	$(\forall\, b, c : B \bullet b \llparenthesis R \rrparenthesis c \equiv c \llparenthesis R \rrparenthesis b)$
antisymmetric	$R \cap R^{\smile} \subseteq \mathsf{Id}$	$(\forall\, b, c \bullet b \llparenthesis R \rrparenthesis c \wedge c \llparenthesis R \rrparenthesis b \Rightarrow b = c)$
asymmetric	$R \cap R^{\smile} = \{\}$	$(\forall\, b, c : B \bullet b \llparenthesis R \rrparenthesis c \Rightarrow \neg(c \llparenthesis R \rrparenthesis b))$
transitive	$R \fatsemi R \subseteq R$	$(\forall b, c, d \bullet b \llparenthesis R \rrparenthesis c \llparenthesis R \rrparenthesis d \Rightarrow b \llparenthesis R \rrparenthesis d)$
idempotent	$R \fatsemi R = R$	

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

Proof: Reflexivity:

$$
\begin{aligned}
& \mathsf{Id} \\
= \;& \langle \text{Symmetry of } \mathbb{I} \rangle \\
& \mathsf{Id}^{\smile} \\
\subseteq \;& \langle \text{Mon. } {}^{\smile} \text{ with Reflexivity of } R \rangle \\
& R^{\smile}
\end{aligned}
$$

Transitivity:

$$
\begin{aligned}
& R^{\smile} \fatsemi R^{\smile} \\
= \;& \langle \text{Converse of } \fatsemi \rangle \\
& (R \fatsemi R)^{\smile} \\
\subseteq \;& \langle \text{Mon. } {}^{\smile} \text{ with Transitivity of } R \rangle \\
& R^{\smile}
\end{aligned}
$$

Reflexive and Transitive Implies Idempotent

reflexive	$\mathsf{Id} \subseteq R$	$(\forall\, b : B \bullet b \llparenthesis R \rrparenthesis b)$
transitive	$R \fatsemi R \subseteq R$	$(\forall b, c, d \bullet b \llparenthesis R \rrparenthesis c \llparenthesis R \rrparenthesis d \Rightarrow b \llparenthesis R \rrparenthesis d)$
idempotent	$R \fatsemi R = R$	

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 $R \subseteq R \fatsemi R$:

$$
\begin{aligned}
& R \\
= \;& \langle \text{Identity of } \fatsemi \rangle \\
& R \fatsemi \mathsf{Id} \\
\subseteq \;& \langle \text{Mon. } \fatsemi \text{ with Reflexivity of } R \rangle \\
& R \fatsemi R
\end{aligned}
$$

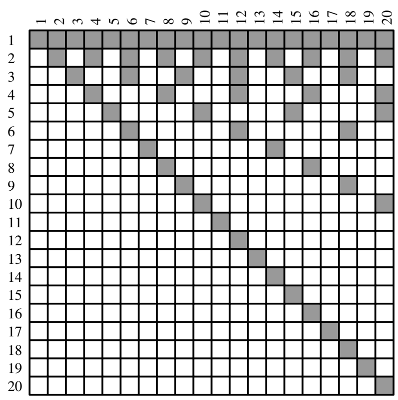
Symmetric and Transitive Implies Idempotent

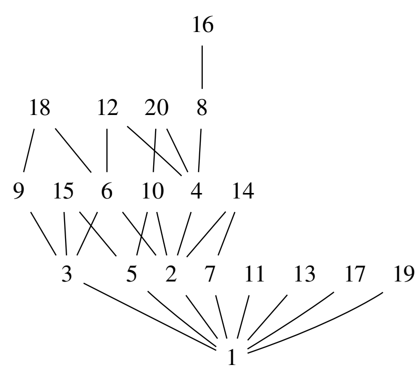
symmetric	$R^\smile$	$=$	R	$(\forall\, b, c : B \bullet b ⦗R⦘ c \equiv c ⦗R⦘ b)$
transitive	$R ⨾ R$	$\subseteq$	R	$(\forall b, c, d \bullet b ⦗R⦘ c ⦗R⦘ d \Rightarrow b ⦗R⦘ d)$
idempotent	$R ⨾ R$	$=$	R	

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

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

Divisibility Order with Hasse Diagram

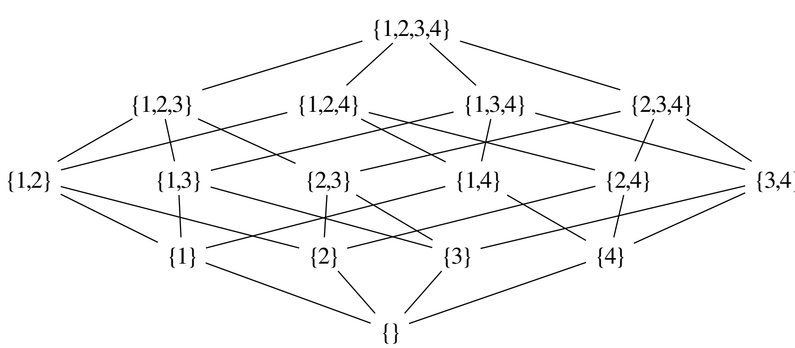




Hasse diagram for an **order**:

- Edge direction is **upwards**
- Loops not drawn
- Transitive edges not drawn

Inclusion Order on Powerset of $\{1, 2, 3, 4\}$



Hasse diagram for an **order**:

- Edge direction is **upwards**
- Loops not drawn
- Transitive edges not drawn

Properties of Heterogeneous Relations

A relation $R : B \leftrightarrow C$ is called:

univalent determinate	$R^{\smile} \mathbin{;} R \;\subseteq\; \mathrm{Id}$	$\forall\, b, c_1, c_2 \bullet b \llparenthesis R \rrparenthesis c_1 \wedge b \llparenthesis R \rrparenthesis c_2 \Rightarrow c_1 = c_2$
total	$\mathit{Dom}\ R \;=\; B$ $\mathrm{Id} \;\subseteq\; R \mathbin{;} R^{\smile}$	$\forall\, b : B \bullet (\exists\, c : C \bullet b \llparenthesis R \rrparenthesis c)$
injective	$R \mathbin{;} R^{\smile} \;\subseteq\; \mathrm{Id}$	$\forall\, b_1, b_2, c \bullet b_1 \llparenthesis R \rrparenthesis c \wedge b_2 \llparenthesis R \rrparenthesis c \Rightarrow b_1 = b_2$
surjective	$\mathit{Ran}\ R \;=\; C$ $\mathrm{Id} \;\subseteq\; R^{\smile} \mathbin{;} R$	$\forall\, c : C \bullet (\exists\, b : B \bullet b \llparenthesis R \rrparenthesis c)$
a **mapping**	iff it is univalent and total	
bijective	iff it is injective and surjective	

Univalent relations are also called **(partial) functions**.

Mappings are also called **total functions**.

Exercise

If $F : A \leftrightarrow B$ is univalent, then $F \mathbin{;} (R \cap S) = (F \mathbin{;} R) \cap (F \mathbin{;} S)$

Hint: Assume determinacy; then show the equation using **relation extensionality** (11.4r), and start from the RHS $\langle b, d \rangle \in (F \mathbin{;} R) \cap (F \mathbin{;} S)$. In the expansions of the two relation compositions here, introduce different bound variables.

Let us assume that $F : B \leftrightarrow C$ and $R, S : C \leftrightarrow D$.

Proving (14.24) $F \mathbin{;} (R \cap S) = (F \mathbin{;} R) \cap (F \mathbin{;} S)$:

$$\begin{array}{ll}
 & \langle b, d \rangle \in (F \mathbin{;} R) \cap (F \mathbin{;} S) \\
= & \langle \text{ (11.21) Intersection } \rangle \\
 & \langle b, d \rangle \in F \mathbin{;} R \wedge \langle b, d \rangle \in F \mathbin{;} S \\
= & \langle \text{ (14.20) Relation composition } \rangle \\
 & (\exists c_1 : C \bullet \langle b, c_1 \rangle \in F \wedge \langle c_1, d \rangle \in R) \wedge (\exists c_2 : C \bullet \langle b, c_2 \rangle \in F \wedge \langle c_2, d \rangle \in S) \\
= & \langle \text{ (9.21) Distributivity of } \wedge \text{ over } \exists \rangle \\
 & (\exists c_1 : C \bullet \langle b, c_1 \rangle \in F \wedge \langle c_1, d \rangle \in R \wedge (\exists c_2 : C \bullet \langle b, c_2 \rangle \in F \wedge \langle c_2, d \rangle \in S)) \\
= & \langle \text{ (9.21) Distributivity of } \wedge \text{ over } \exists \rangle \\
 & (\exists c_1 : C \bullet (\exists c_2 : C \bullet \langle b, c_1 \rangle \in F \wedge \langle c_1, d \rangle \in R \wedge \langle b, c_2 \rangle \in F \wedge \langle c_2, d \rangle \in S)) \\
= & \langle \text{ Assumption } (\forall b, c_1, c_2 \bullet b \llparenthesis F \rrparenthesis c_1 \wedge b \llparenthesis F \rrparenthesis c_2 \Rightarrow c_1 = c_2) \text{, with (9.13) Inst. } \rangle \\
 & (\exists c_1 : C \bullet (\exists c_2 : C \bullet c_1 = c_2 \wedge \langle b, c_1 \rangle \in F \wedge \langle c_1, d \rangle \in R \wedge \langle b, c_2 \rangle \in F \wedge \langle c_2, d \rangle \in S)) \\
= & \langle \text{ (9.19) Trading for } \exists \text{, (1.3) Symmetry of } = \rangle \\
 & (\exists c_1 : C \bullet (\exists c_2 : C \mid c_2 = c_1 \bullet \langle b, c_1 \rangle \in F \wedge \langle c_1, d \rangle \in R \wedge \langle b, c_2 \rangle \in F \wedge \langle c_2, d \rangle \in S)) \\
= & \langle \text{ (8.14) One-point rule } \rangle \\
 & (\exists c_1 : C \bullet \langle b, c_1 \rangle \in F \wedge \langle c_1, d \rangle \in R \wedge \langle b, c_1 \rangle \in F \wedge \langle c_1, d \rangle \in S) \\
= & \langle \text{ (8.21) Dummy renaming } \rangle \\
 & (\exists c : C \bullet \langle b, c \rangle \in F \wedge \langle c, d \rangle \in R \wedge \langle b, c \rangle \in F \wedge \langle c, d \rangle \in S) \\
= & \langle \text{ (3.38) Idempotency of } \wedge \rangle \\
 & (\exists c : C \bullet \langle b, c \rangle \in F \wedge \langle c, d \rangle \in R \wedge \langle c, d \rangle \in S) \\
= & \langle \text{ (11.21) Intersection } \rangle \\
 & (\exists c : C \bullet \langle b, c \rangle \in F \wedge \langle c, d \rangle \in (R \cap S)) \\
= & \langle \text{ (14.20) Relation composition } \rangle \\
 & \langle b, d \rangle \in (F \mathbin{;} (R \cap S))
\end{array}$$

The Same Exercise — Relation-Algebraically

If $F : A \leftrightarrow B$ is univalent, then $F \mathbin{;} (R \cap S) = (F \mathbin{;} R) \cap (F \mathbin{;} S)$

Proof: From sub-distributivity we have $\subseteq$; because of antisymmetry of $\subseteq$ (11.57) we only need to show $\supseteq$:

Assume that F is univalent, that is, $F^{\smile} \mathbin{;} F \subseteq \mathrm{Id}$

$$\begin{array}{ll}
 & (F \mathbin{;} R) \cap (F \mathbin{;} S) \\
\subseteq & \langle \text{ Modal rule } \rangle \\
 & F \mathbin{;} (R \cap (F^{\smile} \mathbin{;} F \mathbin{;} S)) \\
\subseteq & \langle \text{ Assumption } F^{\smile} \mathbin{;} F \subseteq \mathrm{Id} \rangle \\
 & F \mathbin{;} (R \cap (\mathrm{Id} \mathbin{;} S)) \\
= & \langle \text{ Right-identity of } \mathbin{;} \rangle \\
 & F \mathbin{;} (R \cap S)
\end{array}$$

Partial Correctness for Pre-Postcondition Specs in Dynamic Logic Notation

- Program correctness statement in LADM (and much current use):

$$\{ P \}\ C\ \{ Q \}$$

  This is called a "Hoare triple".
- **Partial Correctness Meaning:** If command C is started in a state in which the **precondition** P holds
  then it will terminate **only in states** in which the **postcondition** Q holds.
- **Dynamic logic** notation (used in CalcCheck):

$$P \Rightarrow\!\![\ C\ ]\ Q$$

- **Assignment Axiom:** $\{ Q[x := E] \}\ x := E\ \{ Q \}$ $\qquad Q[x := E] \Rightarrow\!\![\ x := E\ ]\ Q$
- **Sequential composition:**

```
Primitive inference rule “Sequence”:
    `P  ⇒[ C1 ]  Q`,   `Q  ⇒[ C2 ]  R`
 ⊢─────────────────────────────────────
      `P  ⇒[ C1 ; C2 ]  R`
```

Transitivity Rules for Calculational Command Correctness Reasoning

```
Primitive inference rule “Sequence”:
    `P  ⇒[ C1 ]  Q`,   `Q  ⇒[ C2 ]  R`
 ⊢─────────────────────────────────────
      `P  ⇒[ C1 ; C2 ]  R`
```

Strengthening the precondition:

```
    `P1 ⇒ P2`,   `P2 ⇒[ C ] Q`
 ⊢──────────────────────────────
        `P1 ⇒[ C ] Q`
```

Weakening the postcondition:

```
    `P ⇒[ C ] Q1`,    `Q1 ⇒ Q2`
 ⊢──────────────────────────────
        `P ⇒[ C ] Q2`
```

$$\begin{array}{ll} & P \\ \Rightarrow\!\![\ C_1\ ] & \langle\ \ldots\ \rangle \\ & Q \\ \Rightarrow & \langle\ \ldots\ \rangle \\ & Q' \\ \Rightarrow\!\![\ C_2\ ] & \langle\ \ldots\ \rangle \\ & R \end{array}$$

- Activated as transitivity rules
- Therefore used implicitly in calculations, e.g.,
  proving $P \Rightarrow\!\![\ C_1 ⨟ C_2\ ]\ R$ to the right
- No need to refer to these rules explicitly.

Using converse operator for backward presentation:

$$\_[\_] \Leftarrow \_$$

Fact: x = 5 ⇒[(y := x + 1 ⨟ x := y + y)] x = 12
Proof:

    x = 12
[x := y + y]⇐ ⟨ "Assignment" with Substitution ⟩
    y + y = 12
≡ ⟨ "Identity of ·" ⟩
    1 · y + 1 · y = 12
≡ ⟨ "Distributivity of · over +" ⟩
    (1 + 1) · y = 12
≡ ⟨ Evaluation ⟩
    2 · y = 2 · 6
≡ ⟨ "Cancellation of ·" with Fact `2 ≠ 0` ⟩
    y = 6
[y := x + 1]⇐ ⟨ "Assignment" with Substitution ⟩
    x + 1 = 6
≡ ⟨ Fact `5 + 1 = 6` ⟩
    x + 1 = 5 + 1
≡ ⟨ "Cancellation of +" ⟩
    x = 5

Conditional Rule

Primitive inference rule "Conditional":

$$\vdash \frac{`B \wedge P \Rightarrow [\ C_1\ ]\ Q`, \quad `\neg\ B \wedge P \Rightarrow [\ C_2\ ]\ Q`}{`P \Rightarrow [\ \texttt{if}\ B\ \texttt{then}\ C_1\ \texttt{else}\ C_2\ ]\ Q`}$$

"While" Rule

$$\vdash \frac{`B \wedge Q \ \Rightarrow [\ C\ ]\ \ Q`}{`Q \ \Rightarrow [\ \texttt{while}\ B\ \texttt{do}\ C\ \texttt{od}\ ]\ \ \neg\ B \wedge Q`}$$