Discrete Mathematics with Applications I

COMPSCI&SFWRENG 2DM3

McMaster University, Fall 2019

Wolfram Kahl

2019-11-12

Anything Wrong?

```
Theorem:   (∃ y : ℤ • ∀ x : ℤ • x + 2 · y = 5 · x + 6)
Proof:
    (∃ y : ℤ • ∀ x : ℤ • x + 2 · y = 5 · x + 6)
  ⇒⟨ “Interchange of quantifications” ⟩
    (∀ x : ℤ • ∃ y : ℤ • x + 2 · y = 5 · x + 6)
  ≡⟨ Subproof for `(∀ x : ℤ • ∃ y : ℤ • x + 2 · y = 5 · x + 6)`:
    For any `x : ℤ`:
        ∃ y : ℤ • x + 2 · y = 5 · x + 6
      ⇐⟨ “Consequence”, “∃-Introduction” ⟩
        (x + 2 · y = 5 · x + 6)[y ≔ 2 · x + 3]
      ≡⟨ Substitution ⟩
        x + 2 · (2 · x + 3) = 5 · x + 6
      ≡⟨“Distributivity of · over +” ⟩
        x + 2 · 2 · x + 2 · 3 = 5 · x + 6
      ≡⟨ Evaluation, “Identity of ·” ⟩
        1 · x + 4 · x + 6 = 5 · x + 6
      ≡⟨ “Distributivity of · over +”, Evaluation ⟩
        5· x + 6 = 5 · x + 6
      ≡⟨“Reflexivity of =” ⟩
        true
  ⟩
    (∀ x : ℤ • true) — This is “True ∀ body”
```

Experimental New Key-Strokes

— US keyboard only! Firefox only?

- `Alt-=` for ≡
- `Alt-<` for ⟨
- `Alt->` for ⟩
- `Alt-(` for ⦇
- `Alt-)` for ⦈

Plan for Today: Relations

- Operations are easily defined and understood via set theory
- These operations satisfy many algebraic properties
- **Formalisation using relation-algebraic operations needs no quantifiers**
- **Similar to** how matrix operations do away with quantifications and indexed variables a_{ij} in **linear algebra**
- Like linear algebra, **relation algebra**
  - raises the level of abstraction
  - makes reasoning easier by reducing necessity for quantification
- This week: Lots of quantification, while **proving properties via set theory**.
- Starting next week: **Abstract Relation Algebra**
  (avoiding any mention of and quantification over elements)

Binary Relations, Relationship

Consider $R : B \leftrightarrow C$ and $x : B$ and $y : C$.

$$
\begin{array}{ll}
 & R \;:\; B \leftrightarrow C \\
\textit{iff} & \langle \text{ Def. } \leftrightarrow \rangle \\
 & R \;:\; \textbf{set}\, \langle\!\langle B, C \rangle\!\rangle \\
\textit{iff} & \langle \textbf{ set } \text{ to } \llcorner\lrcorner \rangle \\
 & R \subseteq \llcorner \langle\!\langle B, C \rangle\!\rangle \lrcorner \\
\textit{iff} & \langle \text{ Def. } \textbf{set}\text{, Def. } \times\text{, Def. } \llcorner\lrcorner \; \rangle \\
 & R \subseteq \llcorner B \lrcorner \times \llcorner C \lrcorner
\end{array}
$$

Note that for a type A, the universal set

$$\mathbf{U} : \textbf{set}\, A$$

is the set of all members of A.

Or, $(\mathbf{U} : \textbf{set}\, A)$ is "type A as a set".

We **abbreviate**: $\llcorner A \lrcorner := (\mathbf{U} : \textbf{set}\, A)$, and have:

$$S : \textbf{set}\, A \quad \text{iff} \quad S \subseteq \llcorner A \lrcorner$$

"x is in relation R with y"

- explicit membership notation: $\langle x, y \rangle \in R$
- ambiguous traditional infix notation: $x\,R\,y$
- CalcCheck: $x \,(\!\!\{ R \}\!\!)\, y \quad \equiv \quad \langle x, y \rangle \in R$

The Axioms of Set Theory — Applied to Binary Relations

(11.4r) **Relation Extensionality:**

$$R = S \quad \equiv \quad (\forall x, y \bullet x \,(\!\!\{ R \}\!\!)\, y \equiv x \,(\!\!\{ S \}\!\!)\, y)$$

(11.13r) **Relation Inclusion:**

$$R \subseteq S \quad \equiv \quad (\forall x, y \bullet x \,(\!\!\{ R \}\!\!)\, y \Rightarrow x \,(\!\!\{ S \}\!\!)\, y)$$
$$R \subseteq S \quad \equiv \quad (\forall x, y \mid x \,(\!\!\{ R \}\!\!)\, y \bullet x \,(\!\!\{ S \}\!\!)\, y)$$

(11.20r) **Relation Union:**

$$\langle u, v \rangle \in (S \cup T) \quad \equiv \quad \langle u, v \rangle \in S \vee \langle u, v \rangle \in T$$
$$u \,(\!\!\{ S \cup T \}\!\!)\, v \quad \equiv \quad u \,(\!\!\{ S \}\!\!)\, v \vee u \,(\!\!\{ T \}\!\!)\, v$$

(11.21r) **Relation Intersection:**

$$u \,(\!\!\{ S \cap T \}\!\!)\, v \quad \equiv \quad u \,(\!\!\{ S \}\!\!)\, v \wedge u \,(\!\!\{ T \}\!\!)\, v$$

(11.22r) **Relation Difference:**

$$u \,(\!\!\{ S - T \}\!\!)\, v \quad \equiv \quad u \,(\!\!\{ S \}\!\!)\, v \wedge \neg(u \,(\!\!\{ T \}\!\!)\, v)$$

Simple Binary Relations

- The **empty relation** on $\langle t_1, t_2 \rangle$ is $\{\} : t_1 \leftrightarrow t_2$
$$x \llparenthesis \{\} \rrparenthesis y \equiv \mathit{false}$$
$$\langle x, y \rangle \in \{\} \equiv \mathit{false}$$
- The **(sub-)identity relation** on $B : \mathbf{set}\ t$ is $\mathbb{I}\, B : t \leftrightarrow t$:
$$\mathbb{I}\, B = \{x : t \mid x \in B \bullet \langle x, x \rangle\}:$$
$$x \llparenthesis \mathbb{I}\, B \rrparenthesis y \equiv x = y \in B$$
$$\langle x, y \rangle \in \mathbb{I}\, B \equiv x = y \wedge y \in B$$
- The **universal relation** on $B \times C$ is $B \times C$
$$x \llparenthesis B \times C \rrparenthesis y \equiv x \in B \wedge y \in C$$
(14.4)
$$\langle x, y \rangle \in B \times C \equiv x \in B \wedge y \in C$$
- The **complement** of relation $R : t_1 \leftrightarrow t_2$ is $\sim R : t_1 \leftrightarrow t_2$:
$$x \llparenthesis \sim R \rrparenthesis y \equiv \neg(x \llparenthesis R \rrparenthesis y)$$

Domain and Range of Binary Relations

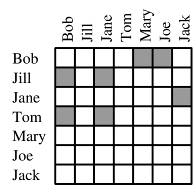
For $R : t_1 \leftrightarrow t_2$, we define:

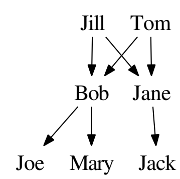
(14.16) $\mathit{Dom}\ R = \{x : t_1 \mid (\exists y : t_2 \bullet x \llparenthesis R \rrparenthesis y)\} = \{p \mid p \in R \bullet \mathsf{fst}\ p\}$

(14.17) $\mathit{Ran}\ R = \{y : t_2 \mid (\exists x : t_1 \bullet x \llparenthesis R \rrparenthesis y)\} = \{p \mid p \in R \bullet \mathsf{snd}\ p\}$

"Membership in `*Dom*`":
$$x \in \mathit{Dom}\ R \equiv (\exists\, y : t_2 \bullet x \llparenthesis R \rrparenthesis y)$$

"Membership in `*Ran*`":
$$y \in \mathit{Ran}\ R \equiv (\exists\, x : t_1 \bullet x \llparenthesis R \rrparenthesis y)$$





$$\mathit{Dom}\ \mathit{parentOf} = \{\mathit{Bob}, \mathit{Jane}, \mathit{Jill}, \mathit{Tom}\}$$
$$\mathit{Ran}\ \mathit{parentOf} = \{\mathit{Bob}, \mathit{Jack}, \mathit{Jane}, \mathit{Joe}, \mathit{Mary}\}$$

Formalise Without Quantifiers!

$$P := \text{type of persons}$$
$$C : P \leftrightarrow P$$
$$p \llparenthesis C \rrparenthesis q :\equiv p \text{ called } q$$

Remember: For $R : t_1 \leftrightarrow t_2$:

"Membership in `*Dom*`":
$$x \in \mathit{Dom}\ R \equiv (\exists\, y : t_2 \bullet x \llparenthesis R \rrparenthesis y)$$

"Membership in `*Ran*`":
$$y \in \mathit{Ran}\ R \equiv (\exists\, x : t_1 \bullet x \llparenthesis R \rrparenthesis y)$$

1. Helen called somebody.

   $\mathit{Helen} \in \mathit{Dom}\ C$

2. For everybody, there is somebody they haven't called.

   $\mathit{Dom}\ (\sim C) = \llcorner P \lrcorner$

   $\mathit{Dom}\ (\sim C) = \mathbf{U}$

Operations on Relations

- Set operations $\cup$, $\cap$, $-$ are all available.
- If $R : B \leftrightarrow C$,
  then its **converse** $R^{\smile} : C \leftrightarrow B$
  (in the textbook called "inverse" and written: R^{-1})
  stands for "going R backwards".
- If $R : B \leftrightarrow C$ and $S : C \leftrightarrow D$,
  then their **composition** $R \mathbin{;} S$
  (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".

The resulting **relation algebra**

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

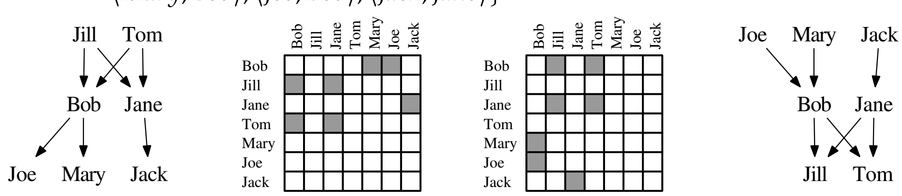
Operations on Relations: Converse

If $R : B \leftrightarrow C$, then its **converse** $R^{\smile} : C \leftrightarrow B$ is defined by:

(14.18) $\quad \langle c, b \rangle \in R^{\smile} \quad \equiv \quad \langle b, c \rangle \in R \qquad$ (for $b : B$ and $c : C$)

$$\begin{aligned} parentOf = \; & \{\langle Jill, Bob \rangle, \langle Jill, Jane \rangle, \langle Tom, Bob \rangle, \langle Tom, Jane \rangle, \\ & \langle Bob, Mary \rangle, \langle Bob, Joe \rangle, \langle Jane, Jack \rangle\} \end{aligned}$$

$$\begin{aligned} childOf \; & = \; parentOf^{\smile} \\ & = \; \{\langle Bob, Jill \rangle, \langle Jane, Jill \rangle, \langle Bob, Tom \rangle, \langle Jane, Tom \rangle, \\ & \quad\; \langle Mary, Bob \rangle, \langle Joe, Bob \rangle, \langle Jack, Jane \rangle\} \end{aligned}$$



Note: Converse corresponds to **matrix transpose**, and **not** to inverse matrix!

Properties of Converse $\quad B \xrightarrow{R} C$

If $R : B \leftrightarrow C$, then its **converse** $R^{\smile} : C \leftrightarrow B$ is defined by:

(14.18) $\quad \langle c, b \rangle \in R^{\smile} \quad \equiv \quad \langle b, c \rangle \in R \qquad$ (for $b : B$ and $c : C$)

(14.18) $\quad c \,(\!|\, R^{\smile} \,|\!)\, b \quad \equiv \quad b \,(\!|\, R \,|\!)\, c \qquad$ (for $b : B$ and $c : C$)

(14.19) **Properties of Converse:** Let $R, S : B \leftrightarrow C$ be relations.

(a) $Dom\ (R^{\smile}) = Ran\ R$

(b) $Ran\ (R^{\smile}) = Dom\ R$

(c) If $R \in B \leftrightarrow C$, then $R^{\smile} \in C \leftrightarrow B$

(d) $(R^{\smile})^{\smile} = R$

(e) $R \subseteq S \quad \equiv \quad R^{\smile} \subseteq S^{\smile}$

Proving Self-inverse of Converse: $(R^{\smile})^{\smile} = R$

$$
\begin{array}{ll}
 & (R^{\smile})^{\smile} = R \\
\equiv & \langle \text{ Relation extensionality } \rangle \\
 & \forall\, x, y \bullet x \llparenthesis (R^{\smile})^{\smile} \rrparenthesis y \equiv x \llparenthesis R \rrparenthesis y \\
\equiv & \langle \ldots \rangle \\
 & \mathit{true}
\end{array}
$$

Using "Relation extensionality":

Subproof for `$\forall\, x, y \bullet x \llparenthesis (R^{\smile})^{\smile} \rrparenthesis y \quad \equiv \quad x \llparenthesis R \rrparenthesis y$`:

For any x, y:

$$
\begin{array}{ll}
 & x \llparenthesis (R^{\smile})^{\smile} \rrparenthesis y \\
\equiv & \langle \text{ Converse } \rangle \\
 & y \llparenthesis R^{\smile} \rrparenthesis x \\
\equiv & \langle \text{ Converse } \rangle \\
 & x \llparenthesis R \rrparenthesis y
\end{array}
$$

Proving Monotonicity of Converse

Proving $R \subseteq S \quad \equiv \quad R^{\smile} \subseteq S^{\smile}$**:**

$$
\begin{array}{ll}
 & R^{\smile} \subseteq S^{\smile} \\
\equiv & \langle \text{ Relation inclusion } \rangle \\
 & \forall\, y, x \mid y \llparenthesis R^{\smile} \rrparenthesis x \bullet y \llparenthesis S^{\smile} \rrparenthesis x \\
\equiv & \langle \text{ Converse, dummy permutation } \rangle \\
 & \forall\, x, y \mid x \llparenthesis R \rrparenthesis y \bullet x \llparenthesis S \rrparenthesis y \\
\equiv & \langle \text{ Relation inclusion } \rangle \\
 & R \subseteq S
\end{array}
$$

Operations on Relations: Composition $\quad B \xrightarrow{R} C \xrightarrow{S} D$

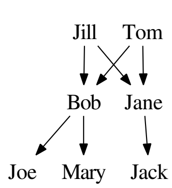
If $R : B \leftrightarrow C$ and $S : C \leftrightarrow D$, then their **composition** $R \fatsemi S : B \leftrightarrow D$ is defined by:

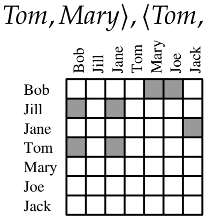
(14.20) $\quad b \llparenthesis R \fatsemi S \rrparenthesis d \;\equiv\; (\exists c : C \bullet b \llparenthesis R \rrparenthesis c \llparenthesis S \rrparenthesis d) \qquad$ (for $b : B, d : D$)

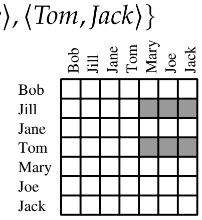
(14.20) $\quad b \llparenthesis R \fatsemi S \rrparenthesis d \;\equiv\; (\exists c : C \bullet b \llparenthesis R \rrparenthesis c \wedge c \llparenthesis S \rrparenthesis d) \qquad$ (for $b : B, d : D$)

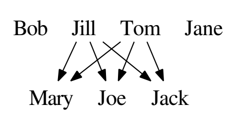
$$
\begin{array}{lll}
\mathit{parentOf} = & \{\langle \mathit{Jill}, \mathit{Bob}\rangle, \langle \mathit{Jill}, \mathit{Jane}\rangle, \langle \mathit{Tom}, \mathit{Bob}\rangle, \langle \mathit{Tom}, \mathit{Jane}\rangle, \\
 & \langle \mathit{Bob}, \mathit{Mary}\rangle, \langle \mathit{Bob}, \mathit{Joe}\rangle, \langle \mathit{Jane}, \mathit{Jack}\rangle\}
\end{array}
$$

$$
\begin{array}{lll}
\mathit{grandparentOf} & = & \mathit{parentOf} \fatsemi \mathit{parentOf} \\
 & = & \{\langle \mathit{Jill}, \mathit{Mary}\rangle, \langle \mathit{Jill}, \mathit{Joe}\rangle, \langle \mathit{Jill}, \mathit{Jack}\rangle \\
 & & \langle \mathit{Tom}, \mathit{Mary}\rangle, \langle \mathit{Tom}, \mathit{Joe}\rangle, \langle \mathit{Tom}, \mathit{Jack}\rangle\}
\end{array}
$$

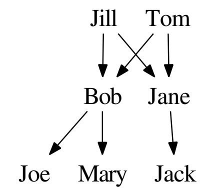






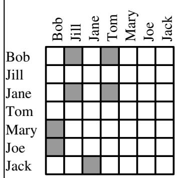


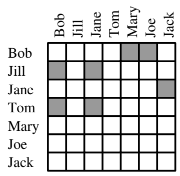
Combining Several Operations

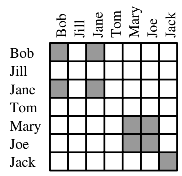


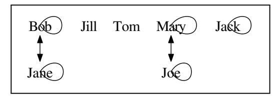
How to define siblings?

- First attempt: $childOf \fatsemi parentOf$

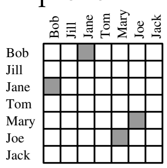


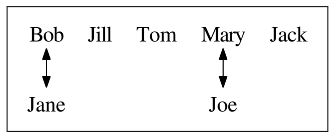


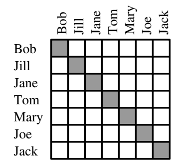




- Improved: $sibling = childOf \fatsemi parentOf - \mathbb{I}\,\llcorner Person \lrcorner$







$P \quad := \quad$ type of persons

$C \quad : \quad P \leftrightarrow P$ — "called"

$B \quad : \quad P \leftrightarrow P$ — "brother of"

$Aos : P$

$Jun : P$

Convert into English (via predicate logic):

$Aos \,(\!|\, C \,|\!)\, Jun$

$Aos \,(\!|\, C \fatsemi B \,|\!)\, Jun$

$Aos \,(\!|\, \sim (C \fatsemi \sim B) \,|\!)\, Jun$

$Aos \,(\!|\, \sim (\sim C \fatsemi B) \,|\!)\, Jun$

$Aos \,(\!|\, \sim ((C \cap \sim (B \fatsemi C^{\smile})) \fatsemi \sim B) \,|\!)\, Jun$

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

Formalise Without Quantifiers! (2)

$P \quad := \quad$ type of persons

$C \quad : \quad P \leftrightarrow P$

$p \,(\!|\, C \,|\!)\, q \quad :\equiv \quad p$ called q

1. Helen called somebody who called her.

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.

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.

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

Translating between Relation Algebra and Predicate Logic

$$
\begin{array}{rcl}
R = S & \equiv & (\forall\, x, y \bullet x ⦇ R ⦈ y \equiv x ⦇ S ⦈ y) \\
R \subseteq S & \equiv & (\forall\, x, y \bullet x ⦇ R ⦈ y \Rightarrow x ⦇ S ⦈ y) \\
u ⦇ \{\} ⦈ v & \equiv & \mathit{false} \\
(u : A) ⦇ A \times B ⦈ (v : B) & \equiv & \mathit{true} \\
u ⦇ {\sim} S ⦈ v & \equiv & \neg(u ⦇ S ⦈ v) \\
u ⦇ S \cup T ⦈ v & \equiv & u ⦇ S ⦈ v \vee u ⦇ T ⦈ v \\
u ⦇ S \cap T ⦈ v & \equiv & u ⦇ S ⦈ v \wedge u ⦇ T ⦈ v \\
u ⦇ S - T ⦈ v & \equiv & u ⦇ S ⦈ v \wedge \neg(u ⦇ T ⦈ v) \\
u ⦇ S \rightarrowtriangle T ⦈ v & \equiv & u ⦇ S ⦈ v \Rightarrow (u ⦇ T ⦈ v) \\
u ⦇ \mathbb{I}\, A ⦈ v & \equiv & u = v \in A \\
u ⦇ R^{\smile} ⦈ v & \equiv & v ⦇ R ⦈ u \\
u ⦇ R \,⨾\, S ⦈ v & \equiv & (\exists\, x \bullet u ⦇ R ⦈ x ⦇ S ⦈ v)
\end{array}
$$