Discrete Mathematics with Applications I

COMPSCI&SFWRENG 2DM3

McMaster University, Fall 2019

Wolfram Kahl

2019-11-22

Limitations of Conditional Rewriting Implementation of `with`$_2$

$\boxed{\textit{ThmA}\ \texttt{with}\ \textit{ThmB}\ \text{and}\ \textit{ThmB}_2\ \ldots}$

- 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 $\textit{ThmB}_2 \ldots$
  - Rewrite goal applying $L\sigma \mapsto R\sigma$ rigidly.
- E.g.: "Transitivity of $\subseteq$" with Assumptions \`$Q \cap S \subseteq Q$\` and \`$Q \subseteq R$\` when trying to prove \`$Q \cap S \subseteq R$\`
  - "Transitivity of $\subseteq$" is: $Q \subseteq R \Rightarrow R \subseteq S \Rightarrow Q \subseteq S$
  - For application, a **fresh renaming** is used: $q \subseteq r \Rightarrow r \subseteq s \Rightarrow q \subseteq s$
  - We try to use: $q \subseteq s \mapsto \textit{true}$, so L is: $q \subseteq s$
  - Matching L against goal produces $\sigma = [q, s := Q \cap S, R]$
  - $(q \subseteq r)\sigma$ is $(Q \cap R \subseteq r) \neq 0$ — **which cannot be proven** by "Assumption '$Q \cap S \subseteq Q$'"
  - $(r \subseteq s)\sigma$ is $r \subseteq R$ — **which cannot be proven** by "Assumption '$Q \subseteq R$'"
  - "Narrowing" or unification would be needed for such cases — **not yet implemented**
  - Adding an explicit substitution should help: "Transitivity of $\subseteq$" with \`$R := Q$\` and assumption \`$Q \cap S \subseteq Q$\` and assumption \`$Q \subseteq R$\`

Plan for Today

- **Properties of Heterogeneous Relations:** Univalence, injectivity, **inverse**, …
- **Graph Concepts via Relations, Closures**
- Some Ex10.1 proofs

Properties of Heterogeneous Relations

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

univalent determinate	$R^{\smile} \fatsemi R \quad \subseteq \quad \mathrm{Id}$	$\forall\, b, c_1, c_2 \bullet b \llparenthesis R \rrparenthesis c_1 \wedge b \llparenthesis R \rrparenthesis c_2 \Rightarrow c_1 = c_2$
total	$\mathit{Dom}\, R \quad = \quad \llcorner B \lrcorner$ $\mathrm{Id} \quad \subseteq \quad R \fatsemi R^{\smile}$	$\forall\, b : B \bullet (\exists\, c : C \bullet b \llparenthesis R \rrparenthesis c)$
injective	$R \fatsemi R^{\smile} \quad \subseteq \quad \mathrm{Id}$	$\forall\, b_1, b_2, c \bullet b_1 \llparenthesis R \rrparenthesis c \wedge b_2 \llparenthesis R \rrparenthesis c \Rightarrow b_1 = b_2$
surjective	$\mathit{Ran}\, R \quad = \quad \llcorner C \lrcorner$ $\mathrm{Id} \quad \subseteq \quad R^{\smile} \fatsemi R$	$\forall\, c : C \bullet (\exists\, b : B \bullet b \llparenthesis R \rrparenthesis c)$
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**.

Properties of Heterogeneous Relations — Examples 1

univalent	$R^{\smile} \fatsemi R \quad \subseteq \quad \mathrm{Id}$	$\forall\, b, c_1, c_2 \bullet b \llparenthesis R \rrparenthesis c_1 \wedge b \llparenthesis R \rrparenthesis c_2 \Rightarrow c_1 = c_2$
total	$\mathit{Dom}\, R \quad = \quad \llcorner B \lrcorner$ $\mathrm{Id} \quad \subseteq \quad R \fatsemi R^{\smile}$	$\forall\, b : B \bullet (\exists\, c : C \bullet b \llparenthesis R \rrparenthesis c)$
a **mapping**	iff it is univalent and total	

Properties of Heterogeneous Relations — Examples 2

injective	$R \fatsemi R^{\smile} \quad \subseteq \quad \mathbb{I}\, B$	$\forall\, b_1, b_2, c \bullet b_1 \llparenthesis R \rrparenthesis c \wedge b_2 \llparenthesis R \rrparenthesis c \Rightarrow b_1 = b_2$
surjective	$\mathit{Ran}\, R \quad = \quad C$ $\mathbb{I}\, C \quad \subseteq \quad R^{\smile} \fatsemi R$	$\forall\, c : C \bullet (\exists\, b : B \bullet b \llparenthesis R \rrparenthesis c)$
bijective	iff it is injective and surjective	

Recall: Composing Univalent Relations with Intersection

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, $F^{\smile} \mathbin{;} F \subseteq \mathrm{Id}$

$$
\begin{array}{ll}
 & (F \mathbin{;} R) \cap (F \mathbin{;} S) \\
\subseteq & \langle \text{ Modal rule } \rangle \\
 & F \mathbin{;} (R \cap (F^{\smile} \mathbin{;} F \mathbin{;} S)) \\
\subseteq & \left\langle \begin{array}{l} \text{“Mon. ;” w. “Mon. } \cap \text{” w. “Mon. ;” w.} \\ \text{Assumption ‘}F\text{ is univalent‘ with “Def. univalence”} \end{array} \right\rangle \\
 & F \mathbin{;} (R \cap (\mathrm{Id} \mathbin{;} S)) \\
= & \langle \text{ Right-identity of ; } \rangle \\
 & F \mathbin{;} (R \cap S)
\end{array}
$$

Exercises...

univalent determinate	$R^{\smile} \mathbin{;} R \subseteq \mathbb{I}\, C$	$\forall\, b, c_1, c_2 \bullet b \,(R)\, c_1 \wedge b \,(R)\, c_2 \Rightarrow c_1 = c_2$
total	$\mathit{Dom}\, R = B$ $\mathbb{I}\, B \subseteq R \mathbin{;} R^{\smile}$	$\forall\, b : B \bullet (\exists\, c : C \bullet b \,(R)\, c)$

- For $R : B \leftrightarrow C$, prove that the two formulations of univalence are equivalent.
- For $R : B \leftrightarrow C$, prove that the three formulations of totality are equivalent.
- Let $F, G : B \leftrightarrow C$ be two relations.

  Prove: If F is total, G is univalent, and $F \subseteq G$, then $G \subseteq F$.

  Hint: If you use quantifiers, you can, for any $b : B$, use instantiation for $\forall$ (9.13) on the predicate-logic definition of totality of F.

Properties of Heterogeneous Relations — Notes

univalent	$R^{\smile} \mathbin{;} R \subseteq \mathrm{Id}$	$\forall\, b, c_1, c_2 \bullet b \,(R)\, c_1 \wedge b \,(R)\, c_2 \Rightarrow c_1 = c_2$
surjective	$\mathrm{Id} \subseteq R^{\smile} \mathbin{;} R$	$\forall\, c : C \bullet (\exists\, b : B \bullet b \,(R)\, c)$
total	$\mathrm{Id} \subseteq R \mathbin{;} R^{\smile}$	$\forall\, b : B \bullet (\exists\, c : C \bullet b \,(R)\, c)$
injective	$R \mathbin{;} R^{\smile} \subseteq \mathrm{Id}$	$\forall\, b_1, b_2, c \bullet b_1 \,(R)\, c \wedge b_2 \,(R)\, c \Rightarrow b_1 = b_2$

All these properties are defined for arbitrary relations! (Not only for functions!)

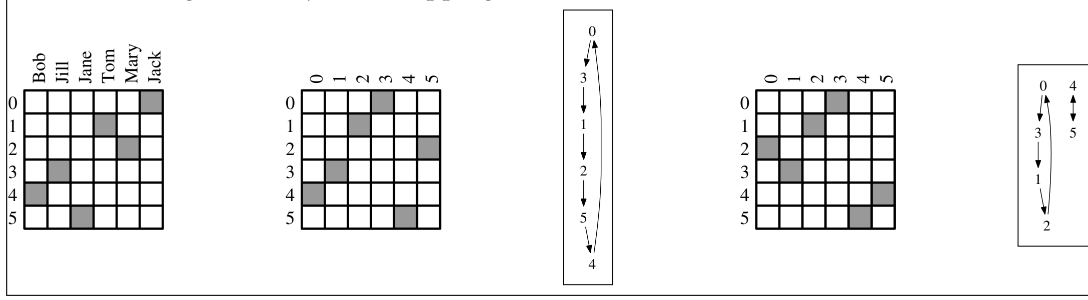
- R is univalent and surjective
  iff $R^{\smile} \mathbin{;} R = \mathit{Id}$
  iff $R^{\smile}$ is a left-inverse of R
- R is total and injective
  iff $R \mathbin{;} R^{\smile} = \mathit{Id}$
  iff $R^{\smile}$ is a right-inverse of R

Inverses of Total Functions

We write "$f : B \longrightarrow C$" for "$f \in B \leftrightarrow C$ and f is a mapping".

(14.43) **Definition:** Let $f : B \leftrightarrow C$ be a **mapping**.
An **inverse of** f is a mapping $g : C \leftrightarrow B$ such that $f \fatsemi g = \mathbb{I}\,\llcorner B \lrcorner$ and $g \fatsemi f = \mathbb{I}\,\llcorner C \lrcorner$.

- f has an inverse iff f is a bijective mapping.
- The inverse of a bijective mapping f is its converse $f^{\smile}$.
- A homogeneous bijective mapping is also called a **permutation**.



Inverses of Total Functions (ctd.)

(14.43) **Definition:** Let $f : B \leftrightarrow C$ be a **mapping**.
An **inverse of** f is a mapping $g : C \leftrightarrow B$ such that $f \fatsemi g = \mathbb{I}\,\llcorner B \lrcorner$ and $g \fatsemi f = \mathbb{I}\,\llcorner C \lrcorner$.

Theorem: If g is an inverse of $f : B \to C$, then $g = f^{\smile}$.
Proof: (Using antisymmetry of $\subseteq$)

$$
\begin{array}{ll}
 & f^{\smile} \\
= & \langle \text{ Identity of } \fatsemi \ \rangle \\
 & f^{\smile} \fatsemi \mathrm{Id} \\
= & \langle\ g \text{ is an inverse of } f\ \rangle \\
 & f^{\smile} \fatsemi f \fatsemi g \\
\subseteq & \langle\ f \text{ is univalent, that is, } f^{\smile} \fatsemi f \subseteq \mathrm{Id}\ \rangle \\
 & \mathrm{Id} \fatsemi g \\
= & \langle \text{ Identity of } \fatsemi \ \rangle \\
 & g \\
\subseteq & \langle \text{ Identity of } \fatsemi;\ \ f \text{ is total, that is, } \mathrm{Id} \subseteq f \fatsemi f^{\smile}\ \rangle \\
 & g \fatsemi f \fatsemi f^{\smile} \\
= & \langle\ g \text{ is an inverse of } f; \text{ Identity of } \fatsemi \ \rangle \\
 & f^{\smile}
\end{array}
$$

Inverses of Total Functions (ctd.)

(14.43) **Definition:** Let $f : B \leftrightarrow C$ be a **mapping**.
An **inverse of** f is a mapping $g : C \leftrightarrow B$ such that $f \fatsemi g = \mathbb{I}\,\llcorner B \lrcorner$ and $g \fatsemi f = \mathbb{I}\,\llcorner C \lrcorner$.

Theorem: A mapping $f : B \leftrightarrow C$ has an inverse iff f is bijective.

Proof: "$\Rightarrow$": If f has an inverse, then $f^{\smile}$ is that inverse;
therefore $f^{\smile}$ is univalent and total,
which means that f is injective and surjective.

"$\Leftarrow$": We know that f is total and injective,
that is, $f \fatsemi f^{\smile} = \mathbb{I}\,\llcorner B \lrcorner$ by antisymmetry of $\subseteq$.
We also know that f is univalent and surjective,
that is, $f^{\smile} \fatsemi f = \mathbb{I}\,\llcorner C \lrcorner$ by antisymmetry of $\subseteq$.

Therefore $f^{\smile}$ is an inverse of f.

Recall: (Graphs), Simple Graphs

A **graph** consists of:

- a set of "nodes" or "vertices"
- a set of "edges" or "arrows"
- "incidence" information specifying how edges connect nodes

— *more details another day.*

A **simple graph** consists of:

- a set of "nodes", and
- a set of "edges", which **are** pairs of nodes.

(A simple graph has no "parallel edges".)

Formally: A **simple graph** (N, E) is a pair consisting of

- a set N, the elements of which are called "nodes", and
- a relation $E \subseteq N \times N$, the element pairs of which are called "edges".

Recall: Simple Graphs: Example

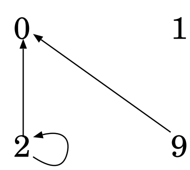
Formally: A **simple graph** (N, E) is a pair consisting of

- a set N, the elements of which are called "nodes", and
- a relation $E \subseteq N \times N$, the element pairs of which are called "edges".

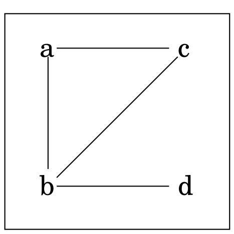
Example:

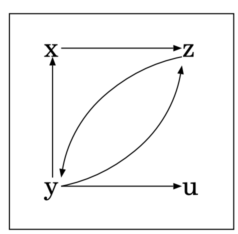
$$G_1 = (\{2, 0, 1, 9\}, \{\langle 2, 0\rangle, \langle 9, 0\rangle, \langle 2, 2\rangle\})$$

Graphs are normally visualised via **graph drawings**:



Directed versus Undirected Graphs





- Edges in undirected graphs can be considered as "unordered pairs" (two-element sets, or one-to-two-element sets)
- The **associated relation** of an undirected graph relates two nodes if there is an edge between them
- **The associated relation of an undirected graph is always symmetric**
- Relations directly represent simple graphs.
- Our **definition:** An **undirected graph** is a simple graph (V, E) where E is symmetric.

Symmetric Closure

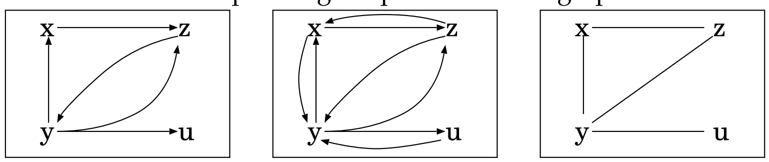
Relation $Q : B \leftrightarrow B$ is the **symmetric closure** of $R : B \leftrightarrow B$
iff Q is the smallest symmetric relation containing R,

or, equivalently, iff

- $R \subseteq Q$
- $Q = Q^{\smile}$
- $(\forall P : B \leftrightarrow B \mid R \subseteq P = P^{\smile} \bullet Q \subseteq P)$

Theorem: The symmetric closure of $R : B \leftrightarrow B$ is $R \cup R^{\smile}$.

Fact: If R represents a simple directed graph, then the symmetric closure of R is the associated relation of the corresponding simple undirected graph.



Reflexive Closure

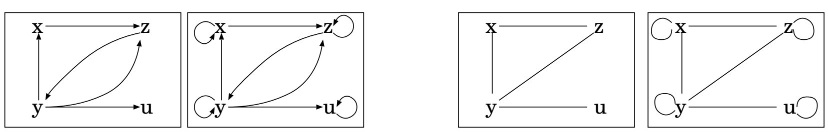
Relation $Q : B \leftrightarrow B$ is the **reflexive closure** of $R : B \leftrightarrow B$
iff Q is the smallest reflexive relation containing R,

or, equivalently, iff

- $R \subseteq Q$
- $\mathrm{Id} \subseteq Q$
- $(\forall P : B \leftrightarrow B \mid R \subseteq P \wedge \mathrm{Id} \subseteq P \bullet Q \subseteq P)$

Theorem: The reflexive closure of $R : B \leftrightarrow B$ is $R \cup \mathrm{Id}$.

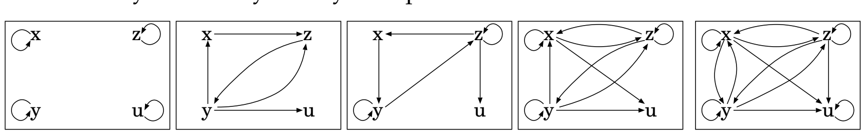
Fact: If R represents a graph, then the reflexive closure of R "ensures that each node has a loop edge".



Transitive and Reflexive Transitive Closure via Powers

Powers of a homogeneous relation $R : B \leftrightarrow B$:

- $R^0 = \mathrm{Id}$
- $R^1 = R$
- $R^{n+1} = R^n \mathbin{;} R$
- $R^2 = R \mathbin{;} R$
- $R^3 = R \mathbin{;} R \mathbin{;} R$
- $R^4 = R \mathbin{;} R \mathbin{;} R \mathbin{;} R$
- R^i is reachability via exactly i many R-steps



R^0 R^1 R^2 R^3 R^*

- $R^+ = (\cup\ i : \mathbb{N} \mid i > 0 \bullet R^i)$
- $R^+ = R \cup R^2 \cup R^3 \cup R^4 \cup \ldots$
- Transitive closure R^+ is reachability via at least one R-step

---

- $R^* = (\cup\ i : \mathbb{N} \bullet R^i)$
- $R^* = \mathrm{Id} \cup R \cup R^2 \cup R^3 \cup R^4 \cup \ldots$
- Reflexive transitive closure R^* is reachability via any number of R-steps

Transitive Closure

Relation $Q : B \leftrightarrow B$ is the **transitive closure** of $R : B \leftrightarrow B$
iff Q is the smallest transitive relation containing R,

or, equivalently, iff

- $R \subseteq Q$
- $Q \mathbin{;} Q \subseteq Q$
- $(\forall P : B \leftrightarrow B \mid R \subseteq P \land P \mathbin{;} P \subseteq P \bullet Q \subseteq P)$

Definition: The transitive closure of $R : B \leftrightarrow B$ is written R^+.

Theorem: $R^+ = (\bigcap P \mid R \subseteq P \land P \mathbin{;} P \subseteq P \bullet P)$.

Theorem: $R^+ = (\bigcup i : \mathbb{N} \mid i > 0 \bullet R^i)$

Powers of a homogeneous relation $R : B \leftrightarrow B$:

- $R^0 = \mathrm{Id}$
- $R^1 = R$
- $R^{n+1} = R^n \mathbin{;} R$

Reflexive Transitive Closure

$Q : B \leftrightarrow B$ is the **reflexive transitive closure** of $R : B \leftrightarrow B$
iff Q is the smallest reflexive transitive relation containing R,

or, equivalently, iff

- $R \subseteq Q$
- $\mathrm{Id} \subseteq Q \land Q \mathbin{;} Q \subseteq Q$
- $(\forall P : B \leftrightarrow B \mid R \subseteq P \land \mathrm{Id} \subseteq P \land P \mathbin{;} P \subseteq P \bullet Q \subseteq P)$

Definition: The reflexive transitive closure of R is written R^*.

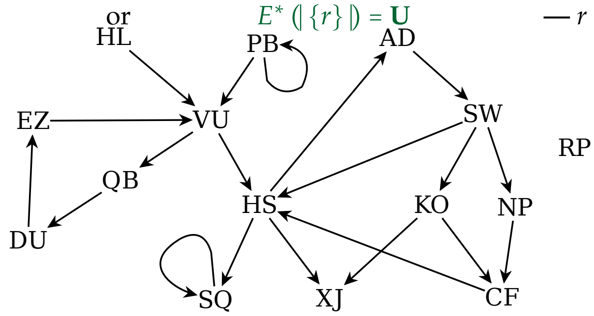
Theorem: $R^* = (\bigcap P \mid R \subseteq P \land \mathrm{Id} \subseteq P \land P \mathbin{;} P \subseteq P \bullet P)$.

Theorem: $R^* = (\bigcup i : \mathbb{N} \bullet R^i)$

- Transitive closure R^+ is reachability via at least one R-step
- Reflexive transitive closure R^* is reachability via any number of R-steps
- Variants of the **Warshall algorithm** calculate these closures in cubic time.

Reachability in graph $G = (V, E)$ — 1 (ctd.)

- No edge ends at node s
  $s \notin \mathit{Ran}\ E$ or $s \in {\sim}(\mathit{Ran}\ E)$ — s is called a **source** of G
- No edge starts at node s
  $s \notin \mathit{Dom}\ E$ or $s \in {\sim}(\mathit{Dom}\ E)$ — s is called a **sink** of G
- Node n_2 is reachable from node n_1 via a three-edge path
  $n_1\ (E^3)\ n_2$ or $n_1\ (E \mathbin{;} E \mathbin{;} E)\ n_2$
- Every node is reachable from node r
  $\{r\} \times \mathbf{U} \subseteq E^*$ or $E^* (\!|\, \{r\} \,|\!) = \mathbf{U}$ — r is called a **root** of G



Ex10.1

```
Theorem “Distributivity of ; over ∪”: Q ; (R ∪ S)  =  Q ; R  ∪  Q ; S
Proof:
  Using “Relation extensionality”:
    Subproof for `∀ a • ∀ c • a ❨ Q ; (R ∪ S) ❩ c ≡ a ❨ Q ; R  ∪  Q ; S ❩ c`:
      For any `a`, `c`:
          a ❨ Q ; (R ∪ S) ❩ c
        ≡⟨ “Relation composition” ⟩
          ∃ b • a ❨ Q ❩ b  ∧  b ❨ R ∪ S ❩ c
        ≡⟨ “Relation union”  ⟩
          ∃ b • a ❨ Q ❩ b  ∧  (b ❨ R ❩ c ∨ b ❨ S ❩ c)
        ≡⟨ “Distributivity of ∧ over ∨”, “Distributivity of ∃ over ∨” ⟩
          (∃ b • a ❨ Q ❩ b ∧ b ❨ R ❩ c)  ∨ (∃ b • a ❨ Q ❩ b ∧ b ❨ S ❩ c)
        ≡⟨ “Relation composition” ⟩
          a ❨ Q ; R ❩ c  ∨  a ❨ Q ; S ❩ c
        ≡⟨ “Relation union” ⟩
          a ❨ Q ; R  ∪  Q ; S ❩ c
```

Ex10.1

```
Theorem “Monotonicity of ;”: Q ⊆ R  ⇒  Q ; S ⊆ R ; S
Proof:
  Assuming `Q ⊆ R`:
    Using “Relation inclusion”:
      Subproof for `∀ a • ∀ c • a ❨ Q ; S ❩ c ⇒ a ❨ R ; S ❩ c`:
        For any `a`, `c`:
            a ❨ Q ; S ❩ c
          ≡⟨ “Relation composition” ⟩
            ∃ 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
          ≡⟨ “Relation composition” ⟩
            a ❨ R ; S ❩ c
```

Ex10.1

```
Theorem “Modal rule”:    (Q ; R) ∩ S ⊆ (Q ∩ S ; R ˘) ; R
Proof:
  Using “Relation inclusion”:
    Subproof for `∀ a • ∀ c • a ❨ (Q ; R) ∩ S ❩ c ⇒ a ❨ (Q ∩ S ; R ˘) ; R ❩ c`:
      For any `a`, `c`:
          a ❨ (Q ∩ S ; R ˘) ; R ❩ c
        ≡⟨ “Relation composition” ⟩
          ∃ b • a ❨ Q ∩ S ; R ˘ ❩ b ∧ b ❨ R ❩ c
        ≡⟨ “Relation intersection”, “Relation composition”, “Relation converse” ⟩
          ∃ b • a ❨ Q ❩ b ∧ (∃ c₂ • a ❨ S ❩ c₂ ∧ b ❨ R ❩ c₂) ∧ b ❨ R ❩ c
        ≡⟨ “Distributivity of ∧ over ∃” ⟩
          ∃ b • ∃ c₂ • a ❨ Q ❩ b ∧ a ❨ S ❩ c₂ ∧ b ❨ R ❩ c₂ ∧ b ❨ R ❩ c
        ⇐⟨ “Consequence”, “Body monotonicity of ∃” with “∃-Introduction” ⟩
          ∃ b • (a ❨ Q ❩ b ∧ a ❨ S ❩ c₂ ∧ b ❨ R ❩ c₂ ∧ b ❨ R ❩ c)[c₂ ≔ c]
        ≡⟨ Substitution, “Idempotency of ∧” ⟩
          ∃ b₂ • a ❨ Q ❩ b₂ ∧ b₂ ❨ R ❩ c ∧ a ❨ S ❩ c
        ≡⟨ “Distributivity of ∧ over ∃” ⟩
          (∃ b₂ • a ❨ Q ❩ b₂ ∧ b₂ ❨ R ❩ c) ∧ a ❨ S ❩ c
        ≡⟨ “Relation intersection”, “Relation composition” ⟩
          a ❨ (Q ; R) ∩ S ❩ c
```