DATA 61

New Models For Relation Algebra (by categorical construction)

Peter Höfner
(with input from B. Möller & W. Guttmann)

www.data61.csiro.au

CSIRO

(Concrete) Relation Algebra

- classical model is based on relation

$$(a,b)\ ;\ (c,d) = (a,d) \qquad \text{if } b = c$$
$$\text{undefined otherwise}$$

- point-wise lifting

$$R \mathbin{;} S = \{r\ ;\ s \mid r \in R, s \in S, r\ ;\ s \text{ defined}\}$$

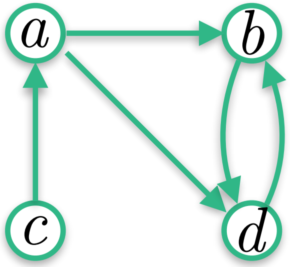
- converse

$$R^{\top} = \{(b,a) \mid (a,b) \in R\}$$

- $(2^{\Sigma\times\Sigma}, \cup, \{\,\}, \mathbin{;}, I, \overline{}, {}^{\top}, {}^{*})$ is (concrete) relation algebra

- **advantage**: pointfree algebraic reasoning
  mathematics of program construction

Models (Concrete) Relation Algebra



- (directed) Graphs
  - for example:

$$G = \{(a,b),(a,d),(b,d),(c,a),(d,b)\}$$

$$G \mathbin{;} G = \{(a,b),(a,d),(b,b),(c,b),(c,d),(d,d)\}$$

  - operators
    - $\mathbin{;}$ path composition
    - $\cup$ union
    - $*$ reachability
    - $\top$ converse

- many more models such as predicate transformers exist

Useful Properties

- Basic Properties

$$R \mathbin{;} (S \cup T) = (R \mathbin{;} S) \cup (R \mathbin{;} T)$$

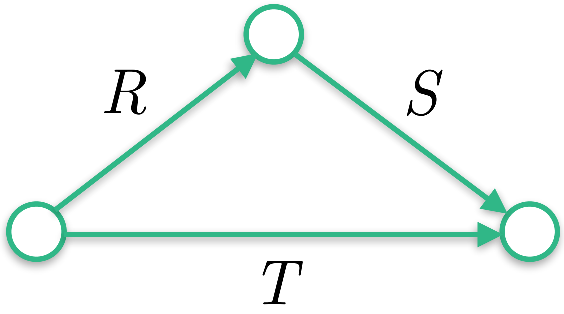
$$(R^\top)^\top = R$$

$$(R \mathbin{;} S)^\top = S^\top \mathbin{;} R^\top$$

- Complex Properties

  Modular laws, e.g.,

$$R \mathbin{;} S \cap T \subseteq (R \cap T \mathbin{;} S^\top) \mathbin{;} S$$



Dedekind law

$$R \mathbin{;} S \cap T \subseteq (R \cap T \mathbin{;} S^\top) \mathbin{;} (S \cap R^\top \mathbin{;} T)$$

Limitations

- relations only reflect start- and endpoints
  (no intermediate states)

- hence reasoning about paths of graphs complicated

Weaker Algebras

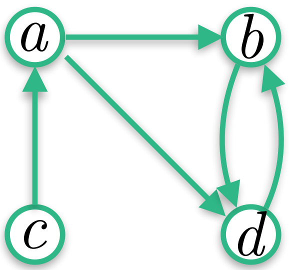
- path algebras (elements are from Σ^+)

$$s \bowtie t = s.\mathrm{tail}(t) \qquad \text{if } \mathrm{last}(s) = \mathrm{first}(t)$$

- example

$$G = \{ab, ad, bd, ca, db\}$$

$$G \,;\, G = \{adb, abd, bdb, \ldots\}$$



- converse: $R^\top = \{\mathrm{rev}(r) \mid r \in R\}$
- point-wise lifting yields Kleene Algebra (with Converse)
- modular laws do not hold (look at length of paths)

$$R \,;\, S \cap T \subseteq (R \cap T \,;\, S^\top) \,;\, S$$

$R, S, T \subseteq \Sigma^+$

Normalform

- we want $s \bowtie \mathrm{rev}(s) = \mathrm{first}(s)$

- normalform $\mathtt{nf} : \Sigma^+ \to \Sigma^+$ using rewrite rules

$$aba \mapsto a \quad (\text{for all } a, b \in \Sigma)$$

$$\begin{tikzcd}[column sep=tiny]
 & \ldots aba \ldots cdc \ldots \arrow[dl] \arrow[dr] & \\
\ldots a \ldots cdc \ldots \arrow[dr] & & \ldots aba \ldots c \ldots \arrow[dl] \\
 & \ldots a \ldots c \ldots &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=tiny]
 & \ldots abaca \ldots \arrow[dl] \arrow[dr] & \\
\ldots aca \ldots \arrow[dr] & & \ldots aba \ldots \arrow[dl] \\
 & \ldots a \ldots &
\end{tikzcd}
\qquad
\begin{tikzcd}
\ldots abab \ldots \arrow[d] \\
\ldots ab \ldots
\end{tikzcd}$$

- equivalence classes: $s \equiv t \Leftrightarrow \mathtt{nf}(s) = \mathtt{nf}(t)$

A New Model for RA

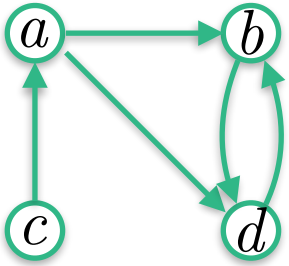
- new path algebra (elements are from $\Sigma^+/\equiv$)

$$s \nabla t = \mathtt{nf}(s.\mathrm{tail}(t)) \qquad \text{if } \mathrm{last}(s) = \mathrm{first}(t)$$

- example

$$G = \{ab, ad, bd, ca, db\}$$

$$G \nabla_S G = \{adb, abd, b\cancel{db}, \ldots\}$$



- converse: $R^\top = \{\mathrm{rev}(r) \mid r \in R\}$
- point-wise lifting yields Relation Algebra

Potential Applications & Question

- (directed) graphs without "forward-backward loops"
- *undirected* graphs
- calculations with backtracking

- Paths of Length n
  - Σ paths of length 1 (neutral element of composition)
  - $\Sigma \times \Sigma$ paths of length 2 (not abstract algebraic)
  - how do we characterise paths of length 3, 4 …
    (preferable as an expression in RA)

- other normal forms are possible (later)

Proof of Modular Laws

- proof point wise (and boring)

```
lemma modular:
 "(P ∇s Q) ∩ R ⊆ P ∇s (Q ∩ (P⌣∇sR))"
proof -
  {fix xs
  assume as: "xs ∈ (P∇sQ) ∩ R"
  hence "∃ps qs sp. ps∈P ∧ qs∈Q ∧ Some xs = ps ∇ qs ∧ xs ∈ R ∧ sp = cnrev ps"
    by (simp add: set_cfusion_def)
  hence "∃ps qs sp. ps∈P ∧ qs∈Q ∧ Some xs = ps ∇ qs ∧ xs ∈ R ∧ sp = cnrev ps ∧ cnhd ps = cnhd xs"
    by (metis first_cfusion fusion_point_definedness)
  hence "∃ps qs sp. ps∈P ∧ qs∈Q ∧ Some xs = ps ∇ qs ∧ xs ∈ R ∧ sp = cnrev ps ∧
          cnlast (cnrev ps) = cnhd xs ∧ cnrev ps∈P⌣"
    by (metis (mono_tags, lifting) set_cconverse_def cnlast_cnrev mem_Collect_eq)
  then have "xs ∈ P ∇s (Q ∩ (P⌣∇sR))"
    by (smt IntI modular_aux1 modular_aux2 cnlast_cnrev mem_Collect_eq
            set_cconverse_def set_cfusion_def)
  }
  thus ?thesis
    by blast
qed
```

Generalising the Construction

- Tarski Jonsson 1941

(Brandt) Groupoid $\xrightarrow[\text{pointwise lifting}]{}$ Relation Algebra

(a) $\cdot : G \times G \hookrightarrow G$ is a partial function, with
$\cdot$ is associative (if defined)

(b) $^{-1} : G \to G$ is inverse function, with
$a^{-1} \cdot a$ and $a \cdot a^{-1}$ is defined and
if $a \cdot b$ is defined then $a \cdot b \cdot b^{-1} = a$ and $a^{-1} \cdot a \cdot b = b$

Category theory:
A groupoid is a small category in which every morphism is an isomorphism, i.e. invertible.

Groupoids

- it is straightforward that cancellative paths (elements of $\Sigma^+/\equiv$) form a groupoid using ∇ and $^\top$

$$s \nabla t = \mathtt{nf}(s.\mathrm{tail}(t)) \qquad \text{if } \mathrm{last}(s) = \mathrm{first}(t)$$

- properties of groupoids

$$(a^{-1})^{-1} = a$$
$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$$

Constructing More RAs

- other normal forms work as well
  - no self-loops

    $$aa \mapsto a$$

  - no self-loops and no trivial loops

    $$aba \mapsto a \qquad aa \mapsto a$$

  - “relations“

    $$s \mapsto \texttt{first}(s)\texttt{last}(s)$$

  - …
    (all “interesting” normal forms lead to groupoid)
  - but **not** loop-free graphs

    $$a\Sigma^* a \mapsto a$$

    not a normal form

Generalising the Generalisation

Semigroupoid	$\longrightarrow$	Quantale (without 1)
Category	$\longrightarrow$	Kleene Algebra (Quantale)
Dagger Category $1_a = (1_a)^{-1}$ $(a^{-1})^{-1} = a$ $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$	$\longrightarrow$	Kleene Algebra with Converse
(Brandt) Groupoid	$\xrightarrow[\text{JonssonTarski41}]{}$	Relation Algebra

$\cdot$ is associative (if defined)
$a^{-1} \cdot a$ and $a \cdot a^{-1}$ is defined
if $a \cdot b$ is defined then $a \cdot b \cdot b^{-1} = a$ and $a^{-1} \cdot a \cdot b = b$

Generalising the Generalisation

Semigroupoid → Quantale (without 1)

+ 1

Category → Kleene Algebra (Quantale)

+ converse

Dagger Category → Kleene Algebra with Converse

+ “non-intuitive” axioms (remove others)

(Brandt) Groupoid → Relation Algebra

JonssonTarski41

From Dagger Categories to Groupoids

Dagger Category

+ “non-intuitive”
  axioms
  (remove others)

(Brandt) Groupoid

Path Model

+ non-trivial
  normalform

Path Model

Is there a relation of (specific) normal forms and the axioms of groupoids?

From Dagger Categories to Groupoids

Dagger Category

+ "non-intuitive"
axioms
(remove others)

(Brandt) Groupoid

small category in which
every morphism is an isomorphism

Path Model

+ non-trivial
normalform

Path Model

When does a normal form correspond to isomorphism?

DATA 61

Trustworthy Systems
Peter Höfner

t +61 2 9490 5861
e Peter.Hoefner@data61.csiro.au
w www.data61.csiro.au

www.data61.csiro.au

CSIRO