Extended Conscriptions Algebraically

Walter Guttmann
University of Canterbury

1. Assumptions
2. Conscriptions
3. Algebras

Assumption ⊩ Commitment

$$(y > 1) \Vdash (\text{while } x > 1 \text{ do } x := x/y)$$

assumption

- refers to pre-state only
- condition for successful execution
- execution might abort or not terminate if assumption is false

commitment

- relates pre- and post-state
- effect of successful execution

Relational model

$$Q \Vdash R$$

state space A

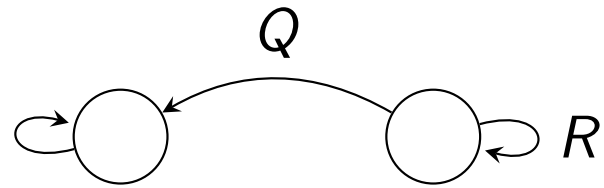
- $Q, R : A \leftrightarrow A$
- $Q = Q\mathsf{T}$

operators

- $(Q_1 \Vdash R_1) + (Q_2 \Vdash R_2) = ((Q_1 \cap Q_2) \Vdash (R_1 \cup R_2))$
- $(Q_1 \Vdash R_1) \cdot (Q_2 \Vdash R_2) = ((Q_1 \cap \overline{R_1 \overline{Q_2}}) \Vdash (R_1 R_2))$
- $(Q \Vdash R)^* = (\overline{R^* \overline{Q}} \Vdash R^*)$

Matrix model

$$(\overline{Q} \Vdash R) = \begin{pmatrix} \mathsf{T} & \mathsf{O} \\ Q & R \end{pmatrix}$$



state space A

- $\mathsf{T}, \mathsf{O}, Q, R : A \leftrightarrow A$
- $Q = Q\mathsf{T}$

operators

- $+$, $\cdot$, * standard matrix operators
- $Q =$ states from which execution might abort or not terminate
- $R =$ possible successors of each state

Further matrix models

- total correctness $\begin{pmatrix} \mathsf{T} & \mathsf{T} \\ Q & R \end{pmatrix}$ $\quad Q \subseteq R \quad Q = Q\mathsf{T}$
- general correctness $\begin{pmatrix} \mathsf{T} & \mathsf{O} \\ Q & R \end{pmatrix}$ $\quad Q = Q\mathsf{T}$
- extended designs $\begin{pmatrix} \mathsf{T} & \mathsf{T} & \mathsf{T} \\ \mathsf{O} & \mathsf{T} & \mathsf{O} \\ P & Q & R \end{pmatrix}$ $\quad P \subseteq Q \quad P = P\mathsf{T}$, $P \subseteq R \quad Q = Q\mathsf{T}$
- $\begin{pmatrix} \mathsf{T} & \mathsf{O} & \mathsf{O} \\ \mathsf{O} & \mathsf{T} & \mathsf{O} \\ P & Q & R \end{pmatrix}$ $\quad P = P\mathsf{T}$, $Q = Q\mathsf{T}$

Problems

- generalise Q to arbitrary relation
- determine properties of operators
- find approximation order
- unify with existing models

Conscriptions (Dunne 2013)

$$\begin{pmatrix} \mathsf{I} & \mathsf{O} \\ Q & R \end{pmatrix}$$

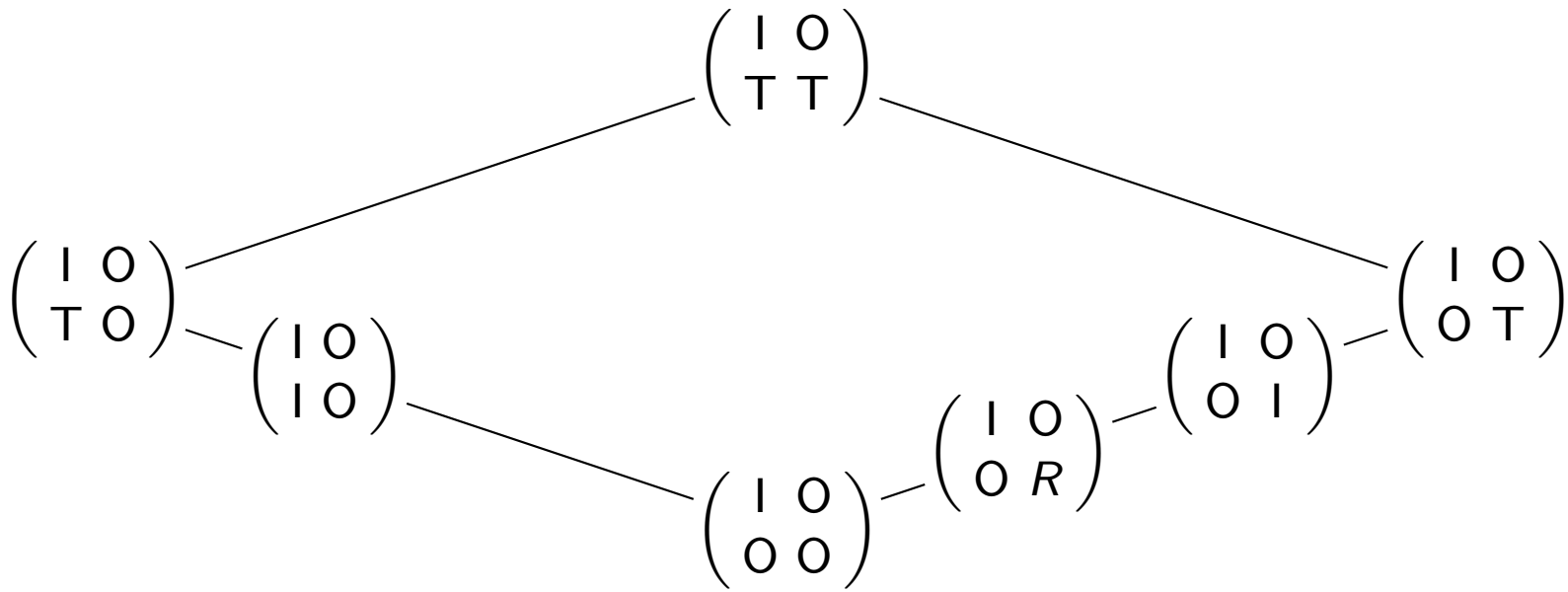
state space A

- $\mathsf{I}, \mathsf{O}, Q, R : A \leftrightarrow A$
- no restriction on Q

Q relates pre- and post-state

- final state of aborting executions
- stable state of non-terminating executions
- abstraction of more detailed models

Operators



- $R \subseteq \mathsf{I}$ for tests
- $+$, $\cdot$ standard matrix operators
- refinement $\leq$ is componentwise $\subseteq$
- approximation?

Non-terminating executions

- all non-terminating executions L

$$\mathsf{L} = \begin{pmatrix} \mathsf{I} & \mathsf{O} \\ \mathsf{T} & \mathsf{O} \end{pmatrix}$$

- $n(x) =$ set of states from which x has non-terminating executions
- $n(x) \leq 1$
- Galois connection

$$n(x)\mathsf{L} \leq y \;\Leftrightarrow\; n(x) \leq n(y)$$

- gives

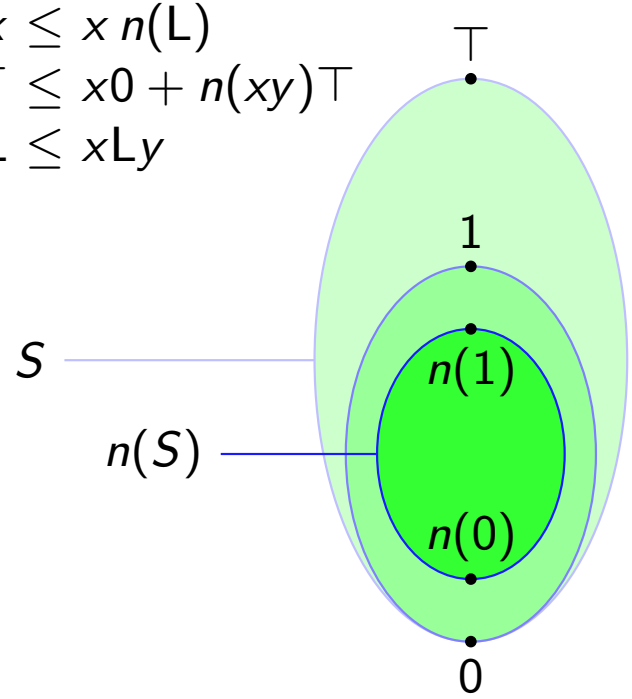
$$n\begin{pmatrix} \mathsf{I} & \mathsf{O} \\ Q & R \end{pmatrix} = \begin{pmatrix} \mathsf{I} & \mathsf{O} \\ \mathsf{O} & \overline{\overline{Q}\mathsf{T}} \cap \mathsf{I} \end{pmatrix}$$

Axioms for n

- bounded distributive lattice $(S, +, \curlywedge, 0, \top)$
- semiring $(S, +, \cdot, 0, 1)$ without $x \cdot 0 = 0$
- n-algebra $(S, +, \curlywedge, \cdot, n, 0, 1, \mathsf{L}, \top)$

$$
\begin{aligned}
n(x) + n(y) &= n(n(x)\top + y) \\
n(x)n(y) &= n(n(x)y) \\
n(x)n(x+y) &= n(x) \\
n(\mathsf{L})x &= (x \curlywedge \mathsf{L}) + n(\mathsf{L}0)x \\
x\mathsf{L} &= x0 + n(x\mathsf{L})\mathsf{L}
\end{aligned}
\qquad
\begin{aligned}
n(x) &\leq n(\mathsf{L}) \curlywedge 1 \\
n(x)\mathsf{L} &\leq x \\
n(\mathsf{L})x &\leq x\, n(\mathsf{L}) \\
x\, n(y)\top &\leq x0 + n(xy)\top \\
x\top y \curlywedge \mathsf{L} &\leq x\mathsf{L}y
\end{aligned}
$$

- $n(S)$ bounded distributive lattice
- many instances of n-algebras



Recursion

- least fixpoint in approximation order $\sqsubseteq$

$$x \sqsubseteq y \;\Leftrightarrow\; x \leq y + \mathsf{L} \;\wedge\; n(\mathsf{L})y \leq x + n(x)\top$$

- gives

$$\begin{pmatrix} \mathsf{I} & \mathsf{O} \\ Q_1 & R_1 \end{pmatrix} \sqsubseteq \begin{pmatrix} \mathsf{I} & \mathsf{O} \\ Q_2 & R_2 \end{pmatrix} \;\Leftrightarrow\; Q_2 \subseteq Q_1 \;\wedge\; R_1 \subseteq R_2 \subseteq R_1 \cup \overline{\overline{Q_1}\mathsf{T}}$$

- $\sqsubseteq$ partial order with least element L
- $+$, $\cdot$, $\curlywedge\mathsf{L}$ are $\sqsubseteq$-isotone

Recursion theorem

- assume f is $\leq$-, $\sqsubseteq$-isotone and μf, νf exist
  - $\mu f / \nu f / \kappa f$ is $\leq / \geq / \sqsubseteq$-least fixpoint
  - $\sqcap$ is $\sqsubseteq$-meet
- then equivalent
  - κf exists
  - κf and $\mu f \sqcap \nu f$ exist and $\kappa f = \mu f \sqcap \nu f$
  - κf exists and $\kappa f = (\nu f \curlywedge \mathsf{L}) + \mu f$
  - $n(\mathsf{L})\nu f \leq (\nu f \curlywedge \mathsf{L}) + \mu f + n(\nu f)\top$
  - $n(\mathsf{L})\nu f \leq (\nu f \curlywedge \mathsf{L}) + \mu f + n((\nu f \curlywedge \mathsf{L}) + \mu f)\top$
  - $(\nu f \curlywedge \mathsf{L}) + \mu f \sqsubseteq \nu f$
  - $\mu f \sqcap \nu f$ exists and $\mu f \sqcap \nu f = (\nu f \curlywedge \mathsf{L}) + \mu f$
  - $\mu f \sqcap \nu f$ exists and $\mu f \sqcap \nu f \leq \nu f$

Iteration theorem

- while p do w = if p then (w ; while p do w) else skip
- $f(x) = yx + z$

$$\kappa f = (y^\omega \curlywedge \mathsf{L}) + y^* z = n(y^\omega)\mathsf{L} + y^* z = y \star z$$

- omega algebra $(S, +, \cdot, ^*, ^\omega, 0, 1, \top)$ without $x \cdot 0 = 0$
- n-omega algebra $(S, +, \curlywedge, \cdot, n, ^*, ^\omega, 0, 1, \mathsf{L}, \top)$

$$n(\mathsf{L})x^\omega \leq x^* n(x^\omega)\top \qquad x\mathsf{L} \leq x\mathsf{L}x\mathsf{L}$$

- *, $^\omega$ are $\sqsubseteq$-isotone

Strict models

- n-algebras developed for non-strict computations
- $\mathsf{L}x = \mathsf{L}$ in strict models
- $\kappa f = y^\circ z$
- $y^\circ = n(y^\omega)\mathsf{L} + y^*$
- sumstar, productstar, simulation properties

$$(x+y)^\circ = (x^\circ y)^\circ x^\circ \qquad zx \leq yy^\circ z + w \Rightarrow zx^\circ \leq y^\circ(z + wx^\circ)$$
$$(xy)^\circ = 1 + x(yx)^\circ y \qquad xz \leq zy^\circ + w \Rightarrow x^\circ z \leq (z + x^\circ w)y^\circ$$

- models
  - Kleene algebra $x^\circ = x^*$
  - omega algebra $x^\circ = x^\omega 0 + x^*$
  - demonic refinement algebra $x^\circ = x^\Omega$

Extended conscriptions (Dunne 2013)

$$\begin{pmatrix} \mathsf{I} & \mathsf{O} & \mathsf{O} \\ \mathsf{O} & \mathsf{T} & \mathsf{O} \\ P & Q & R \end{pmatrix}$$

- $P =$ aborting executions
- $Q =$ states with non-terminating executions
- no restriction on P
- $Q = Q\mathsf{T}$
- obtain n, $\sqsubseteq$, $\star$, $^\circ$ similarly

Further computation models

$$\begin{pmatrix} \mathsf{I} & \mathsf{O} & \mathsf{O} \\ \mathsf{O} & \mathsf{I} & \mathsf{O} \\ P & Q & R \end{pmatrix}$$

- no restriction on P, Q
- obtain n, $\sqsubseteq$, $\star$, $^\circ$ similarly

Conclusion

- theory developed in Isabelle/HOL
- approximation for new models
  - derive n using Galois connection
  - show n-algebra axioms
  - use approximation in n-algebras
- future work
  - non-strict computations with general correctness
  - multirelations with infinite, aborting executions