Mechanised Theory Engineering in Isabelle

Heterogeneous Semantics for CML

Jim Woodcock

University of York

Marktoberdorf

5th August 2014
From relations to designs

Galois connection

- lattice of nondeterministic programs and relational contracts
- lattice of designs with same signature
- these two theories constitute basic CML

Left adjoint: $Des$

- $Des : Relations \rightarrow Designs$. 
- both lattices are ordered by refinement
- Relations excludes treatment of termination
- must decide how to handle termination
- relation $R$ has no description of termination
- correctness must be judged with assumption of termination
- statement of partial correctness
Left adjoint

Definition (*Des*)

\[ \text{Des}(R) \triangleq H(R \land ok') \]

Law (*Des Design*)

\[ \text{Des}(R) = \text{true} \vdash R \]
From designs to relations

Right adjoint $\text{Rel}$

- $\text{Rel} : \text{Designs} \rightarrow \text{Relations}$
- forget information about initiation and termination
- consider only proper initiation and termination
  \[ \text{Rel}(D) = D[\text{true, true}/\text{ok, ok}'] \]
- shorthand : $D^{tt}$

Definition ($\text{Rel}$)

$\text{Rel}(D) \equiv D^{tt}$

Law ($\text{Rel$ Design$}$)

$\text{Rel}(P \vdash Q) = P \Rightarrow Q$
Galois connection

\((\text{Des}, \text{Rel})\)

- \((\text{Des}, \text{Rel})\) is a Galois connection:
  \[(\text{Designs}, \supseteq) \overset{\text{Des}}{\leftrightarrow} (\text{Relations}, \supseteq) \overset{\text{Rel}}{\leftrightarrow}\]

Theorem \(((\text{Des}, \text{Rel})\text{ Galois connection})\)

- \((\text{Des}, \text{Rel})\) is a Galois connection

Lemma \((\text{Des} \text{ injective})\)

- the Galois connection \((\text{Des}, \text{Rel})\) is a coretract
  \[\text{Des} \text{ is injective}\]
Lemma \(((Des, Rel)\) Properties)\n
1. \(Rel\) is surjective
2. \((Des, Rel)\) is a coretract
3. \(Des\) is an order similarity: \((Des(R) \sqsubseteq Des(S)) = (R \sqsubseteq S)\)

Proof

since \(Des\) is injective
Reactive processes

Observation variables

- $ok' \land wait'$, the process is in a stable intermediate state
- $ok' \land \neg wait'$, the process is in a stable final state
- $\neg ok'$, the process is in an unstable state
- process’s history: $tr' - tr$.
- events being refused: $ref'$

Reactive healthiness conditions

- $R1(P) = P \land tr \leq tr'$
- $R2(P) = P[\langle \rangle, tr' - tr/\bar{tr}, tr']$
- $R3(P) = \Pi \triangleleft wait \triangleright P$
From designs to reactive processes and back again

- $R2$ and $R3$ commute with $H1$ and $H2$
- $R1$ doesn’t commute with $H1$

$$H1 \circ R1(P) = \text{ok} \Rightarrow P \land (tr \leq tr')$$
$$R1 \circ H1(P) = (\text{ok} \Rightarrow P) \land (tr \leq tr')$$

- actually, $R1 \circ H1 = \text{CSP1}$.

Theorem

$(H, R1)$ is a Galois connection
Timed reactive processes

Semantic domain

- traces with embedded refusal sets
- similar to Lowe and Ouaknine’s timed testing model
- record passing of time with explicit tock event
- allow refusal experiments only before tocks
- let $\Sigma$ be the universe of events
- $tock \notin \Sigma$
- observe passage of time through refusal experiments
- traces: $\text{timedTrace} \triangleq (\Sigma + \mathcal{P}(\Sigma))^*$
- observations: $rt, ok, wait$
Timed traces

Example: \( \langle a, b, \{b, c\}, \emptyset, c \rangle \)

- \( \langle a, b \rangle \) occurred in first interval
- process refused \( \{b, c\} \)
- no events observed during second interval
- process refused no events
- third interval incomplete, \( \langle c \rangle \) observed

Example: alternator

- timed testing traces can record quite subtle information
- \( P \): universe of events \( a, b \)
- \( P \) never offers \( b \)
- \( P \) offers \( a \) during every other time interval
- possible trace of \( P \): \( \langle \{a, b\}, \{b\}, \{a, b\}, \{b\}, \{a, b\} \rangle \).
Healthiness conditions

Definition (Monotonic history)

\[ RT1(P) = P \land rt \leq rt' \]

Definition (Independence)

\[ RT2(P) = P[\langle \rangle, tt'/rt, rt'] \quad tt' = rt' - rt \]

Definition (Sequence)

\[ RT3(P) = RT1(true \vdash wait' \land tt' = \langle \rangle) \triangleleft wait \triangleright P \]

Definition (Pre-stability)

\[ RT4(P) = RT1(\neg ok) \lor P \]

Definition (Stability)

\[ RT5(P) = P ; J \]
From reactive processes to time

Definition (Galois connection)

\[ L(P) \equiv \exists rt, rt' \bullet P \]
\[ \quad \land (tr = events(rt)) \]
\[ \quad \land (tr' = events(rt')) \]
\[ \quad \land (ref = last(refsduring(rt))) \]
\[ \quad \land (ref' = last(refsduring(rt'))) \]

\[ R(Q) \equiv \{ P \mid L(P) \supseteq Q \} \]

Applications

- Celoxica’s *Handel-C* design technique
- Sherif’s *CircusTime* architectural design pattern
Conclusion

- mechanised theory engineering in Isabelle and UTP
- everything proved in Isabelle/UTP
- model-based engineering
- **problem**: how do you deal with diversity in engineering?
- address the *semantic* diversity of models
- FMI interfaces for simulation tools
- UTP + Galois connections to compose building block theories
- Isabelle/HOL provides sound reasoning systems
- build integrated tool-chains as infrastructure
- example: SysML + CML
- application:
  - SoS & CPS with heterogeneous component models
  - reasoning about global emergent SoS behaviours