Conf. AMAST, Lac-Beauport, Québec, 23-25 June 2010

MODEL REFINEMENT USING BISIMULATION QUOTIENTS

Roland Glück [1], Bernhard Möller [1] and Michel Sintzoff [2]

[1] Universität Augsburg, Germany
[2] Université de Louvain, Belgium

Color code: red alert, blue sky.

Principle: Refining Models by Refining their Reductions

Step 1. Reduce a large, possibly infinite system-model M into a much smaller, finite model N. The latter is a bisimulation quotient of M.

Step 2. Construct a submodel N' of N that satisfies a given goal formula, using any known finite-state method.

Step 3. Expand N' back into a submodel M' of M. This M' should (a) be the largest possible submodel and (b) preserve satisfaction.

♡ *A basic running example:* minimizing costs of paths in infinite models.

Framework: Simple Models and Refinement by Submodels

- A *model* M is an labeled transition system (Q, H, T) where Q may be infinite, H is finite, and $T \subseteq Q \times H \times Q$.

  ♡ Running example: the labels in H are edge costs. The set Z of target nodes is $Q - Dom(T)$ and must be reachable from each node.

- A model M' is a *submodel* of M, written $M' \subseteq M$, if $Q' \subseteq Q$, $H' = H$, and $T' \subseteq T$. Unsuitable transitions may form $T - T'$.

  ♡ Running example: the submodels must be "node-complete", namely $M' \subseteq M \Rightarrow (Q' = Q) \wedge (Dom(T') = Dom(T))$.

- Let $Sub(M) \doteq \{M' \mid M' \subseteq M\}$ for any M . Then $(Sub(M), \subseteq)$ is a complete lattice: suprema are obtained as componentwise unions.

Step 1: Reduction to Quotient Models

- Consider $M = (Q, H, T)$ and an equivalence $E \subseteq Q^2$. We define
  $x/E \doteq \{y \mid x\, E\, y\}$ for $x \in Q$, $Q/E \doteq \{x/E \mid x \in Q\}$,
  $T/E \doteq \{(x/E, h, y/E) \mid (x, h, y) \in T\}$, $M/E \doteq (Q/E, H, T/E)$.

- The coarsest bisimulation equivalence for M is its *reducer*, written *Red*(M) . Then $M/$*Red*(M) is the *reduction of* M.

  ♡ Running example: LTS bisimulation equivalences are used.

  The time to reduce a finite M is polynomial in $|M|$ [Fernandez 89, Clarke et al. 99]. The reduction of a "well-structured" infinite M is finite and can be generated symbolically [Henzinger et al. 05].

Step 2: Solution of Finite-State Design Problems

- A *design problem* is a pair (φ, M) of a goal formula φ and a model M.

  A *solution* of (φ, M) is a model M' such that $(M' \subseteq M) \wedge (M' \models \varphi)$.
  We say that M' *is a* φ*-refinement of* M and write $M' \sqsubseteq_\varphi M$.

  ♡ Running example: we define φ_{mcp}. Given any M and any $M' \subseteq M$, $M' \models \varphi_{mcp}$ iff for each $x \in Q'$, the cost of each path by M' from x to Z is the minimum of the costs of the paths by M from x to Z.

- Step 2 uses known methods for solving (φ, M) when Q is finite.

  ♡ Running example: for any finite M, the problem $(\varphi_{mcp}\,, M)$ is solvable in polynomial time.

Consider pre-orders $(A, \leq_A)$ and $(B, \leq_B)$, and total functions $F : A \to B$ and $G : B \to A$. The pair (F, G) is a *Galois connection* between A and B iff $\forall x \in A, y \in B : \; F(x) \leq_B y \;\equiv\; x \leq_A G(y)$.

- Let $(A, \leq_A)$ and $(B, \leq_B)$ be complete lattices and let $F : A \to B$ be a total map preserving all suprema. Two properties are known:

  1. Assume $\forall y \in B : G(y) = \sup\{x \in A \mid F(x) \leq_B y\}$ where $G : B \to A$. Then (F, G) is a Galois connection.

  2. Given the latter (F, G), let $f \doteq F \downarrow G(B)$ and $g \doteq G \downarrow F(A)$. Then $f = g^\circ$ and $\forall y \in F(A) : g(y) = \sup\{x \in A \mid F(x) = y\}$ [Erné et al. 94]. We say that the function g is *result-maximal*.

Step 3: (a_1) Expansion as Upper Adjoint of Quotient

- Choose any M . Let $E \doteq \mathit{Red}(M)$ and $F \doteq /E : A \to B$ where $A \doteq \mathit{Sub}(M)$ and $B \doteq \mathit{SubRed}(M) = \mathit{Sub}(M/E)$.
  Both $(A, \subseteq)$ and $(B, \subseteq)$ are complete lattices. We also proved that the quotient operation $F = /E$ is total and preserves all suprema.

- We define the expansion operation $\backslash E : B \to A$ constructively by

$$(Q_N, H, T_N)\backslash E \doteq (\bigcup Q_N\,,\, H\,,\, \bigcup_{(X,h,Y)\in T_N} (X \times \{h\} \times Y) \cap T\ ).$$

We proved that $G = \backslash E$ verifies the supremum hypothesis in Property 1.
Hence $(\ /\mathit{Red}(M)\ , \backslash \mathit{Red}(M))$ is a Galois connection.

Step 3: (a_2) Restricted Expansion as Result-Maximal Inverse of Restricted Quotient

---

- As above $E = \mathit{Red}(M)$. The restricted domains of $/E$ and $\backslash E$ are
  $A \cap (B\backslash E) = B\backslash E = \mathit{SubRed}(M)\backslash E = \mathit{ClSub}(M)$, and
  $B \cap (A/E) = \mathit{SubRed}(M) \cap (\mathit{Sub}(M)/E) \; = \mathit{SubRed}(M)$.

- So the restrictions of $/E$, $\backslash E$ are $\mathit{Shrink}\ M, \mathit{Grow}\ M$ such that

  $\boxed{(\mathit{Shrink}\ M)\ M' = M'/\mathit{Red}(M)}$, $\boxed{(\mathit{Grow}\ M)\ N = N\backslash\mathit{Red}(M)}$,

  with $\mathit{Shrink} : (M : \mathcal{M}) \to (\mathit{ClSub}(M) \to \mathit{SubRed}(M))$,
  $\mathit{Grow} : (M : \mathcal{M}) \to (\mathit{SubRed}(M) \to \mathit{ClSub}(M))$,
  where $\mathcal{M}$ is a given set of considered models.

By Property 2, $\mathit{Grow}\ M$ is the result-maximal inverse of $\mathit{Shrink}\ M$.
Thus $(\mathit{Grow}\ M)\ N = \sup\{M' \in \mathit{Sub}(M) \mid M'/\mathit{Red}(M) = N\}$.

Step 3: (b) Expansion of Refinements using Admissible Formulae

---

- A predicate φ over states is *admissible* if for any model M and any bisimulation equivalence E for M,

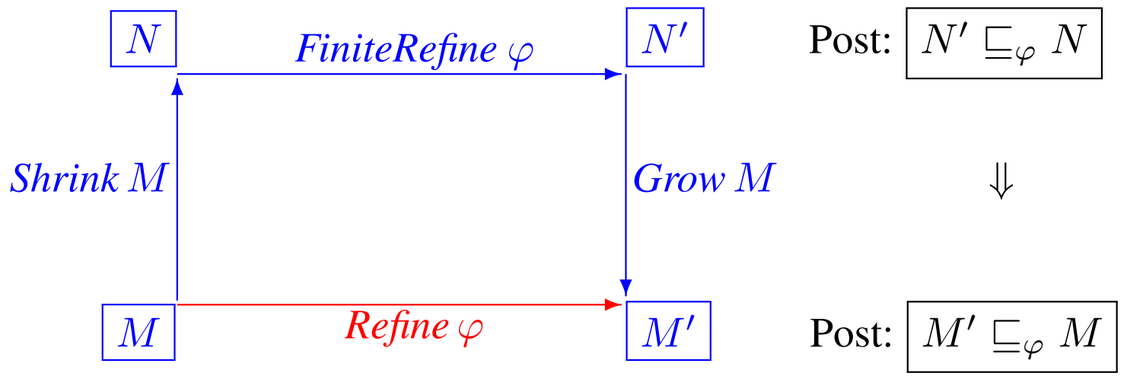
$$M/E \models \varphi \;\Rightarrow\; M \models \varphi\,.$$

- *Little Proposition (Expansion of Abstract Refinements).* If a formula φ is admissible then for all $M \in \mathcal{M}$ and all $N, N' \in \mathit{SubRed}(M)$,

$$\boxed{N' \sqsubseteq_\varphi N} \;\Rightarrow\; \boxed{(\mathit{Grow}\ M)\ N' \sqsubseteq_\varphi (\mathit{Grow}\ M)\ N}\,.$$

♡ Running example: the admissibility of φ_{mcp} has been proven.

A Bird's-Eye View



$$(\mathit{Refine}\ \varphi)\ M = (\mathit{Grow}\ M \circ \mathit{FiniteRefine}\ \varphi \circ \mathit{Shrink}\ M)\ M$$

$$\mathit{Refine} : \mathit{Frml} \to ((M \in \mathcal{M}) \to \mathit{Sub}(M))$$
$$\mathit{FiniteRefine} : \mathit{Frml} \to ((N \in \mathcal{N}) \to \mathit{Sub}(N))$$

Frml is a set of admissible formulae
$\mathcal{N}$ is a set of finite models.

Generalization and Conclusion

A generalized model is a tuple $(Q, T, A_1, \ldots, A_n)$ where $T \subseteq Q^2$ and each A_i labels nodes or edges, viz. $A_i \subseteq Q \to S_i$ or $A_i \subseteq T \to S_i$. The present results hold for these models and related bisimulations.

The method has been applied to optimality properties and temporal ones.

Its usefulness depends on various critical factors:

- The goal formulae must be admissible.
- Very large models must collapse to drastically smaller quotients.
- We should know efficient algorithms to solve finite-state problems.