Conjoining Specifications II

Wolfgang Schreiner
Research Institute for Symbolic Computation
Johannes Kepler University, Linz, Austria

Wolfgang.Schreiner@risc.uni-linz.ac.at
http://www.risc.uni-linz.ac.at/people/schreine

Decomposing a Complete Specification

- Specifying a Component M
  - Output variables m
  - Input variables e
  - $\exists x$: *Init* $\wedge \Box[\mathsf{N}]_v \wedge L$.
- State function v
  - Tuple $\langle x, m, e\rangle$
- Initial condition *Init*
  - Initial values of m and x.
- Next-state action N
  - Component steps N_m ($\Rightarrow e' = e$)
  - Environment steps.
  - $\mathsf{N} \equiv \mathsf{N}_m \vee (\langle m, x\rangle' = \langle m, x\rangle)$
- Fairness conditions L
  - Conjunction of formulas $\mathsf{WF}_{\langle m,x\rangle}$ and/or $\mathsf{SF}_{\langle m,x\rangle}$

Component Specification

- Specification of M
  - $\exists x$: *Init* $\wedge \Box[\mathsf{N}_m \vee (\langle m, x\rangle' = \langle m, x\rangle)]_{\langle e,m,x\rangle} \wedge L$.
  - $\exists x$: *Init* $\wedge \Box[\mathsf{N}_m]_{\langle m,x\rangle} \wedge L$.
- GCD: Specification M_a
  - $\mathit{Init}_a \equiv a = 233344$
  - $M_a \equiv (a > b) \wedge (a' = a - b) \wedge (b' = b)$
  - $\mathsf{M}_a \equiv \mathit{Init}_a \wedge \Box[\mathsf{N}_a]_a \wedge \mathsf{WF}_a(\mathsf{N}_a)$
- GCD: Specification M_a^l
  - $M_a^l \equiv \exists\ ai,\ pca\colon\ \mathit{Init}_a^l \wedge \Box[\mathsf{N}_a^l]_{\langle a,ai,pca\rangle} \wedge \mathsf{WF}_{\langle a,ai,pca\rangle}(\mathsf{N}_a^l)$

Queue Component

- Queue Component
  - $m = \langle i.ack, o.snd \rangle$
  - $\mathit{QM} \equiv \exists q\colon \mathit{IQM}$
  - $\mathit{IQM} \equiv \mathit{Init}_M \land \Box[\mathrm{Q}_M]_{\langle i.ack, o.snd, q \rangle} \land \mathit{ICL}$
- Environment
  - $e = \langle i.snd, o.ack \rangle$
  - $\mathit{QE} \equiv \mathit{Init}_E \land \Box[\mathrm{Q}_E]_{\langle i.snd, o.ack \rangle}$
- Non-interleaving representation
  - Change *Enq* and *Deq* such that they do not constrain e'
  - Define *EnqDeq* that simultaneously enqueues an input value and dequeues and output value.

Queue Component

Non-interleaving Specification

$\mathit{QM}^{ni} \equiv \exists q\colon\ \mathit{IQM}^{ni}$
$\mathit{IQM}^{ni} \equiv \mathit{Init}_M \land \Box[\mathsf{Q}_M^{ni}]_{\langle i.ack, o.snd, q\rangle}$
$\land\ \mathsf{WF}_{\langle i.ack, o.snd, q\rangle}(\mathsf{Q}_M^{ni})$
$\mathit{Init}_M \equiv \mathit{CInit}(o) \land (q = \langle\rangle)$

$\mathsf{Q}_M^{ni} \equiv \mathit{Enq}^{ni} \lor \mathit{Deq}^{ni} \lor \mathit{DeqEnq}^{ni}$

$\mathsf{Enq}^{ni} \equiv |q| < N$
$\land\ \mathit{Ack}(i) \land (q' = q \circ \langle i.val\rangle)$
$\land\ o.snd' = o.snd$
$\mathit{Deq}^{ni} \equiv |q| > 0$
$\land\ \mathit{Send}(\mathit{Head}(q), o) \land (q' = \mathit{Tail}(q))$
$\land\ (i.ack' = i.ack)$
$\mathit{DeqEnq}^{ni} \equiv |q| > 0$
$\land\ \mathit{Send}(\mathit{Head}(q), o)$
$\land\ \mathit{Ack}(i) \land q' = \mathit{Tail}(q) \circ \langle i.val\rangle)$

Conjoining Specifications

- Current Situation
  - Specification of complete system.
  - Specification of individual component.
  - Missing: composition of components.
- Idea: *composition is conjunction*
  - Behavior satisfies both M_1 and M_2
  - Behavior satisfies $M_1 \wedge M_2$
- Conjunction of component specfications
  - $\mathit{CQ} \equiv \mathit{CM} \wedge \mathit{CE}$.
  - Complete system is conjunction of component and environemnt.
- Detailed definitions
  - $\mathit{CQ} \equiv \exists q\colon\ \mathit{Init}_E \wedge \mathit{Init}_M$
    $\wedge \Box[(Q_E \wedge (q' = q)) \vee Q_M]_{\langle i,o,q \rangle} \wedge \mathit{ICL}$
  - $\mathit{QE} \equiv \mathit{Init}_E \wedge \Box[\mathrm{Q}_E]_{\langle i.snd, o.ack \rangle}$
  - $\mathit{QM} \equiv \exists q\colon\ \mathit{Init}_M \wedge \Box[\mathrm{Q}_M]_{\langle i.ack, o.snd, q \rangle} \wedge \mathit{ICL}$

Proposition

- Proposition
  - If $M_i \equiv \exists x_i$: $\mathit{Init}_i \wedge \Box[\mathsf{N}_i]_{\langle m_i, x_i \rangle} \wedge L_i$
    and $\mathsf{N}_i \Rightarrow (m_j{}' = m_j)$
  - then $\models (\wedge_{i=1}^{n} M_i) = \exists x$: $\wedge_{i=1}^{n} \mathit{Init}_i$
    and $\wedge \Box[\vee_{i=1}^{n} \mathsf{N}_i \wedge (\widehat{x_i}{}' = \widehat{x_i})]_{\langle m, x \rangle} \wedge \wedge_{i=1}^{n} L_i$
  - where $m \equiv \langle m_1, \ldots, m_n \rangle$
    and m_i all free variables of M_i
    and $\widehat{x_i} \equiv \langle x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n \rangle$
- GCD:
  - $M_{gcd} \equiv M_a \wedge M_b$

Two Queues in Series

- Components:
  - Queue 1: $\exists q_1$: $\mathit{Init}_M^{[1]}$ $\land \Box[\mathsf{Q}_M^{[1]} \land (o' = o)]_{\langle i.ack, z.snd, q_1 \rangle} \land \mathit{ICL}^{[1]}$
  - Queue 2: $\exists q_2$: $\mathit{Init}_M^{[2]}$ $\land \Box[\mathsf{Q}_M^{[2]} \land (i' = i)]_{\langle z.ack, o.snd, q_2 \rangle} \land \mathit{ICL}^{[2]}$
  - Environment: Init_E $\land \Box[\mathsf{Q}_E \land (z' = z)]_{\langle i.snd, o.ack \rangle}$
- Interleaving representation required:
  - Conjoining $o' = o$, $i' = i$, $z' = z$
- From Proposition:
  - Equivalence to CDQ

The Decomposition Theorem

- Complete system Π of components Π_i
  - Low-level system Π^l of components Π_i^l
  - Prove that Π^l implements Π by proving that Π_i^l implements Π_i
- Proof:
  - Prove $\wedge_{i=1}^l M_i^l \Rightarrow \wedge_{i=1}^l M_i$
  - In general $M_i^l \Rightarrow M_i$ does *not* hold!
- Introduction of *environments* E_i
  - $E_i \wedge M_i^l \Rightarrow M_i$
  - E_i much simpler than $\wedge_i M_i^l$
- How to prove E_i?
  - $\wedge_{i=1}^l M_i^l \Rightarrow E_i$
  - Again reasoning about whole low-level system!
- Suffices to prove $\wedge_{i=1}^l M_i \Rightarrow E_i$
  - $\wedge_{i=1}^l M_i$ simpler than $\wedge_{i=1} M_i$
  - Only high-level specification required.

Decomposition Theorem

- The Basic Theorem
  - If $\models \wedge_{j=1}^{n}\ \mathsf{C}(M_j) \Rightarrow E_i$
    and $\models \mathsf{C}(E_i)_{+v} \wedge \mathsf{C}(M_i^l) \Rightarrow \mathsf{C}(M_i)$
    and $\models E_i \wedge M_i^l \Rightarrow M_i$
  - then $\models \wedge_{i=1}^{n}\ M_i^l \Rightarrow \wedge_{i=1}^{n}\ M_i$
- GCD Example
  - $E_a \equiv \Box\, [(a < b) \wedge (a' = a)]_b$
  - $E_a \wedge M_a^l \Rightarrow M_a$
- E_i is only implied by safety properties
  - E_i can only contain safety properties.
  - E_i *are* safety properties.

Verifying the Hypotheses

- How to prove hypotheses of theorem?
  - Simplify by Propositions 1 and 2.
  - $\models \bigwedge_{i=1}^{n} (\mathit{Init}_i \wedge \Box[\mathsf{N}_i]_{v_i}) \Rightarrow E_i$.
  - Apply Proposition 5 to rewrite $\mathit{Init}_i \wedge \Box[\mathsf{N}_i]_{v_i}$ in canonical form.
- First hypothesis (GCD example)
  - $\mathsf{C}(M_a) \wedge \mathsf{C}(M_b) \Rightarrow E_a$.
  - Apply Proposition 1 to construct $C(M_a)$ (strip fairness condition).
  - Since N_b implies $(a < b) \wedge (a' = a)$, $\mathsf{C}(M_a)$ implies E_b.
- Second hypothesis (general).
  - Apply Propositions 4 and 5 to eliminate $+$.
  - Use Proposition 2 to eliminate quantifiers.
  - Use Proposition 1 to compute closures.
  - Perform implementation proof with refinement mapping.

Verifying the Hypotheses

- Third hypothesis (general).
  - Implementation proof with same refinement mapping as before.
  - Since E_i implies $\mathsf{C}(E_i)_{+v}$ and M_i^l implies $\mathsf{C}(M_i^l)$, we know from previous proof that $E_i \wedge M_i^l$ implies $\mathsf{C}(M_i)$.
  - Thus only the lifeness part remains open.

GCD Example (Contd)

- Second and third hypotheses (GCD).
  - Prove $\mathsf{C}(E_a)_{+\langle a,b\rangle} \wedge \mathsf{C}(M_a^l) \Rightarrow \mathsf{C}(M_a)$ and $E_a \wedge M_a^l \Rightarrow M_a$.
  - Apply Propositions 4 and 5 to reduce first part to. $\mathsf{C}(E_a) \wedge \mathsf{C}(M_a^l) \Rightarrow \mathsf{C}(M_a)$.
  - Apply Proposition 2 to remove quantifiers from $\mathsf{C}(M_a^l)$ and Proposition 1 to remove Cs.
  - Prove $E_a \wedge \mathit{Init}_a^l \wedge \Box[\mathsf{N}_a^l]_{+\langle a,ai,pca\rangle} \Rightarrow \mathit{Init}_a \wedge \Box[\mathsf{N}_a^l]_a$.
  - Prove $E_a \wedge \mathit{Init}_a^l \wedge \Box[\mathsf{N}_a^l]_{+\langle a,ai,pca\rangle} \wedge \mathsf{WF}_{+\langle a,ai,pca\rangle}(\mathsf{N}_a^l) \Rightarrow \mathsf{WF}_a(\mathsf{N}_a)$
  - Apply Proposition 6 to rewrite lhs of both formulas to canonical form and apply TLA implementation proof.
- Summary
  - Applying propositions in standard sequence, use Decomposition Theorem to reduce decompostional reasoning to ordinary TLA reasoning.

The General Theorem

- Correctness of systems defined inductively:
  - At stage $N+1$, specfications are defined as k copies of specfications of state N.
  - Example: 2^{N+1}-bit multiplier implemented by combining four 2^N bit multipliers.
- General decomposition theorem:
  - If $\models \mathsf{C}(E) \wedge \wedge_{j=1}^{n} \mathsf{C}(M_j) \Rightarrow E_i$
    and $\models \mathsf{C}(E_i)_{+v} \wedge \mathsf{C}(M_i^l) \Rightarrow \mathsf{C}(M_i)$
    and $\models E_i \wedge M_i^l \Rightarrow M_i$
    and v is a tuple of variables including all free variables of M_i
  - Then $\models \mathsf{C}(E)_{+v} \wedge \wedge_{j=1}^{n} \mathsf{C}(M_j^l) \Rightarrow \wedge_{j=1}^{n} \mathsf{C}(M_j)$
    and $\models E \wedge \wedge_{j=1}^{n} M_j^l \Rightarrow \wedge_{j=1}^{n} M_j$
- Both decomposition theorems are equivalent.

Composing Assumption/Guarantee Specifications

- General form:
  - Assertion that system guarantees M under assumption that environment satisfies E.
  - $E \stackrel{+}{\rhd} M$.
  - If environment satisfies E till time n, then system must satisfy M till time $n+1$.
- Composition:
  - Write environment assumptions are safety properties.
  - Write systems's fairness guarantee as conjunction of properties $E_L \Rightarrow \mathsf{WF}_v(\mathsf{A})$ and $E_L \Rightarrow \mathsf{SF}_v(\mathsf{A})$ where E_L is an environment fairness assumption.
  - By Proposition 1, resulting specification is machine-closed (if (P, L) is machine-closed and $L \Rightarrow R$, then (P, R) is machine-closed).

The Composition Theorem

- n a/g specifications $E_j \stackrel{+}{\rightharpoonup\!\triangleright} M_j$.
  - Composition implements $E \stackrel{+}{\rightharpoonup\!\triangleright} M$.
  - Prove $\wedge_{j=1}^{n} (E_j \stackrel{+}{\rightharpoonup\!\triangleright} M_j) \Rightarrow E \stackrel{+}{\rightharpoonup\!\triangleright} M$
- Composition Theorem
  - If $\models \mathsf{C}(E) \wedge \wedge_{j=1}^{n} \mathsf{C}(M_j) \Rightarrow E_i$
    and $\models \mathsf{C}(E)_{+v} \wedge \mathsf{C}(M_j) \Rightarrow \mathsf{C}(M)$
    and $\models E \wedge \wedge_{j=1}^{n} M_j \Rightarrow M$
  - then $\models \wedge_{j=1}^{n} (E_j \stackrel{+}{\rightharpoonup\!\triangleright} M_j) \Rightarrow (E \stackrel{+}{\rightharpoonup\!\triangleright} M)$.
- Hypotheses
  - Proved similar to Decomposition Theorem.
  - Each structured $\models P \wedge \wedge_j Q_j \Rightarrow R$.
  - Each form of specification of complete system.
- Reasoning about a/g specifications reduced to reasoning about complete systems.

Corollary

- Proof that lower-level specification implements a higher-level one.
- Corollary
  - If E is a safety property
    and $\models E_{+v} \wedge \mathsf{C}(M^l) \Rightarrow \mathsf{C}(M)$
    and $\models E \wedge M^l \wedge M$
  - then $\models (E \stackrel{+}{-\!\triangleright} M^l) \Rightarrow (E \stackrel{+}{-\!\triangleright} M)$.
- Fixed evironment assumption E.

Queue Example

- A/G specification $QE \stackrel{+}{\rightharpoonup\!\!\triangleright} QM$.
- Composition of two queues:
  - $QE^{[1]} \stackrel{+}{\rightharpoonup\!\!\triangleright} QM^{[1]}$
  - $QE^{[2]} \stackrel{+}{\rightharpoonup\!\!\triangleright} QM^{[2]}$
  - $QE^{[dbl]} \stackrel{+}{\rightharpoonup\!\!\triangleright} QM^{[dbl]}$
  - Prove $(QE^{[1]} \stackrel{+}{\rightharpoonup\!\!\triangleright} QM^{[1]}) \wedge QE^{[2]} \stackrel{+}{\rightharpoonup\!\!\triangleright} QM^{[2]}$ $\Rightarrow QE^{[dbl]} \stackrel{+}{\rightharpoonup\!\!\triangleright} QM^{[dbl]}$
- Not valid for interleaving representation:
  - First queue spec does not mention o.
  - Second queue spec does not mention i.
  - Conjunction allows simultaneous enqueue action of first queue and dequeue action of second queue.

Queue Example

- Disallow simultaneous changes of component outputs:
  - $G \wedge (QE^{[1]} \overset{+}{\rightharpoondown} QM^{[1]}) \wedge QE^{[2]} \overset{+}{\rightharpoondown} QM^{[2]}$
    $\Rightarrow QE^{[dbl]} \overset{+}{\rightharpoondown} QM^{[dbl]}$
  - $G \equiv \mathit{Disjoint}(\langle i.snd, o.ack \rangle,$
    $\langle z.snd, i.ack \rangle, \langle o.snd, z.ack \rangle)$
- Proof sketched in paper.

Conclusion

- Components of concurrent systems
  - TLA formulas.
- Complete systems.
  - Conjunction of component specfications.
- Open systems.
  - $E \stackrel{+}{\rhd} M$.
  - Environment specification E.
  - Component specifcation M.
- Rules for proving properties of large systems
  - Reasoning about components.
  - Composition and decomposition theorems.