Challenge Problem: Subject-Observer Specification with Component-Interaction Automata

Pavlína Vařeková and Barbora Zimmerova

Faculty of Informatics, Masaryk University
Brno, Czech Republic

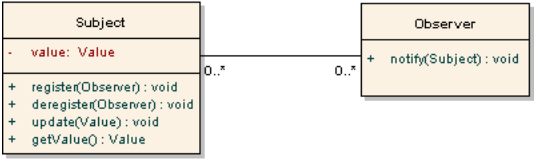
SAVCBS'07, Dubrovnik, Croatia

September 3, 2007

Challenge Problem: Subject-Observer Specification

The problem statement

- Subject-Observer system - many Subjects, many Observers
- Update of a Subject → notification of registered Observers
- When a Subject is notifying Observers, no state changes allowed
- Each Observer is called at most once per state change



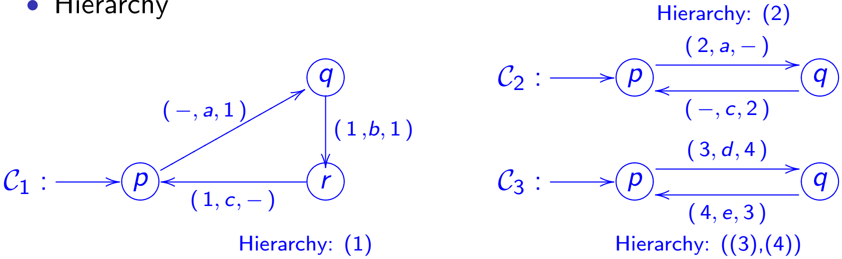
In addition

- We add a possibility of Observers to deregister from Subjects
- The number of Subjects is fixed, number of Observers is not
- Asynchronous updating

Component-interaction automata

A component-Interaction automaton (CI automaton)

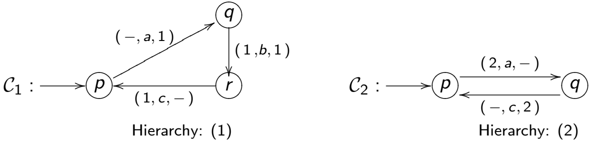
- States (initial)
- Labeled transitions
- Labels (structured - component names, actions)
  - input, output and internal
- Hierarchy

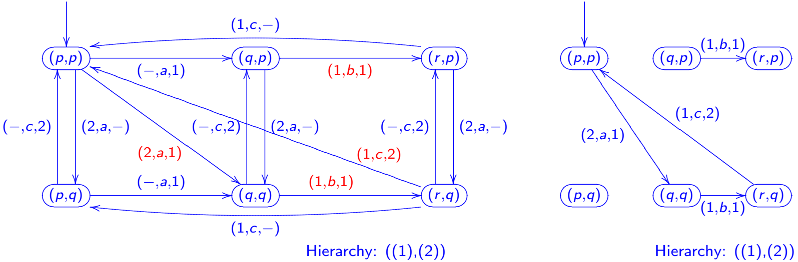


Composition of CI automata

Handshake-like composition via operator $\otimes^{\mathcal{F}}$

→ composite automaton $\mathcal{C} = \otimes^{\mathcal{F}}\{\mathcal{C}_1, \mathcal{C}_2\}$ where $\mathcal{F} = \{(2,a,1),(1,b,1),(1,c,2)\}$

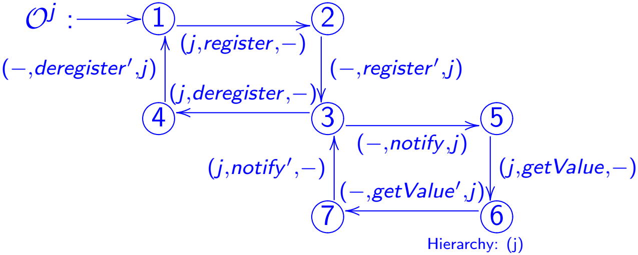




Model with one Subject

Model of an Observer $\mathcal{O}^j$

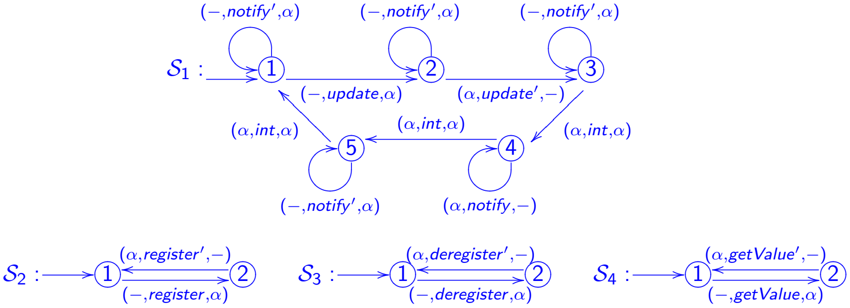
- Models of all Observers $\mathcal{O}^1, \mathcal{O}^2, \ldots$ are the same
- Each method, e.g. `register()`, is assigned a tuple of actions: **register** represents its start, **register'** its return



Model with one Subject

Model of a Subject $\mathcal{S}$

- Subject implements four methods
  → model consists of four parts connected via $\otimes$
- $\mathcal{S} = \otimes\{\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3, \mathcal{S}_4\}$

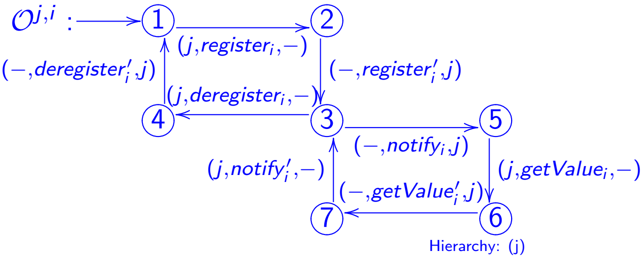


Hierarchy: (α)

Model with several Subjects

Model of an Observer $\mathcal{O}^j$

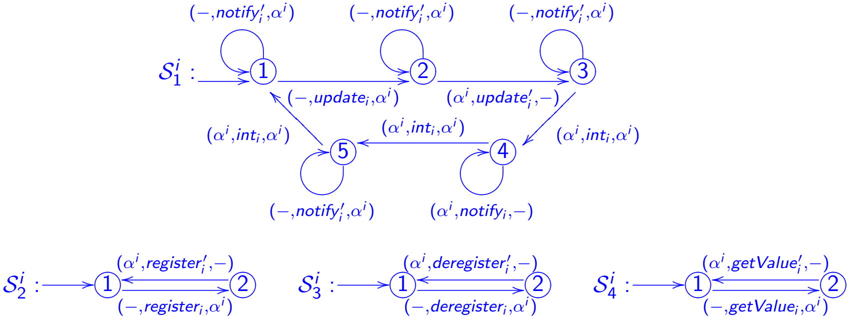
- Suppose n Subjects $\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_n$
- The model of an Observer consists of n identical parts, each for communication with one Subject
- $\mathcal{O}^j = \otimes\{\mathcal{O}^{j,i}\}_{i\in\{1,\ldots,n\}}$



Model with several Subjects

Model of a Subject $\mathcal{S}^i$

- Each model $\mathcal{S}^i$ analogical to $\mathcal{S}$
- $\mathcal{S}^i = \otimes\{\mathcal{S}^i_1, \mathcal{S}^i_2, \mathcal{S}^i_3, \mathcal{S}^i_4\}$

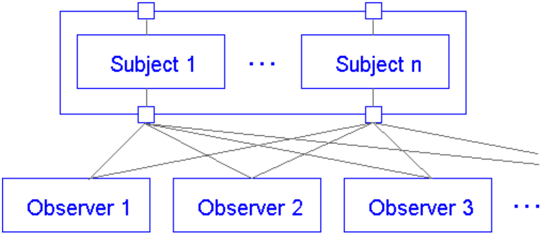


Hierarchy: (α)

Model with several Subjects

The composite model $\mathcal{D}$

- Subjects $\mathcal{S}^1, \mathcal{S}^2, \ldots, \mathcal{S}^n$
  $\rightarrow$ composite Subject $\mathcal{S} = \otimes\{\mathcal{S}^i\}_{i \in \{1,\ldots,n\}}$
- Observers $\mathcal{O}^1, \mathcal{O}^2, \ldots$
- $\mathcal{F}$ realizing the handshake-like composition of these



Verification technique

Complexity of the model $\mathcal{D}$

- Estimate the maximal number of clients that the provider is able to regard w.r.t. observable labels X
- Denote the number $|\mathcal{D}|_X$

Complexity of the temporal property $\{\varphi_i\}_{i\in\mathbb{N}}$

- Find the minimal number m of clients that suffice to violate the property
- Then $\{\varphi_i\}_{i\in\mathbb{N}} \in \mathit{Property}(\mathcal{D}, m)$

A number of clients needed for the verification

- It suffices to verify the model with $0, 1, 2, \ldots, k = |\mathcal{D}|_X + m$ to conclude on the general validity of the property

Verification technique

Problem: In our model, the maximal number of regarded clients $|\mathcal{D}|_X$ is often ∞.

Solution: We introduce the following optimizations

- Move m clients inside the provider $\rightarrow \overline{\mathcal{D}}$
- Narrow the property down to these clients $\rightarrow \{\overline{\varphi}_i\}_{i \in \mathbb{N}}$
- Minimize X used in the computation of $|\mathcal{D}|_X$ to observe only the clients inside the provider $\rightarrow \overline{X}$

Then $\overline{\mathcal{D}_n} \models \overline{\varphi}_n$ iff $\mathcal{D}_{n+m} \models \varphi_{n+m}$ and $\{\overline{\varphi_i}\}_{i \in \mathbb{N}_0} \in Property(\overline{\mathcal{D}}, 0)$. Hence we only need to verify $\{\overline{\varphi}_i\}_{i \in \mathbb{N}}$ on $\overline{\mathcal{D}}_0, \overline{\mathcal{D}}_1, \ldots, \overline{\mathcal{D}}_{|\overline{\mathcal{D}}|_{\overline{X}}}$ and $\{\varphi_i\}_{i \in \mathbb{N}}$ on $\mathcal{D}_0, \mathcal{D}_1, \ldots, \mathcal{D}_{m-1}$.

Property 1

If a run contains infinitely many steps concerning some Observer, then the Observer is infinitely many times enabled to receive notifications.

- Temporal formulas $\{\varphi_i\}_{i\in\mathbb{N}_0}$, $\varphi_i = \bigwedge_{j\leq i} \varphi(\alpha, j)$ where
  $\varphi(\alpha, j) = [\mathcal{G}\,\mathcal{F} \bigvee_{l\in Lab_j} \mathcal{P}(l)] \Rightarrow [\mathcal{G}\,\mathcal{F}\,\mathcal{E}(\alpha, notify_1, j)]$
  $Lab_j = \{(j, register_1, \alpha), (\alpha, register'_1, j), (j, deregister_1, \alpha), (\alpha, deregister'_1, j), \ldots\}$
- If $\pi \not\models \varphi_i$ then $\exists j \in \mathbb{N} : \pi \not\models \varphi(\alpha, j)$
  Hence it suffices to observe one client to confirm the violation
  $\{\varphi_i\}_{i\in\mathbb{N}_0} \in Property(\mathcal{D}, 1)$
- **Optimization:** We modify the model to $\overline{\mathcal{D}}$ by moving Observer β inside the provider, then $\overline{X} = Lab_\beta$ and $|\overline{\mathcal{D}}_{\overline{X}}| = 0$.
- The verification (2 models) confirms that the property is valid!

Property 2

After any update, each Observer receives at most one notification about value change. This reflects that each Observer is called at most once per state change.

- Temporal formulas $\{\varphi_i\}_{i\in\mathbb{N}_0}$, $\varphi_i = \bigwedge_{j\leq i} \neg\mathcal{F}\,\varphi(\alpha,j)$ where
  $\varphi(\alpha,j) = \mathcal{P}(\alpha, notify_1, j) \wedge \mathcal{X}\,[\neg\mathcal{P}(-, update_1, \alpha)\;\mathcal{U}\;\mathcal{P}(\alpha, notify_1, j)]$
  Modified to $\varphi(\alpha,j) = \mathcal{P}(\alpha, notify_1, j) \wedge [\neg\mathcal{P}(-, update_1, \alpha)\;\mathcal{U}$
  $\{\mathcal{P}(j, notify_1', \alpha) \wedge [\neg\mathcal{P}(-, update_1, \alpha)\;\mathcal{U}\;\mathcal{P}(\alpha, notify_1, j)]\}]$
- Again $\{\varphi_i\}_{i\in\mathbb{N}_0} \in Property(\mathcal{D}, 1)$
- **Optimization:** We modify the model to $\overline{\mathcal{D}}$ by moving Observer β inside the provider, then
  $\overline{X} = \{(-, update_1, \alpha), (\alpha, notify_1, \beta), (\beta, notify_1', \alpha)\}$ and $|\overline{\mathcal{D}}_{\overline{X}}| = 1$.
- The verification (3 models) confirms that the property is valid!

Property 3

If one of the registered Observers receives a notification and some other Observer is also ready to receive one (is registered and has not receive it yet), it will receive the notification too.

- Formulas $\{\varphi_i\}_{i\in\mathbb{N}_0}$, $\varphi_i = \bigwedge_{j_1,j_2\leq i, j_1\neq j_2} \varphi(\alpha, j_1, j_2)$ where $\varphi(\alpha, j_1, j_2) = \mathcal{G}\left[(\mathcal{P}(\alpha, \mathit{notify}_1, j_1) \wedge \mathcal{E}(\alpha, \mathit{notify}_1, j_2)) \Rightarrow (\mathit{true}\ \mathcal{U}\ \mathcal{P}(\alpha, \mathit{notify}_1, j_2))\right]$
- It suffice to observe two distinct Observers, hence $\{\varphi_i\}_{i\in\mathbb{N}_0} \in \mathit{Property}(\mathcal{D}, 2)$
- **Optimization:** Two Observers β, $\beta\beta$ need to be moved inside the provider. Then $\overline{X}$ regards only these two, and $|\mathcal{D}_{\overline{X}}| = 0$.
- The verification (3 models) shows the property is not valid!

Conclusion

Summary of the talk

- Solution to the *Subject-Observer challenge problem*
- Specification via Component-Interaction automata
- Verification via a technique presented at the workshop for verification of systems with a dynamic number of components

Thank you

Thank you for your attention