MIA 2.0: Richer Interface Automata

with Optimistic and Pessimistic Compatibility

Gerald Lüttgen
Software Technologies Research Group
University of Bamberg, Germany

(Joint work with Walter Vogler, University of Augsburg, Germany)

MIA 2.0: Further Improvements over IOMTS

- In our IA-inspired optimistic approach – MIA_{opt}
  - Making our MIA-setting more practical
  - Exploring the limitations of the MIA-setting
- **Disjunctive must-transitions not only for outputs but also for**
  - *Inputs* – more relaxed meaning of input-determinism
  - *Internal action τ* – more natural encoding of disjunction
- **MIA-refinement as a `better´ IOMTS-refinement**
  - Also considering *τ-must-transitions* on the specification side
  - Permitting *alphabet extension* on the implementation side
- **Alphabet extension is a crux in MIA_{opt}**
  - Exploring Bauer et al.'s *pessimistic view of compatibility* – MIA_{pes}

MIA_{opt}: Weak Transition Relation

- *Not done before in the presence of disjunctive transitions*
  - To the best of our knowledge
- Weak may-transition relation ::::::> as usual
  - Leading and trailing τ-may-transitions
- Weak output-must-transition relation as the least relation s.t.
  - $p = \varepsilon \Rightarrow \{p\}$
  - $p = \varepsilon \Rightarrow P'$, $p' \in P'$ and $p' - \tau \rightarrow P''$ implies $p = \varepsilon \Rightarrow (P' \setminus \{p'\}) \cup P''$
  - **$p = \varepsilon \Rightarrow P' = \{p_1, \ldots, p_n\}$ and $\forall j.\ p_j - o \rightarrow P_j$ implies $p = o \Rightarrow \bigcup_j P_j$**
  - $p = o \Rightarrow P'$, $p' \in P'$ and $p' - \tau \rightarrow P''$ implies $p = o \Rightarrow (P' \setminus \{p'\}) \cup P''$

MIA_{opt}: MIA-refinement

- Refinement relation as before, but in addition
  - **Considering τ-must-transitions on the specification side**
  - *Permitting alphabet extensions on the implementation side*

- MIA-refinement ≤

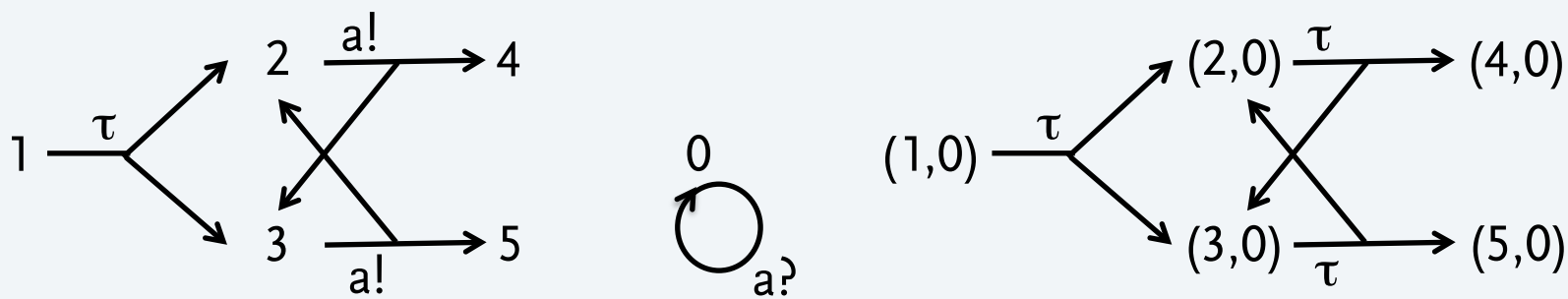
  Given MIAs P, Q s.t. $I_P \supseteq I_Q$, $O_P \supseteq O_Q$ and $p \leq q$

  1. $q - i \rightarrow Q'$ implies $\exists P'.\ p - i \rightarrow P'$ and $\forall p' \in P'\ \exists q' \in Q'.\ p' \leq q'$
  2. **$q - \tau \rightarrow Q'$ implies $\exists P'.\ p = \varepsilon \Rightarrow P'$ and $\forall p' \in P'\ \exists q' \in Q'.\ p' \leq q'$**
  3. $q - o \rightarrow Q'$ implies $\exists P'.\ p = o \Rightarrow P'$ and $\forall p' \in P'\ \exists q' \in Q'.\ p' \leq q'$

  4. $p - i \rightarrow P'$ and $i \notin I_Q$ implies $\forall p' \in P'.\ p' \leq q$
  5. $p \cdots \tau \cdots\rightarrow p'$ implies $\exists q'.\ q \cdots \varepsilon \cdots\rightarrow q'$ and $p' \leq q'$
  6. $p \cdots o \cdots\rightarrow p'$ and $o \in O_Q$ implies $\exists q'.\ q \cdots o \cdots\rightarrow q'$ and $p' \leq q'$
  7. $p \cdots o \cdots\rightarrow p'$ and $o \notin O_Q$ implies $\exists q'.\ q \cdots \varepsilon \cdots\rightarrow q'$ and $p' \leq q'$

MIA_{opt}: Parallel Composition

- Compatibility as before, but one new transition rule is needed
  - *Let action a be an input of p and an output of q, or vice versa*
  - *(Must3)* (p,q) – τ –> P'×Q' if p – a –> P' and q – a –> Q'
- Compositionality result still holds
  - *Provided an alphabet extension does not result in new communications*
- Proof requires a subtle lemma for weak must-transitions
  - If p = a => P' and q – a –> Q' then (p,q) = ε => R for some R⊆P'×Q'
  - *Observe that R = P'×Q' does not hold in general*



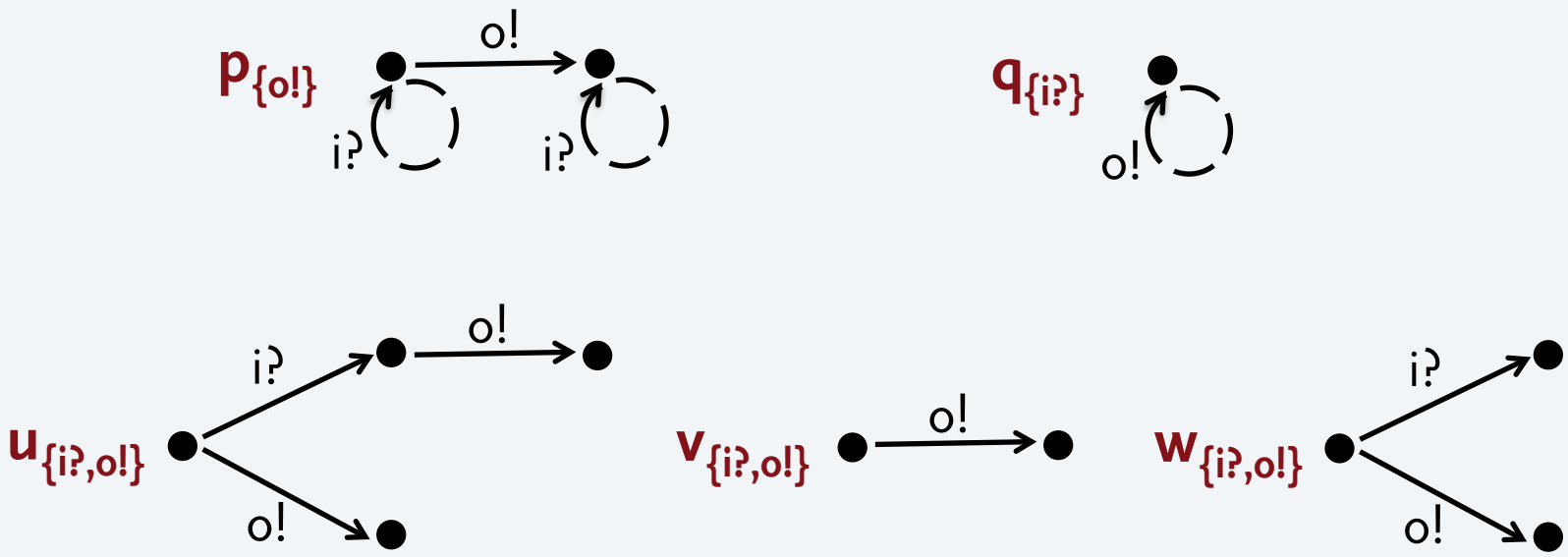
MIA_{opt}: Disjunction & Conjunction

- Simplifying assumption, for the moment
  - **Operands have the same input/output alphabets**

- Disjunction ∨
  - *More intuitive encoding, now using disjunctive τ- and input-must-transitions*
    - *(Must)* $p \vee q - \tau \rightarrow \{p, q\}$
    - *(IMust)* $p \vee q - i \rightarrow P' \cup Q'$ if $p - i \rightarrow P'$ and $q - i \rightarrow Q'$
    - Plus the underlying may-transitions
  - ∨ is the least upper bound wrt. ≤, which implies compositionality

- Conjunction ∧
  - *As before, where must-τs are treated in the same way as must-outputs*
  - ∧ is the greatest lower bound wrt. ≤, which implies compositionality

MIA_{opt}: Dissimilar Alphabets & Conjunction

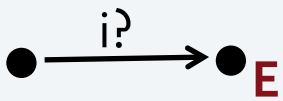
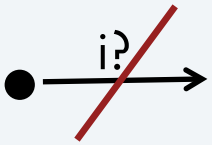


- *Extending alphabets morally means to add `neutral´ may-loops*
  - Here, **p∧q** should intuitively be implementable by **u** and **v** but not **w**
  - **No MIA_{opt}** has **u** and **v** but not **w** as implementations, since it cannot have an initial i?-transition because of **v**
- In MIA_{opt} one cannot forbid an input in some state – *crux!*

The Pessimistic Approach – MIA_{pes}

- Advocated by Bauer, Hennicker and co-workers (MIO [BMSH10])
  - *Pessimistic view of compatibility in an MTS-based interface theory*
  - **Our contributions:** (1) conjunction and disjunction operators, (2) disjunctive must-transitions, (3) alphabet extension
- Relaxed MIA
  - Defined as our original MIA but **no requirement for input-determinism** and **no requirement that may-inputs are must-inputs**
- Standard modal-refinement on relaxed MIA, i.e., $p \leq q$ implies
  - *Must-input of q matched by p*
    - Possibly with **trailing-only** must-τs
  - *Must-output or must-τ of q matched by p*
    - Possibly with leading and/or trailing must-τs
  - *May-action of p matched by q*
    - Possibly with leading and/or trailing may-τs

MIA_{pes}: Compatibility & Parallel Composition

- Restrictive form of compatibility
  - *If any error state in a parallel composition can be reached via **any** action (including an input), then this composition is not defined*
  - This approach distinguishes between  and 

- Parallel composition operator defined as before
  - Compositionality of $\leq$ in MIA_{pes} holds, as to be expected
- Crucial trade-off here
  - **Classic view of may-inputs** (i.e., input allowed or prohibited) is possible for a large class of systems that must not be input-deterministic
  - *But pessimistic view of compatibility means that* **much fewer parallel compositions are permitted**, *which is bad for component-based design*

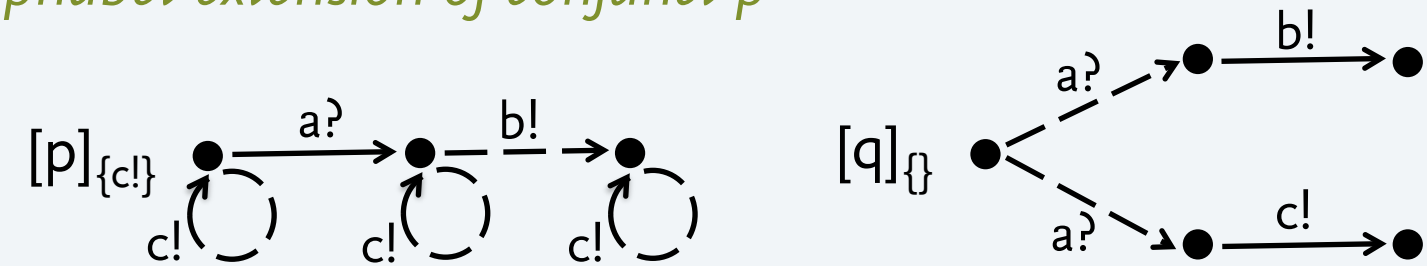
MIA_{pes}: Disjunction & Conjunction

- First defined on MIAs with the same input/output alphabets
  - Disjunction exactly as in MIA_{opt}
  - Conjunction simpler as in MIA_{opt}
    - Inputs are treated the same way as outputs and τ
- Lifted to MIAs with dissimilar alphabets
  - *Via alphabet extension operator* $[p]_A$ *(for A disjoint to p's alphabet), which adds an a-may-loop to every state of p, for every a in A*
  - $[]_A$ is monotonic wrt. $\leq$
  - $[]_A$ is a homorphism for conjunction
- Results, as to be expected
  - $\vee$ is least upper bound *and* $\leq$ is compositional for $\vee$
  - $\wedge$ is greatest lower bound *and* $\leq$ is compositional for $\wedge$

MIA_{pes}: Conjunction Example

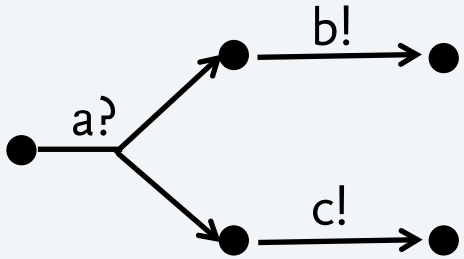
- *Conjuncts with dissimilar alphabets*

- *Alphabet extension of conjunct p*



- *Conjunctive composition*

$$p \wedge q = [p]_{\{c!\}} \wedge [q]_{\{\}}$$



Summary

Optimistic Approach

- IA, IOMTS, MIA_{opt}
- **True open-systems view**
  - Generous compatibility
- *IA-style modal refinement*
  - Inputs: required, allowed
  - Input-determinism
- *Alphabet extension*
  - Conjunction and disjunction restricted to same alphabets

Pessimistic Approach

- MIO, MIA_{pes}
- **Blurred open-systems view**
  - Restrictive compatibility
- *Standard modal refinement*
  - Inputs: required, allowed, **forbidden**
  - No input-determinism
- *General alphabet extension*
  - Alphabet extension operator

Conclusions & Future Work

- **MIA is a well-founded interface theory that allows one to**
  - Enforce outputs
  - *Express disjunctive must-transitions*
  - Specify non-deterministic behaviour
  - Abstract from internal computation
  - Interpret compatibility optimistically or pessimistically
  - *Compose interfaces also conjunctively and disjunctively*
  - *Extend alphabets while refining*

- Some questions left to future work
  - Are there `clean´ interface theories in-between the optimistic and pessimistic approaches?
  - *Is there a possibility to allow may-inputs while maintaining a true open-systems view?*

Selected Literature

- L. de Alfaro, T. Henzinger. *Interface-based design*. In Engineering Theories of Software-Intensive Systems. NATO Science Series 195. Springer, 2005.
- S. Bauer, P. Mayer, A. Schroeder, R. Hennicker. *On weak modal compatibility, refinement, and the MIO Workbench*. In TACAS '10, LNCS 6015, pp. 175-189. Springer, 2010.
- K. Larsen, U. Nyman, A. Wasowski. *Modal I/O automata for interface and product line theories*. In ESOP '07. LNCS 4421, pp. 64-79. Springer, 2007.
- G. Lüttgen, W. Vogler. *Modal Interface Automata*. In TCS '12. LNCS 7604, pp. 265-279. Springer, 2012. Extended version to appear in the LMCS journal.
- J. Raclet, E. Badouel, A. Benveniste, B. Caillaud, A. Legay, R. Passerone. *A modal interface theory for component-based design*. Fund. Inform. 107:1-32, 2011.