Automated Component-Based Verification

Dimitra Giannakopoulou and Corina Păsăreanu
CMU / NASA Ames Research Center
component-based development

- component-based verification, for increased scalability, at design level
- early detection of integration problems
- use design level artifacts to improve/aid coding and testing

![Component-based development diagram]

- cost of detecting/fixing defects increases
- integration issues handled early
<table>
<thead>
<tr>
<th>structure</th>
</tr>
</thead>
<tbody>
<tr>
<td>part 1 (Dimitra)</td>
</tr>
<tr>
<td>assume-guarantee reasoning</td>
</tr>
<tr>
<td>computing assumptions</td>
</tr>
<tr>
<td>learning assumptions</td>
</tr>
<tr>
<td>discussion</td>
</tr>
<tr>
<td>lunch</td>
</tr>
<tr>
<td>part 3 (Dimitra)</td>
</tr>
<tr>
<td>component interfaces</td>
</tr>
<tr>
<td>compositional JavaPathfinder</td>
</tr>
<tr>
<td>examples</td>
</tr>
<tr>
<td>discussion</td>
</tr>
</tbody>
</table>
void add(Object o) {
    buffer[head] = o;
    head = (head+1)%size;
}

Object take() {
    ...
    tail=(tail+1)%size;
    return buffer[tail];
}

program / model

model checker

property

always(ϕ or ψ)

YES (property holds)

NO + counterexample:
(provides a violating execution)
model checking vs. testing

testing

model checking
compositional verification
Prof. Howard Barringer (Univ. of Manchester)
Colin Blundell (Upenn, IBM Research)
Jamieson Cobleigh (UMass, MathWorks)
Michael Emmi (UCLA)
Mihaela Gheorgiu (Univ. of Toronto, JPL)
Chang-Seo Park (UC Berkeley)
Suzette Person (Univ. of Nebraska, NASA Langley)
Rishabh Singh (MIT)
does system made up of $M_1$ and $M_2$ satisfy property $P$?

- check $P$ on entire system: too many states!
- use system’s natural decomposition into components to break-up the verification task
- check components in isolation:
  - does $M_1$ satisfy $P$?
“when we try to pick out anything by itself, we find it hitched to everything else in the universe”

John Muir
assumes-guarantee reasoning

introduces assumptions / reasons about triples:

\[ \langle A \rangle M \langle P \rangle \]
is true if whenever \( M \) is part of a system that satisfies \( A \), then the system must also guarantee \( P \)

simplest assume-guarantee rule (\textsc{Asym}): 

1. \( \langle A \rangle M_1 \langle P \rangle \)
2. \( \langle true \rangle M_2 \langle A \rangle \)

\[ \langle true \rangle M_1 \parallel M_2 \langle P \rangle \]

“discharge” the assumption
examples of assumptions

- will not invoke “close” on a file if “open” has not previously been invoked
- accesses to shared variable “X” must be protected by lock “L”
- **(rover executive)** whenever thread “A” reads variable “V”, no other thread can read “V” before thread “A” clears it first
- **(spacecraft flight phases)** a docking maneuver can only be invoked if the launch abort system has previously been jettisoned from the spacecraft
assume-guarantee reasoning

how do we come up with the assumption?
components modeled as finite state machines (FSM)
  - FSMs assembled with parallel composition operator “||”
    • synchronizes shared actions, interleaves remaining actions

a safety property P is a FSM
  - P describes all legal behaviors in terms of its alphabet
  - P_{err} — complement of P
    • determinize & complete P with an “error” state;
    • bad behaviors lead to error
  - component M satisfies P iff error state unreachable in (M || P_{err})

assume-guarantee reasoning
  - assumptions and guarantees are FSMs
  - $\langle A \rangle M \langle P \rangle$ holds iff error state unreachable in $(A || M || P_{err})$
require in and out to alternate (property Order)
parallel composition

Input

||

Output

in  send

ack

send  out

ack
property satisfaction

crex. 1: \((l_0, o_0)\) out \((l_0, o_{\text{error}})\)

crex. 2: \((l_0, o_0)\) in \((l_1, o_1)\) send \((l_2, o_1)\) out \((l_2, o_0)\) out \((l_2, o_{\text{error}})\)
assume-guarantee reasoning

**Input**

```
Input
\[
\begin{array}{c}
0 & \xrightarrow{\text{in}} & 1 & \xrightarrow{\text{send}} & 2 \\
\scriptstyle\text{ack} & & & & \\
\end{array}
\]
```

**Assumption**

```
Assumption
\[
\begin{array}{c}
0 & \xrightarrow{\text{send}} & 1 \\
\scriptstyle\text{ack} & & \\
0 & \xrightarrow{\text{send}} & 1 \\
\scriptstyle\text{out} & & \\
\end{array}
\]
```

**Order**

```
Order_{\text{err}}
\[
\begin{array}{c}
0 & \xrightarrow{\text{in}} & 1 \\
0 & \xrightarrow{\text{out}} & \phantom{\text{in}} \\
0 & \xrightarrow{\text{out}} & \phantom{\text{in}} \\
\end{array}
\]
```

**Crex 1:** \((I_0, A_0, O_0) \xrightarrow{\text{out}} X\)

**Crex 2:** \((I_0, A_0, O_0) \xrightarrow{\text{in}} (I_1, A_0, O_1) \xrightarrow{\text{send}} (I_2, A_1, O_1) \xrightarrow{\text{out}} (I_2, A_0, O_0) \xrightarrow{\text{out}} X\)
given component M, property P, and the interface of M with its environment, generate the weakest environment assumption WA such that: \( \langle \text{WA} \rangle M \langle P \rangle \) holds

weakest means that for all environments E:

\[ \langle \text{true} \rangle M \parallel E \langle P \rangle \iff \langle \text{true} \rangle E \langle \text{WA} \rangle \]
weakest assumption in AG reasoning

1. $\langle A \rangle M_1 \langle P \rangle$
2. $\langle true \rangle M_2 \langle A \rangle$

$\langle true \rangle M_1 || M_2 \langle P \rangle$

 weakest assumption makes rule complete

for all E, $\langle true \rangle M || E \langle P \rangle$ IFF $\langle true \rangle E \langle WA \rangle$

$\langle WA \rangle M_1 \langle P \rangle$ holds (WA could be false)

$\langle true \rangle M_2 \langle WA \rangle$ holds implies $\langle true \rangle M_1 || M_2 \langle P \rangle$ holds

$\langle true \rangle M_2 \langle WA \rangle$ not holds implies $\langle true \rangle M_1 || M_2 \langle P \rangle$ not holds
STEP 1: composition, hiding, minimization

STEP 2: backward propagation of error along $\tau$ transitions

STEP 3: property extraction (subset construction & completion)

property true! (all environments)

property false! (all environments)

assumption
step 1: composition & hiding

Input $\parallel$ Order$_{err}$ \{in\}

Diagram with states and transitions:
- States: 0, 1, 2, 3, 4, 5
- Transitions:
  - Input $\rightarrow$ send $\rightarrow$ Output
  - 0 $\rightarrow$ send $\rightarrow$ 3
  - 1 $\rightarrow$ send $\rightarrow$ 3
  - 2 $\rightarrow$ send $\rightarrow$ 3
  - 3 $\rightarrow$ out $\rightarrow$ 0
  - 4 $\rightarrow$ ack $\rightarrow$ 1
  - 5 $\rightarrow$ ack $\rightarrow$ 1
  - 1 $\rightarrow$ out $\rightarrow$ 0
  - 3 $\rightarrow$ out $\rightarrow$ 0
  - 3 $\rightarrow$ out $\rightarrow$ 0
  - 3 $\rightarrow$ out $\rightarrow$ 0
  - 3 $\rightarrow$ out $\rightarrow$ 0

Symbols:
- $\tau$ (tau): Holds for internal transitions.
- $\tau_{in}$: Internal transition from 0 to 1.
- $\tau_{out}$: Internal transition from 3 to 0.
step 2: error propagation

Diagram showing a network with nodes labeled 0 to 4, with arrows indicating the flow of messages labeled 'out', 'τ', 'send', and 'ack'.
step 3: subset construction
step 3: subset construction
step 3: property construction
weakest assumption in AG reasoning

1. \( \langle A \rangle M_1 \langle P \rangle \)
2. \( \langle true \rangle M_2 \langle A \rangle \)

\( \langle true \rangle M_1 \ || \ M_2 \langle P \rangle \)

weakest assumption makes rule complete

\( \langle WA \rangle M_1 \langle P \rangle \) holds (WA could be false)
\( \langle true \rangle M_2 \langle WA \rangle \) holds implies \( \langle true \rangle M_1 \ || \ M_2 \langle P \rangle \) holds
\( \langle true \rangle M_2 \langle WA \rangle \) not holds implies \( \langle true \rangle M_1 \ || \ M_2 \langle P \rangle \) not holds
iterative solution + intermediate results

$L^*$ learns unknown regular language $U$ (over alphabet $\Sigma$) and produces minimal DFA $A$ such that $L(A) = U$ 
($L^*$ originally proposed by Angluin)
L* learner

(queries)
should word w be included in L(A)?

(conjectures)
here is an A – is L(A) = U?

yes /
no

yes!

no: word w should (not) be in L(A)
oracle for WA in assume-guarantee reasoning

1. $\langle A \rangle M_1 \langle P \rangle$
2. $\langle true \rangle M_2 \langle A \rangle$

$s$ is a string

$s \ Kendrick\ M_1 \langle P \rangle$

$\langle s \rangle M_1 \langle P \rangle$

$s$ is simulated on $M_1 || P_{err}$

$\langle A \rangle M_1 \langle P \rangle$

Conjecture $A_i$

$\langle A_i \rangle M_1 \langle P \rangle$

(model check)

$\langle true \rangle M_2 \langle A_i \rangle$

$\langle true \rangle M_2 \langle A_i \rangle$

$\langle true \rangle M_1 || M_2 \langle P \rangle$ holds

$\langle true \rangle M_1 || M_2 \langle P \rangle$ holds implies $\langle true \rangle M_1 || M_2 \langle P \rangle$ holds

$\langle true \rangle M_2 \langle WA \rangle$ does not hold implies $\langle true \rangle M_1 || M_2 \langle P \rangle$ does not hold
characteristics

assumptions conjectured by L* are not comparable semantically

- terminates with *minimal* automaton $A$ for $U$
- generates DFA candidates $A_i: |A_1| < |A_2| < \ldots < |A|$
- produces at most $n$ candidates, where $n = |A|$
- # queries: $O(kn^2 + n \log m)$,
  - $m$ is size of largest counterexample, $k$ is size of alphabet
- for assume-guarantee reasoning, may terminate early with a smaller assumption than the weakest
example

we check: \langle\text{true}\rangle \text{Input} \parallel \text{Output} \langle\text{Order}\rangle

M_1 = \text{Input}, M_2 = \text{Output}, P = \text{Order}

assumption alphabet: \{\text{send, out, ack}\}
### Queries

**Input**
- **in**
- **send**
- **ack**

**Order**
- **in**
- **out**
- **send**
- **ack**

**Output**
- **send**
- **out**
- **ack**

<table>
<thead>
<tr>
<th>Table $T$</th>
<th>$\lambda$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S$</td>
<td>$\lambda$</td>
</tr>
<tr>
<td></td>
<td>true</td>
</tr>
<tr>
<td></td>
<td>false</td>
</tr>
<tr>
<td>$S \cdot \Sigma$</td>
<td>ack</td>
</tr>
<tr>
<td></td>
<td>true</td>
</tr>
<tr>
<td>$S \cdot \Sigma$</td>
<td>out</td>
</tr>
<tr>
<td></td>
<td>false</td>
</tr>
<tr>
<td>$S \cdot \Sigma$</td>
<td>send</td>
</tr>
<tr>
<td></td>
<td>true</td>
</tr>
<tr>
<td>$S \cdot \Sigma$</td>
<td>out, ack</td>
</tr>
<tr>
<td></td>
<td>false</td>
</tr>
<tr>
<td>$S \cdot \Sigma$</td>
<td>out, out</td>
</tr>
<tr>
<td></td>
<td>false</td>
</tr>
<tr>
<td>$S \cdot \Sigma$</td>
<td>out, send</td>
</tr>
<tr>
<td></td>
<td>false</td>
</tr>
</tbody>
</table>

$S = \text{set of prefixes}$

$E = \text{set of suffixes}$
S = set of prefixes
E = set of suffixes

**Table T**

<table>
<thead>
<tr>
<th>S</th>
<th>E</th>
<th>λ</th>
</tr>
</thead>
<tbody>
<tr>
<td>S · Σ</td>
<td>ack</td>
<td>true</td>
</tr>
<tr>
<td></td>
<td>out</td>
<td>false</td>
</tr>
<tr>
<td></td>
<td>send</td>
<td>true</td>
</tr>
<tr>
<td></td>
<td>out, ack</td>
<td>false</td>
</tr>
<tr>
<td></td>
<td>out, out</td>
<td>false</td>
</tr>
<tr>
<td></td>
<td>out, send</td>
<td>false</td>
</tr>
</tbody>
</table>

**Order**

in → send → out, send

2 states – error state omitted

Assumption A₁

counterexamples add to S
conjectures

Oracle 1: \( \langle A_1 \rangle \) Input \( \langle \text{Order} \rangle \)

Counterexample:
\[ c = \langle \text{in}, \text{send}, \text{ack}, \text{in} \rangle \]

Return to \( L^* \):
\[ c \uparrow \Sigma = \langle \text{send}, \text{ack} \rangle \]

Oracle 2:
\[ \langle \text{true} \rangle \) Output \( \langle A_2 \rangle \) True

property \( \text{Order} \) holds on \( \text{Input} || \text{Output} \)
please ask LOTS of questions!
Automated Component-Based Verification

part II

Dimitra Giannakopoulou and Corina Păsăreanu
CMU / NASA Ames Research Center
Recap from part I

- Compositional Verification
- Assume-guarantee reasoning
- Weakest assumption
- Learning framework for reasoning about 2 components
compositional verification

- Check P on entire system: too many states!
- Use the natural decomposition of the system into its components to break-up the verification task
- Check components in isolation:
  - Does $M_1$ satisfy P?
  - Typically a component is designed to satisfy its requirements in specific contexts / environments
- Assume-guarantee reasoning:
  - Introduces assumption A representing $M_1$’s “context”
assume-guarantee reasoning

- Reason about triples:
  \[ \langle A \rangle M \langle P \rangle \]
  The formula is *true* if whenever \( M \) is part of a system that satisfies \( A \), then the system must also guarantee \( P \)

- Simplest assume-guarantee rule – ASYM

1. \[ \langle A \rangle M \langle P \rangle \]
2. \[ \langle true \rangle M_2 \langle A \rangle \]
\[ \langle true \rangle M_1 \parallel M_2 \langle P \rangle \]

How do we come up with the assumption \( A \)?
(usually a difficult manual process)

**Solution:** synthesize \( A \) automatically
the weakest assumption

- Given component M, property P, and the interface of M with its environment, generate the **weakest** environment assumption *WA* such that: $\langle WA \rangle M \langle P \rangle$ holds

- Weakest means that for all environments E:

  $\langle true \rangle M || E \langle P \rangle$ IFF $\langle true \rangle E \langle WA \rangle$
STEP 1: composition, hiding, minimization

property true!
(all environments)

STEP 2: backward propagation of error along $\tau$ transitions

property false!
(all environments)

STEP 3: property extraction (subset construction & completion)

assumption
Use an off-the-shelf learning algorithm to build appropriate assumption for rule ASYM

1. $\langle A \rangle \ M_1 \ \langle P \rangle$
2. $\langle \text{true} \rangle \ M_2 \ \langle A \rangle$

$\langle \text{true} \rangle \ M_1 \| M_2 \ \langle P \rangle$

- Process is *iterative*
- Assumptions are generated by querying the system, and are gradually refined
- Queries are answered by model checking
- Refinement is based on counterexamples obtained by model checking
- Termination is guaranteed
learning assumptions

- Use $L^*$ to generate candidate assumptions
- $\alpha A = (\alpha M_1 \cup \alpha P) \cap \alpha M_2$

Model Checking
1. $\langle A \rangle M_1 \langle P \rangle$
2. $\langle \text{true} \rangle M_2 \langle A \rangle$

\[ \langle \text{true} \rangle M_1 \parallel M_2 \langle P \rangle \]

- Guaranteed to terminate
- Reaches weakest assumption or terminates earlier
part II

- compositional verification
- assume-guarantee reasoning
- weakest assumption
- learning framework for reasoning about 2 components

extensions:
- reasoning about $n > 2$ components
- symmetric and circular assume-guarantee rules
- alphabet refinement
To check if $M_1 || M_2 || \ldots || M_n$ satisfies $P$
- decompose it into $M_1$ and $M'_2 = M_2 || \ldots || M_n$
- apply learning framework recursively for $2^{nd}$ premise of rule
- $A$ plays the role of the property

1. $\langle A \rangle M_1 \langle P \rangle$
2. $\langle true \rangle M_2 || \ldots || M_n \langle A \rangle$

\[ \langle true \rangle M_1 || M_2 \ldots || M_n \langle P \rangle \]

At each recursive invocation for $M_j$ and $M'_j = M_{j+1} || \ldots || M_n$
- use learning to compute $A_j$ such that
  - $\langle A_i \rangle M_j \langle A_{j-1} \rangle$ is true
  - $\langle true \rangle M_{j+1} || \ldots || M_n \langle A_i \rangle$ is true
- Model derived from Mars Exploration Rover (MER) Resource Arbiter
  - Local management of resource contention between resource consumers (e.g. science instruments, communication systems)
  - Consists of \( k \) user threads and one server thread (arbiter)

- Checked mutual exclusion between resources
  - E.g. driving while capturing a camera image are mutually incompatible

- Compositional verification scaled to >5 users vs. monolithic verification ran out of memory [SPIN’06]
recursive invocation

Compute $A_1 \ldots A_5$ s.t.

\[ \langle A_1 \rangle U_1 \langle P \rangle \]
\[ \langle \text{true} \rangle U_2 \parallel U_3 \parallel U_4 \parallel U_5 \parallel \text{ARB} \langle A_1 \rangle \]
\[ \langle A_2 \rangle U_2 \langle A_1 \rangle \]
\[ \langle \text{true} \rangle U_3 \parallel U_4 \parallel U_5 \parallel \text{ARB} \langle A_2 \rangle \]
\[ \langle A_3 \rangle U_3 \langle A_2 \rangle \]
\[ \langle \text{true} \rangle U_4 \parallel U_5 \parallel \text{ARB} \langle A_2 \rangle \]
\[ \langle A_4 \rangle U_4 \langle A_3 \rangle \]
\[ \langle \text{true} \rangle U_5 \parallel \text{ARB} \langle A_4 \rangle \]
\[ \langle A_5 \rangle U_5 \langle A_4 \rangle \]
\[ \langle \text{true} \rangle \text{ARB} \langle A_5 \rangle \]

Result:

\[ \langle \text{true} \rangle U_1 \parallel \ldots \parallel U_5 \parallel \text{ARB} \langle P \rangle \]
symmetric rules: motivation

\[ M_1 = \text{Input}, \; M_2 = \text{Output}, \; P = \text{Order} \]

\[ A_1: \]
\[ \begin{align*}
\text{ack} & \quad \text{send} \\
\text{send} & \quad \text{ack}
\end{align*} \]

\[ A_2: \]
\[ \begin{align*}
\text{send} & \quad \text{ack} \\
\text{ack} & \quad \text{out, send}
\end{align*} \]

\[ A_4: \]
\[ \begin{align*}
\text{send} & \quad \text{out} \\
\text{ack, out, send} & \quad \text{ack}
\end{align*} \]

\[ M_1 = \text{Output}, \; M_2 = \text{Input}, \; P = \text{Order} \]

\[ A_1: \]
\[ \begin{align*}
\text{ack} & \quad \text{in} \\
\text{in} & \quad \text{ack}
\end{align*} \]

\[ A_2: \]
\[ \begin{align*}
\text{in} & \quad \text{ack} \\
\text{ack} & \quad \text{send}
\end{align*} \]

\[ A_4: \]
\[ \begin{align*}
\text{send} & \quad \text{ack, out, send} \\
\text{ack, out, send} & \quad \text{send}
\end{align*} \]
symmetric rules

- Assumptions for both components at the same time
  - Early termination; smaller assumptions
- Example symmetric rule – SYM

1. \langle A_1 \rangle M_1 \langle P \rangle
2. \langle A_2 \rangle M_2 \langle P \rangle
3. \text{L}(\text{coA}_1 \parallel \text{coA}_2) \subseteq \text{L}(P)

\langle true \rangle M_1 \parallel M_2 \langle P \rangle

- coA_i = complement of A_i, for i=1,2
- Requirements for alphabets:
  - \( \alpha P \subseteq \alpha M_1 \cup \alpha M_2 \); \( \alpha A_i \subseteq (\alpha M_1 \cap \alpha M_2) \cup \alpha P \), for i =1,2
- The rule is sound and complete
- Completeness needed to guarantee termination
- Straightforward extension to \( n \) components

Ensure that any common trace ruled out by both assumptions satisfies P.
learning framework for rule SYM

- \( A_1 \) \( \langle A_1 \rangle M_1 \langle P \rangle \)
- \( A_2 \) \( \langle A_2 \rangle M_2 \langle P \rangle \)
- \( L^* \)
- \( L(coA_1 \parallel coA_2) \subseteq L(P) \)
- P holds in \( M_1 \parallel M_2 \)
- P violated in \( M_1 \parallel M_2 \)

Counterex. analysis

Add counterex.
Remove counterex.
circular rule

- Rule **CIRC** – from [Grumberg&Long – Concur’91]

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>$\langle A_1 \rangle M_1 \langle P \rangle$</td>
</tr>
<tr>
<td>2.</td>
<td>$\langle A_2 \rangle M_2 \langle A_1 \rangle$</td>
</tr>
<tr>
<td>3.</td>
<td>$\langle \text{true} \rangle M_1 \langle A_2 \rangle$</td>
</tr>
</tbody>
</table>

$\langle \text{true} \rangle M_1 \parallel M_2 \langle P \rangle$

- Similar to rule ASYM applied recursively to 3 components
  - First and last component coincide
  - Hence learning framework similar
- Straightforward extension to $n$ components
Rule ASYM
- Assumption alphabet was fixed during learning
- $\alpha A = (\alpha M_1 \cup \alpha P) \cap \alpha M_2$

[SPIN’06]: A subset alphabet
- May be sufficient to prove the desired property
- May lead to smaller assumption

How do we compute a good subset of the assumption alphabet?

Solution – iterative alphabet refinement
- Start with small alphabet
- Add actions as necessary
- Discovered by analysis of counterexamples obtained from model checking
1. Initialize $\Sigma$ to subset of alphabet $\alpha A = (\alpha M_1 \cup \alpha P) \cap \alpha M_2$

2. If learning with $\Sigma$ returns true, return true and go to 4. (END)

3. If learning returns false (with counterexample $c$), perform extended counterexample analysis on $c$.
   - If $c$ is real, return false and go to 4. (END)
   - If $c$ is spurious, add more actions from $\alpha A$ to $\Sigma$ and go to 2.

4. END
extended counterexample analysis

\[ \alpha A = (\alpha M_1 \cup \alpha P) \cap \alpha M_2 \]

\[ \Sigma \subseteq \alpha A \text{ is the current alphabet} \]

\[ \langle s \rangle M_1 \langle P \rangle \]

query

\[ \langle A_i \rangle M_1 \langle P \rangle \]

conjecture: \( A_i \)

\[ \langle \text{true} \rangle M_2 \langle A_i \rangle \]

\[ \langle c \uparrow \Sigma \rangle M_1 \langle P \rangle \]

false + cex c

\[ \langle c \uparrow \alpha A \rangle M_1 \langle P \rangle \]

false + cex t

P holds

true

\[ \langle c \uparrow \Sigma \rangle M_1 \langle P \rangle \]

c \uparrow \Sigma

false

P violated

false

Refiner: compare \( c \uparrow \alpha A \) and \( t \uparrow \alpha A \)

Add actions to \( \Sigma \) and restart learning
alphabet refinement

\[ \Sigma = \{ \text{out} \} \quad \alpha A = \{ \text{send, out, ack} \} \]

\[ \langle \text{true} \rangle \text{ Output } \langle A_i \rangle \rightarrow \text{ false with } c = \langle \text{send, out} \rangle \]

\[ \langle c \uparrow \Sigma \rangle \text{ Input } \langle P \rangle \rightarrow \text{ false with counterex. } t = \langle \text{out} \rangle \]

\[ \langle c \uparrow \alpha A \rangle \text{ Input } \langle P \rangle \rightarrow \text{ true} \]

compare \langle \text{out} \rangle \text{ with } \langle \text{send, out} \rangle \quad \rightarrow \quad \text{ add “send” to } \Sigma
characteristics

- Initialization of $\Sigma$
  - Empty set or property alphabet $\alpha P \cap \alpha A$
- Refiner
  - Compares $t^{\uparrow \alpha A}$ and $c^{\uparrow \alpha A}$
  - Heuristics:
    - **AllDiff** adds all actions in the symmetric difference of the trace alphabets
    - **Forward** scans traces in parallel forward adding first action that differs
    - **Backward** symmetric to previous
- Termination
  - Refinement produces at least one new action and the interface is finite
- Generalization to $n$ components
  - Through recursive invocation
- See also learning with optimal alphabet refinement
  - Developed independently by Chaki & Strichman 07
Implementation in the LTSA tool
- Learning using rules ASYM, SYM and CIRC
- Supports reasoning about two and \( n \) components
- Alphabet refinement for all the rules

Experiments
- Compare effectiveness of different rules
- Measure effect of alphabet refinement
- Measure scalability as compared to non-compositional verification

Extensions for
- SPIN
- JavaPathFinder
case studies

➤ Model of Ames K9 Rover Executive
  – Executes flexible plans for autonomy
  – Consists of main Executive thread and ExecCondChecker thread for monitoring state conditions
  – Checked for specific shared variable: if the Executive reads its value, the ExecCondChecker should not read it before the Executive clears it

➤ Model of JPL MER Resource Arbiter
  – Local management of resource contention between resource consumers (e.g. science instruments, communication systems)
  – Consists of $k$ user threads and one server thread (arbiter)
  – Checked mutual exclusion between resources
results

- Rule ASYM more effective than rules SYM and CIRC
- Recursive version of ASYM the most effective
  - When reasoning about more than two components
- Alphabet refinement improves learning based assume guarantee verification significantly
- Backward refinement slightly better than other refinement heuristics
- Learning based assume guarantee reasoning
  - Can incur significant time penalties
  - Not always better than non-compositional (monolithic) verification
  - Sometimes, significantly better in terms of memory
### Analysis Data

| Case      | $|A|$ | Mem (MB) | Time (s) | $|A|$ | Mem (MB) | Time (s) | Mem (MB) | Time (s) |
|-----------|-----|----------|----------|-----|----------|----------|----------|----------|
| MER 2     | 40  | 8.65     | 21.90    | 6   | 1.23     | 1.60     | 1.04     | 0.04     |
| MER 3     | 501 | 240.06   | --       | 8   | 3.54     | 4.76     | 4.05     | 0.111    |
| MER 4     | 273 | 101.59   | --       | 10  | 9.61     | 13.68    | 14.29    | 1.46     |
| MER 5     | 200 | 78.10    | --       | 12  | 19.03    | 35.23    | 14.24    | 27.73    |
| MER 6     | 162 | 84.95    | --       | 14  | 47.09    | 91.82    | --       | 600      |
| K9 Rover  | 11  | 2.65     | 1.82     | 4   | 2.37     | 2.53     | 6.27     | 0.015    |

$|A|$ = assumption size
Mem = memory (MB)
Time (seconds)
-- = reached time (30min) or memory limit (1GB)
please ask LOTS of questions!
Automated Component-Based Verification

part III

Dimitra Giannakopoulou and Corina Păsăreanu
CMU / NASA Ames Research Center
example: autonomous rendezvous and docking

- input provided as UML state-charts, properties of type:
  - “you need at least two operational sensors to proceed to next mode”
  - “your state estimator will only return good values if it has good readings from at least 2 sensors”

- 3 bugs detected

- scaling achieved with compositional verification:
  - non-compositional verification runs out of memory after exploring > 13M states
  - compositional verification terminates successfully in secs. Analyzes one component at a time. The largest assumption has 10 states and the largest component has 5947 states (so largest state space explored is less than 60K states, as opposed to 13M)
SPT (star planet tracker)

GPS

SPT (star planet tracker)

OrbitalState

IN (inertial navigation)

DS (docking sensor)
<table>
<thead>
<tr>
<th>Structure</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Part 1 (Dimitra)</strong></td>
<td><strong>Part 2 (Corina)</strong></td>
</tr>
<tr>
<td>assume-guarantee reasoning</td>
<td>multiple components</td>
</tr>
<tr>
<td>computing assumptions</td>
<td>alphabet refinement</td>
</tr>
<tr>
<td>learning assumptions</td>
<td>case studies</td>
</tr>
<tr>
<td>discussion</td>
<td>discussion</td>
</tr>
<tr>
<td><strong>Lunch</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Part 3 (Dimitra)</strong></td>
<td><strong>Part 4 (Corina)</strong></td>
</tr>
<tr>
<td>component interfaces</td>
<td>reasoning about code</td>
</tr>
<tr>
<td>compositional JavaPathfinder</td>
<td>abstraction</td>
</tr>
<tr>
<td>examples</td>
<td>related work</td>
</tr>
<tr>
<td>discussion</td>
<td>conclusion</td>
</tr>
</tbody>
</table>
recap in reverse order…

- assume-guarantee reasoning
- learning framework for 2 components
- weakest assumption
assume-guarantee reasoning

M₁

A

M₂

M₁

reasons about triples:

〈A〉 M 〈P〉

is true if whenever M is part of a system that satisfies A, then the system must also guarantee P

simplest assume-guarantee rule (ASYM):

1. 〈A〉 M₁ 〈P〉

2. 〈true〉 M₂ 〈A〉

〈true〉 M₁ || M₂ 〈P〉
learning assumptions for AG reasoning

\[ \text{query: string } s \]
\[ \langle s \rangle M_1 \langle P \rangle \]

\[ \text{c } \uparrow \alpha A \]
\[ \text{false + crex c} \]
\[ \text{conjecture: } A_i \]
\[ \langle A_i \rangle M_1 \langle P \rangle \]
\[ \text{true} \]
\[ \text{true} \]
\[ \langle true \rangle M_2 \langle A_i \rangle \]
\[ \text{false + crex c} \]
\[ \text{query c } \uparrow \alpha A \]
\[ \text{true} \]

\[ 1. \langle A \rangle M_1 \langle P \rangle \]
\[ 2. \langle true \rangle M_2 \langle A \rangle \]

\[ \langle true \rangle M_1 \parallel M_2 \langle P \rangle \]

\[ P \text{ holds in } M_1 \parallel M_2 \]
\[ P \text{ violated in } M_1 \parallel M_2 \]
given component $M$, property $P$, and the interface $\Sigma$ of $M$ with its environment, generate the weakest environment assumption $WA$ such that: $\langle WA \rangle M \langle P \rangle$ holds

weakest means that for all environments $E$:

$\langle true \rangle M \parallel E \langle P \rangle$ IFF $\langle true \rangle E \langle WA \rangle$
STEP 1: composition, hiding, minimization

STEP 2: backward propagation of error along $\tau$ transitions

STEP 3: property extraction (subset construction & completion)

property true! (all environments)

property false! (all environments)

assumption
part III

- assume-guarantee reasoning
- learning framework for 2 components
- weakest assumption WA

- component interfaces / learning WA
- compositional JavaPathFinder
- examples and discussion
- beyond syntactic interfaces ("open" file before "close")
- document implicit assumptions

Weakest assumption (WA):
- **safe**: accept NO illegal sequence of calls
- **permissive**: accept ALL legal sequences of calls
safety check
permissiveness check
permissiveness: the problem
(queries)
should word $w$ be included in $L(A)$?

(yes / no)

(conjectures)
here is an $A$ – is $L(A) = U$? (is $A$ safe and permissive?)

(yes!)

no: word $w$ should (not) be in $L(A)$
learning interfaces

queries (simulate / model check)

conjecture – safe (model check)

conjecture – permissive

Alur et al, 2005, Henzinger et al, 2005
our approach (Giannakopoulou & Pasareanu, FASE 2009)

model check for \((M_i, A_{error})\)

reached \((M_1, A_{error})\) by “a b”
query “a b”
no (“a b” should not be in A)
backtrack and continue search…
invoke a model checker within a model checker?
permissiveness check

**MC:** model check for \((M_i, A_{error})\)

reached \((M_i, A_{error})\) by trace \(t\)

if (memoized(t) == no) // t is spurious
    backtrack and continue search

else // memoized(t) == yes or t not in memoized
    model checker produces \(t\)

if (query(t) == yes)
    return \(t\) to \(L^*\) // not permissive

else restart at **MC**
module M

Input

Order_{err}

Output

assumption learned for AG reasoning

⟨ack, out⟩?
complete module for permissiveness check

module M

Input

Order_{err}

Complete_Input

queries performed on Input || Order_{err}
safety checked on Input || Order_{err} || A_{err}
permissiveness performed on Complete_Input || Order_{err} || A_{err}
check reachability of states: (sink, *, error) or (*, non error, error)

\langle \text{ack, out} \rangle: (\text{sink, error, error})
in summary…

resolve non-determinism
dynamically & selectively
remember, it’s a heuristic
assume-guarantee reasoning

\[ \langle A_i \rangle M_1 \langle P \rangle \]

true

\[ \langle true \rangle M_2 \langle A_i \rangle \]

true

\[ false+crex c \]

false

query c \[ \uparrow \alpha A \]

\[ c \uparrow \alpha A \]

\[ \text{query: string } s \]

false+crex c

\[ L^* \]

\[ P \text{ holds in } M_1 \parallel M_2 \]

\[ P \text{ violated in } M_1 \parallel M_2 \]

only need permissiveness with respect to \( M_2 \)!
JavaPathfinder
UML statecharts

assume-guarantee reasoning

interface generation / discharge

jpf-cv
http://babelfish.arc.nasa.gov/trac/jpf
JPF supports model checking of UML state-machines with an approach that consists of three steps:

- translate the UML model into a corresponding Java program, using JPF’s state chart (sc) extension and application model
- choose model properties to verify, and configure verification tools accordingly
- optionally provide a guidance script that represents the environment of the model (external event sequence)
package ICSETutorial;

import gov.nasa.jpf.sc.State;

public class Input extends State {
    class S0 extends State {
        public void input() {
            setState(s1);
        }
    } S0 s0 = makeInitial(new S0());
    class S1 extends State {
        public void send() {
            setState(s2);
        }
    } S1 s1 = new S1();
    class S2 extends State {
        public void acknowledge() {
            setState(s0);
        }
    } S2 s2 = new S2();
}
AG reasoning in JPF

JavaPathfinder
(CVState.AutomatonState)

SCSafetyListener

SCSafetyAutomaton
assumptions

- choiceGeneratorAdvanced
  - if selected action leads assumption to error state then do "vm.getSystemState().setIgnored(true)" (backtrack)

- instructionExecuted
  - advance automaton & set CVState.AutomatonState

- stateBacktracked
  - get CVState.AutomatonState

JavaPathfinder
(CVState.AutomatonState)

SCSafetyListener
SCSafetyAutomaton
properties

- **instructionExecuted**
  - advance automaton & set CVState.AutomatonState
  - if automaton reaches error state, then check() returns false

- **stateBacktracked**
  - get CVState.AutomatonState

JavaPathfinder
(CVState.AutomatonState)

SCSafetyListener
SCSafetyAutomaton
interface generation in JPF

- queries and assumption safety checks
  - same as assume-guarantee reasoning
- assumption permissiveness check
  - requires special listener
conformance listener

- **executelInstruction**
  - if instruction to be executed is assertion violation, then perform
    
    “ti.skipInstruction()” *(do not process exception)* and
    “vm.getSystemState().setIgnored(true)” *(backtrack)*

- **instructionExecuted**
  - advance automaton & set CVState.AutomatonState
  - if automaton reaches error state, check memoized table *(why?)*
    
    if counterexample stored and spurious, backtrack
    else check() returns false

- **stateBacktracked**
  - get CVState.AutomatonState
boolean done = false;
while (!done){
    counterexample = null;

    SCConformanceListener assumption = new SCConformanceListener(
        new SCSafetyAutomaton(false, assume, alphabet_, "Assumption",
            CompleteModule, memoized_));
    JPF jpf = createJPFInstance(assumption, property, CompleteModule);
    jpf.run();

    Path jpfPath = assumption.getCounterexample();
    if (jpfPath != null){
        // nonerror in M & error in Aerr - this is what we are looking for

        counterexample = assumption.convert(jpfPath);
        if( query(counterexample)){ // cex is in L(A)
            done = true; // a real counterexample for L*
        } // otherwise you need to continue with your loop
    } else
    done = true; // interface is permissive
}
package ICSETutorial;
import gov.nasa.jpf.sc.State;
import gov.nasa.jpf.cv.CVState;

public class InputWithProperty extends CVState {
    class S0 extends State {
        public void input() {
            setState(s1);
        }

        public void output() {
            assert(false);
        }
    }

    S0 s0 = makeInitial(new S0());

    ...
}
example 2
tool: JavaPathfinder

UML statechart model of the Ascent and EarthOrbit flight phases of a spacecraft

properties:

- “An event IsamRendezvous, which represents a docking maneuver with another spacecraft, fails if the LAS (launch abort system) is still attached to the spacecraft”

- “Event tliBurn (trans-lunar interface burn takes spacecraft out of the earth orbit and gets it into transition to the moon) can only be invoked if EDS (Earth Departure Stage) rocket is available”
Assumption 1:

Assumption 2:

generated interface assumptions encode Flight Rules in terms of events
## Conclusions

- **Learning assumptions is not a panacea**
  - may perform worse than monolithic verification
  - performs well when alphabets & assumptions are small

- **Computed interfaces may not be permissive**
  - in our studies interfaces were satisfactory
  - there is more to say about this in part IV

- **Limited to statecharts**
  - but wish to extend; it’s open source, help us!!!

- **Got funding**
  - so expect a lot of activity on jpf-cv over the next year
Automated Component-Based Verification

part IV

Dimitra Giannakopoulou and Corina Păsăreanu
CMU / NASA Ames Research Center
part IV

- reasoning about code
- introducing abstraction
  - to reason about very large or infinite state spaces
- related approaches
Does \( M_1 \parallel M_2 \) satisfy \( P \)? Model check; \textbf{build} assumption \( A \)

Does \( C_1 \parallel C_2 \) satisfy \( P \)? Model check; \textbf{use} assumption \( A \)

[ICSE’2004] – good results but may not scale

\textbf{Solution: replace model checking with testing!}
introducing abstraction...

- apply predicate abstraction [Graf & Saidi, CAV 1997]
- apply learning to abstracted components
- use counterexamples to automatically refine abstractions as needed, using CEGAR (Counter-example Guided Abstraction Refinement) [Clarke et al., CAV 2000]

- **interfaces:** novel combination of under- and over- approximations with L* avoids exponentially expensive determinization step and generates minimal and precise interfaces [CAV 2010]

- implemented in ARMC model checker (and previously Magic)
- successfully applied to several benchmarks (Java2SDK library classes, OpenSSL)
CEGAR: counterexample guided abstraction refinement – Clarke et al. 00
- incremental construction of abstractions
- abstractions are conservative
- abstract counterexamples obtained may be spurious (due to over-approximation)
- spurious counterexamples are used for abstraction refinement

two level compositional abstraction refinement – Chaki et al. 03
- analyze $C_1 \parallel C_2 \parallel \ldots \parallel C_n \models P$
- build finite-state abstractions: $A_1, A_2, \ldots A_n$
- minimize: $M_1, M_2, \ldots M_n$
- analyze: $M_1 \parallel M_2 \parallel \ldots \parallel M_n \models P$?
- refine based on counterexamples

permissive interfaces – Henzinger et al. 05
- uses CEGAR to compute interfaces
assume-guarantee abstraction refinement (AGAR)

- Challenge: instead of learning $A$, build $A$ as an abstraction of $M_2$

\[
\begin{align*}
1. & \quad \langle A \rangle \quad M_1 \quad \langle P \rangle \\
2. & \quad \langle \text{true} \rangle \quad M_2 \quad \langle A \rangle \\
\hline \\
\langle \text{true} \rangle & \quad M_1 \parallel M_2 \quad \langle P \rangle 
\end{align*}
\]

- build $A$ as an abstraction of $M_2$; $\langle \text{true} \rangle \ M_2 \langle A \rangle$ holds by construction

- check Premise 1: $\langle A \rangle \ M_1 \langle P \rangle$
- obtained counterexamples are analyzed and used to refine $A$
- variant of CEGAR with differences:
  - use counterexample from $M_1$ to refine abstraction of $M_2$
  - $A$ keeps information only about the interface (abstracts away the internal info)
- implemented in LTSA; combined with alphabet refinement;
- compares favorably with learning approach
- [CAV’08]
## Table 1. Comparison of AGAR and learning for 2 components, with and without alphabet refinement.

<table>
<thead>
<tr>
<th>Case</th>
<th>k</th>
<th>No alpha. ref.</th>
<th>AGAR</th>
<th>Learning</th>
<th>AGAR</th>
<th>Learning</th>
<th>AGAR</th>
<th>Learning</th>
<th>Sizes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>k</td>
<td>Mem.</td>
<td>Time</td>
<td>A</td>
<td>Mem.</td>
<td>Time</td>
<td>A</td>
<td>Mem.</td>
</tr>
<tr>
<td>Gas Station</td>
<td>3</td>
<td>16</td>
<td>4.11</td>
<td>3.33</td>
<td>177</td>
<td>42.83</td>
<td>–</td>
<td>5</td>
<td>2.99</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>19</td>
<td>37.43</td>
<td>23.12</td>
<td>195</td>
<td>100.17</td>
<td>–</td>
<td>5</td>
<td>22.79</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>22</td>
<td>359.53</td>
<td>278.63</td>
<td>45</td>
<td>206.61</td>
<td>–</td>
<td>5</td>
<td>216.07</td>
</tr>
<tr>
<td>Chiron, Property 2</td>
<td>2</td>
<td>10</td>
<td>1.30</td>
<td>0.92</td>
<td>9</td>
<td>1.30</td>
<td>1.69</td>
<td>10</td>
<td>1.30</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>36</td>
<td>2.59</td>
<td>5.94</td>
<td>21</td>
<td>5.59</td>
<td>7.08</td>
<td>36</td>
<td>2.44</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>160</td>
<td>8.71</td>
<td>152.34</td>
<td>39</td>
<td>27.1</td>
<td>32.05</td>
<td>160</td>
<td>8.22</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>4</td>
<td>55.14</td>
<td>–</td>
<td>111</td>
<td>560.23</td>
<td>676.02</td>
<td>3</td>
<td>58.71</td>
</tr>
<tr>
<td>Chiron, Property 3</td>
<td>2</td>
<td>4</td>
<td>1.07</td>
<td>0.50</td>
<td>9</td>
<td>1.14</td>
<td>1.57</td>
<td>4</td>
<td>1.23</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>8</td>
<td>1.84</td>
<td>1.60</td>
<td>25njmj</td>
<td>4.45</td>
<td>7.72</td>
<td>8</td>
<td>2.00</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>16</td>
<td>4.01</td>
<td>18.75</td>
<td>45</td>
<td>25.49</td>
<td>36.33</td>
<td>16</td>
<td>5.08</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>4</td>
<td>52.53</td>
<td>–</td>
<td>122</td>
<td>134.21</td>
<td>271.30</td>
<td>1</td>
<td>81.89</td>
</tr>
<tr>
<td>MER</td>
<td>2</td>
<td>34</td>
<td>1.42</td>
<td>11.38</td>
<td>40</td>
<td>6.75</td>
<td>9.89</td>
<td>5</td>
<td>1.42</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>67</td>
<td>8.10</td>
<td>247.73</td>
<td>335</td>
<td>133.34</td>
<td>–</td>
<td>9</td>
<td>11.09</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>58</td>
<td>341.49</td>
<td>–</td>
<td>38</td>
<td>377.21</td>
<td>–</td>
<td>9</td>
<td>532.49</td>
</tr>
<tr>
<td>Rover Exec.</td>
<td>2</td>
<td>10</td>
<td>4.07</td>
<td>1.80</td>
<td>11</td>
<td>2.70</td>
<td>2.35</td>
<td>3</td>
<td>2.62</td>
</tr>
</tbody>
</table>
compositional verification for C

- Check composition of software C components

$$C_1 || C_2 \models P$$

![Diagram showing the compositional verification process]
Theorem:
An interface $A$ permissive w.r.t $C$'s $\textbf{must}$ abstraction safe w.r.t $C$'s $\textbf{may}$ abstraction and is safe and permissive for $C$. 

interface generation for infinite-state components
interface generation for infinite-state components

- conceptually simple and elegant
- expensive learning restarts
- need of tighter integration of abstraction refinement with L*
- LearnReuse method
1. if checkSafe(σ, Cmust) != null
2. return "no"
3. cex = checkSafe(σ, Cmay)
4. if cex == null
5. return "yes"
6. Preds = Preds U Refine(cex)
7. Query(σ, C)
Conjecture : Oracle 1

1. cex = checkSafe(A, Cmay)
2. if cex == null
3. invoke Oracle2
4. If Query(cex, C) == “no”
5. return cex to L*
6. else
7. goto 1
Conjecture : Oracle 2

1. \( \text{cex} = \text{checkPermissive}(A, C_{\text{must}}) \)
2. if cex == null
3. return A
4. If Query(cex, C) == “yes”
5. return cex to L*
6. else
7. goto 1
NASA CEV 1.5 EOR-LOR mission
26 methods

Only LearnReuse finished
74 predicates, 14 states
52 minutes
our previous work at a glance

- learning-based AG reasoning (TACAS 2003)
- recursive application of simple rule for reasoning about \( n > 2 \) components (FMSD 2009)
- symmetric and circular assume-guarantee rules (SAVCBS 2003, FMSD 2009)
- learning with alphabet refinement (TACAS 2007)
- learning assumptions for interface automata (FM 2008)
- assume-guarantee abstraction refinement (CAV 2008)
- interface generation in JPF (FASE 2009)
- interface generation for large/infinite-state components (CAV 2010)
### Other Related Work

<table>
<thead>
<tr>
<th>(L* for separating automata)</th>
<th>(interfaces)</th>
<th>(L* for AG reasoning)</th>
<th>(L* for model extraction)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(L* for NFAs &amp; liveness)</td>
<td>Tkachuk et al, 2003</td>
<td>Cobleigh et al, 2006</td>
<td></td>
</tr>
<tr>
<td>Gupta et al, 2007</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chen et al, 2009</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(L* for model extraction)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bollig et al, 2009</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Farzan et al, 2008</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
minimal separating automaton for disjoint languages $L_1$ and $L_2$
- accept all words in $L_1$
- accept no words in $L_2$
- have the least number of states

assume-guarantee reasoning
- minimal separating automaton for $L(M_2)$ and $L(M_1) \cap L(coP)$

algorithms
- Gupta at al. 07: query complexity exponential in the size of the minimal DFAs for the two input languages
- Chen et al. 09: query complexity quadratic in the product of the sizes of the minimal DFAs for the two input languages. Use 3 valued DFAs

compositional verification in symbolic setting (Alur et al. 05)
learning omega-regular languages for liveness (Farzan et al. 08)
learning non-deterministic automata (Bollig et al. 09)
thank you!
part IV

- parts I – III: reasoning about finite-state models

- reasoning about code

- introducing abstraction
to reason about very large or infinite state spaces

- related approaches
Does $M_1 \parallel M_2$ satisfy $P$? Model check; **build** assumption $A$

Does $C_1 \parallel C_2$ satisfy $P$? Model check; **use** assumption $A$

[ICSE’2004] – good results but may not scale

**Solution:** replace model checking with testing! [IET Software 2009]
abstraction

- Reduces large/infinite data domains into small/finite abstract domains; e.g. replace `int` with `{ZERO, POS, NEG}`
- Produces a finite state abstract model that operates on the abstract domain
- Abstraction maps
  - Concrete states to abstract states
  - Concrete transitions to abstract transitions
- Framework of abstract interpretation
May and must abstraction

- May abstraction produces a finite over-approximation
- Must abstraction produces a finite under-approximation
abstraction in compositional verification

- apply (predicate) abstraction [Graf & Saidi, CAV 1997]
- apply learning to abstracted components
- use counterexamples to automatically refine abstractions/assumptions as needed [Magic]

- use abstraction refinement as an alternative to learning for building assumptions [AGAR, CAV 2008]

- interfaces: novel combination of under- and over- approximations with $L^*$ avoids exponentially expensive determinization step and generates minimal and precise interfaces [CAV 2010]
- implemented in ARMC model checker
- successfully applied to several benchmarks (Java2SDK library classes, OpenSSL)
CEGAR: counterexample guided abstraction refinement [Clarke et al. 00]
- incremental construction of (may) abstractions
- abstract counterexamples obtained may be spurious (due to over-approximation)
- spurious counterexamples are used for abstraction refinement
CEGAR for compositional verification

- **two level compositional abstraction refinement** – Chaki et al. 03
  - analyze $C_1 || C_2 || \ldots || C_n \models P$
  - build finite-state abstractions: $A_1, A_2, \ldots A_n$
  - minimize: $M_1, M_2, \ldots M_n$
  - analyze: $M_1 || M_2 || \ldots || M_n \models P$?
  - refine based on counterexamples

- **permissive interfaces** – Henzinger et al. 05
  - uses CEGAR to compute interfaces
learning-based compositional verification for C code

- Check composition of software C components $C_1 || C_2 \models P$
- $C_1, C_2$ are large/infinite state

```
<table>
<thead>
<tr>
<th>predicate abstraction</th>
<th>predicate abstraction</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_1^{\text{may}}$</td>
<td>$C_2^{\text{may}}$</td>
</tr>
<tr>
<td>refine</td>
<td>refine</td>
</tr>
</tbody>
</table>
```

```
<table>
<thead>
<tr>
<th>learning framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>true</td>
</tr>
<tr>
<td>$C_1</td>
</tr>
</tbody>
</table>
```

```
<table>
<thead>
<tr>
<th>counterexample analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>false</td>
</tr>
<tr>
<td>spurious</td>
</tr>
</tbody>
</table>
```

```
<table>
<thead>
<tr>
<th>refine</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_1^{\text{may}}$</td>
</tr>
<tr>
<td>$C_2^{\text{may}}$</td>
</tr>
</tbody>
</table>
```

```
| $C_1 || C_2 \models P$ |
|-------------------------|
```

```
<table>
<thead>
<tr>
<th>refine</th>
</tr>
</thead>
<tbody>
<tr>
<td>spurious</td>
</tr>
</tbody>
</table>
```

```
| $C_1^{\text{may}}$    |
| $C_2^{\text{may}}$    |
```

```
| $C_1 || C_2 \models P$ |
|-------------------------|
```

assume-guarantee abstraction refinement (AGAR)

- Challenge: instead of learning $A$, build $A$ as an abstraction of $M_2$

1. $\langle A \rangle \quad M_1 \quad \langle P \rangle$
2. $\langle true \rangle \quad M_2 \quad \langle A \rangle$

$\langle true \rangle \ M_1 \parallel M_2 \quad \langle P \rangle$
assume-guarantee abstraction refinement (AGAR)

- Challenge: instead of learning $A$, build $A$ as an abstraction of $M_2$

$$
\begin{array}{ccc}
1. & \langle A \rangle & M_1 & \langle P \rangle \\
2. & \langle true \rangle & M_2 & \langle A \rangle \\
\hline
\langle true \rangle & M_1 || M_2 & \langle P \rangle
\end{array}
$$

- build $A$ as an (may) abstraction of $M_2$; $\langle true \rangle M_2 \langle A \rangle$ holds by construction

- check Premise 1: $\langle A \rangle M_1 \langle P \rangle$
- obtained counterexamples are analyzed and used to refine $A$
- variant of CEGAR with differences:
  - use counterexample from $M_1$ to refine abstraction of $M_2$
  - $A$ keeps information only about the interface (abstracts away the internal info)

- implemented in LTSA; combined with alphabet refinement;
- compares favorably with learning approach
- [CAV’08]
<table>
<thead>
<tr>
<th>Case</th>
<th>k</th>
<th>No alpha. ref.</th>
<th>Learning</th>
<th>With alpha. ref.</th>
<th>Learning</th>
<th>Sizes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>AGAR</td>
<td>Mem.</td>
<td>Time</td>
<td>AGAR</td>
<td>Mem.</td>
</tr>
<tr>
<td>Gas Station</td>
<td>3</td>
<td>16</td>
<td>4.11</td>
<td>3.33</td>
<td>177</td>
<td>42.83</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>19</td>
<td>37.43</td>
<td>23.12</td>
<td>195</td>
<td>100.17</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>22</td>
<td>359.53</td>
<td>278.63</td>
<td>45</td>
<td>206.61</td>
</tr>
<tr>
<td>Chiron,</td>
<td>2</td>
<td>10</td>
<td>1.30</td>
<td>0.92</td>
<td>9</td>
<td>1.30</td>
</tr>
<tr>
<td>Property 2</td>
<td>3</td>
<td>36</td>
<td>2.59</td>
<td>5.94</td>
<td>21</td>
<td>5.59</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>160</td>
<td>8.71</td>
<td>152.34</td>
<td>39</td>
<td>27.1</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>4</td>
<td>55.14</td>
<td>–</td>
<td>111</td>
<td>560.23</td>
</tr>
<tr>
<td>Chiron,</td>
<td>2</td>
<td>4</td>
<td>1.07</td>
<td>0.50</td>
<td>9</td>
<td>1.14</td>
</tr>
<tr>
<td>Property 3</td>
<td>3</td>
<td>8</td>
<td>1.84</td>
<td>1.60</td>
<td>25 n jmj</td>
<td>4.45</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>16</td>
<td>4.01</td>
<td>18.75</td>
<td>45</td>
<td>25.49</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>4</td>
<td>52.53</td>
<td>–</td>
<td>122</td>
<td>134.21</td>
</tr>
<tr>
<td>MER</td>
<td>2</td>
<td>34</td>
<td>1.42</td>
<td>11.38</td>
<td>40</td>
<td>6.75</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>67</td>
<td>8.10</td>
<td>247.73</td>
<td>335</td>
<td>133.34</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>58</td>
<td>341.49</td>
<td>–</td>
<td>38</td>
<td>377.21</td>
</tr>
<tr>
<td>Rover Exec.</td>
<td>2</td>
<td>10</td>
<td>4.07</td>
<td>1.80</td>
<td>11</td>
<td>2.70</td>
</tr>
</tbody>
</table>
Use predicate abstraction to build may and must abstractions of component C

\[ L_{\text{safe}}(C) = L_{\text{err}}(C) \]

- Interface A is safe: \( L(A) \subseteq L_{\text{safe}}(C) \)
- Interface A is permissive: \( L_{\text{safe}}(C) \subseteq L(A) \)

**Theorem:**

An interface \( A \) permissive w.r.t. C's **must** abstraction and safe w.r.t C's **may** abstraction is safe and permissive for C.
Correctness: If algorithm terminates then the returned interface $A$ is safe and permissive for $C$. 
interface generation for infinite-state components

- conceptually simple and elegant
- expensive learning restarts

- need of tighter integration of abstraction refinement with \( L^* \)
- LearnReuse method
Query($\sigma, C$)

1. if checkSafe($\sigma, C^{\text{must}}$) != null
2. return “no”
3. cex = checkSafe($\sigma, C^{\text{may}}$)
4. if cex == null
5. return “yes”
6. Preds = Preds U Refine(cex)
7. Query($\sigma, C$)

Gives answers consistent with $C$
Conjecture : Oracle 1

1. cex = checkSafe(A, C\text{may})
2. if cex == null
3. invoke Oracle2
4. If Query(cex, C) == “no”
5. return cex to L*
6. else
7. goto 1
Conjecture : Oracle 2

1. cex = checkPermissive(A, C^{must})
2. if cex == null
3. return A
4. If Query(cex, C) == “yes”
5. return cex to L^*
6. else
7. goto 1
NASA case study

- NASA CEV 1.5 EOR-LOR mission
- 26 methods
- Only LearnReuse finished
- 74 predicates, 14 states
- 52 minutes
our previous work at a glance

- learning-based AG reasoning (TACAS 2003)
- recursive application of simple rule for reasoning about $n > 2$ components (FMSD 2009)
- symmetric and circular assume-guarantee rules (SAVCBS 2003, FMSD 2009)
- learning with alphabet refinement (TACAS 2007)
- learning assumptions for interface automata (FM 2008)
- assume-guarantee abstraction refinement (CAV 2008)
- interface generation in JPF (FASE 2009)
- interface generation for large/infinite-state components (CAV 2010)
<table>
<thead>
<tr>
<th>Other related work</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>(interfaces)</strong></td>
</tr>
<tr>
<td>Ammons et al, 2002</td>
</tr>
<tr>
<td>Whaley et al, 2002</td>
</tr>
<tr>
<td>Tkachuk et al, 2003</td>
</tr>
<tr>
<td><em><em>(L</em> for AG reasoning)</em>*</td>
</tr>
<tr>
<td>Alur et al, 2005 (2)</td>
</tr>
<tr>
<td>Chaki et al, 2005-2007</td>
</tr>
<tr>
<td>Cobleigh et al, 2006</td>
</tr>
<tr>
<td><em><em>(L</em> for separating automata)</em>*</td>
</tr>
<tr>
<td>Gupta et al, 2007</td>
</tr>
<tr>
<td>Chen et al, 2009</td>
</tr>
<tr>
<td><em><em>(L</em> for NFAs &amp; liveness)</em>*</td>
</tr>
<tr>
<td>Bollig et al, 2009</td>
</tr>
<tr>
<td>Farzan et al, 2008</td>
</tr>
<tr>
<td><em><em>(L</em> for model extraction)</em>*</td>
</tr>
<tr>
<td>Groce et al, 2002</td>
</tr>
<tr>
<td>Margaria et al, 2007</td>
</tr>
</tbody>
</table>
### other related work

- **minimal separating automaton for disjoint languages** $L_1$ and $L_2$
  - accept all words in $L_1$
  - accept no words in $L_2$
  - have the **least number of states**

- **assume-guarantee reasoning**
  - minimal separating automaton for $L(M_2)$ and $L(M_1) \cap L(coP)$

- **algorithms**
  - Gupta at al. 07: query complexity exponential in the size of the minimal DFAs for the two input languages
  - Chen et al. 09: query complexity quadratic in the product of the sizes of the minimal DFAs for the two input languages. Use 3 valued DFAs

- **compositional verification in symbolic setting** (Alur et al. 05)
- learning omega-regular languages for liveness (Farzan et al. 08)
- learning non-deterministic automata (Bollig et al. 09)
Conclusion

- Compositional verification and assume-guarantee reasoning
- Techniques for automatic assumption generation and compositional verification
  - Finite state systems and safety properties
- Data abstraction to deal with very large/infinite state spaces
- Techniques are promising in practice

Future:

- Techniques for discovering good system decompositions
- Parallelization for increased scalability
- Beyond safety: liveness, timed properties, probabilistic reasoning
- Run-time analysis
- More?
thank you!