

# COMP424/524-06A Topics in Software Engineering

Part I – Model Checking Algorithms  
18. Incremental Verification

Robi Malik

## Subsets and Intersection

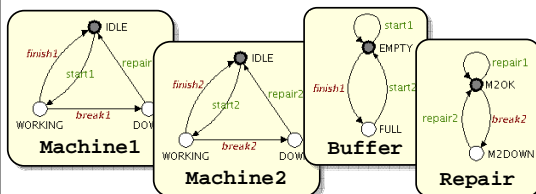
Strict synchronous composition is intersection of languages:

$$\mathcal{L}(A_1 \parallel A_2 \parallel \dots \parallel A_n) = \mathcal{L}(A_1) \cap \mathcal{L}(A_2) \cap \dots \cap \mathcal{L}(A_n)$$

Language inclusion check tests for subset of languages:

$$\mathcal{L}(A_1 \parallel A_2 \parallel \dots \parallel A_n) \stackrel{?}{\subseteq} \mathcal{L}(P)$$

## Modelling Automata in VALID



- Each automaton imposes new constraints.
- Behaviour is restricted by adding automata.

## Result about Language Inclusion

**Proposition.**

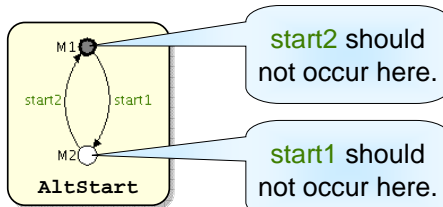
Let  $A = A_1 \parallel A_2 \parallel \dots \parallel A_n$ .  
If  $A_i$  satisfies a property  $P$ ,  
then  $A$  satisfies  $P$ .

**Proof.**

$$\mathcal{L}(A) = \mathcal{L}(A_1) \cap \dots \cap \mathcal{L}(A_n) \subseteq \mathcal{L}(A_i) \subseteq \mathcal{L}(P)$$

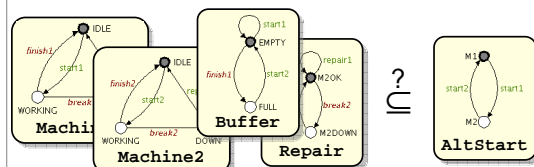
## Language Inclusion Check

Language inclusion is a safety property.



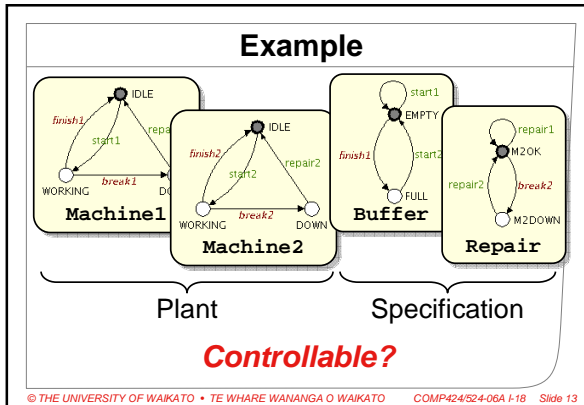
## Applying the Result

Does small factory satisfy AltStart?



If one of the automata, e.g. Buffer,  
satisfies AltStart, then we are done.



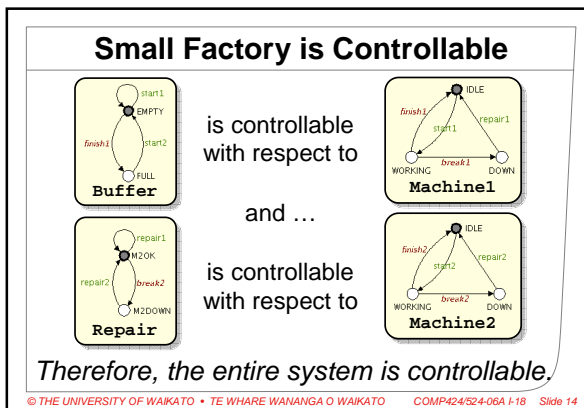


### Incremental Verification

*An automatic abstraction procedure*

- Abstractions, i.e. subsystems, computed automatically.
- Counterexamples used to augment subsystems until the property is proven or shown to be not satisfied.

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-18 Slide 16



### A Problem

There may be several components not accepting a counterexample.

*Which ones to choose?*

- All of them?
- First one found?
- Most promising one?

▶ **Heuristics!**

© THE UNIVERSITY OF WAIKATO • TE WHARE WANANGA O WAIKATO COMP424/524-06A I-18 Slide 17

