Towards Safer Composition

How to verify lots of similar systems

A. Classen, P. Heymans, T. T. Tun and B. Nuseibeh

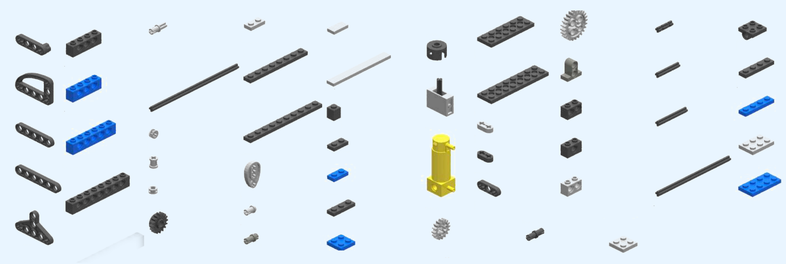
The Open University

FUNDP NAMUR

Context: Software product line engineering and model-based verification

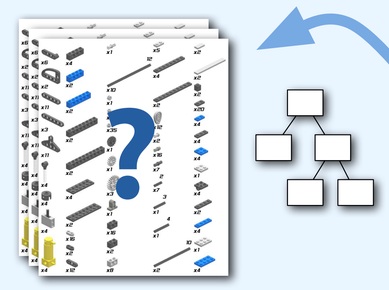
Produce different products from reusable assets

Reusable Assets



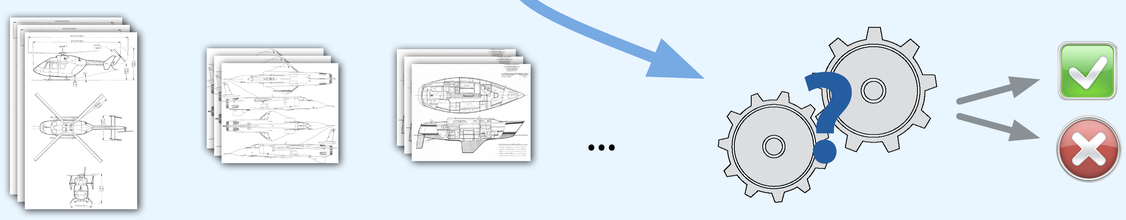
Products

Verify behavioural models



Challenges

- Scalable representation
- Efficient reasoning



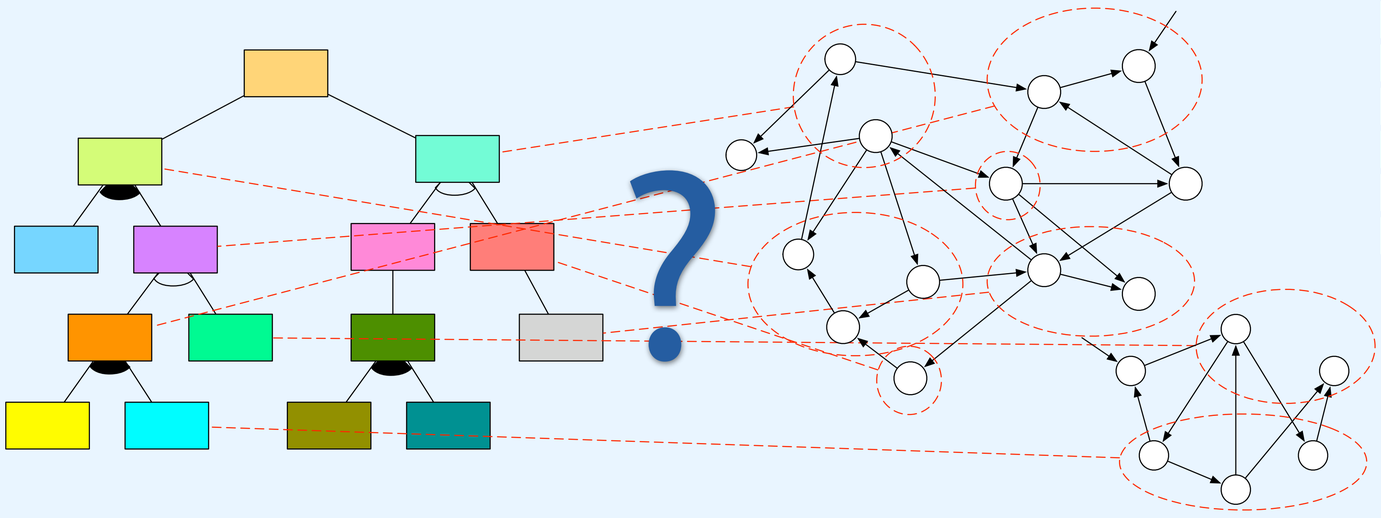
Research questions

How to map behavioural models to feature diagrams?

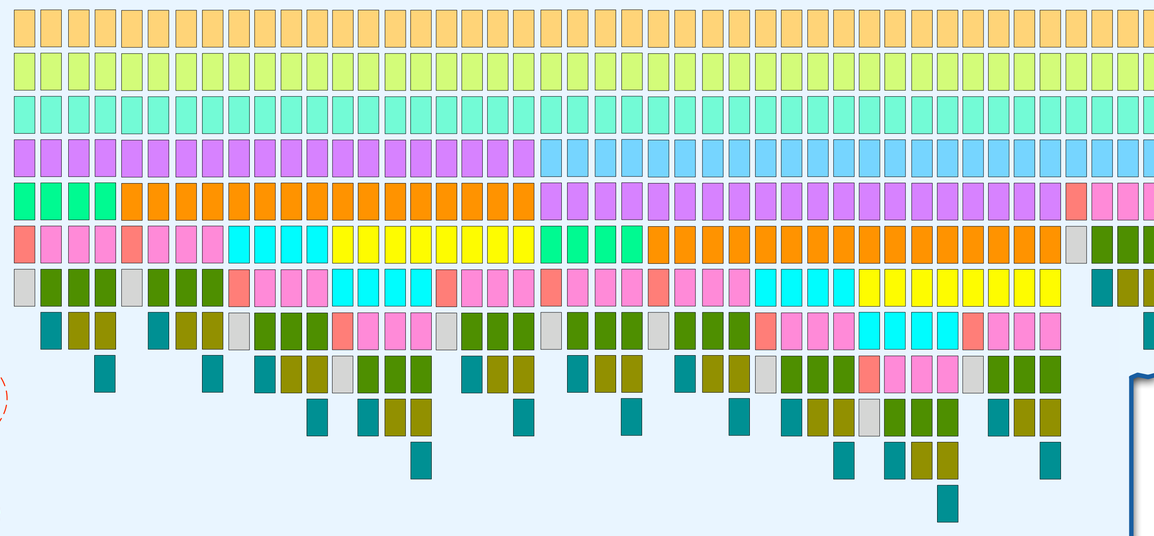
How to efficiently model check an exponential number of different products?

Feature diagram: high-level view of variability within the family

Behavioural model fragments: detailed description of features or products



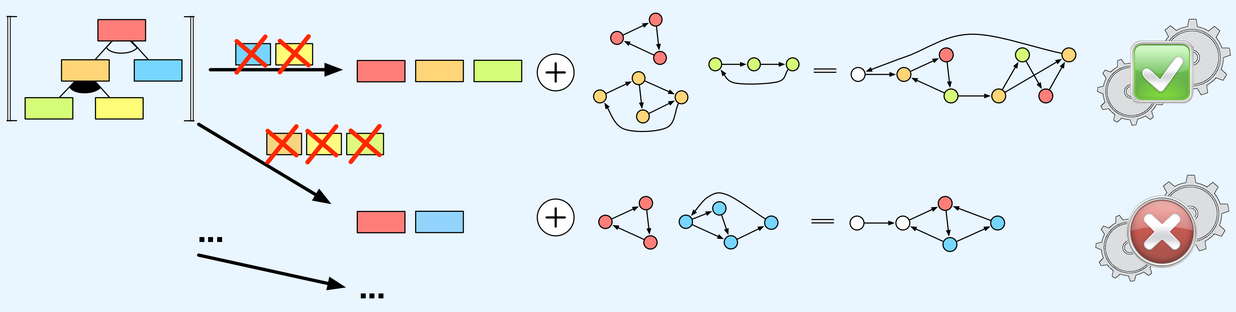
Verify temporal logic properties for each one of them:



Solution: merge behaviour from fragments -- two approaches

Single. One merge per product

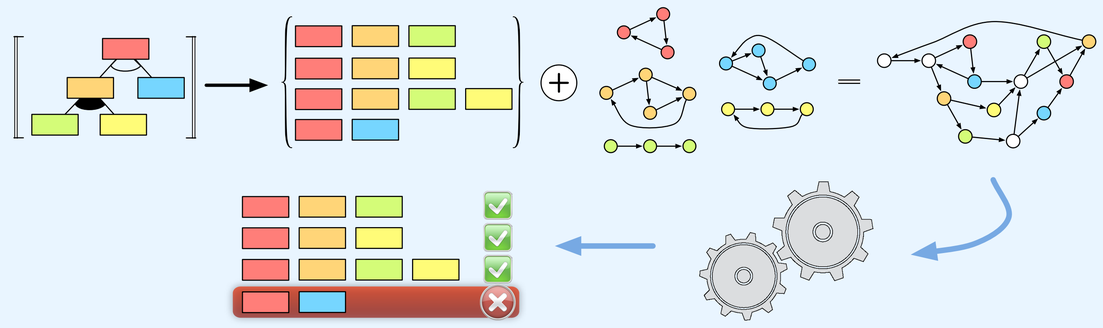
Each product verified individually



Problem: exponential number explicitly considered

Multi. Merge once and take variability into account

One verification for all products



Problem: verification is harder, not as fine-grained

Current results

- Proposed multimerge approach
- Proposed enhanced transition systems for product family behaviour
- Algorithm for reachability
- Model-checking LTL safety properties

Ongoing and future work

- Implement a prototype
- Extend model-checking algorithm to ω-regular properties
- Investigate optimisation techniques
- Define merge operation

Funding

FNRS

EPSRC

MoVES

Modelling, Verification and Evolution of Software

Contact: acs@info.fundp.ac.be -- www.classen.be