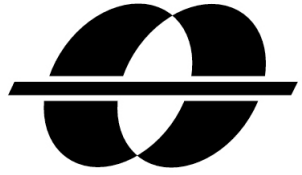
Cost Optimisation in Certification of Software Product Lines

Ricardo J. Rodríguez, Sasikumar Punnekkat
rj.rodriguez@unileon.es, sasikumar.punnekkat@mdh.se


ETSINF, Technical University of Madrid
RIASC, University of León
Madrid, Spain – León, Spain



School of Innovation, Design and Engineering
Mälardalen University
Västerås, Sweden

November 3, 2014

4th edition of the IEEE International Workshop on Software Certification (WoSoCer)
Naples (Italy)

Agenda

1. Introduction
2. Related Work
3. A Cost Model for Certification
   - Software Product Line (Formal) Definition
   - Certification Cost Model
4. Cost Optimisation Problem for Certification
   - Performance Evaluation
5. Conclusions and Future Work

Agenda

1. Introduction
2. Related Work
3. A Cost Model for Certification
   - Software Product Line (Formal) Definition
   - Certification Cost Model
4. Cost Optimisation Problem for Certification
   - Performance Evaluation
5. Conclusions and Future Work

Introduction (I)

Software Product Line Engineering (SPLE)

- Widely adopted approach in software-intensive systems
- Platform: Core Asset Base
  - Collection of artifacts (software components) that can be reused across a company portfolio
- Features: Differences among product platforms
  - A set of features = product variant

Introduction (I)

Software Product Line Engineering (SPLE)

- Widely adopted approach in software-intensive systems
- Platform: Core Asset Base
  - Collection of artifacts (software components) that can be reused across a company portfolio
- Features: Differences among product platforms
  - A set of features = product variant

Main benefit

- Reuse of software components leads to save production costs
- Master key in many industrial domains (e.g., automotive)
  - Software development cost estimated as 13% of production cost of a vehicle (2010)

Introduction (II)

SPLE in safety-critical systems

- Safety-critical systems: Failures $\rightarrow$ fatal consequences
- Safety certification: The product is "safe'
  - Time consuming
  - Budget cost increased

Introduction (II)

SPLE in safety-critical systems

- Safety-critical systems: Failures $\rightarrow$ fatal consequences
- Safety certification: The product is "safe'
  - Time consuming
  - Budget cost increased

Adoption of SPLE in these systems rises several challenges $\rightarrow$ cost optimization non-essential issue (in advance)

Introduction (II)

SPLE in safety-critical systems

- Safety-critical systems: Failures $\rightarrow$ fatal consequences
- Safety certification: The product is "safe'
  - Time consuming
  - Budget cost increased

Adoption of SPLE in these systems rises several challenges $\rightarrow$ cost optimization non-essential issue (in advance)

Cost savings

- Reuse of software components
- Reuse of safety evidences and argument fragments

Introduction (III)

Contribution

- Cost model accounting for certification issues
- Formal model of a SPL + a heuristic strategy to minimise cost
  - Computes the platform members that compound a new product variant with a given level of confidence at minimum cost
  - Make efficient design decisions

Agenda

1. Introduction
2. Related Work
3. A Cost Model for Certification
   - Software Product Line (Formal) Definition
   - Certification Cost Model
4. Cost Optimisation Problem for Certification
   - Performance Evaluation
5. Conclusions and Future Work

Related Work (I)

Software cost estimation models in software reuse

1. Expert judgement models
   - Experience and knowledge of one or more experts
2. Algorithmic (or parametric)
   - Consider input parameters
3. Machine Learning approaches
   - Approximate cost considering previous knowledge, with dynamic adjusting

Related Work (I)

Software cost estimation models in software reuse

1. Expert judgement models
   - Experience and knowledge of one or more experts
2. Algorithmic (or parametric)
   - Consider input parameters
3. Machine Learning approaches
   - Approximate cost considering previous knowledge, with dynamic adjusting

We focus on algorithmic models

Related Work (II)

Algorithmic software cost estimation models

- SLIM, COCOMO-II, FPA, SEEM-SEM
- Open models vs. non-open models
- Wide range of project attributes
  - Development effort, complexity, experience, ...
- Some accounts for reuse, risk plans, team cohesion, ...

Related Work (II)

Algorithmic software cost estimation models

- SLIM, COCOMO-II, FPA, SEEM-SEM
- Open models vs. non-open models
- Wide range of project attributes
  - Development effort, complexity, experience, ...
- Some accounts for reuse, risk plans, team cohesion, ...

Current models lack for certification aspects
but they could easily add these as another factor in the cost equation...

Related Work (II)

Algorithmic software cost estimation models

- SLIM, COCOMO-II, FPA, SEEM-SEM
- Open models vs. non-open models
- Wide range of project attributes
  - Development effort, complexity, experience, ...
- Some accounts for reuse, risk plans, team cohesion, ...

Current models lack for certification aspects
but they could easily add these as another factor in the cost equation...
They compute cost but not consider best suitable options to minimise it

Related Work (III)

Algorithmic software cost estimation models in SPL

- Safety certification is neither considered
  - Models not initially planned to safety-critical systems

Related Work (III)

Algorithmic software cost estimation models in SPL

- Safety certification is neither considered
  - Models not initially planned to safety-critical systems

Cost optimisation – variability models

- Olaechea et al., NFPinDSML, 2012
  - Tool based on Alloy language
  - Exact, discrete multi-objective optimization

Agenda

1. Introduction
2. Related Work
3. A Cost Model for Certification
   - Software Product Line (Formal) Definition
   - Certification Cost Model
4. Cost Optimisation Problem for Certification
   - Performance Evaluation
5. Conclusions and Future Work

A Cost Model for Certification (I)

A formal definition of SPL

$$\mathcal{S} = \langle \mathcal{X}, \mathcal{P}, \mathcal{F}, \mathcal{R}, \mathcal{E}, \mathcal{D} \rangle$$

- $\mathcal{X} = \{x_1, x_2 \ldots, x_n\}$: Set of components
- $\mathcal{P} = \{p_1, p_2 \ldots, p_m\}$: Set of product variants
- $\mathcal{F} = \{f_1, f_2 \ldots, f_u\}$: Set of features available
- $\mathcal{R} : \mathcal{P} \times \mathcal{F} \rightarrow \{0, 1\}$: Features provided by a product
- $\mathcal{E} : \mathcal{F} \times \mathcal{X} \rightarrow \{0, 1\}$: Components that provide a feature
  - $x, x' \in \mathcal{X}, \mathcal{E}(f, x) = \mathcal{E}(f, x') = 1$ means that we can pick either x or x' to provide the feature f
- $\mathcal{D} : \mathcal{X} \times \mathcal{X} \rightarrow \{0, 1\}$: Dependencies among the components

RIASC

A Cost Model for Certification (II)

Towards a certification cost model

Bockle et al.'s cost model

$$C = C_{org} + C_{cab} + \sum_{i=1}^{n}(C_{unique}(p_i) + C_{reuse}(p_i))$$

- C_{org}: Cost to an organization for adopting the software product line approach for its set of products
- C_{cab}: Cost to develop a core asset base to support the product line being adopted
- C_{unique}: Cost to develop unique software for a new artifact p_i
- C_{reuse}: Cost to reuse a core asset p_i

A Cost Model for Certification (III)

Towards a certification cost model

Safety-critical systems

- Set of mandatory requirements to assure a certain level of safety
- Specified by standards
  - IEC 61508, ISO 26262, DO-178C
  - NOTE: Certification of a product $p = \{x_1, \ldots, x_n\}$ implies certification of components $\{x_1, \ldots, x_n\}$
- When fulfilled, the system is safety-certified

A Cost Model for Certification (III)

Towards a certification cost model

Safety-critical systems

- Set of mandatory requirements to assure a certain level of safety
- Specified by standards
  - IEC 61508, ISO 26262, DO-178C
  - NOTE: Certification of a product $p = \{x_1, \ldots, x_n\}$ implies certification of components $\{x_1, \ldots, x_n\}$
- When fulfilled, the system is safety-certified

Safety Integrity Level (SIL)

- Target level of risk reduction
- In a safety-critical systems, it forces products (and its sub-components) to a minimum SIL

$$\mathcal{I} : \mathcal{X} \rightarrow [1, SIL_{max}]$$

- SIL_{max}: Maximum achievable SIL in the system

A Cost Model for Certification (IV)

Towards a certification cost model

Adding costs of certification

- $\mathcal{C}_{cert} : \mathcal{P} \rightarrow c, c \in \mathbb{R}^{+}_{>0}$: Cost of certification
- $\mathcal{C}_{recert} : \mathcal{X} \times \mathcal{I} \rightarrow c, c \in \mathbb{R}^{+}_{\geq 0}$: Cost $c \geq 0$ of re-certifying to a given safety integrity level s for a component x
  - $\mathcal{C}_{recert}(x_i, s) = 0$ when x_i cannot achieve a level s
- $\mathcal{C}_{other} : \mathcal{X} \rightarrow c, c \in \mathbb{R}^{+}_{>0}$: Other costs (e.g., cost of reuse and cost of unique development)

A Cost Model for Certification (V)

Refining the Bockle et al.'s cost model

$$C = C_{org} + C_{cab} + \sum_{i=1}^{n}(C_{unique}(p_i) + C_{reuse}(p_i)) \Rightarrow$$

$$C' = C_{org} + C_{cab} + \sum_{p' \in \mathcal{P}'} C_{cert}(p') + \sum_{i=1}^{n}(C_{unique}(p_i) + C_{reuse}(p_i) + C_{recert}(p_i, s'))$$

- $\mathcal{P}' \subseteq \mathcal{P}$: Set of products that needs to be initially certified to a given SIL
- $C_{recert}(p_i, s')$: Cost of re-certification of a product p_i to an s' level
  - $C_{recert}(p_i, s') =$

$$\sum_{x \in \mathcal{X}'_i} \left(\mathcal{C}_{recert}(x, s') + \sum_{\forall x' \notin \mathcal{X}'_i, x' \in \mathcal{D}, \mathcal{D}(x,x')=1} \mathcal{C}_{recert}(x', s') \right), \text{ where}$$

$$\mathcal{X}'_i = \{x | x \in \mathcal{X} \wedge f \in \mathcal{F}, \mathcal{R}(p_i, f) = 1 \Rightarrow \mathcal{E}(f, x) = 1\}$$

Agenda

1. Introduction
2. Related Work
3. A Cost Model for Certification
   - Software Product Line (Formal) Definition
   - Certification Cost Model
4. Cost Optimisation Problem for Certification
   - Performance Evaluation
5. Conclusions and Future Work

Cost Optimisation Problem for Certification (I)

Heuristic strategy algorithm

- Input: $\mathcal{S}, \mathcal{I}, \mathcal{C}_{other}, \mathcal{C}_{recert}, SIL_{new}, \mathcal{F}'$
- Output: $\mathcal{Z}$ (set of eligible components that minimise the cost)

Steps

1. Initialise $\mathcal{D}', \mathcal{X}', \mathcal{I}', \mathcal{C}'$
2. For each element (x, s) that can be recertified and not yet processed
   1. Create a temporary path $\mathcal{P}'$ checking all nodes have a SIL $\geq s$
   2. When $\mathcal{P}'$ is feasible, add these new components to $\mathcal{X}'$ with its SIL and mark (x, s) as *processed*
   3. Add cost of recertification of each component x' to $\mathcal{C}'(x')$
   4. Set the features and dependencies properly
3. Set diagonal elements of $\mathcal{D}'$ as the number of dependent elements
4. Compute $\mathcal{A}$ as the solution of the Binary Integer Problem
   - Next slide!
5. Extract the set of components from $\mathcal{A}$

Cost Optimisation Problem for Certification (II)

Heuristic strategy algorithm – Binary Integer Programming problem

$$
\begin{aligned}
\mathcal{A} = \mathit{minimize}\ & \mathcal{C}' \cdot \mathcal{X}'^{\top} \\
\mathit{subject\ to}\ & \mathcal{E}' \cdot \mathcal{X}'^{\top} = \mathbf{1} \\
& \mathcal{D}' \cdot \mathcal{X}'^{\top} \geq \mathbf{0} \\
& (\mathcal{E}' \cdot \mathcal{I}') \cdot \mathcal{X}'^{\top} \geq \mathbf{1} \cdot \mathit{SIL}_{new} \\
& x \in \{0,1\}, \forall x \in \mathcal{X}'
\end{aligned}
\tag{1}
$$

- $\mathcal{E}' \subseteq \mathcal{E}, \forall f \in \mathcal{F}', \mathcal{E}'(f,:) = \mathcal{E}(f,:)$

Cost Optimisation Problem for Certification (II)

Heuristic strategy algorithm – Binary Integer Programming problem

$$
\begin{aligned}
\mathcal{A} = \mathit{minimize}\ & \mathcal{C}' \cdot \mathcal{X}'^{\top} \\
\mathit{subject\ to}\ & \mathcal{E}' \cdot \mathcal{X}'^{\top} = \mathbf{1} \\
& \mathcal{D}' \cdot \mathcal{X}'^{\top} \geq \mathbf{0} \\
& (\mathcal{E}' \cdot \mathcal{I}') \cdot \mathcal{X}'^{\top} \geq \mathbf{1} \cdot \mathit{SIL}_{new} \\
& x \in \{0,1\}, \forall x \in \mathcal{X}'
\end{aligned}
\tag{1}
$$

- $\mathcal{E}' \subseteq \mathcal{E}, \forall f \in \mathcal{F}', \mathcal{E}'(f,:) = \mathcal{E}(f,:)$
- Two scenarios of working:
  - Allows adding a new product variant
  - Recertification of existing product variant in the SPL to a higher SIL

Cost Optimisation Problem for Certification (III)

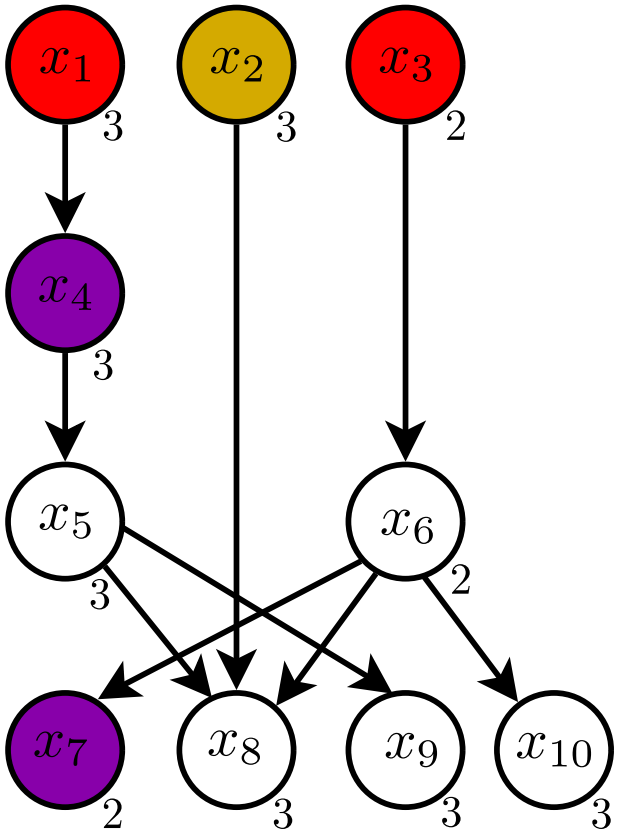
An example

- $|\mathcal{X}| = 10$ components
- Suppose an airbag equipment composed of three features

$\mathcal{R} = \{1, 1, 1\}$
$\mathcal{F} = \{f_1, f_2, f_3\}$

$$\mathcal{E} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

- $\mathcal{I} = \{3, 3, 2, 3, 3, 2, 2, 3, 3, 3\}$
- $C_{other} = \{\$1500, \$1000, \$1000, \$1200, \$1200, \$900, \$750, \$1500, \$1350, \$1000\}$



First scenario

- $C_{recert} = \mathbf{0}$ (no recertification)

Cost Optimisation Problem for Certification (III)

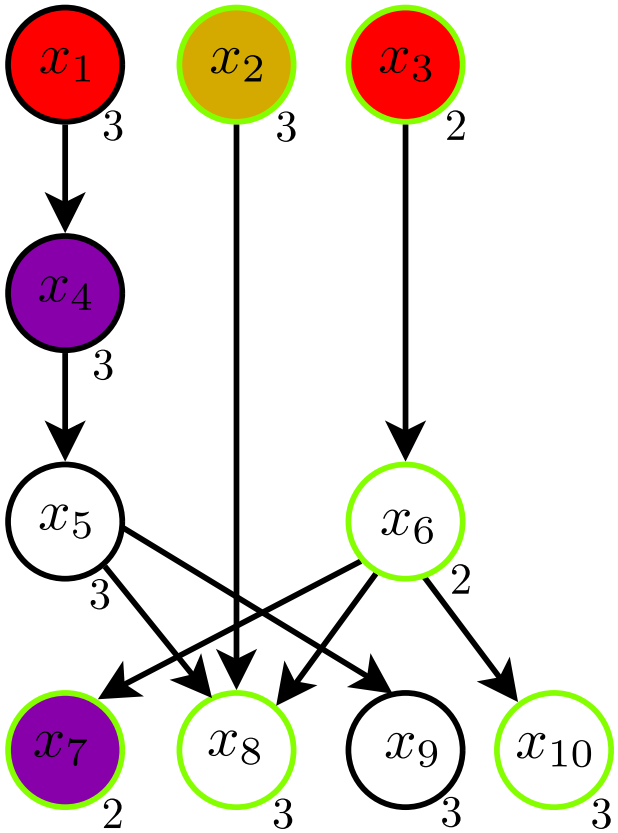
An example

- $|\mathcal{X}| = 10$ components
- Suppose an airbag equipment composed of three features

$\mathcal{R} = \{1, 1, 1\}$
$\mathcal{F} = \{f_1, f_2, f_3\}$

$$\mathcal{E} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

- $\mathcal{I} = \{3, 3, 2, 3, 3, 2, 2, 3, 3, 3\}$
- $\mathcal{C}_{other} = \{\$1500, \$1000, \$1000, \$1200, \$1200, \$900, \$750, \$1500, \$1350, \$1000\}$



First scenario

- $C_{recert} = \mathbf{0}$ (no recertification)
- $SIL_{new} = 1$
  - $\{x_2, x_3, x_6, x_7, x_8, x_{10}\}$, \$6150
  - f_1, f_2, f_3 provided by x_3, x_2, x_7 (respectively)

Cost Optimisation Problem for Certification (III)

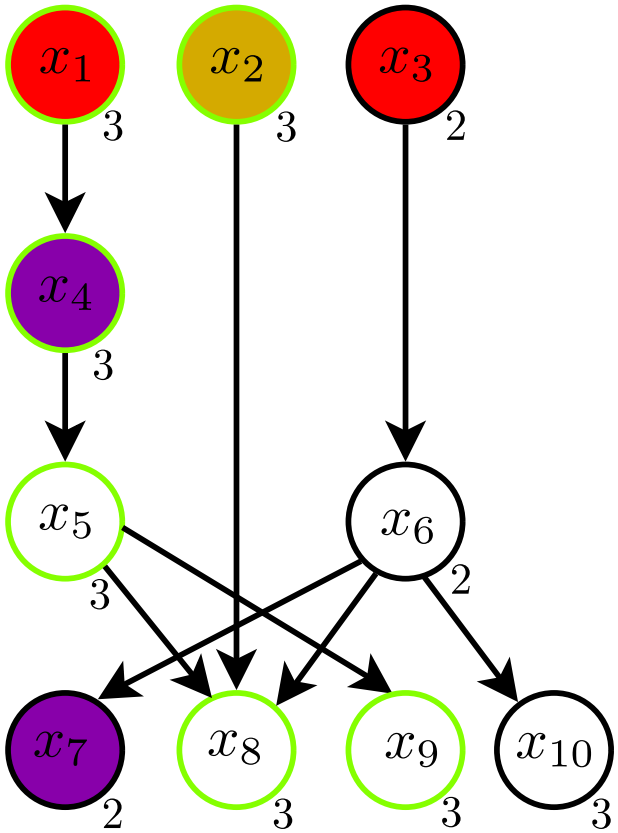
An example

- $|\mathcal{X}| = 10$ components
- Suppose an airbag equipment composed of three features

$\mathcal{R} = \{1, 1, 1\}$
$\mathcal{F} = \{f_1, f_2, f_3\}$

$$\mathcal{E} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

- $\mathcal{I} = \{3, 3, 2, 3, 3, 2, 2, 3, 3, 3\}$
- $C_{other} = \{\$1500, \$1000, \$1000, \$1200, \$1200, \$900, \$750, \$1500, \$1350, \$1000\}$



First scenario

- $C_{recert} = \mathbf{0}$ (no recertification)
- $SIL_{new} = 1$
  - $\{x_2, x_3, x_6, x_7, x_8, x_{10}\}$, \$6150
  - f_1, f_2, f_3 provided by x_3, x_2, x_7 (respectively)
- $SIL_{new} = 3$
  - $\{x_1, x_2, x_4, x_5, x_8, x_9\}$, \$7750
  - f_1, f_2, f_3 provided by x_1, x_2, x_4 (respectively)

Cost Optimisation Problem for Certification (III)

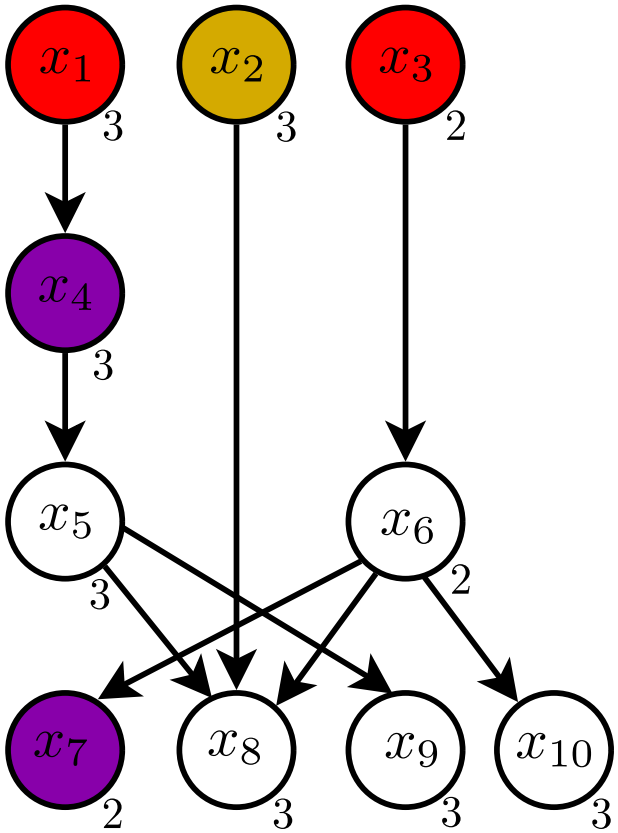
An example

- $|\mathcal{X}| = 10$ components
- Suppose an airbag equipment composed of three features

$\mathcal{R} = \{1, 1, 1\}$
$\mathcal{F} = \{f_1, f_2, f_3\}$

$$\mathcal{E} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

- $\mathcal{I} = \{3, 3, 2, 3, 3, 2, 2, 3, 3, 3\}$
- $\mathcal{C}_{other} = \{\$1500, \$1000, \$1000, \$1200, \$1200, \$900, \$750, \$1500, \$1350, \$1000\}$



Second scenario

- $\mathcal{C}(x_3, 3) = \mathcal{C}(x_6, 3) = \mathcal{C}(x_7, 3) = 200$

RIASC

Cost Optimisation Problem for Certification (III)

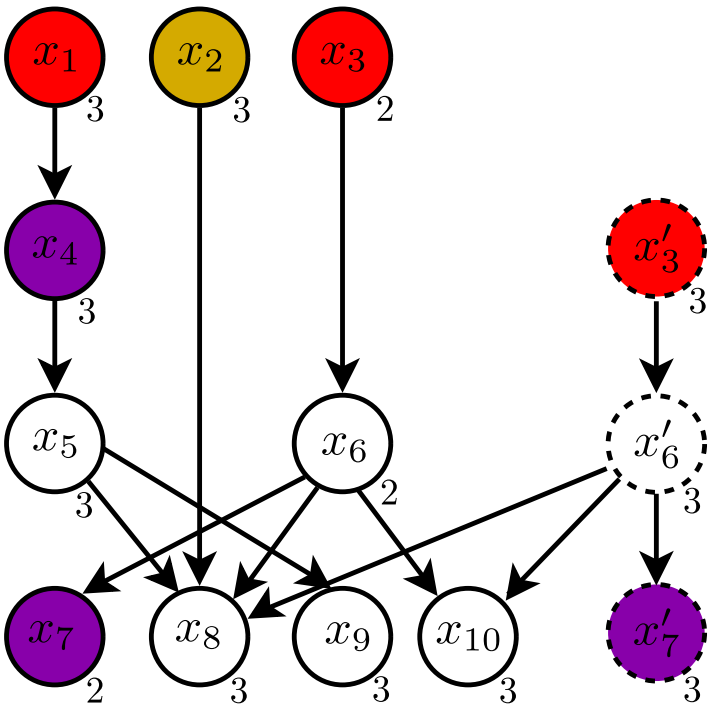
An example

- $|\mathcal{X}| = 10$ components
- Suppose an airbag equipment composed of three features

$\mathcal{R} = \{1, 1, 1\}$
$\mathcal{F} = \{f_1, f_2, f_3\}$

$$\mathcal{E} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

- $\mathcal{I} = \{3, 3, 2, 3, 3, 2, 2, 3, 3, 3\}$
- $\mathcal{C}_{other} = \{\$1500, \$1000, \$1000, \$1200, \$1200, \$900, \$750, \$1500, \$1350, \$1000\}$



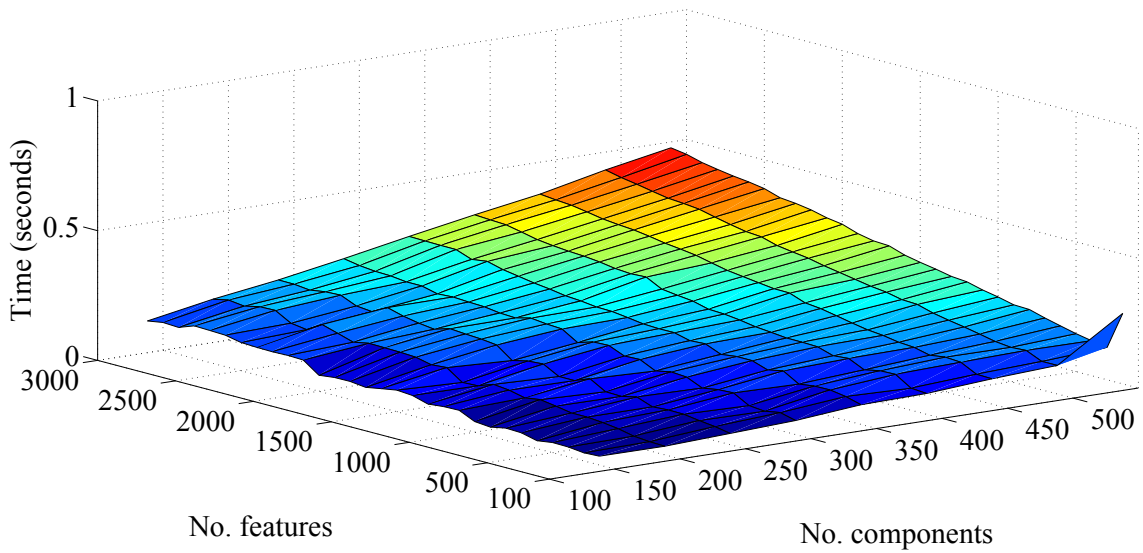
Second scenario

- $\mathcal{C}(x_3, 3) = \mathcal{C}(x_6, 3) = \mathcal{C}(x_7, 3) = 200$
- $SIL_{new} = 3$
  - $\{x_2, x'_3, x'_6, x'_7, x_8, x_{10}\}$, \$6750
  - f_1, f_2, f_3 provided by x'_3, x_2, x'_7

RIASC

Cost Optimisation Problem for Certification (IV)

Binary Integer Programming problem – Performance evaluation (average execution time)

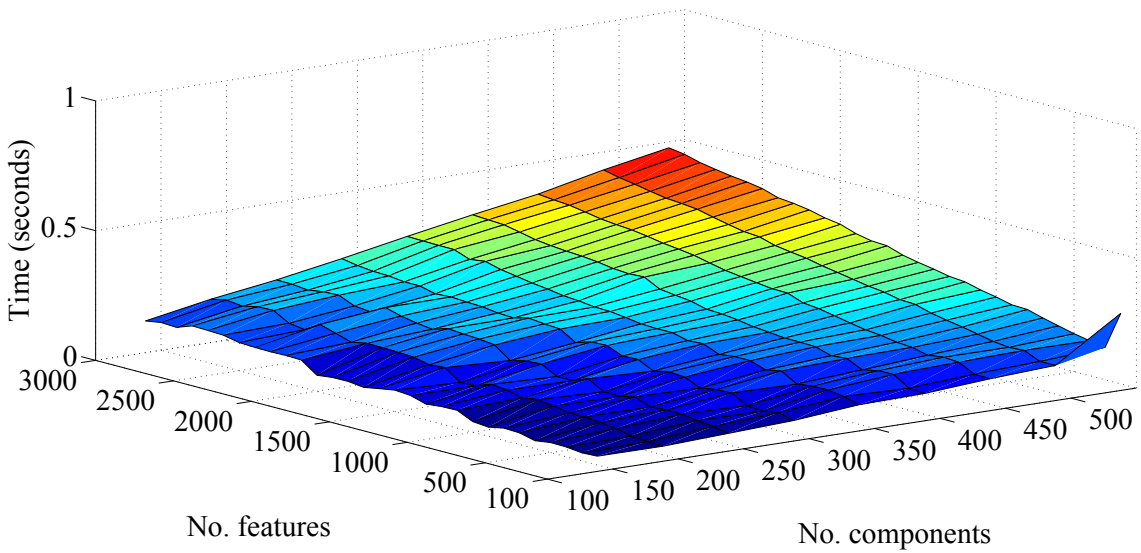


Sensitive analysis

- Features: $[100, 3000]$, step 100
- Components: $[100, 500]$, step 50
- Features and dependency matrices randomly created

Cost Optimisation Problem for Certification (IV)

Binary Integer Programming problem – Performance evaluation (average execution time)



Sensitive analysis

- Features: $[100, 3000]$, step 100
- Components: $[100, 500]$, step 50
- Features and dependency matrices randomly created

- Strong dependence on the number of components, almost independently on the number of features
- Execution time is relatively small (less than 0.5 seconds)
  - Negligible compared to the time needed to gather data as we propose

RIASC

Agenda

1. Introduction
2. Related Work
3. A Cost Model for Certification
   - Software Product Line (Formal) Definition
   - Certification Cost Model
4. Cost Optimisation Problem for Certification
   - Performance Evaluation
5. Conclusions and Future Work

Conclusions and Future Work (I)

- Reuse of software products save production cost
- SPL approach can be adopted in safety-critical systems
  - Aware of safety standards: Safety certification
    - Time consuming
    - Increases production costs

Summary of contributions

- Cost model for SPL that addresses certification aspects
- Formal definition of a SPL
- Heuristic strategy with optimisation theory to minimise cost
  - Binary Integer Programming problem
  - Compute the set of artifacts that conforms a product variant at an optimised cost assuring also a certain level of confidence
  - Good trade-off accuracy/time complexity
    - Execution time depends on the no. of components
    - Negligible compared to the time of gathering data as we propose :(

Conclusions and Future Work (II)

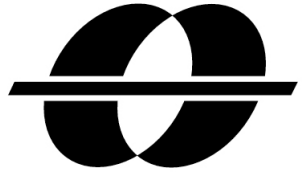
Future Work

- Tool to collect data, solve the problem and report feedback to the user
- Evaluate in real industrial case studies
- Extend to eliminate assumption of SIL independent

Cost Optimisation in Certification of Software Product Lines

Ricardo J. Rodríguez, Sasikumar Punnekkat
rj.rodriguez@unileon.es, sasikumar.punnekkat@mdh.se


ETSINF, Technical University of Madrid
RIASC, University of León
Madrid, Spain – León, Spain



School of Innovation, Design and Engineering
Mälardalen University
Västerås, Sweden

November 3, 2014

4th edition of the IEEE International Workshop on Software Certification (WoSoCer)
Naples (Italy)