Formal Description of Variability in Product Families

Maurice H. ter Beek
ISTI–CNR, Pisa, Italy

joint work with

P. Asirelli
ISTI–CNR

A. Fantechi
University of Florence

S. Gnesi
ISTI–CNR

SPLC 2011

München, Germany
24 August 2011
1. Background and aim of our research activity
2. Running example: Coffee machine family
3. Logic \textsc{vACTL} interpreted over MTSs
4. Advanced variability management
5. Model checking families and products
6. Conclusions and future work
Variability management

Key difference between SPLE and ‘conventional’ software engineering

Variability modeling

How to explicitly define optional, alternative, mandatory, required, or excluded features of a product family as variation points

Managing variability with formal methods

Show that a certain product belongs to a product family or, instead, derive a product from a family by properly selecting features

Formally prove characteristics of products and families alike
Variability management

Key difference between SPLE and ‘conventional’ software engineering

Variability modeling

How to explicitly define optional, alternative, mandatory, required, or excluded features of a product family as variation points

Managing variability with formal methods

Show that a certain product belongs to a product family or, instead, derive a product from a family by properly selecting features

Formally prove characteristics of products and families alike
Variability management

Key difference between SPLE and ‘conventional’ software engineering

Variability modeling

How to explicitly define optional, alternative, mandatory, required, or excluded features of a product family as variation points

Managing variability with formal methods

Show that a certain product belongs to a product family or, instead, derive a product from a family by properly selecting features

Formally prove characteristics of products and families alike
Aim of our research activity at large

Aim

- One formal framework to express both feature-based constraints over the products of a family and constraints over their behavior
- Tool support for derivation of products and formal verification over products and families alike

Outcome

- IFM’10, ACOTA @ ASE’10, PLEASE @ ICSE’11, FMOODS’11, SEW-34 @ FM’11
- MTS: Modal Transition Systems (Larsen, Wasowski et alii)
- VACTL: variability and action-based CTL
- VMC: Variability Model Checker

Comparison

- FTS: Featured Transition Systems, LTL/fCTL, and SNIP/NuSMV (Classen, Heymans et alii @ ICSE’10/’11)
Aim of our research activity at large

Aim

- One formal framework to express both feature-based constraints over the products of a family and constraints over their behavior.
- Tool support for derivation of products and formal verification over products and families alike.

Outcome

IFM’10, ACOTA @ ASE’10, PLEASE @ ICSE’11, FMOODS’11, SEW-34 @ FM’11

- MTS: Modal Transition Systems (Larsen, Wasowski et alii)
- $\forall$ACTL: variability and action-based CTL
- VMC: Variability Model Checker

Comparison

FTS: Featured Transition Systems, LTL/fCTL, and SNIP/NuSMV (Classen, Heymans et alii @ ICSE’10/’11)
Aim of our research activity at large

**Aim**
- One formal framework to express both feature-based constraints over the products of a family and constraints over their behavior
- Tool support for derivation of products and formal verification over products and families alike

**Outcome**
- IFM’10, ACOTA @ ASE’10, PLEASE @ ICSE’11, FMOODS’11, SEW-34 @ FM’11
- MTS: Modal Transition Systems (Larsen, Wasowski et alii)
- $\mathsf{vACTL}$: variability and action-based CTL
- VMC: Variability Model Checker

**Comparison**
- FTS: Featured Transition Systems, LTL/fCTL, and SNIP/NuSMV (Classen, Heymans et alii @ ICSE’10/’11)
Modal Transition Systems (MTSs)

Originally introduced by Larsen & Thomsen @ LICS 1988

MTSs are now an established model to formalize a product family’s

- *underlying behavior*, shared among all products, and
- *variation points*, differentiating between products

MTS is an LTS that distinguishes between may and must transitions
(modeling *optional* or *mandatory* features, resp.)

MTS cannot model variability constraints regarding *alternative* features
nor those regarding *requires* and *excludes* inter-feature relations

We will model such advanced variability constraints by means of an
associated set of logical formulae expressed in our variability and
action-based branching-time temporal logic VA$\text{CTL}$. 

P. Asirelli et al. (ISTI–CNR, Univ. Firenze)
Modal Transition Systems (MTSs)

Originally introduced by Larsen & Thomsen @ LICS 1988

MTSs are now an established model to formalize a product family’s
- underlying behavior, shared among all products, and
- variation points, differentiating between products

MTS is an LTS that distinguishes between may and must transitions (modeling optional or mandatory features, resp.)

MTS cannot model variability constraints regarding alternative features nor those regarding requires and excludes inter-feature relations

We will model such advanced variability constraints by means of an associated set of logical formulae expressed in our variability and action-based branching-time temporal logic $\mathcal{VACTL}$.
Modal Transition Systems (MTSs)

Originally introduced by Larsen & Thomsen @ LICS 1988

MTSs are now an established model to formalize a product family’s

- underlying behavior, shared among all products, and
- variation points, differentiating between products

MTS is an LTS that distinguishes between may and must transitions
(modeling optional or mandatory features, resp.)

MTS cannot model variability constraints regarding alternative features
nor those regarding requires and excludes inter-feature relations

We will model such advanced variability constraints by means of an
associated set of logical formulae expressed in our variability and
action-based branching-time temporal logic \(\text{VACTL}\)
Definition of MTS

\((Q, A, \overline{q}, \rightarrow, \rightarrow_\Diamond)\) is an MTS with

- **underlying LTS** \((Q, A, \overline{q}, \rightarrow, \rightarrow_\square)\)
- **may** transition relation \(\rightarrow_\Diamond \subseteq Q \times A \times Q\) (**possible** transitions)
- **must** transition relation \(\rightarrow_\square \subseteq Q \times A \times Q\) (**mandatory** transitions)

By definition, mandatory transitions must also be possible: \(\rightarrow_\square \subseteq \rightarrow_\Diamond\)

The set of all must paths from \(q_1\) is denoted by \(\square\text{-path}(q_1)\)

\[\sigma_\square = q_1 a_1 q_2 a_2 q_3 \ldots\] is a **must path** (from \(q_1\)) if \(q_i \xrightarrow{a_j} \square q_{i+1}\) \(\forall i > 0\)

Subfamilies/products are obtained by preserving all must transitions, turning some may transitions into must transitions, and removing some/all remaining ones (resulting in MTS/LTS)
Definition of MTS

(Q, A, \overline{q}, \rightarrow_{\Box}, \rightarrow_{\Diamond}) is an MTS with

- **underlying** LTS (Q, A, \overline{q}, \rightarrow_{\Box} \cup \rightarrow_{\Diamond})
- *may* transition relation \( \rightarrow_{\Diamond} \subseteq Q \times A \times Q \) (**possible** transitions)
- *must* transition relation \( \rightarrow_{\Box} \subseteq Q \times A \times Q \) (**mandatory** transitions)

By definition, mandatory transitions must also be possible: \( \rightarrow_{\Box} \subseteq \rightarrow_{\Diamond} \)

The set of all must paths from \( q_1 \) is denoted by **\( \Box \)-path**(\( q_1 \))

\[ \sigma_{\Box} = q_1 a_1 q_2 a_2 q_3 \cdots \] is a *must path* (from \( q_1 \)) if \( q_i \xrightarrow{a_i} \Box q_{i+1} \forall i > 0 \)

Subfamilies/products are obtained by preserving all must transitions, turning some may transitions into must transitions, and removing some/all remaining ones (resulting in MTS/LTS)
Definition of MTS

\((Q, A, \bar{q}, \rightarrow^\square, \rightarrow^\diamond)\) is an MTS with

- **underlying LTS** \((Q, A, \bar{q}, \rightarrow^\square \cup \rightarrow^\diamond)\)
- **may** transition relation \(\rightarrow^\diamond \subseteq Q \times A \times Q\) (*possible* transitions)
- **must** transition relation \(\rightarrow^\square \subseteq Q \times A \times Q\) (*mandatory* transitions)

By definition, mandatory transitions must also be possible: \(\rightarrow^\square \subseteq \rightarrow^\diamond\)

The set of all must paths from \(q_1\) is denoted by \(\square\text{-path}(q_1)\)

\[\sigma^\square = q_1a_1q_2a_2q_3\cdots\text{ is a must path (from }q_1\text{) if }q_i \xrightarrow{a_i}^\square q_{i+1} \ \forall \ i > 0\]

Subfamilies/products are obtained by preserving **all** must transitions, turning **some** may transitions into must transitions, and removing **some/all** remaining ones (resulting in MTS/LTS)
Running example: Coffee machine family

Cappuccino

Coffee

Tea

Sugar

No sugar

Pour sugar

Pour coffee

Pour milk

Pour tea

Take cup

Ring a tone

Skip
Static & behavioral requirements of product families

Static requirements: features constituting different products

- Only accepted coins are 1€, exclusively for European products, and 1$, exclusively for Canadian products (alternative features)
- All products offer coffee (mandatory feature); cappuccino only offered by European products (excludes relation among features)
- A ringtone is rung in products that offer cappuccino (requires relation among features)

Behavioral requirements: admitted sequences of operations

- After coin insertion, user must press a button to choose whether (s)he wants sugar, after which (s)he may select a beverage
- Optionally, a ringtone is rung after delivering a beverage
- The machine returns to its idle state when the beverage is taken
### Static requirements: features constituting different products

- Only accepted coins are 1€, exclusively for European products, and 1$, exclusively for Canadian products (**alternative** features).
- All products offer coffee (**mandatory** feature); cappuccino only offered by European products (**excludes** relation among features).
- A ringtone is rung in products that offer cappuccino (**requires** relation among features).

### Behavioral requirements: admitted sequences of operations

- After coin insertion, user must press a button to choose whether (s)he wants sugar, after which (s)he may select a beverage.
- Optionally, a ringtone is rung after delivering a beverage.
- The machine returns to its idle state when the beverage is taken.
Coffee machine family: Feature model

10 different valid products (coffee machines defined by features)

\[
\{ \{m, s, o, b, c, \epsilon\}, \{m, s, o, b, c, \epsilon, r\}, \{m, s, o, b, c, \epsilon, t\}, \{m, s, o, b, c, \$, r\}, \{m, s, o, b, c, \$, t\}, \{m, s, o, b, c, \epsilon, t, r\}, \{m, s, o, b, c, \epsilon, p, r\}, \{m, s, o, b, c, \$, t, r\}, \{m, s, o, b, c, \epsilon, p, r, t\}\}
\]
A European coffee machine \(\{m, s, o, b, c, \varepsilon, p, r\}\)
A Canadian coffee machine ($\{m, s, o, b, c, $, r\}$)
FTS associated to feature model of family
Product derivation: MTS versus FTS

FTS  All and only products that are correct w.r.t. the requirements are derived (price: include a feature diagram in each FTS)

MTS  Also correctly derived products may violate constraints of the type that MTSs cannot model (cf. LTS on next slide)
**Product derivation: MTS versus FTS**

**FTS**  All and only products that are correct w.r.t. the requirements are derived (price: include a feature diagram in each FTS)

**MTS**  Also correctly derived products may violate constraints of the type that MTSs cannot model (cf. LTS on next slide)
A correct but not valid product LTS of MTS

Formal Description of Variability in SPLE
Definition of \textit{vACTL} (slight revision of MHML from paper)

Variability and action-based branching-time temporal logic

A temporal logic based on the “Hennessy-Milner logic with until”, but augmented with deontic \(O\) (\textit{obligatory}) and \(P\) (\textit{permitted}) operators, CTL’s path operators \(E\) and \(A\) and ACTL’s action-based Until operator, both with and without a deontic interpretation

Syntax of \textit{vACTL}

\[
\phi ::= \text{true} | \neg \phi | \phi \land \phi' | \langle a \rangle \phi | [a] \phi | \langle a \rangle \Box \phi | [a] \Box \phi | E \pi | A \pi
\]

\[
\pi ::= \phi \{ \varphi \} U \{ \varphi' \} \phi' | \phi \{ \varphi \} U \Box \{ \varphi' \} \phi'
\]

Thus defines state formulae \(\phi\), path formulae \(\pi\) and action formulae \(\varphi\) (boolean compositions of actions) over set of atomic actions \{a, b, \ldots\}

\(\langle a \rangle \Box\) and \([a] \Box\) represent the classic deontic modalities \(O\) and \(P\), resp.
Definition of \( \text{VACTL} \) (slight revision of MHML from paper)

Variability and action-based branching-time temporal logic

A temporal logic based on the “Hennessy-Milner logic with until”, but augmented with deontic \( O \) (obligatory) and \( P \) (permitted) operators, CTL’s path operators \( E \) and \( A \) and ACTL’s action-based Until operator, both with and without a deontic interpretation.

Syntax of \( \text{VACTL} \)

\[
\phi ::= \text{true} \mid \neg \phi \mid \phi \land \phi' \mid \langle a \rangle \phi \mid [a] \phi \mid \langle a \rangle \Box \phi \mid [a] \Box \phi \mid E \pi \mid A \pi
\]

\[
\pi ::= \phi \{ \varphi \} U \{ \varphi' \} \phi' \mid \phi \{ \varphi \} U \Box \{ \varphi' \} \phi'
\]

Thus defines state formulae \( \phi \), path formulae \( \pi \) and action formulae \( \varphi \) (boolean compositions of actions) over set of atomic actions \( \{a, b, \ldots\} \).
Definition of \textit{vACTL} (slight revision of MHML from paper)

Variability and action-based branching-time temporal logic

A temporal logic based on the “Hennessy-Milner logic with until”, but augmented with deontic $O$ (obligatory) and $P$ (permitted) operators, CTL’s path operators $E$ and $A$ and ACTL’s action-based Until operator, both with and without a deontic interpretation.

Syntax of \textit{vACTL}

$$\phi ::= \text{true} \mid \neg \phi \mid \phi \land \phi' \mid \langle a \rangle \phi \mid [a] \phi \mid \langle a \rangle \Box \phi \mid [a] \Box \phi \mid E \pi \mid A \pi$$

$$\pi ::= \phi \{\varphi\} U \{\varphi'\} \phi' \mid \phi \{\varphi\} U \Box \{\varphi'\} \phi'$$

Thus defines state formulae $\phi$, path formulae $\pi$ and action formulae $\varphi$ (boolean compositions of actions) over set of atomic actions $\{a, b, \ldots\}$.

$\langle a \rangle \Box$ and $[a] \Box$ represent the classic deontic modalities $O$ and $P$, resp.
VACTL: Semantics over MTS

- $q \models true$ always holds
- $q \models \neg \phi$ iff not $q \models \phi$
- $q \models \phi \land \phi'$ iff $q \models \phi$ and $q \models \phi'$
- $q \models \langle a \rangle \phi$ iff $\exists q' \in Q$ such that $q \overset{a}{\rightarrow} q'$, and $q' \models \phi$
- $q \models [a] \phi$ iff $\forall q' \in Q$ such that $q \overset{a}{\rightarrow} q'$, we have $q' \models \phi$
- $q \models \langle a \rangle \Box \phi$ iff $\exists q' \in Q$ such that $q \overset{a}{\rightarrow} \Box q'$, and $q' \models \phi$
- $q \models [a] \Box \phi$ iff $\forall q' \in Q$ such that $q \overset{a}{\rightarrow} \Box q'$, we have $q' \models \phi$
- $q \models E \pi$ iff $\exists \sigma' \in \text{path}(q)$ such that $\sigma' \models \pi$
- $q \models A \pi$ iff $\forall \sigma' \in \text{path}(q)$ such that $\sigma' \models \pi$
- $\sigma \models \phi \{ \varphi \} U \{ \varphi' \} \phi'$ iff $\exists j \geq 1: \sigma(j) \models \phi'$, $\sigma\{j\} \models \varphi'$, and $\sigma(j + 1) \models \phi'$, and $\forall 1 \leq i < j: \sigma(i) \models \phi$ and $\sigma\{i\} \models \varphi$
- $\sigma \models \phi \{ \varphi \} U \Box \{ \varphi' \} \phi'$ iff $\sigma$ is a must path $\sigma \Box$ and $\sigma \Box \models \phi \{ \varphi \} U \{ \varphi' \} \phi'$

Abbreviations: $EF \phi = E(\text{true} \{ \text{true} \} U \{ \text{true} \} \phi)$; $EF \Box \phi = E(\text{true} \{ \text{true} \} U \Box \{ \text{true} \} \phi)$; $EF \{ \varphi \} \text{true} = E(\text{true} \{ \text{true} \} U \{ \varphi \} \text{true})$; $EF \Box \{ \varphi \} \text{true} = E(\text{true} \{ \text{true} \} U \Box \{ \varphi \} \text{true})$; $AG \phi = \neg EF \neg \phi$; $AG \Box \phi = \neg EF \Box \neg \phi$; etc.
VACTL: Semantics over MTS

- $q \models true$ always holds
- $q \models \neg \phi$ iff not $q \models \phi$
- $q \models \phi \land \phi'$ iff $q \models \phi$ and $q \models \phi'$
- $q \models \langle a \rangle \phi$ iff $\exists q' \in Q$ such that $q \overset{a}{\to} q'$, and $q' \models \phi$
- $q \models [a] \phi$ iff $\forall q' \in Q$ such that $q \overset{a}{\to} q'$, we have $q' \models \phi$
- $q \models \langle a \rangle \Box \phi$ iff $\exists q' \in Q$ such that $q \overset{a}{\to} q'$, and $q' \models \phi$
- $q \models [a] \Box \phi$ iff $\forall q' \in Q$ such that $q \overset{a}{\to} q'$, we have $q' \models \phi$
- $q \models E \pi$ iff $\exists \sigma' \in \text{path}(q)$ such that $\sigma' \models \pi$
- $q \models A \pi$ iff $\forall \sigma' \in \text{path}(q)$ such that $\sigma' \models \pi$
- $\sigma \models \phi \{\varphi\} U \{\varphi'\} \phi'$ iff $\exists j \geq 1: \sigma(j) \models \phi'$, $\sigma\{j\} \models \varphi'$, and $\sigma(j + 1) \models \phi'$, and $\forall 1 \leq i < j: \sigma(i) \models \phi$ and $\sigma\{i\} \models \varphi$
- $\sigma \models \phi \{\varphi\} U \Box \{\varphi'\} \phi'$ iff $\sigma$ is a must path $\sigma \Box$ and $\sigma \Box \models \phi \{\varphi\} U \{\varphi'\} \phi'$

Abbreviations: $EF \phi = E(true \{true\} U \{true\} \phi)$; $EF \Box \phi = E(true \{true\} U \Box \{true\} \phi)$; $EF \{\varphi\} true = E(true \{true\} U \{\varphi\} true)$; $EF \Box \{\varphi\} true = E(true \{true\} U \Box \{\varphi\} true)$; $AG \phi = \neg EF \neg \phi$; $AG \Box \phi = \neg EF \Box \neg \phi$; etc.
VACTL can complement behavioral description of MTS by expressing constraints over possible products of a family that MTS cannot model.

**Template ALT**: Features F1 and F2 are *alternative*

\[ (EF \{ F1 \} true \lor EF \{ F2 \} true) \land \neg (EF \{ F1 \} true \land EF \{ F2 \} true) \]

**Template EXC**: Feature F1 *excludes* feature F2

\[ ((EF \{ F1 \} true) \implies (AG \neg \langle F2 \rangle true)) \land ((EF \{ F2 \} true) \implies (AG \neg \langle F1 \rangle true)) \]

**Template REQ**: Feature F1 *requires* feature F2

\[ (EF \{ F1 \} true) \implies (EF \Box \{ F2 \} true) \]

Define no full temporal ordering among the related features

Duty of behavioral LTS/MTS model, to be verified by VACTL formulae.
VA-CTL can complement behavioral description of MTS by expressing constraints over possible products of a family that MTS cannot model.

**Template ALT:** Features F1 and F2 are *alternative*

\[(EF \Box \{ F1 \} true \lor EF \Box \{ F2 \} true) \land \neg (EF \{ F1 \} true \land EF \{ F2 \} true)\]

**Template EXC:** Feature F1 *excludes* feature F2

\[((EF \{ F1 \} true) \implies (AG \neg \langle F2 \rangle true)) \land ((EF \{ F2 \} true) \implies (AG \neg \langle F1 \rangle true))\]

**Template REQ:** Feature F1 *requires* feature F2

\[(EF \{ F1 \} true) \implies (EF \Box \{ F2 \} true)\]

Define no full temporal ordering among the related features.

Duty of behavioral LTS/MTS model, to be verified by VA-CTL formulae.
VACTL can complement behavioral description of MTS by expressing constraints over possible products of a family that MTS cannot model.

**Template ALT:** Features F1 and F2 are *alternative*

\[(EF \Box \{ F1 \} \text{true} \lor EF \Box \{ F2 \} \text{true}) \land \neg (EF \{ F1 \} \text{true} \land EF \{ F2 \} \text{true})\]

**Template EXC:** Feature F1 *excludes* feature F2

\[((EF \{ F1 \} \text{true}) \implies (AG \neg \langle F2 \rangle \text{true})) \land ((EF \{ F2 \} \text{true}) \implies (AG \neg \langle F1 \rangle \text{true}))\]

**Template REQ:** Feature F1 *requires* feature F2

\[(EF \{ F1 \} \text{true}) \implies (EF \Box \{ F2 \} \text{true})\]

Define no full temporal ordering among the related features.
VACTL can complement behavioral description of MTS by expressing constraints over possible products of a family that MTS cannot model.

**Template ALT:** Features F1 and F2 are *alternative*

\[
(\text{EF} \square \{F1\} \text{ true} \lor \text{EF} \square \{F2\} \text{ true}) \land \neg (\text{EF} \{F1\} \text{ true} \land \text{EF} \{F2\} \text{ true})
\]

**Template EXC:** Feature F1 *excludes* feature F2

\[
((\text{EF} \{F1\} \text{ true}) \implies (\text{AG} \neg \langle F2 \rangle \text{ true})) \land ((\text{EF} \{F2\} \text{ true}) \implies (\text{AG} \neg \langle F1 \rangle \text{ true}))
\]

**Template REQ:** Feature F1 *requires* feature F2

\[
(\text{EF} \{F1\} \text{ true}) \implies (\text{EF} \square \{F2\} \text{ true})
\]

Define no full temporal ordering among the related features.

Duty of behavioral LTS/MTS model, to be verified by VACTL formulae.
VACTL can complement behavioral description of MTS by expressing constraints over possible products of a family that MTS cannot model.

**Template ALT:** Features F1 and F2 are *alternative*

\[(EF □ \{F1\} true \lor EF □ \{F2\} true) \land \neg (EF \{F1\} true \land EF \{F2\} true)\]

**Template EXC:** Feature F1 *excludes* feature F2

\[((EF \{F1\} true) \implies (AG \neg \langle F2 \rangle true)) \land ((EF \{F2\} true) \implies (AG \neg \langle F1 \rangle true))\]

**Template REQ:** Feature F1 *requires* feature F2

\[(EF \{F1\} true) \implies (EF □ \{F2\} true)\]

Define no full temporal ordering among the related features. Duty of behavioral LTS/MTS model, to be verified by VACTL formulae.
Model checking families and products

Verify property expressed as logical formula $\psi$ over model $T$
- Decide whether $T \models \psi$, where $\models$ is the logic’s satisfaction relation
- If $T \not\models \psi$, then it is usually easy to generate a counterexample
- If $T$ is finite, model checking thus reduces to a graph search

On the fly: Only a fragment of the overall state space might need to be generated and analysed to be able to produce the correct result

VMC: http://fmtlab.isti.cnr.it/vmc/

An on-the-fly model-checker for $\nu$ACTL is defined as particularization of the FMC model checker for ACTL over a CCS-like input language

Recently implemented also our algorithm for product derivation
- Explore and verify product families (MTS)
- Generate all valid products, explore and verify products (LTS)
Verify property expressed as logical formula $\psi$ over model $T$

- Decide whether $T \models \psi$, where $\models$ is the logic’s satisfaction relation
- If $T \not\models \psi$, then it is usually easy to generate a counterexample
- If $T$ is finite, model checking thus reduces to a graph search

On the fly: Only a fragment of the overall state space might need to be generated and analysed to be able to produce the correct result

**VMC:** [http://fmtlab.isti.cnr.it/vmc/](http://fmtlab.isti.cnr.it/vmc/)

An on-the-fly model-checker for $\text{vACTL}$ is defined as particularization of the FMC model checker for $\text{ACTL}$ over a CCS-like input language

Recently implemented also our algorithm for product derivation

- Explore and verify product families (MTS)
- Generate all valid products, explore and verify products (LTS)
Model checking families and products

Verify property expressed as logical formula $\psi$ over model $T$
- Decide whether $T \models \psi$, where $\models$ is the logic’s satisfaction relation
- If $T \not\models \psi$, then it is usually easy to generate a counterexample
- If $T$ is finite, model checking thus reduces to a graph search

On the fly: Only a fragment of the overall state space might need to be generated and analysed to be able to produce the correct result

**VMC**: [http://fmtlab.isti.cnr.it/vmc/](http://fmtlab.isti.cnr.it/vmc/)

An on-the-fly model-checker for $\textit{vACTL}$ is defined as particularization of the FMC model checker for ACTL over a CCS-like input language

Recently implemented also our algorithm for product derivation
- Explore and verify product families (MTS)
- Generate all valid products, explore and verify products (LTS)
Property D: Always once a coffee has been selected, a coffee is eventually delivered

\[ AG \left[ \text{coffee} \right] \quad AF \left[ \{ \text{pour coffee} \} \right] \quad \text{true} \]

Property E: A coffee machine may never deliver a coffee before a coin has been inserted

\[ A \left[ \text{true} \quad \{ \neg \text{pour coffee} \} \right] \quad U \left[ \{ 1\$ \lor 1\€ \} \right] \quad \text{true} \]

<table>
<thead>
<tr>
<th>Property</th>
<th>MTS family</th>
<th>European</th>
<th>Canadian</th>
<th>LTS product</th>
</tr>
</thead>
<tbody>
<tr>
<td>A: ALT</td>
<td>false</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>B: EXC</td>
<td>false</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>C: REQ</td>
<td>false</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>D</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>E</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
</tbody>
</table>
Model checking temporal orderings

Property D: Always once a coffee has been selected, a coffee is eventually delivered

\[ AG [\text{coffee}] \ AF \{\text{pour coffee}\} \ true \]

Property E: A coffee machine may never deliver a coffee before a coin has been inserted

\[ A [\text{true} \ \{\neg \text{pour coffee}\} \ U \{1\$ \lor 1\€\} \ true] \]

<table>
<thead>
<tr>
<th>Property</th>
<th>MTS family</th>
<th>European</th>
<th>Canadian</th>
<th>LTS product</th>
</tr>
</thead>
<tbody>
<tr>
<td>A: ALT</td>
<td>false</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>B: EXC</td>
<td>false</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>C: REQ</td>
<td>false</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>D</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>E</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
</tbody>
</table>
Property D: Always once a coffee has been selected, a coffee is eventually delivered

$$\text{AG} \ [\text{coffee}] \ \text{AF} \ □ \ \{\text{pour coffee}\} \ \text{true}$$

Property E: A coffee machine may never deliver a coffee before a coin has been inserted

$$\text{A} \ [\text{true} \ \{\neg \text{pour coffee}\} \ \text{U} \ □ \ \{1$ \lor 1€\} \ \text{true}]$$

<table>
<thead>
<tr>
<th>Property</th>
<th>MTS family</th>
<th>European</th>
<th>Canadian</th>
<th>LTS product</th>
</tr>
</thead>
<tbody>
<tr>
<td>A: ALT</td>
<td>false</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>B: EXC</td>
<td>false</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>C: REQ</td>
<td>false</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>D</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>E</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
</tbody>
</table>
MTS specification of coffee machine family in VMC

\[ T_0 = \text{may(euro)}.T_1 + \text{may(dollar)}.T_1 \\
T_1 = \text{must(sugar)}.T_2 + \text{must(no_sugar)}.T_3 \\
T_2 = \text{must(coffee)}.T_4 + \text{may(tea)}.T_5 + \text{may(cappuccino)}.T_6 \\
T_3 = \text{may(cappuccino)}.T_7 + \text{may(tea)}.T_8 + \text{must(coffee)}.T_9 \\
T_4 = \text{must(pour_sugar)}.T_9 \\
T_5 = \text{must(pour_sugar)}.T_8 \\
T_6 = \text{must(pour_sugar)}.T_7 \\
T_7 = \text{must(pour_milk)}.T_10 + \text{must(pour_coffee)}.T_11 \\
T_8 = \text{must(pour_tea)}.T_12 \\
T_9 = \text{must(pour_coffee)}.T_12 \\
T_{10} = \text{must(pour_coffee)}.T_{12} \\
T_{11} = \text{must(pour_milk)}.T_{12} \\
T_{12} = \text{may(no_ring)}.T_{13} + \text{may(ring_a_tone)}.T_{13} \\
T_{13} = \text{must(cup_taken)}.T_0 \]

\text{net SYS} = T_{0} \]

Constraints \{
\text{euro ALT dollar} \\
\text{dollars EXC cappuccino} \\
\text{cappuccino REQ ring_a_tone} \}

\text{AF} <\text{ring_a_tone}> \text{true}
Evaluation of formula "AF true" on products

| product11.txt | Formula evaluates | FALSE |
| product12.txt | Formula evaluates | TRUE  |
| product13.txt | Formula evaluates | TRUE  |
| product20.txt | Formula evaluates | FALSE |
| product21.txt | Formula evaluates | TRUE  |
| product22.txt | Formula evaluates | TRUE  |
| product26.txt | Formula evaluates | FALSE |
| product27.txt | Formula evaluates | TRUE  |
| product28.txt | Formula evaluates | TRUE  |
| product33.txt | Formula evaluates | TRUE  |
| product34.txt | Formula evaluates | TRUE  |
| product39.txt | Formula evaluates | TRUE  |
| product40.txt | Formula evaluates | TRUE  |
| product42.txt | Formula evaluates | TRUE  |
| product43.txt | Formula evaluates | TRUE  |
| product44.txt | Formula evaluates | FALSE |
| product45.txt | Formula evaluates | TRUE  |
| product46.txt | Formula evaluates | TRUE  |
| product48.txt | Formula evaluates | TRUE  |
| product49.txt | Formula evaluates | TRUE  |
| product53.txt | Formula evaluates | FALSE |
VMC: Variability Model Checker

VMC can be used to automatically derive, from an MTS description of a product family and an associated set of $\text{vACTL}$ formulae expressing further constraints for this family, all its valid products (i.e. a set of LTS descriptions of products, each one correct w.r.t. all $\text{vACTL}$ constraints).

Future work required before possible application in industry

- A high-level language hiding all semantic details (investigate relation between features and actions)
- A predefined taxonomy for properties specified in $\text{vACTL}$ (like specification patterns repository for LTL, (A)CTL, etc.)
- Scale to large, industrial-size product families (with many variation points and many features)
VMC can be used to automatically derive, from an MTS description of a product family and an associated set of \( \text{vACTL} \) formulae expressing further constraints for this family, all its valid products (i.e. a set of LTS descriptions of products, each one correct w.r.t. all \( \text{vACTL} \) constraints).

VMC can also be used to experiment with products, using \( \text{vACTL} \) to verify further (temporal) constraints, etc.

Future work required before possible application in industry:

- A high-level language hiding all semantic details (investigate relation between features and actions)
- A predefined taxonomy for properties specified in \( \text{vACTL} \) (like specification patterns repository for LTL, (A)CTL, etc.)
- Scale to large, industrial-size product families (with many variation points and many features)
VMC: Variability Model Checker

VMC can be used to automatically derive, from an MTS description of a product family and an associated set of $\forall$ACTL formulae expressing further constraints for this family, all its valid products (i.e. a set of LTS descriptions of products, each one correct w.r.t. all $\forall$ACTL constraints).

VMC can also be used to experiment with products, using $\forall$ACTL to verify further (temporal) constraints, etc.

Future work required before possible application in industry

- A high-level language hiding all semantic details (investigate relation between features and actions)
- A predefined taxonomy for properties specified in $\forall$ACTL (like specification patterns repository for LTL, (A)CTL, etc.)
- Scale to large, industrial-size product families (with many variation points and many features)
Variability Modelling of Software-Intensive Systems (VaMoS’12)
6th International Workshop
Leipzig, Germany, January 25–27, 2012

⇒ http://www.vamos-workshop.net

Submission: October 30, 2011
Notification: November 27, 2011

with keynotes by:

- Paulo Borba, Centro de Informatica, Universidade Federal de Pernambuco, BR
- Charles Krueger, BigLever Software, Inc., USA