Family-based model checking with a feature $\mu$-calculus

Maurice ter Beek, Erik de Vink, and Tim Willemse

ISTI-CNR, Pisa, Italy & TU/e, Eindhoven, The Netherlands

Modelling and Analysis of Variability in Software Product Lines
ISTI–CNR, Pisa, June 26–30, 2017
Outline

1. Context: verification of behavioural SPL models
   - Family-based modelling and analysis

2. Towards family-based model checking with mCRL2
   - Recall: the $\mu$-calculus $\mu L$ over LTSs
   - A feature $\mu$-calculus $\mu L_f$ over FTSs

3. Main results of paper @ FMSPLE’16
   - From $\mu L_f$ to $\mu L$

4. Main results of paper @ FASE’17
   - A $\mu$-calculus with data $\mu L_{FO}$ over parametrised LTSs
   - From $\mu L_f$ to $\mu L_{FO}$ (and back to $\mu L$)
   - Family-based partitioning algorithm for $\mu L_f$
   - Case study: minepump SPL benchmark

5. Conclusions and future work
   - The quest for an efficient partitioning strategy
Family-based modelling and analysis

Software product line (SPL) or product family

- Configurable (software) system whose variants (products) differ by the provided features, i.e. the functionality that is relevant for an end-user
- Popular in embedded and critical systems domain: formal modelling and analysis techniques for proving SPL behaviour correct are widely studied
  Thüm et al., A classification and survey of analysis strategies for SPLs @ ACM Comput. Surv. (2014)
- Challenge existing formal methods and tools by potentially high number of different products, each giving rise to a large state space in general

⇒ Lift success stories from products to families exploiting variability

Dedicated family-based SPL behavioural models and model checkers (e.g. FTSs, Feature Nets, MTSs, PL-CCS, DeltaCCS, QFLan, SNIP, ProVeLines, VMC) but recently...

Dimovski et al., Family-based model checking without a family-based model checker @ SPIN’15
Chrszon et al., Family-based modeling and analysis for probabilistic systems – featuring ProFeat @ FASE’16
Dimovski et al., Variability-specific Abstraction Refinement for Family-based Model Checking @ FASE’17
Family-based modelling and analysis

Software product line (SPL) or product family

- Configurable (software) system whose variants (products) differ by the provided features, i.e. the functionality that is relevant for an end-user
- Popular in embedded and critical systems domain: formal modelling and analysis techniques for proving SPL behaviour correct are widely studied
  Thüm et al., A classification and survey of analysis strategies for SPLs @ ACM Comput. Surv. (2014)
- Challenge existing formal methods and tools by potentially high number of different products, each giving rise to a large state space in general

⇒ Lift success stories from products to families exploiting variability

Dedicated family-based SPL behavioural models and model checkers (e.g. FTSs, Feature Nets, MTSs, PL-CCS, DeltaCCS, QFLan, SNIP, ProVeLines, VMC) but recently...

Dimovski et al., Family-based model checking without a family-based model checker @ SPIN’15
Chrszon et al., Family-based modeling and analysis for probabilistic systems – featuring ProFeat @ FASE’16
Dimovski et al., Variability-specific Abstraction Refinement for Family-based Model Checking @ FASE’17
Family-based modelling and analysis

Software product line (SPL) or product family

- Configurable (software) system whose variants (products) differ by the provided features, i.e. the functionality that is relevant for an end-user
- Popular in embedded and critical systems domain: formal modelling and analysis techniques for proving SPL behaviour correct are widely studied
  Thüm et al., A classification and survey of analysis strategies for SPLs @ ACM Comput. Surv. (2014)
- Challenge existing formal methods and tools by potentially high number of different products, each giving rise to a large state space in general

⇒ Lift success stories from products to families exploiting variability

Dedicated family-based SPL behavioural models and model checkers (e.g. FTSs, Feature Nets, MTSs, PL-CCS, DeltaCCS, QFLan, SNIP, ProVeLines, VMC)

but recently...

Dimovski et al., Family-based model checking without a family-based model checker @ SPIN’15
Chrszon et al., Family-based modeling and analysis for probabilistic systems – featuring ProFeat @ FASE’16
Dimovski et al., Variability-specific Abstraction Refinement for Family-based Model Checking © FASE’17
Family-based modelling and analysis

Software product line (SPL) or product family

- Configurable (software) system whose variants (products) differ by the provided features, i.e. the functionality that is relevant for an end-user
- Popular in embedded and critical systems domain: formal modelling and analysis techniques for proving SPL behaviour correct are widely studied
  
  Thüm et al., A classification and survey of analysis strategies for SPLs @ ACM Comput. Surv. (2014)

- Challenge existing formal methods and tools by potentially high number of different products, each giving rise to a large state space in general

⇒ Lift success stories from products to families exploiting variability

Dedicated family-based SPL behavioural models and model checkers (e.g. FTSs, Feature Nets, MTSs, PL-CCS, DeltaCCS, QFLan, SNIP, ProVeLines, VMC) but recently...

Dimovski et al., Family-based model checking without a family-based model checker @ SPIN’15
Chrszon et al., Family-based modeling and analysis for probabilistic systems – featuring ProFeat @ FASE’16
Dimovski et al., Variability-specific Abstraction Refinement for Family-based Model Checking @ FASE’17
FTS: featured transition systems

Classen et al., Model Checking Lots of Systems @ ICSE’10

FTS $F = (S, \theta, s_\star)$ over actions $\mathcal{A}$ and features $\mathcal{F}$ (typical element $f$)

- $S$ a finite set of states
- $\theta : S \times \mathcal{A} \times S \rightarrow \mathcal{B}[\mathcal{F}]$ the transition constraint function
- $s_\star \in S$ the initial state

LTS $L = (S, \rightarrow, s_\star)$ over actions $\mathcal{A}$

- $S$ a finite set of states
- $\rightarrow \subseteq S \times \mathcal{A} \times S$ the transition relation
- $s_\star \in S$ the initial state
FTS: featured transition systems

Classen et al., Model Checking Lots of Systems @ ICSE’10

FTS $F = (S, \theta, s_*)$ over actions $\mathcal{A}$ and features $\mathcal{F}$ (typical element $f$)

- $S$ a finite set of states
- $\theta : S \times \mathcal{A} \times S \rightarrow \mathbb{B}[\mathcal{F}]$ the transition constraint function
- $s_* \in S$ the initial state

LTS $F|_p = (S, \rightarrow_{F|_p}, s_*)$ projection of $F$ with respect to product $p$

$$
\rightarrow_{F|_p} \subseteq S \times \mathcal{A} \times S \text{ such that } s \xrightarrow{a}_{F|_p} t \text{ iff } p \models \theta(s, a, t)
$$

$\mathcal{P} \subseteq 2^\mathcal{F}$ set of products $p, q, \ldots$

$\mathcal{P} \subseteq \mathcal{P}$ product family, identified by feature expression $\gamma_p \in \mathbb{B}[\mathcal{F}]$

$\gamma \in \mathbb{B}[\mathcal{F}]$ interpreted as set of products $Q_\gamma$,

i.e. products $p$ for which the induced truth assignment ($\text{true}$ for $f \in p$, $\text{false}$ for $f \notin p$) validates $\gamma$
FTS of example SPL

Product line of (four) coffee machines with independent features \{\$, €\}

Products with feature \$ can obtain an xxl coffee upon coin insertion, but products without cannot.

how to express this? and how to model check this efficiently?
FTS of example SPL

Product line of (four) coffee machines with independent features \{\$, €\}

Products with feature \$ can obtain an xxl coffee upon coin insertion, but products without cannot

how to express this? and how to model check this efficiently?
Towards family-based model checking

- We showed how to use mCRL2 for product-based model checking of SPL models
  ter Beek & de Vink @ FormaliSE’14, SPLC’14

- We proposed a feature-oriented modular verification technique for SPL models with mCRL2
  ter Beek & de Vink @ FMSPLE’14, ISoLA’14

- We extended branching bisimulation for LTSs to branching feature bisimulation for FTSs
  Belder, ter Beek & de Vink @ FMSPLE’15

- We defined feature-oriented modal $\mu$-calculi to reason on FTSs by explicitly incorporating feature expressions in the modal operators
  ter Beek, de Vink & Willemse @ FMSPLE’16

- We showed how to use off-the-shelf tools like mCRL2 for family-based model checking of SPL models
  ter Beek, de Vink & Willemse @ FASE’17
Towards family-based model checking

- We showed how to use mCRL2 for product-based model checking of SPL models  
  ter Beek & de Vink @ FormaliSE’14, SPLC’14

- We proposed a feature-oriented modular verification technique for SPL models with mCRL2  
  ter Beek & de Vink @ FMSPLE’14, ISoLA’14

- We extended branching bisimulation for LTSs to branching feature bisimulation for FTSs  
  Belder, ter Beek & de Vink @ FMSPLE’15

- We defined feature-oriented modal $\mu$-calculi to reason on FTSs by explicitly incorporating feature expressions in the modal operators  
  ter Beek, de Vink & Willemse @ FMSPLE’16

- We showed how to use off-the-shelf tools like mCRL2 for family-based model checking of SPL models  
  ter Beek, de Vink & Willemse @ FASE’17
The modal $\mu$-calculus $\mu L$

set of actions $\mathcal{A}$, set of variables $X$

$\mu$-calculus $\mu L$ over $\mathcal{A}$ and $X$, formula $\varphi \in \mu L$ given by

$$\varphi :: = \bot | \top |$$
$$\ \ \ \ \ \ \neg \varphi | \varphi \lor \psi | \varphi \land \psi |$$
$$\langle a \rangle \varphi | [a] \varphi |$$
$$X | \mu X.\varphi | \nu X.\varphi$$

duality $\langle a \rangle \varphi \equiv \neg [a] \neg \varphi$, a positive normal form avoids negations

for $\mu X.\varphi$ and $\nu X.\varphi$, all free occurrences of $X$ in $\varphi$ are in the scope of an even number of negations (guarantees well-definedness fixpoint formulae)
A feature $\mu$-calculus $\mu L_f$

set of actions $\mathcal{A}$, set of features $\mathcal{F}$, set of variables $\mathcal{X}$

feature $\mu$-calculus $\mu L_f$ over $\mathcal{A}$, $\mathcal{F}$, and $\mathcal{X}$, formula $\varphi_f \in \mu L_f$ given by

$$\varphi_f ::= \bot \mid \top \mid
\neg \varphi_f \mid \varphi_f \lor \psi_f \mid \varphi_f \land \psi_f \mid
\langle a \mid \chi \rangle \varphi_f \mid [a \mid \chi] \varphi_f \mid
\mathcal{X} \mid \mu \mathcal{X}.\varphi_f \mid \nu \mathcal{X}.\varphi_f$$

for $\mu \mathcal{X}.\varphi_f$ and $\nu \mathcal{X}.\varphi_f$ an even number of negations as before
A semantics of $\mu L_f$ over FTSs

state-family pairs $(s, P) \in sPSet = 2^{S \times 2^P}$
state-family environments $\zeta \in sPEnv = X \rightarrow sPSet$
semantics $[\cdot]_F : \mu L_f \rightarrow sPEnv \rightarrow sPSet$

\[
\begin{align*}
[\bot]_F(\zeta) &= \emptyset \\
[\top]_F(\zeta) &= S \times 2^P \\
[\neg \phi_f]_F(\zeta) &= (S \times 2^P) \setminus [\phi_f]_F(\zeta) \\
[(\phi_f \lor \psi_f)]_F(\zeta) &= [\phi_f]_F(\zeta) \cup [\psi_f]_F(\zeta) \\
[(\phi_f \land \psi_f)]_F(\zeta) &= [\phi_f]_F(\zeta) \cap [\psi_f]_F(\zeta) \\
[\langle a|\chi \rangle \phi_f]_F(\zeta) &= \ldots \\
[[a|\chi] \phi_f]_F(\zeta) &= \ldots \\
[X]_F(\zeta) &= \zeta(X) \\
[\mu X. \phi_f]_F(\zeta) &= \text{lfp}(W \mapsto [\phi_f]_F(\zeta(W/X))) \\
[\nu X. \phi_f]_F(\zeta) &= \text{gfp}(W \mapsto [\phi_f]_F(\zeta(W/X)))
\end{align*}
\]
A semantics of $\mu L_f$ over FTSs

$$\llbracket \langle a \mid \chi \rangle \varphi_f \rrbracket_F(\zeta) = \{ (s, P) \mid P \subseteq Q_\chi \land \exists \gamma, t: s \xrightarrow{a\mid\gamma} F t \land P \subseteq Q_\gamma \land (t, P \cap Q_\chi \cap Q_\gamma) \in \llbracket \varphi_f \rrbracket_F(\zeta) \}$$

$\langle a \mid \chi \rangle \varphi_f$ holds (for a family $P$ with respect to an FTS $F$ in a state $s$)
if all products in $P$ satisfy the feature expression $\chi$ and
there is an $a$-transition, shared among all products in $P$,
that leads to a state where $\varphi_f$ holds for $P$

$$\llbracket [a \mid \chi] \varphi_f \rrbracket_F(\zeta) = \{ (s, P) \mid \forall \gamma, t: s \xrightarrow{a\mid\gamma} F t \land P \cap Q_\chi \cap Q_\gamma \neq \emptyset \Rightarrow (t, P \cap Q_\chi \cap Q_\gamma) \in \llbracket \varphi_f \rrbracket_F(\zeta) \}$$

$[a \mid \chi] \varphi_f$ holds (for a family $P$ with respect to an FTS $F$ in a state $s$)
if for each subset $P'$ of $P$ for which an $a$-transition is possible,
$\varphi_f$ holds for $P'$ in the target state of that $a$-transition
A semantics of $\mu L_f$ over FTSs

$$\ll [a|\chi] \varphi_f \rr_F(\zeta) = \{(s, P) \mid P \subseteq Q_\chi \land \exists \gamma, t: s \xrightarrow{a|\gamma}_F t \land P \subseteq Q_\gamma \land (t, P \cap Q_\chi \cap Q_\gamma) \in \ll \varphi_f \rr_F(\zeta)\}$$

$[a|\chi] \varphi_f$ holds (for a family $P$ with respect to an FTS $F$ in a state $s$) if all products in $P$ satisfy the feature expression $\chi$ and there is an $a$-transition, shared among all products in $P$, that leads to a state where $\varphi_f$ holds for $P$.

$$\ll [a|\chi] \varphi_f \rr_F(\zeta) = \{(s, P) \mid \forall \gamma, t: s \xrightarrow{a|\gamma}_F t \land P \cap Q_\chi \cap Q_\gamma \neq \emptyset \Rightarrow (t, P \cap Q_\chi \cap Q_\gamma) \in \ll \varphi_f \rr_F(\zeta)\}$$

$[a|\chi] \varphi_f$ holds (for a family $P$ with respect to an FTS $F$ in a state $s$) if for each subset $P'$ of $P$ for which an $a$-transition is possible, $\varphi_f$ holds for $P'$ in the target state of that $a$-transition.
Example $\mu L_f$ formula: duality lost

$s, P \models F \varphi_f$ iff $(s, P) \in \| \varphi_f \|_F$

Products $p_1 = \{ f, g \}$ and $p_2 = \{ g \}$

Clearly: $\{ f, g \} \models F|_{p_1} \langle a \rangle_T$

$\{ g \} \models F|_{p_2} \langle a \rangle_T$

but $\ldots \{ p_1, p_2 \} \not\models F \langle a|\top \rangle_T$

Hence, since neither $\{ p_1, p_2 \} \models F \langle a|\top \rangle_T$ nor $\{ p_1, p_2 \} \models F \langle a|\top \rangle_{\bot}$, $\langle a|\chi \rangle$ and $[a|\chi]$ are not each other’s dual.
Example $\mu L_f$ formula: duality lost

$s, P \models_F \varphi_f$ iff $(s, P) \in \llbracket \varphi_f \rrbracket_F$

Products $p_1 = \{f, g\}$ and $p_2 = \{g\}$

Clearly: $\{f, g\} \models_{F|p_1} \langle a \rangle T$

$\{g\} \models_{F|p_2} \langle a \rangle T$

but... $\{p_1, p_2\} \not\models_F \langle a|\top \rangle T$

Hence, since neither $\{p_1, p_2\} \models_F \langle a|\top \rangle T$ nor $\{p_1, p_2\} \models_F [a|\top] \bot$, $\langle a|\chi \rangle$ and $[a|\chi]$ are not each other's dual
Example $\mu L_f$ formula: duality lost

$s, P \models_F \varphi_f \iff (s, P) \in \llbracket \varphi_f \rrbracket_F$

Products $p_1 = \{f, g\}$ and $p_2 = \{g\}$

Clearly: $\{f, g\} \models_F \langle a \rangle_T$

$\{g\} \models_F \langle a \rangle_T$

but... $\{p_1, p_2\} \not\models_F \langle a | T \rangle_T$

Hence, since neither $\{p_1, p_2\} \models_F \langle a | T \rangle_T$ nor $\{p_1, p_2\} \models_F [a | T] \perp$, $\langle a | \chi \rangle$ and $[a | \chi]$ are not each other’s dual
Examples of $\mu L_f$-formulae

- $\langle ins \mid T \rangle ( [ins \mid e] \perp \land \langle std \mid T \rangle \top )$
  
  “the family of products $P$ that can execute $ins$, after which $ins$ cannot be executed by products satisfying $e$, while $std$ can be executed by all products of $P$”

- $\nu X. \mu Y. (([ins \mid e] Y \land [xxl \mid e] Y) \land [std \mid e] X)$$
  
  “for the (sub)family of products with feature $e$, action $std$ occurs infinitely often on all infinite runs over $\{ins, xxl, std\}$”

- $[true^* \mid T] ([ins \mid $] <true^*. xxl \mid T \top \top ) \land [xxl \mid \neg $]) \perp$
  
  “products with feature $\$$ can obtain an $xxl$ coffee upon coin insertion, but products without cannot”
Examples of $\mu L_f$-formulae

- $\langle \text{ins} \mid T \rangle (\langle \text{ins} \mid e \rangle \perp \land \langle \text{std} \mid T \rangle \top)$
  
  “the family of products $P$ that can execute $\text{ins}$, after which $\text{ins}$ cannot be executed by products satisfying $e$, while $\text{std}$ can be executed by all products of $P$”

- $\nu X. \mu Y. ((\langle \text{ins} \mid e \rangle Y \land \langle \text{xxl} \mid e \rangle Y) \land \langle \text{std} \mid e \rangle X)$

  “for the (sub)family of products with feature $e$, action $\text{std}$ occurs infinitely often on all infinite runs over $\{\text{ins}, \text{xxl}, \text{std}\}$”

- $\langle \text{true}^* \mid T \rangle (\langle \text{ins} \mid $ \langle \text{true}^*. \text{xxl} \mid T \rangle \top \rangle \top) \land \langle \text{xxl} \mid \neg $ \rangle \perp )$
  
  “products with feature $\$ \$ can obtain an $\text{xxl}$ coffee upon coin insertion, but products without cannot”
Examples of $\mu L_f$-formulae

- $\langle ins\mid \top \rangle ( [ins\mid \notin] \bot \land \langle std\mid \top \rangle \top )$
  “the family of products $P$ that can execute $ins$, after which $ins$ cannot be executed by products satisfying $\notin$, while $std$ can be executed by all products of $P$”

- $\nu X.\mu Y.(( [ins\mid \notin] Y \land [xxl\mid \notin] Y ) \land [std\mid \notin] X )$
  “for the (sub)family of products with feature $\notin$, action $std$ occurs infinitely often on all infinite runs over $\{ins, xxl, std\}$”

- $[true^\ast \mid \top] ( ( [ins \mid \$] \langle true^\ast. xxl \mid \top \rangle \top ) \land [xxl \mid \neg \$ ] \bot )$
  “products with feature $\$ can obtain an $xxl$ coffee upon coin insertion, but products without cannot”

multi-feature $\mu L_f$ formula, novel also w.r.t. fLTL and fCTL
From $\mu L_f$ to $\mu L$

Model checking a $\mu L_f$-formula over an FTS for an individual product reduces to model checking a $\mu L$-formula over the corresponding LTS.

projection function $pr : \mu L_f \times \mathcal{P} \rightarrow \mu L$

$pr(\bot, p) = \bot$

$pr(\top, p) = \top$

$pr(\neg \varphi_f, p) = \neg pr(\varphi_f, p)$

$pr(\varphi_f \lor \psi_f, p) = pr(\varphi_f) \lor pr(\psi_f)$

$pr(\varphi_f \land \psi_f, p) = pr(\varphi_f) \land pr(\psi_f)$

$pr(\langle a|\chi \rangle \varphi_f, p) = \text{if } p \in Q_{\chi} \text{ then } \langle a \rangle pr(\varphi_f, p) \text{ else } \bot \text{ end}$

$pr([a|\chi] \varphi_f, p) = \text{if } p \in Q_{\chi} \text{ then } [a] pr(\varphi_f, p) \text{ else } \top \text{ end}$

$pr(X, p) = X$

$pr(\mu X.\varphi_f, p) = \mu X.pr(\varphi_f, p)$

$pr(\nu X.\varphi_f, p) = \nu X.pr(\varphi_f, p)$
From $\mu L_f$ to $\mu L$

Model checking a $\mu L_f$-formula over an FTS for an individual product reduces to model checking a $\mu L$-formula over the corresponding LTS projection function $pr : \mu L_f \times P \rightarrow \mu L$

$$
pr(\perp, p) = \perp \\
pr(\top, p) = \top \\
pr(\neg \varphi_f, p) = \neg pr(\varphi_f, p) \\
pr(\varphi_f \lor \psi_f, p) = pr(\varphi_f) \lor pr(\psi_f) \\
pr(\varphi_f \land \psi_f, p) = pr(\varphi_f) \land pr(\psi_f) \\
pr(\langle a|\chi \rangle \varphi_f, p) = \textbf{if } p \in Q_{\chi} \textbf{ then } \langle a \rangle pr(\varphi_f, p) \textbf{ else } \perp \textbf{ end} \\
pr([a|\chi] \varphi_f, p) = \textbf{if } p \in Q_{\chi} \textbf{ then } [a] pr(\varphi_f, p) \textbf{ else } \top \textbf{ end} \\
pr(X, p) = X \\
pr(\mu X. \varphi_f, p) = \mu X. pr(\varphi_f, p) \\
pr(\nu X. \varphi_f, p) = \nu X. pr(\varphi_f, p)
$$
Main results of paper © FMSPLE’16

Given an FTS $F$ and a set of products $\mathcal{P}$

**Theorem 1**  \[ s, \{p\} \models_F \varphi_f \iff s \models_{F|p} \text{pr}(\varphi_f, p) \]

closed $\varphi_f \in \mu L_f$, $s \in S$, product $p \in \mathcal{P}$

**Theorem 2**  \[ s, \mathcal{P} \models_F \varphi_f \implies \forall p \in \mathcal{P}: s \models_{F|p} \text{pr}(\varphi_f, p) \]

closed, negation-free $\varphi_f \in \mu L_f$, $s \in S$, family $\mathcal{P} \subseteq \mathcal{P}$

Note: in general $s, \mathcal{P} \not\models_F \varphi_f$ does not imply $s \not\models_{F|p} \text{pr}(\varphi_f, p)$ for all products in family $\mathcal{P}$
Main results of paper @ FMSPLE’16

Given an FTS $F$ and a set of products $\mathcal{P}$

**Theorem 1**  
$s, \{p\} \models_F \varphi_f \iff s \models_{F|p} \pr(\varphi_f, p)$

Closed $\varphi_f \in \mu L_f$, $s \in S$, product $p \in \mathcal{P}$

**Theorem 2**  
$s, \mathcal{P} \models_F \varphi_f \implies \forall p \in \mathcal{P}: s \models_{F|p} \pr(\varphi_f, p)$

Closed, negation-free $\varphi_f \in \mu L_f$, $s \in S$, family $\mathcal{P} \subseteq \mathcal{P}$

Note: in general $s, \mathcal{P} \not\models_F \varphi_f$ does not imply $s \not\models_{F|p} \pr(\varphi_f, p)$ for all products in family $\mathcal{P}$.
Main results of paper @ FMSPLE’16

Given an FTS $F$ and a set of products $\mathcal{P}$

**Theorem 1**  
$s, \{p\} \models_F \varphi_f \iff s \models_{F|p} \text{pr}(\varphi_f, p)$

closed $\varphi_f \in \mu L_f$, $s \in S$, product $p \in \mathcal{P}$

**Theorem 2**  
$s, \mathcal{P} \models_F \varphi_f \implies \forall p \in \mathcal{P}: s \models_{F|p} \text{pr}(\varphi_f, p)$

closed, negation-free $\varphi_f \in \mu L_f$, $s \in S$, family $\mathcal{P} \subseteq \mathcal{P}$

Note: in general $s, \mathcal{P} \not\models_F \varphi_f$ does not imply $s \not\models_{F|p} \text{pr}(\varphi_f, p)$ for all products in family $\mathcal{P}$
Given an FTS $F$ and a set of products $\mathcal{P}$

**Theorem 1** \[ s, \{p\} \models_F \varphi_f \iff s \models_{F|p} \text{pr}(\varphi_f, p) \]

closed $\varphi_f \in \mu L_f$, $s \in S$, product $p \in \mathcal{P}$

**Theorem 2** \[ s, \mathcal{P} \models_F \varphi_f \implies \forall p \in \mathcal{P}: s \models_{F|p} \text{pr}(\varphi_f, p) \]

closed, negation-free $\varphi_f \in \mu L_f$, $s \in S$, family $\mathcal{P} \subseteq \mathcal{P}$

Note: in general $s, \mathcal{P} \not\models_F \varphi_f$ does not imply $s \not\models_{F|p} \text{pr}(\varphi_f, p)$ for all products in family $\mathcal{P}$
A first-order $\mu$-calculus with data $\mu L_{FO}$

set of ‘sorted’ actions $\mathcal{A}$, set of features $\mathcal{F}$, set of data variables $\mathcal{V}$, set of recursion variables $\tilde{\mathcal{X}}$

$\mu$-calculus with data $\mu L_{FO}$ over $\mathcal{A}, \mathcal{F}, \mathcal{V}$ and $\tilde{\mathcal{X}}$, formula $\varphi \in \mu L_{FO}$ given by

$$\varphi_f ::= \bot \mid T \mid$$

$$\neg \varphi \mid \varphi \lor \psi \mid \varphi \land \psi \mid$$

$$\gamma_1 \Rightarrow \gamma_2 \mid \quad (Q_{\gamma_1} \subseteq Q_{\gamma_2})$$

$$\exists v. \varphi \mid \forall v. \varphi \mid$$

$$\langle a(v) \rangle \varphi \mid [a(v)] \varphi \mid$$

$$\tilde{X}(\gamma) \mid \mu \tilde{X}(v_{\tilde{X}}:=\gamma).\varphi \mid \nu \tilde{X}(v_{\tilde{X}}:=\gamma).\varphi$$

with the usual restrictions on free variables and the number of negations
Semantics $\mu L_{\text{FO}}$ over parametrised LTSs

FTS $F = (S, \theta, s_*)$ over actions $\mathcal{A}$ and features $F$
- $S$ a finite set of states
- $\theta : S \times \mathcal{A} \times S \rightarrow \mathbb{B}[F]$ the transition constraint function
- $s_* \in S$ the initial state

LTS $L = (S, \rightarrow, s_*)$ over actions $\mathcal{A}$
- $S$ a finite set of states
- $\rightarrow \subseteq S \times \mathcal{A} \times S$ the transition relation
- $s_* \in S$ the initial state
Semantics $\mu L_{\text{FO}}$ over parametrised LTSs

FTS $F = (S, \theta, s_*)$ over actions $\mathcal{A}$ and features $\mathcal{F}$
- $S$ a finite set of states
- $\theta : S \times \mathcal{A} \times S \rightarrow B[\mathcal{F}]$ the transition constraint function
- $s_* \in S$ the initial state

parametrised LTS $L(F) = (S, \rightarrow, s_*)$ for $F$ over actions $\mathcal{A}[\mathcal{F}] = \{ a(\gamma) \mid a \in \mathcal{A}, \gamma \in B[\mathcal{F}] \}$
- $\rightarrow$ is defined by $s \xrightarrow{a(\gamma)} t$ iff $\theta(s, a, t) = \gamma$ and $\gamma \not\equiv \perp$

$\mu L_{\text{FO}}$ is a fragment of the logic from:
- Groote & Mateescu, Verification of temporal properties of processes in a setting with data @ AMAST'99

where its full semantics can be found
Semantics $\mu L_{FO}$ over parametrised LTSs

FTS $F = (S, \theta, s_*)$ over actions $\mathcal{A}$ and features $\mathcal{F}$

- $S$ a finite set of states
- $\theta : S \times \mathcal{A} \times S \rightarrow \mathbb{B}[\mathcal{F}]$ the transition constraint function
- $s_* \in S$ the initial state

parametrised LTS $L(F) = (S, \rightarrow, s_*)$ for $F$ over actions $\mathcal{A}[\mathcal{F}] = \{ a(\gamma) | a \in \mathcal{A}, \gamma \in \mathbb{B}[\mathcal{F}] \}$

- $\rightarrow$ is defined by $s \xrightarrow{a(\gamma)} t$ iff $\theta(s, a, t) = \gamma$ and $\gamma \neq \bot$

e.g.

\[
\llangle a(v) \rrangle_{FO}(\xi)(\theta) = \{ s | \exists \gamma, t : s \xrightarrow{a(\gamma)} t \land \theta(v) = Q_\gamma \land t \in \llangle \varphi \rrangle_{FO}(\xi)(\theta) \}
\]
i.e.

$\llangle a(v) \rrangle \varphi$ holds if there is a transition $s \xrightarrow{a(\gamma)} t$ such that family $\theta(v)$ equals family $Q_\gamma$ (associated with transition’s feature expression $\gamma$) and $t$ satisfies $\varphi$
From $\mu L_f$ to $\mu L_{FO}$

translation function $tr : \mathcal{B}[F] \times \mu L_f \to \mu L_{FO}$

$$tr(\gamma, \bot) = \bot$$
$$tr(\gamma, T) = T$$
$$tr(\gamma, \neg \varphi_f) = \neg tr(\gamma, \varphi_f)$$
$$tr(\gamma, \varphi_f \lor \psi_f) = tr(\gamma, \varphi_f) \lor tr(\gamma, \psi_f)$$
$$tr(\gamma, \varphi_f \land \psi_f) = tr(\gamma, \varphi_f) \land tr(\gamma, \psi_f)$$

$$tr(\gamma, \langle a \mid \chi \rangle \varphi_f) = (\gamma \Rightarrow \chi) \land \exists v.\langle a(v)\rangle((\gamma \Rightarrow v) \land tr(\gamma \land \chi \land v, \varphi_f))$$
$$tr(\gamma, [a \mid \chi] \varphi_f) = \forall v.[a(v)]((\gamma \land \chi \land v \Rightarrow \bot) \lor tr(\gamma \land \chi \land v, \varphi_f))$$

$$tr(\gamma, X) = \tilde{X}(\gamma)$$
$$tr(\gamma, \mu X. \varphi_f) = \mu \tilde{X}(v:=\gamma).tr(v, \varphi_f)$$
$$tr(\gamma, \nu X. \varphi_f) = \nu \tilde{X}(v:=\gamma).tr(v, \varphi_f)$$
A main result of paper @ FASE’17

Given an FTS $F$ and a set of products $\mathcal{P}$

**Theorem 3**  
$s, P \models_{F} \varphi_{f} \iff s \models_{L(F)} tr(\gamma_{P}, \varphi_{f})$

closed $\varphi_{f} \in \mu L_{f}$, $s \in S$, family $P \subseteq \mathcal{P}$

**Theorem 2**  
$s, P \models_{F} \varphi_{f} \implies \forall p \in P: s \models_{F|p} pr(\varphi_{f}, p)$

closed, negation-free $\varphi_{f} \in \mu L_{f}$, $s \in S$, family $P \subseteq \mathcal{P}$

**Lemma 1**  
$s, P \models_{F} \varphi_{f}^{c} \implies \forall p \in P: s \not\models_{F|p} pr(\varphi_{f}, p)$

closed, negation-free $\varphi_{f} \in \mu L_{f}$, $s \in S$, family $P \subseteq \mathcal{P}$
Given an FTS $F$ and a set of products $P$

**Theorem 3** \( s, P \models_F \varphi_f \iff s \models_{L(F)} tr(\gamma_P, \varphi_f) \)  
closed \( \varphi_f \in \mu L_f \), \( s \in S \), family \( P \subseteq P \)

**Theorem 2** \( s, P \models_F \varphi_f \implies \forall p \in P : s \models_{F|p} pr(\varphi_f, p) \)  
closed, negation-free \( \varphi_f \in \mu L_f \), \( s \in S \), family \( P \subseteq P \)

**Lemma 1** \( s, P \models_F \varphi^c_f \implies \forall p \in P : s \not\models_{F|p} pr(\varphi_f, p) \)  
closed, negation-free \( \varphi_f \in \mu L_f \), \( s \in S \), family \( P \subseteq P \)
Recall a result of paper @ FMSPLE’16

Given an FTS $F$ and a set of products $\mathcal{P}$

**Theorem 3** \[ s, P \models_F \varphi_f \iff s \models_{L(F)} tr(\gamma_P, \varphi_f) \]
closed $\varphi_f \in \mu L_f$, $s \in S$, family $P \subseteq \mathcal{P}$

**Theorem 2** \[ s, P \models_F \varphi_f \implies \forall p \in P : s \models_{F|p} pr(\varphi_f, p) \]
closed, negation-free $\varphi_f \in \mu L_f$, $s \in S$, family $P \subseteq \mathcal{P}$

**Lemma 1** \[ s, P \models_F \varphi_f^c \implies \forall p \in P : s \not\models_{F|p} pr(\varphi_f, p) \]
closed, negation-free $\varphi_f \in \mu L_f$, $s \in S$, family $P \subseteq \mathcal{P}$
Another result of paper @ FASE’17

Given an FTS $F$ and a set of products $\mathcal{P}$

**Theorem 3** \[ s, P \models_F \varphi_f \iff s \models_{L(F)} \text{tr}(\gamma_P, \varphi_f) \]
closed $\varphi_f \in \mu L_f$, $s \in S$, family $P \subseteq \mathcal{P}$

**Theorem 2** \[ s, P \models_F \varphi_f \implies \forall p \in P : s \models_{F|p} \text{pr}(\varphi_f, p) \]
closed, negation-free $\varphi_f \in \mu L_f$, $s \in S$, family $P \subseteq \mathcal{P}$

**Lemma 1** \[ s, P \models_F \varphi_f^c \implies \forall p \in P : s \not\models_{F|p} \text{pr}(\varphi_f, p) \]
closed, negation-free $\varphi_f \in \mu L_f$, $s \in S$, family $P \subseteq \mathcal{P}$
Family-based partitioning for \( \mu L_f \)

Given a negation-free \( \varphi_f \) and a family \( P \), compute a partitioning \((P_\oplus, P_\ominus)\) of \( P \) satisfying

\[
\forall p \in P_\oplus: s_*, p \models_{F|p} pr(\varphi_f, p) \text{ and } \forall p \in P_\ominus: s_*, p \not\models_{F|p} pr(\varphi_f, p)
\]

closed, negation-free \( \varphi_f \in \mu L_f \), family \( P \subseteq \mathcal{P} \)

**Algorithm 1** Family-Based Partitioning

1: function \( \text{FBP}(P, \varphi_f) \)
2: \hspace{1em} if \( s_*, P \models F \varphi_f \) then return \((P, \emptyset)\)
3: \hspace{1em} else
4: \hspace{2em} if \( s_*, P \models F \varphi_f^c \) then return \((\emptyset, P)\)
5: \hspace{2em} else partition \( P \) into \((P_1, P_2)\)
6: \hspace{3em} \((P_1^+, P_1^-) \leftarrow \text{FBP}(P_1, \varphi_f)\)
7: \hspace{3em} \((P_2^+, P_2^-) \leftarrow \text{FBP}(P_2, \varphi_f)\)
8: \hspace{1em} return \((P_1^+ \cup P_2^+, P_1^- \cup P_2^-)\)
9: \hspace{1em} end if
10: \hspace{1em} end if
11: end function
Family-based partitioning algorithm

**Theorem 4** \( \text{FBP}(P, \varphi_f) \) terminates and returns a partitioning \((P_\oplus, P_\ominus)\) of \( P \) satisfying

\[
\forall p \in P_\oplus: s_*, p \models_{F|p} pr(\varphi_f, p) \quad\text{and}\quad \forall p \in P_\ominus: s_*, p \not\models_{F|p} pr(\varphi_f, p)
\]

closed, negation-free \( \varphi_f \in \mu L_f \), family \( P \subseteq \mathcal{P} \)

**Algorithm 1** Family-Based Partitioning

1: function \( \text{FBP}(P, \varphi_f) \)
2: if \( s_*, P \models_F \varphi_f \) then return \( (P, \emptyset) \)
3: else
4: if \( s_*, P \models_F \varphi_f^c \) then return \( (\emptyset, P) \)
5: else partition \( P \) into \((P_1, P_2)\)
6: \( (P_1^+, P_1^-) \leftarrow \text{FBP}(P_1, \varphi_f) \)
7: \( (P_2^+, P_2^-) \leftarrow \text{FBP}(P_2, \varphi_f) \)
8: return \( (P_1^+ \cup P_2^+, P_1^- \cup P_2^-) \)
9: end if
10: end if
11: end function
### Minepump SPL benchmark ($|\mathcal{P}| = 2^7$)


<table>
<thead>
<tr>
<th>$\Phi$</th>
<th>property in $\mu L_f$</th>
<th>result</th>
<th>one-by-one</th>
<th>all-in-one</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\varphi_1$</td>
<td>Absence of deadlock</td>
<td>[true$^*$] $\langle$true$\rangle \top$</td>
<td>128/0</td>
<td>10.02</td>
</tr>
<tr>
<td>$\varphi_2$</td>
<td>The controller cannot infinitely often receive water level readings</td>
<td>$\mu X.[(\neg \text{levelMsg})^* \cdot \text{levelMsg}] \ X$</td>
<td>0/128</td>
<td>10.18</td>
</tr>
<tr>
<td>$\varphi_3$</td>
<td>The controller cannot fairly receive each of the three message types</td>
<td>$\mu X.[(\text{true}^* \cdot \text{commandMsg}) \ X \lor (\text{true}^* \cdot \text{alarmMsg}) \ X \lor (\text{true}^* \cdot \text{levelMsg}) \ X]$</td>
<td>0/128</td>
<td>24.33</td>
</tr>
<tr>
<td>$\varphi_4$</td>
<td>The pump cannot be switched on infinitely often</td>
<td>$(\mu X.\nu Y.[\text{pumpStart}.(\neg \text{pumpStop})^* \cdot \text{pumpStop}] \ X \land [\neg \text{pumpStart}] \ Y))$</td>
<td>96/32</td>
<td>21.09</td>
</tr>
<tr>
<td>$\varphi_5$</td>
<td>The system cannot be in a situation in which the pump runs indefinitely in the presence of methane</td>
<td>$(\text{true}^<em>([\text{pumpStart}.(\neg \text{pumpStop})^</em> \cdot \text{methaneRise}] \mu X.[R] \ X))$</td>
<td>96/32</td>
<td>17.26</td>
</tr>
<tr>
<td>$\varphi_6$</td>
<td>Assuming fairness ($\varphi_3$), the system cannot be in a situation in which the pump runs indefinitely in the presence of methane ($\varphi_5$)</td>
<td>$(\text{true}^<em>([\text{pumpStart}.(\neg \text{pumpStop})^</em> \cdot \text{methaneRise}] \Psi))$</td>
<td>112/16</td>
<td>27.32</td>
</tr>
<tr>
<td>$\varphi_7$</td>
<td>The controller can always eventually receive/ read a message, i.e. return to its initial state from any state</td>
<td>$[\text{true}^* \langle \text{true}^* \cdot \text{receiveMsg} \rangle \top)$</td>
<td>128/0</td>
<td>18.36</td>
</tr>
<tr>
<td>$\varphi_8$</td>
<td>Invariantly the pump is not started when the low water level signal fires</td>
<td>$[\text{true}^* \cdot \text{lowLevel}.(\neg (\text{normalLevel} + \text{highLevel}))^* \cdot \text{pumpStart}] \bot$</td>
<td>128/0</td>
<td>5.67</td>
</tr>
<tr>
<td>$\varphi_9$</td>
<td>Invariantly, when the level of methane rises, it inevitably decreases</td>
<td>$[\text{true}^* \cdot \text{methaneRise}] \mu X.[\neg \text{methaneLower}] \ X \land (\text{true}) \top)$</td>
<td>0/128</td>
<td>20.47</td>
</tr>
<tr>
<td>$\varphi_{10}$</td>
<td>Products with feature Ct can switch on the pump</td>
<td>$\langle \text{true}^* \cdot \text{pumpStart}</td>
<td>\text{Ct} \rangle \top$</td>
<td>32/96</td>
</tr>
<tr>
<td>$\varphi_{11}$</td>
<td>Products with feature Ct can always switch on the pump</td>
<td>$[\text{true}^*</td>
<td>\text{Ct}] \langle \text{true}^* \cdot \text{pumpStart}</td>
<td>\text{Ct} \rangle \top$</td>
</tr>
<tr>
<td>$\varphi_{12}$</td>
<td>Products with features [Ct, Ma, Lh] can start the pump upon a high water level, but products without feature Lh cannot</td>
<td>$[\text{true}^* \top)(([\text{highLevel}</td>
<td>\text{Ct} \land \text{Ma} \land \text{Lh}] \ (\text{true}^* \cdot \text{pumpStart}</td>
<td>\top) \top) \land [\text{pumpStart} \neg \text{Lh}] \bot)$</td>
</tr>
</tbody>
</table>

---

mCRL2 code distributed with mCRL2 toolset (svn revision 14493)
Conclusions and future work

Introduced and compared feature-oriented $\mu$-calculi with FTS semantics

Resembles fLTL and fCTL by Classen et al., but $\muL_f$ is more expressive

Translation to $\muL_{FO}$ allows family-based model checking multi-feature properties of configurable systems with off-the-shelf tools (e.g. mCRL2)

Defined a first (naive) family-based partitioning procedure for $\muL_f$; its efficiency depends on initial partitioning of $P$ and quality of refinements

Future work: improve partitioning strategy

1. Determine heuristics for finding a good initial partitioning of $P$
2. Extract information from failed model-checking problems to find a good split-up of the family of products in line 5 of Algorithm 1

(difficult in particular for $\mu$-calculus, since easily-interpretable feedback from its model checkers is generally missing so far)
Conclusions and future work

Introduced and compared feature-oriented $\mu$-calculi with FTS semantics

Resembles fLTL and fCTL by Classen et al., but $\mu L_f$ is more expressive

Translation to $\mu L_{FO}$ allows family-based model checking multi-feature properties of configurable systems with off-the-shelf tools (e.g. mCRL2)

Defined a first (naive) family-based partitioning procedure for $\mu L_f$; its efficiency depends on initial partitioning of $P$ and quality of refinements

Future work: improve partitioning strategy

1. Determine heuristics for finding a good initial partitioning of $P$
2. Extract information from failed model-checking problems to find a good split-up of the family of products in line 5 of Algorithm 1 (difficult in particular for $\mu$-calculus, since easily-interpretable feedback from its model checkers is generally missing so far)
Conclusions and future work

Introduced and compared feature-oriented $\mu$-calculi with FTS semantics

Resembles fLTL and fCTL by Classen et al., but $\mu L_f$ is more expressive

Translation to $\mu L_{FO}$ allows family-based model checking multi-feature properties of configurable systems with off-the-shelf tools (e.g. mCRL2)

Defined a first (naive) family-based partitioning procedure for $\mu L_f$; its efficiency depends on initial partitioning of $P$ and quality of refinements

Future work: improve partitioning strategy
1. Determine heuristics for finding a good initial partitioning of $P$
2. Extract information from failed model-checking problems to find a good split-up of the family of products in line 5 of Algorithm 1
   (difficult in particular for $\mu$-calculus, since easily-interpretable feedback from its model checkers is generally missing so far)
Conclusions and future work

Introduced and compared feature-oriented $\mu$-calculi with FTS semantics
Resembles fLTL and fCTL by Classen et al., but $\mu L_f$ is more expressive
Translation to $\mu L_{FO}$ allows family-based model checking multi-feature properties of configurable systems with off-the-shelf tools (e.g. mCRL2)
Defined a first (naive) family-based partitioning procedure for $\mu L_f$; its efficiency depends on initial partitioning of $P$ and quality of refinements

Future work: improve partitioning strategy
1. Determine heuristics for finding a good initial partitioning of $P$
2. Extract information from failed model-checking problems to find a good split-up of the family of products in line 5 of Algorithm 1 (?) (difficult in particular for $\mu$-calculus, since easily-interpretable feedback from its model checkers is generally missing so far)
Conclusions and future work

Introduced and compared feature-oriented \( \mu \)-calculi with FTS semantics

Resembles fLTL and fCTL by Classen et al., but \( \mu L_f \) is more expressive

Translation to \( \mu L_{FO} \) allows family-based model checking multi-feature properties of configurable systems with off-the-shelf tools (e.g. mCRL2)

Defined a first (naive) family-based partitioning procedure for \( \mu L_f \); its efficiency depends on initial partitioning of \( P \) and quality of refinements

Future work: improve partitioning strategy

1. Determine heuristics for finding a good initial partitioning of \( P \)
2. Extract information from failed model-checking problems to find a good split-up of the family of products in line 5 of Algorithm 1

? (difficult in particular for \( \mu \)-calculus, since easily-interpretable feedback from its model checkers is generally missing so far)
Conclusions and future work

Introduced and compared feature-oriented $\mu$-calculi with FTS semantics

Resembles fLTL and fCTL by Classen et al., but $\mu L_f$ is more expressive

Translation to $\mu L_{\text{FO}}$ allows family-based model checking multi-feature properties of configurable systems with off-the-shelf tools (e.g. mCRL2)

Defined a first (naive) family-based partitioning procedure for $\mu L_f$; its efficiency depends on initial partitioning of $P$ and quality of refinements

Future work: improve partitioning strategy

1. Determine heuristics for finding a good initial partitioning of $P$

2. Extract information from failed model-checking problems to find a good split-up of the family of products in line 5 of Algorithm 1

? (difficult in particular for $\mu$-calculus, since easily-interpretable feedback from its model checkers is generally missing so far)
Conclusions and future work

Introduced and compared feature-oriented $\mu$-calculi with FTS semantics
Resembles fLTL and fCTL by Classen et al., but $\mu L_f$ is more expressive
Translation to $\mu L_{FO}$ allows family-based model checking multi-feature properties of configurable systems with off-the-shelf tools (e.g. mCRL2)
Defined a first (naive) family-based partitioning procedure for $\mu L_f$; its efficiency depends on initial partitioning of $P$ and quality of refinements

Future work: improve partitioning strategy

1. Determine heuristics for finding a good initial partitioning of $P$
2. Extract information from failed model-checking problems to find a good split-up of the family of products in line 5 of Algorithm 1

? (difficult in particular for $\mu$-calculus, since easily-interpretable feedback from its model checkers is generally missing so far)
Conclusions and future work

Introduced and compared feature-oriented $\mu$-calculi with FTS semantics.

Resembles fLTL and fCTL by Classen et al., but $\mu L_f$ is more expressive.

Translation to $\mu L_{FO}$ allows family-based model checking multi-feature properties of configurable systems with off-the-shelf tools (e.g. mCRL2).

Defined a first (naive) family-based partitioning procedure for $\mu L_f$; its efficiency depends on initial partitioning of $P$ and quality of refinements.

Future work: improve partitioning strategy

1. Determine heuristics for finding a good initial partitioning of $P$.
2. Extract information from failed model-checking problems to find a good split-up of the family of products in line 5 of Algorithm 1.

? (Difficult in particular for $\mu$-calculus, since easily-interpretable feedback from its model checkers is generally missing so far.)
The quest for an efficient strategy

Execution of Algorithm 1 for deadlock freedom (φ₁) and with initial family $\top$ (family characterised at node is conjunction of features along path from root)

Optimal partitioning strategy

Total computation time: 27.9
Computation time leaves: 8.4
(i.e. $Mq$, $\neg Mq$, and $\neg Ct$ nodes)
At once ∀ possible families: 2.07

Non-optimal partitioning strategy
(splitting $Ln$ and $\neg Ln$, then optimal)
Total computation time: 45.0 (+60%)