Quantitative Partial Model-Checking Function and Its Optimisation

Stefano Bistarelli\textsuperscript{1}, Fabio Martinelli\textsuperscript{2}, Ilaria Matteucci\textsuperscript{2}, Francesco Santini\textsuperscript{1}

\textsuperscript{1} Department of Maths and CS, University of Perugia, Italy
\textsuperscript{2} Institute of Informatics and Telematics, Pisa, Italy
Outline

- Introduction and motivations
- C-semirings
- Logic and Quantitative Partial Model-Checking
- Simplification Rules and Complexity
- Conclusion
Introduction
Motivations

Model Checking is a well-established method to formally verify finite-state concurrent systems

- Specifications about the system are expressed as temporal logic formulas $\varphi$
- Efficient symbolic algorithms are used to traverse the model defined by the system and check if the specification holds or not

A key limitation to its use is due to the state explosion problem

Partial Model Checking [Andersen ‘95].

- Parts of the concurrent system are gradually removed while transforming $\varphi$ accordingly (such operation is also known as “quotienting”). When the intermediate specifications constructed in this manner can be kept small, the state-explosion problem is avoided
Quantitative evaluation

- Functional aspects of a system add to the overall picture costs, execution times, and rates (for instance).

- We consider a quantitative score that is more informative to understand how costly it is to satisfy a property $\varphi$:
  - We take advantage of a valued logic (with fix points), where the evaluation of a formula is a value, not true/false
  - Properties are checked on processes described in ``à-la-CSS” Generalised Process Algebra: transitions are labelled with a weight
  - Values are taken from a parametric algebraic-structure: a semiring
  - Different semiring instantiations represent different metrics
Use simplification rules to reduce the size of $\varphi$!
C-semirings
A $c$-semiring is a tuple $K = \langle K, \otimes, \oplus, \bot, \top \rangle$

- $K$ is the (possibly infinite) set of preference values
- $\bot$ and $\top$ represent the bottom and top preference values
- $\oplus$ defines a partial order ($\geq_K$) over $A$ such that $a \geq_K b$ iff $a \oplus b = a$
- $\oplus$ is commutative, associative, and idempotent, it is closed, $\bot$ is its unit element and $\top$ is its absorbing element
- $\otimes$ closed, associative, commutative, and distributes over $\oplus$, $\top$ is its unit element and $\bot$ is its absorbing element
- $\langle K, \leq_K \rangle$ is a complete lattice

\[ a \geq_K b \text{ means } a \text{ is better than } b \]

$\otimes$ to compose the preferences and $\oplus$ to find the best one

\[ \otimes \text{ is monotonic: } a \otimes b \leq_K a \]
Classical instantiations

Weighted  $\langle \mathbb{R}^+ \cup \{+\infty\}, \min, \hat{+}, \infty, 0 \rangle$  $4 \geq_k 5$

Fuzzy  $\langle [0..1], \max, \min, 0, 1 \rangle$  $0.5 \geq_k 0.4$

Probabilistic  $\langle [0..1], \max, \land, 0, 1 \rangle$  $0.5 \geq_k 0.4$

Boolean  $\langle \{false, true\}, \lor, \land, false, true \rangle$  $true \geq_k false$

The Cartesian product is still a semiring

$\langle [0..1], \mathbb{R}^+ \cup \{+\infty\}, \langle \max, \min \rangle, \langle \min, \land \rangle, \langle 0, +\infty \rangle, \langle 1, 0 \rangle \rangle$
Let $K$ be a tropical semiring. It is residuated if the set $\{x \in K \mid b \otimes x \leq_K a\}$ admits a maximum $\forall a, b \in K$, denoted $a \odot b$.

\[
s \otimes t \quad \min\{x \mid t \hat{\vee} x \geq s\} = \begin{cases} 
0 & \text{if } t \geq s \\
 s \hat{\vee} t & \text{if } s > t
\end{cases} \quad s_{\text{weighted}}
\]

\[
\max\{x \mid \min(t, x) \leq s\} = \begin{cases} 
1 & \text{if } t \leq s \\
 s & \text{if } s < t
\end{cases} \quad s_{\text{fuzzy}}
\]
Logic and Quantitative PMC
A (finite) Multi Labelled Transition System (MLTS) is a five-tuple $\text{MLTS} = (S, Act, K, T, s_0)$, where $S$ is the countable (finite) state space, $s_0 \in S$ is the initial state, $Act$ is a finite set of actions, $K$ is a semiring used to weigh actions, and $T : (S \times Act \times S) \rightarrow K$ is a transition function.

The set $P$ of terms in GPA over a set of finite transition labels $(a, k)$ where $a \in Act$ and $k \in K$ from a semiring $\langle K, \oplus, \otimes, \bot, \top \rangle$ is defined by $P ::= 0 \mid (a, k).P \mid P + P \mid P||P \mid X$, where $X$ is a countable set of process variables, coming from a system of co-recursive equations of the form $X \triangleq P$. 
GPA à la CCS

\[ (a, k).P \xrightarrow{a,k} P \]

\[ \frac{P \xrightarrow{a,k} P_1 \quad X \triangleq P}{X \xrightarrow{a,k} P_1} \]

\[ \frac{P \xrightarrow{a,k} P_1}{P + P' \xrightarrow{a,k_j} P_1} \quad j \in I \]

\[ P \xrightarrow{a,k} P_1 \quad \tau^k \xrightarrow{\kappa \otimes l} P_1 \parallel P'_1 \]

\[ \frac{P \xrightarrow{a,k} P_1}{P \parallel P' \xrightarrow{a,k} P_1 \parallel P'} \]

\[ \frac{P' \xrightarrow{a,k} P'_1}{P \parallel P' \xrightarrow{a,k} P \parallel P'_1} \]

- Generalised Process Algebra [Buchholz&Kemper01]
- Communications “à la CSP”
- Transitions are labelled with a semiring value
Example

\[ P = (a, 1).((b, 2).0 + (b, 7).0) + (a.5).(b, 1).0 \]
Logic

Given a MLTS $M = \langle S, Act, K, T \rangle$, and let $k \in K$ and $a \in Act$, the syntax of a formula $\phi \in \Phi_M$ is as follows:

\[
\phi \ ::= \ k \mid v \mid \phi_1 \oplus \phi_2 \mid \phi_1 \otimes \phi_2 \mid \phi_1 \circ \phi_2 \mid \langle a \rangle \phi \mid [a] \phi
\]

\[
E \ ::= \ v =_{\mu} \phi E \mid v =_{v} \phi E \mid \epsilon
\]

- Instead of classical logic operators, lub, glb, and composition
- c-semring equational $\mu$-calculus
- Not only true and false, every value in $K$ is a truth value
- Evaluated as

\[
[\ ]_{\rho}(s) : (\Phi_M \times S) \rightarrow K
\]
t-satisfiability
A process $P$ satisfies a c-$E\mu$ formula $\phi$ with a threshold-value $t$, i.e., $P \vDash_t \phi$, if and only if the evaluation of $\phi$ on $P$ is not worse than $t$, considering the order $\leq_K$. Formally, $P \vDash_t \phi \iff t \leq_K \llbracket \phi \rrbracket_\rho(P)$.

In a weighted semiring, if $t=5$ and $\llbracket \phi \rrbracket_\rho(P)$ is 3 then it is satisfied
Logic

$$\text{fix} = \bigoplus \{ k \mid k \leq_K \tau(k) \}, \text{FIX} = \bigoplus \{ k \mid k \leq_K \tau(k) \}$$

$$\llbracket k \rrbracket_{\rho}(s) = k \in K \quad \forall s \in S$$

$$\llbracket v \rrbracket_{\rho}(s) = \rho(v, s)$$

$$\llbracket \phi_1 \oplus \phi_2 \rrbracket_{\rho}(s) = \llbracket \phi_1 \rrbracket_{\rho}(s) \oplus \llbracket \phi_2 \rrbracket_{\rho}(s)$$

$$\llbracket \phi_1 \otimes \phi_2 \rrbracket_{\rho}(s) = \llbracket \phi_1 \rrbracket_{\rho}(s) \otimes \llbracket \phi_2 \rrbracket_{\rho}(s)$$

$$\llbracket \phi_1 \ominus \phi_2 \rrbracket_{\rho}(s) = \llbracket \phi_1 \rrbracket_{\rho}(s) \ominus \llbracket \phi_2 \rrbracket_{\rho}(s)$$

$$\llbracket \langle a \rangle \phi \rrbracket_{\rho}(s) = \bigoplus \{ T(s, a, s') \otimes \llbracket \phi \rrbracket_{\rho}(s') \mid s' \in S \mid s \xrightarrow{a} s' \in T \}$$

$$\llbracket [a] \phi \rrbracket_{\rho}(s) = \bigoplus \{ T(s, a, s') \otimes \llbracket \phi \rrbracket_{\rho}(s') \mid s' \in S \mid s \xrightarrow{a} s' \in T \}$$

$$\llbracket v =_{\mu} \phi E \rrbracket_{\rho}(s) = \text{fix } \lambda k'. \llbracket \phi E \rrbracket_{\rho[k'/v]}(s)$$

$$\llbracket v =_{v} \phi E \rrbracket_{\rho}(s) = \text{FIX } \lambda k'. \llbracket \phi E \rrbracket_{\rho[k'/v]}(s)$$

$$\llbracket e \rrbracket_{\rho}(s) = \top$$

where $$\llbracket \phi E \rrbracket_{\rho[k'/v]}(s) = \llbracket \phi \rrbracket_{\rho'}(s), \rho'(y, s) = \begin{cases} \rho(y, s) & \forall y \in \text{free}(V) \\ k' & \text{if } y = v \\ \llbracket E \rrbracket_{\rho[k'/v]}(s) & \forall y \notin \text{free}(V) \end{cases}$$
QPMC function

(1) \[ k_{//p} = k \]
(2) \[ v_{//p} = v_p \]
(3) \[ (\phi_1 \otimes \phi_2)_{//p} = (k_{P,\phi_1} \otimes k_{P,\phi}) \otimes (\phi_1)_{//p} \otimes (k_{P,\phi_2} \otimes k_{P,\phi}) \otimes (\phi_2)_{//p} \]
(4) \[ (\phi_1 \oplus \phi_2)_{//p} = (k_{P,\phi_1} \otimes k_{P,\phi}) \otimes (\phi_1)_{//p} \oplus (k_{P,\phi_2} \otimes k_{P,\phi}) \otimes (\phi_2)_{//p} \]
(5) \[ (\phi_1 \odot \phi_2)_{//p} = (k_{P,\phi_1} \otimes k_{P,\phi}) \otimes (\phi_1)_{//p} \odot (k_{P,\phi_2} \otimes k_{P,\phi}) \otimes (\phi_2)_{//p} \]

(6) \[ (\langle a \rangle \phi_1)_{//p} = (k_{P,\phi_1} \otimes k_{P,\phi}) \otimes \langle a \rangle (\phi_1)_{//p} \oplus \bigoplus (k_a \otimes (k_{P',\phi_1} \otimes k_{P,\phi}) \otimes (\phi_1)_{//p'}) \]

(7) \[ (\langle \tau \rangle \phi_1)_{//p} = (k_{P,\phi_1} \otimes k_{P,\phi}) \otimes \langle \tau \rangle (\phi_1)_{//p} \oplus \bigoplus (k_\tau \otimes (k_{P',\phi_1} \otimes k_{P,\phi}) \otimes (\phi_1)_{//p'}) \]

(8) \[ (\langle [a] \rangle \phi_1)_{//p} = (k_{P,\phi_1} \otimes k_{P,\phi}) \otimes [a] (\phi_1)_{//p} \oplus \bigoplus (k_a \otimes (k_{P',\phi_1} \otimes k_{P,\phi}) \otimes (\phi_1)_{//p'}) \]

(9) \[ (\langle [\tau] \rangle \phi_1)_{//p} = (k_{P,\phi_1} \otimes k_{P,\phi}) \otimes [\tau] (\phi_1)_{//p} \oplus \bigoplus (k_\tau \otimes (k_{P',\phi_1} \otimes k_{P,\phi}) \otimes (\phi_1)_{//p'}) \]

\[ \bigoplus p_{a,k_a} \]
$k_{P,\phi}$ is an amount of weight that QPMC can safely extract from each $\phi$

$k_{P,\phi}$ is a lub for the evaluation of $\phi$
Why $K_{P,\varphi}$

- When the considered semiring is uniquely invertible, e.g. in case of totally ordered values

$$[[\varphi]](P \parallel Q) = k_{P,\varphi} \otimes [[\varphi_{//P}]](Q)$$

When $k_{P,\varphi}$ is already worse than $t$, i.e., $k_{P,\varphi} <_K t$, we can avoid evaluating $[[\varphi_{//P}]]_{\rho}(Q)$

- In case it is not uniquely invertible, then

$$[[\varphi]]_{\rho}(P \parallel Q) \geq_K k_{P,\varphi} \otimes [[\varphi_{//P}]]_{\rho}(Q)$$
Example

\[ P = (a, 1).((b, 2).0 + (b, 7).0) + (a.5).(b, 1).0 \]

\[ \phi = [a][b]0 \]

\[ \phi_{/\phi} = (T \otimes 3 \otimes [a]T) \square ((1 \otimes 2) \otimes 3) \otimes [a](\phi_{1/\phi}) \square \\
(5 \otimes 1) \otimes 3 \otimes [a](\phi_{1/\phi}) = (a)([b]0 \uplus [b]0 \uplus (5 \otimes [b]0)) \\
\square ([b]0 \uplus 3 \otimes [a][b]0) \]
(Weighted) Arc Consistency

\[ K = 5 \]

\[ V = \{x, y\} \]

\[ D = \{a, b\} \]
Simplification Rules
Simple evaluation

From [Andersen ’95], valued
Constant Propagation

\[ \vdash_t v = \mu/v \phi \]

\[ \vdash_t w = \mu/v h \]

\[ \vdash_t v = \mu/v \phi \]

\[ \vdash_t w = \mu/v h \]

\[ \vdash_t v = \mu/v [h/w] \]

\[ \vdash_t w = \mu/v h \quad \text{if } h \geq_K t \]

\[ \vdash_t v = \mu/v \phi[\bot/w] \]

\[ \vdash_t w = \mu/v \bot \quad \text{if } h \leq_K t \]
Trivial equation elimination

Trivial Equation Elimination

\[ \text{TEE1} \vdash_t \nu = \mu \langle a \rangle \nu \]
\[ \text{TEE2} \vdash_t \nu =_v [a] \nu \]
\[ \text{TEE3} \vdash_t \phi \oplus \phi \]
\[ \text{TEE4} \vdash_t \phi \oplus \phi \]
\[ \text{TEE5} \vdash_t \phi_1 \oplus (\phi_1 \otimes \phi_2) \]
\[ \text{TEE6} \vdash_t \phi_1 \oplus (\phi_1 \ominus \phi_2) \]
\[ \text{TEE7} \vdash_t \phi_1 \ominus (\phi_1 \otimes \phi_2) \]
\[ \text{TEE8} \vdash_t \phi_1 \ominus (\phi_1 \ominus \phi_2) \]
Complexity
Complexity

**Theorem 5.1** (Bound for distributive c-semirings). Given a distributive c-semiring $K = \langle K, \oplus, \otimes, \bot, \top \rangle$ and $M = (S, Act, K, T, s_0), \models t E_{\downarrow v}$ can be computed in $O(|E| \cdot h(FD(g(\Phi))))$, where $\Phi$ collects all the formulas in $E_{\downarrow v}$ with only free variables.

$|FD(K')| = 2^{(2^K)}$

$\otimes$ is the glb

$|FD(K')| = |K'|$ in case of fuzzy

$\langle \mathbb{R}^+ \cup \{\infty\}, min, \hat{+}, \infty, 0 \rangle$

$\phi = (v =_\mu v \otimes 2)$

**Theorem 5.2** ($t$-limited upper-bound). Given the weighted semiring $\langle \mathbb{N}^+ \cup \{\infty\}, min, +, +\infty, 0 \rangle$ and an MLTS $= (S, Act, K, T, s_0), \models t E_{\downarrow n}$, can be computed in $O(|E| \cdot N)$, where $N$ is the number of solutions of a Linear Diophantine Inequality $a_1 x_1 + a_2 x_2 + \ldots + a_r x_r \leq t$; $\{a_1, \ldots, a_n\}$ is the subset of co-prime generators of the lattice in which the computation happens.

$$\frac{t^r}{r! \prod_{i=1}^r a_i} \leq N \leq \frac{(t + a_1 + a_2 + \ldots + a_r)^r}{r! \prod_{i=1}^r a_i}$$
Conclusions and future work

- A formal framework to avoid state explosion while model checking quantitative processes

- Different heuristics to simplify its evaluation
  - $K_{P,\varphi}$ to stop $\varphi$ evaluation in case of uniquely invertible semirings
  - Simplification rules to cut the size of $\varphi$ before evaluating it

- Complexity results for the weighted semiring, granted by $t$

- Future work is
  - Prototype in Maude of QPMC and simplifications
  - Improve the simplifications and the extraction of $k_{P,\varphi}$
  - Complexity results for other semirings
Thank you for your time!

Contacts:
francesco.santini@dmi.unipg.it
Last simplifications

**Unguardedness Removal** (\( w \) unguaraded [1])

\[
\vdash_t v =_{\mu/v} \psi
\]

**UR**
\[
\vdash_t w =_{\mu/v} \phi
\]

\[
\vdash_t v =_{\mu/v} \psi[\phi/w]
\]

\[
\vdash_t w =_{\mu/v} \phi
\]

**Equivalence Reduction**

**ER1**
\[
\vdash_t v =_{\mu} \phi_1
\]
\[
\vdash_t w =_{\mu} \phi_2
\]
\[
\vdash_t v =_{v} \phi_1
\]
\[
\vdash_t w =_{v} \phi_2
\]

\[\iff\]

\[
\vdash_t v =_{\mu} \phi_1 \oplus \phi_2
\]
\[
\vdash_t w =_{\mu} \nu
\]

\[
\vdash_t v =_{v} \phi_1 \ominus \phi_2
\]
\[
\vdash_t w =_{v} \nu
\]
QPMC function (2)

(10) \( (\nu = \mu \phi_1 E)_{// P} = \begin{cases} 
\nu_{P_1} = \mu & \phi_{1//P_1} \\
\vdots \\
\nu_{P_n} = \mu & \phi_{1//P_n} \\
E_{//P} 
\end{cases} \)

(11) \( (\nu = \nu \phi_1 E)_{// P} = \begin{cases} 
\nu_{P_1} = \nu & \phi_{1//P_1} \\
\vdots \\
\nu_{P_n} = \nu & \phi_{1//P_n} \\
E_{//P} 
\end{cases} \)

(12) \( \epsilon_{//P} = \epsilon \)