Quantitative Partial Model-Checking Function and Its Optimisation

Stefano Bistarelli[1], Fabio Martinelli[2], Ilaria Matteucci[2], Francesco Santini[1]

[1] Department of Maths and CS, University of Perugia, Italy
[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

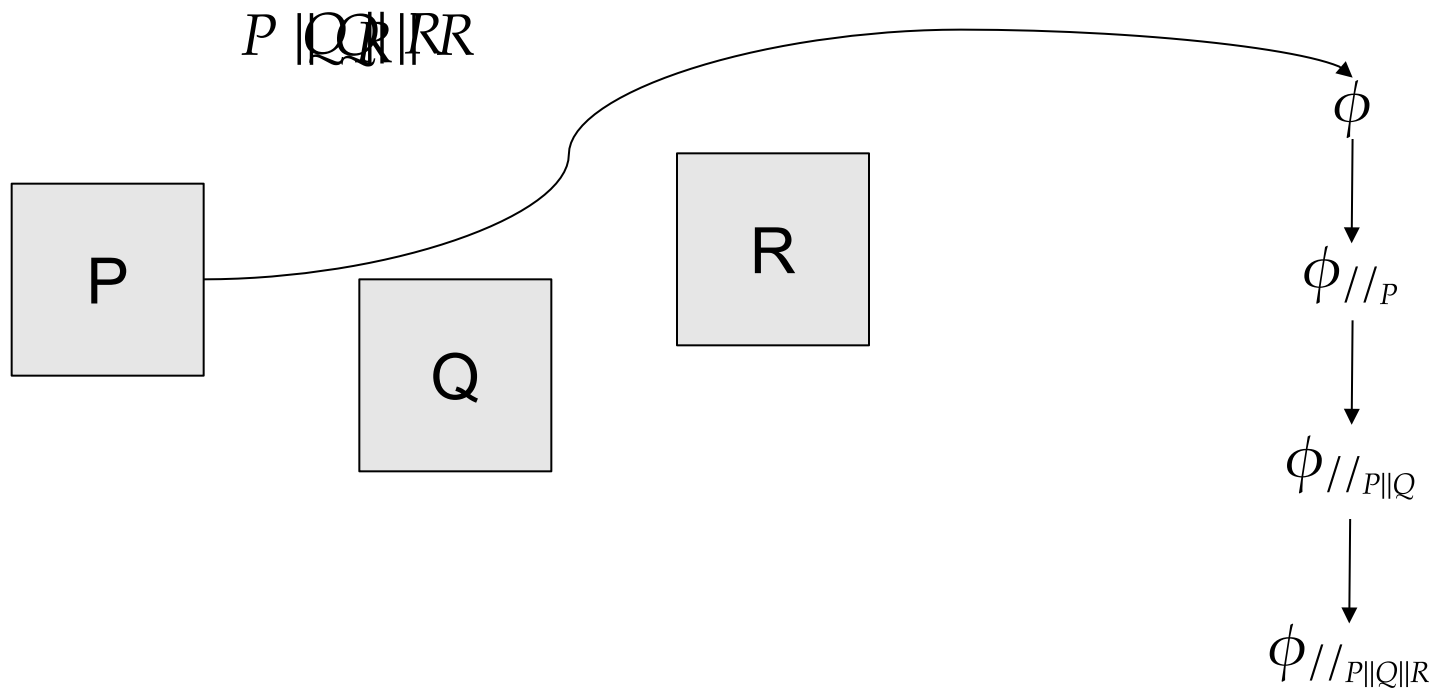
- Model Checking is a well-established method to formally verify finite-state concurrent systems
  - Specifications about the system are expressed as temporal logic formulas φ
  - Efficient symbolic algorithms are used to traverse the model defined by the system and check if the specification holds or 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 φ 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 φ:
  - 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

Approach



QPMC —extraction→ $k_{P,\phi}$

$$[\![\phi]\!]_\rho(P \,\|\, Q \,\|\, R) = k_{P,\phi} \otimes k_{Q,\phi'} \otimes k_{R,\phi''}$$

$$[\![\phi]\!]_\rho(P \,\|\, Q \,\|\, R) = k_{P,\phi} \otimes [\![\phi /\!/_P]\!]_\rho(Q \,\|\, R)$$

Use simplification rules to reduce the size of φ!

C-semirings

C-semirings

A c-semiring is a tuple $\mathbb{K} = \langle K, \otimes, \oplus, \bot, \top \rangle$

- 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 means a is better than b

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

$\otimes$ 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	$\langle [0..1], \max, \hat{\times}, 0, 1 \rangle$	$0.5 \geq_K 0.4$
Boolean	$\langle \{false, true\}, \vee, \wedge, false, true \rangle$	true $\geq_K$ false

The Cartesian product is still a semiring

$$\langle [0..1], \mathbb{R}^+ \cup \{+\infty\} \rangle, \langle \max, \min \rangle, \langle \min, \hat{\times} \rangle, \langle 0, +\infty \rangle, \langle 1, 0 \rangle \rangle$$

Weak inverse of oplus

Let $\mathbb{K}$ 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 $a \oslash b$.

$s \oslash t$

$$\min\{x \mid t \hat{+} x \geq s\} = \begin{cases} 0 & \text{if } t \geq s \\ s \hat{-} t & \text{if } s > t \end{cases} \qquad \mathbb{S}_{weighted}$$

$$\max\{x \mid \min(t, x) \leq s\} = \begin{cases} 1 & \text{if } t \leq s \\ s & \text{if } s < t \end{cases} \qquad \mathbb{S}_{fuzzy}$$

Logic and Quantitative PMC

MLTS (finite) and GPAs

A (finite) Multi Labelled Transition System (MLTS) is a five-tuple $MLTS = (S, Act, \mathbb{K}, T, s_0)$, where S is the countable (finite) state space, $s_0 \in S$ is the initial state, Act is a finite set of actions, $\mathbb{K}$ is a semiring used to weigh actions, and $T : (S \times Act \times S) \longrightarrow K$ is a transition function.

The set $\mathcal{P}$ 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

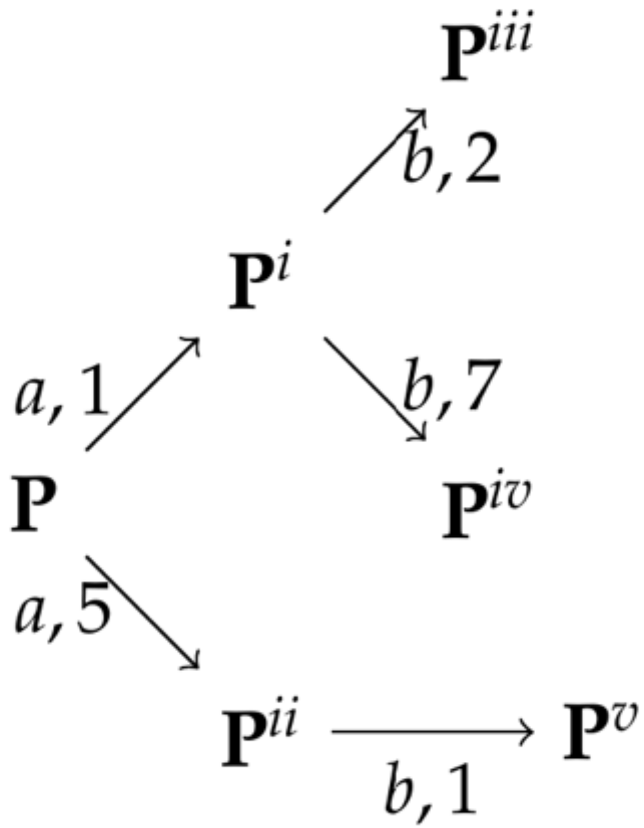
$$\frac{}{(a,k).P \xrightarrow{a,k} P} \qquad \frac{P \xrightarrow{a,k} P_1}{X \xrightarrow{a,k} P_1} X \triangleq P \qquad \frac{P \xrightarrow{a,k_j} P_1}{P + P' \xrightarrow{a,k_j} P_1} j \in I$$

$$\frac{P \xrightarrow{a,k} P_1 \quad P' \xrightarrow{\bar{a},l} P_1'}{P \| P' \xrightarrow{\tau, k \otimes l} P_1 \| P_1'} \qquad \frac{P \xrightarrow{a,k} P_1}{P \| P' \xrightarrow{a,k} P_1 \| P'} \qquad \frac{P' \xrightarrow{a,k} P_1'}{P \| P' \xrightarrow{a,k} P \| P_1'}$$

- Generalised Process Algebra [Buchholz&Kemper01]
- Comnunications “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 $M = \langle S, Act, \mathbb{K}, T \rangle$, and let $k \in K$ and $a \in Act$, the syntax of a formula $\phi \in \Phi_M$ is as follows:

$$
\begin{array}{lcl}
\phi & ::= & k \mid v \mid \phi_1 \overset{\bigvee}{\oplus} \phi_2 \mid \phi_1 \overset{\bigwedge}{\otimes} \phi_2 \mid \phi_1 \overset{\bigwedge}{\ominus} \phi_2 \mid \langle a \rangle \phi \mid [a]\phi \\
E & ::= & v =_{\mu} \phi E \mid v =_{\nu} \phi E \mid \epsilon
\end{array}
$$

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

$$[\![\ ]\!]_{\rho}(s) : (\Phi_M \times S) \longrightarrow K$$

Satisfiability of a formula

t-satisfiability
A process P satisfies a c-Eμ formula ϕ with a threshold-value t, i.e., $P \models_t \phi$, if and only if the evaluation of ϕ on P is not worse than t, considering the order $\leq_K$. Formally, $P \models_t \phi \Leftrightarrow t \leq_K [\![\phi]\!]_\rho(P)$.

In a weighted semiring, if t=5 and $[\![\phi]\!]_\rho(P)$ is 3 then it is satisfied

Logic

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

$$
\begin{aligned}
[\![k]\!]_\rho(s) &= k \in K \quad \forall s \in S \\
[\![v]\!]_\rho(s) &= \rho(v,s) \\
[\![\phi_1 \oplus \phi_2]\!]_\rho(s) &= [\![\phi_1]\!]_\rho(s) \oplus [\![\phi_2]\!]_\rho(s) \\
[\![\phi_1 \otimes \phi_2]\!]_\rho(s) &= [\![\phi_1]\!]_\rho(s) \otimes [\![\phi_2]\!]_\rho(s) \\
[\![\phi_1 \bigcap \phi_2]\!]_\rho(s) &= [\![\phi_1]\!]_\rho(s) \bigcap [\![\phi_2]\!]_\rho(s) \\
[\![\langle a \rangle \phi]\!]_\rho(s) &= \bigoplus_{\{s' \in S \mid s \xrightarrow{a} s' \in T\}} (T(s,a,s') \otimes [\![\phi]\!]_\rho(s')) \\
[\![[a]\phi]\!]_\rho(s) &= \bigcap_{\{s' \in S \mid s \xrightarrow{a} s' \in T\}} (T(s,a,s') \otimes [\![\phi]\!]_\rho(s')) \\
[\![v =_\mu \phi E]\!]_\rho(s) &= fix\ \lambda k'.[\![\phi E]\!]_{\rho[k'/v]}(s) \\
[\![v =_\nu \phi E]\!]_\rho(s) &= FIX\ \lambda k'.[\![\phi E]\!]_{\rho[k'/v]}(s) \\
[\![\epsilon]\!]_\rho(s) &= \top
\end{aligned}
$$

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

QPMC function

(1) $k_{//_P} = k$

(2) $v_{//_P} = v_P$

(3) $(\phi_1 \otimes \phi_2)_{//_P} = (k_{P,\phi_1} \oslash k_{P,\phi}) \otimes (\phi_1)_{//_P} \otimes (k_{P,\phi_2} \oslash k_{P,\phi}) \otimes (\phi_2)_{//_P}$

(4) $(\phi_1 \oplus \phi_2)_{//_P} = (k_{P,\phi_1} \oslash k_{P,\phi}) \otimes (\phi_1)_{//_P} \oplus (k_{P,\phi_2} \oslash k_{P,\phi}) \otimes (\phi_2)_{//_P}$

(5) $(\phi_1 \mathbin{\ominus} \phi_2)_{//_P} = (k_{P,\phi_1} \oslash k_{P,\phi}) \otimes (\phi_1)_{//_P} \mathbin{\ominus} (k_{P,\phi_2} \oslash k_{P,\phi}) \otimes (\phi_2)_{//_P}$

(6) $$(\langle a \rangle \phi_1)_{//_P} = (k_{P,\phi_1} \oslash k_{P,\phi}) \otimes \langle a \rangle (\phi_1)_{//_P} \oplus \bigoplus_{P \xrightarrow{a,k_a} P'} (k_a \otimes (k_{P',\phi_1} \oslash k_{P,\phi}) \otimes (\phi_1)_{//_{P'}})$$

(7) $$\begin{aligned}(\langle \tau \rangle \phi_1)_{//_P} = {} & (k_{P,\phi_1} \oslash k_{P,\phi}) \otimes \langle \tau \rangle (\phi_1)_{//_P} \oplus \bigoplus_{P \xrightarrow{\tau,k_\tau} P'} (k_\tau \otimes (k_{P',\phi_1} \oslash k_{P,\phi}) \otimes (\phi_1)_{//_{P'}}) \\ & \oplus \bigoplus_{P \xrightarrow{a,k_a} P'} ((k_a \otimes k_{P',\phi_1}) \oslash k_{P,\phi}) \otimes \langle \bar{a} \rangle (\phi_1)_{//_{P'}})\end{aligned}$$

(8) $$([a]\phi_1)_{//_P} = (k_{P,\phi_1} \oslash k_{P,\phi}) \otimes [a](\phi_1)_{//_P} \mathbin{\ominus} \bigominus_{P \xrightarrow{a,k_a} P'} (k_a \otimes (k_{P',\phi_1} \oslash k_{P,\phi}) \otimes (\phi_1)_{//_{P'}})$$

(9) $$\begin{aligned}([\tau]\phi_1)_{//_P} = {} & (k_{P,\phi_1} \oslash k_{P,\phi}) \otimes [\tau](\phi_1)_{//_P} \mathbin{\ominus} \bigominus_{P \xrightarrow{\tau,k_\tau} P'} (k_\tau \otimes (k_{P',\phi_1} \oslash k_{P,\phi}) \otimes (\phi_1)_{//_{P'}}) \\ & \mathbin{\ominus} \bigominus_{P \xrightarrow{a,k_a} P'} ((k_a \otimes k_{P',\phi_1}) \oslash k_{P,\phi}) \otimes [\bar{a}](\phi_1)_{//_{P'}})\end{aligned}$$

$K_{P,\varphi}$

(1) $\top$

(2) $\top$

(3) $k_{P,\phi_1} \oplus k_{P,\phi_2}$

(4) $k_{P,\phi_1} \oplus k_{P,\phi_2}$

(5) $k_{P,\phi_1} \oplus k_{P,\phi_2}$

(6) $k_{P,\phi_1} \oplus \bigoplus_{P'} k_{P',\phi_1}$

(7) $k_{P,\phi_1} \oplus (\bigoplus_{P'} k_{P',\phi_1}) \oplus \bigoplus_{P'} (k_a \otimes k_{P',\phi_1})$

(8) $k_{P,\phi_1} \oplus \bigoplus_{P'} k_{P',\phi_1}$

(9) $k_{P,\phi_1} \oplus (\bigoplus_{P'} k_{P',\phi_1}) \oplus \bigoplus_{P'} (k_a \otimes k_{P',\phi_1})$

(10) $k_{P,E} \oplus \bigoplus_{P_i \in DerP} k_{P_i,\phi_1} \oplus k_{P,E}$

(11) $k_{P,E} \oplus \bigoplus_{P_i \in DerP} k_{P_i,\phi_1}$

(12) $\top$

$k_{P,\varphi}$ is an amount of weight that QPMC can safely extract from each φ

$k_{P,\varphi}$ is a lub for the evaluation of φ

Why $K_{P,\varphi}$

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

$$[\![\phi]\!](P \parallel Q) = k_{P,\phi} \otimes [\![\phi_{//_P}]\!](Q)$$

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

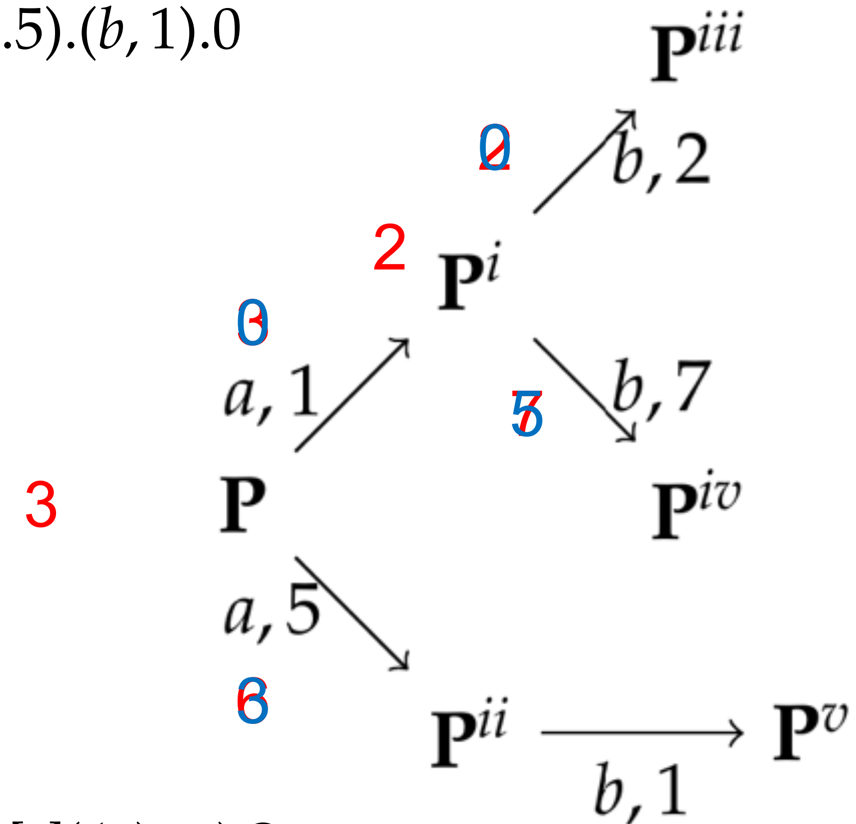
- In case it is not uniquely invertible, then

$$[\![\phi]\!]_\rho(P \parallel Q) \geq_K k_{P,\phi} \otimes [\![\phi_{//_P}]\!]_\rho(Q)$$

Example

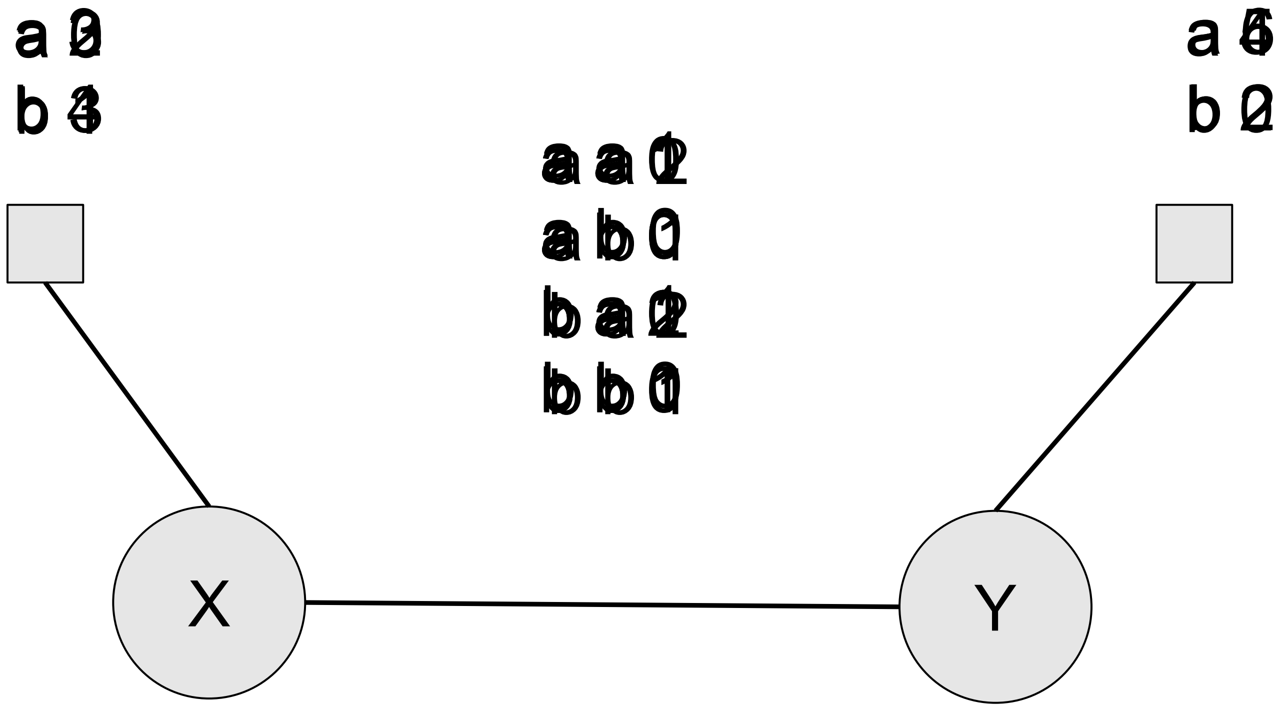
$$P = (a,1).((b,2).0 + (b,7).0) + (a.5).(b,1).0$$

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



$\phi_{//_P} = (\top \oslash 3 \otimes [a]\top) \Box (((1 \otimes 2) \ominus 3) \otimes [a](\phi_1)_{//_{P'}}) \Box (((5 \otimes 1) \oslash 3 \otimes [a](\phi_1)_{//_{P''}}) = ([a]([b]0 \Box [b]0 \Box (5 \otimes [b]0))) \Box (([b]0) \Box 3 \otimes [a][b]0)$

(Weighted) Arc Consistency



K=

V= {x, y}
D= {a, b}

Simplification Rules

Simple evaluation

Simple Evaluation

SE1	$\models_t v =_{\mu/\nu} \bigotimes\{h, \phi_1, \ldots, \phi_n\}$	$\Longleftrightarrow$	$\models_t v =_{\mu/\nu} \bot$ *if* $h <_K t$
SE2	$\models_t v =_{\mu/\nu} \bigotimes\{\top, \phi_1, \ldots, \phi_n\}$	$\Longleftrightarrow$	$\models_t v =_{\mu/\nu} \bigotimes\{\phi_1, \ldots, \phi_n\}$
SE3	$\models_t v =_{\mu/\nu} \textcircled{$\sqcap$}\{h, \phi_1, \ldots, \phi_n\}$	$\Longleftrightarrow$	$\models_t v =_{\mu/\nu} \bot$ *if* $h <_K t$
SE5	$\models_t v =_{\mu/\nu} \textcircled{$\sqcap$}\{\top, \phi_1, \ldots, \phi_n\}$	$\Longleftrightarrow$	$\models_t v =_{\mu/\nu} \textcircled{$\sqcap$}\{\phi_1, \ldots, \phi_n\}$
SE6	$\models_t v =_{\mu/\nu} \bigoplus\{\top, \phi_1, \ldots, \phi_n\}$	$\Longleftrightarrow$	$\models_t v =_{\mu/\nu} \top$
SE7	$\models_t v =_{\mu/\nu} \bigoplus\{h, \phi_1, \ldots, \phi_n\}$	$\Longleftrightarrow$	$\models_t v =_{\mu/\nu} \bigoplus\{\phi_1, \ldots, \phi_n\}$ *if* $h <_K t$
SE8	$\models_t v =_{\mu/\nu} \langle a \rangle h$	$\Longleftrightarrow$	$\models_t v =_{\mu/\nu} \bot$ *if* $h <_K t$
SE9	$\models_t v =_{\mu/\nu} [a]h$	$\Longleftrightarrow$	$\models_t v =_{\mu/\nu} \bot$ *if* $h <_K t$

From [Andersen ’95], valued

Constant Propagation

Constant Propagation

CP1

$$\begin{array}{c} \models_t v =_{\mu/\nu} \phi \\ \vdots \\ \models_t w =_{\mu/\nu} h \end{array} \quad \Longleftrightarrow \quad \begin{array}{c} \models_t v =_{\mu/\nu} \phi[h/w] \\ \vdots \\ \models_t w =_{\mu/\nu} h \end{array} \qquad \textit{if } \ h \geqslant_K t$$

CP2

$$\begin{array}{c} \models_t v =_{\mu/\nu} \phi \\ \vdots \\ \models_t w =_{\mu/\nu} h \end{array} \quad \Longleftrightarrow \quad \begin{array}{c} \models_t v =_{\mu/\nu} \phi[\bot/w] \\ \vdots \\ \models_t w =_{\mu/\nu} \bot \end{array} \qquad \textit{if } \ h <_K t$$

Trivial equation elimination

Trivial Equation Elimination

TEE1 $\models_t v =_\mu \langle a \rangle v$	$\Longleftrightarrow$	$\models_t v =_\mu \bot$
TEE2 $\models_t v =_\nu [a] v$	$\Longleftrightarrow$	$\models_t v =_\nu \top$
TEE3 $\models_t \phi \circledcap \phi$	$\Longleftrightarrow$	$\models_t \phi$
TEE4 $\models_t \phi \oplus \phi$	$\Longleftrightarrow$	$\models_t \phi$
TEE5 $\models_t \phi_1 \oplus (\phi_1 \otimes \phi_2)$	$\Longleftrightarrow$	$\models_t \phi_1$
TEE6 $\models_t \phi_1 \oplus (\phi_1 \circledcap \phi_2)$	$\Longleftrightarrow$	$\models_t \phi_1$
TEE7 $\models_t \phi_1 \circledcap (\phi_1 \otimes \phi_2)$	$\Longleftrightarrow$	$\models_k \phi_1 \otimes \phi_2$
TEE8 $\models_t \phi_1 \circledcap (\phi_1 \circledcap \phi_2)$	$\Longleftrightarrow$	$\models_t \phi_1 \circledcap \phi_2$

Complexity

Complexity

$\otimes$ is the glb

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

|FD(K')| = |2^(2^K)|

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

$$\langle \mathbb{R}^+ \cup \{+\infty\}, min, \hat{+}, \infty, 0 \rangle \qquad \phi = (v =_\mu v \otimes 2)$$

Theorem 5.2 (t-limited upper-bound). *Given the weighted semiring $\langle \mathbb{N}^+ \cup \{+\infty\}, \min, +, +\infty, 0 \rangle$ and an MLTS $= (S, Act, \mathbb{K}, T, s_0)$, $\models_t E_{\downarrow v}$ can be computed in $O(|E| \cdot N)$, where N is the number of solutions of a* Linear Diophantine Inequality $a_1x_1 + a_2x_2 + \ldots + a_rx_r \leqslant t$; $\{a_1, \ldots, a_n\}$ *is the subset of co-prime generators of the lattice in which the computation happens.*

$$\frac{t^r}{r! \prod_{i=1}^{r} a_i} \leqslant N \leqslant \frac{(t + a_1 + a_2 + \ldots + a_r)^r}{r! \prod_{i=1}^{r} a_i}$$

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 φ evaluation in case of uniquely invertible semirings
  - Simplification rules to cut the size of φ 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 unguarded [1])

UR

$$\begin{array}{c} \models_t v =_{\mu/\nu} \psi \\ \vdots \\ \models_t w =_{\mu/\nu} \phi \end{array} \iff \begin{array}{c} \models_t v =_{\mu/\nu} \psi[\phi/w] \\ \vdots \\ \models_t w =_{\mu/\nu} \phi \end{array}$$

Equivalence Reduction

ER1

$$\begin{array}{c} \models_t v =_{\mu} \phi_1 \\ \models_t w =_{\mu} \phi_2 \end{array} \iff \begin{array}{c} \models_t v =_{\mu} \phi_1 \oplus \phi_2 \\ \models_t w =_{\mu} v \end{array}$$

ER2

$$\begin{array}{c} \models_t v =_{\nu} \phi_1 \\ \models_t w =_{\nu} \phi_2 \end{array} \iff \begin{array}{c} \models_t v =_{\nu} \phi_1 \circledsqcap \phi_2 \\ \models_t w =_{\nu} v \end{array}$$

QPMC function (2)

$$(10) \quad (v =_\mu \phi_1 E)_{//_P} = \begin{cases} v_{P_1} =_\mu \quad \phi 1_{//_{P_1}} \\ \vdots \\ v_{P_n} =_\mu \quad \phi 1_{//_{P_n}} \\ E_{//_P} \end{cases}$$

$$(11) \quad (v =_\nu \phi_1 E)_{//_P} = \begin{cases} v_{P_1} =_\nu \quad \phi 1_{//_{P_1}} \\ \vdots \\ v_{P_n} =_\nu \quad \phi 1_{//_{P_n}} \\ E_{//_P} \end{cases}$$

$$(12) \quad \epsilon_{//_P} = \epsilon$$