Parameterized model-checking problems

Stéphane Demri

Laboratoire Spécification et Vérification (LSV)
CNRS UMR 8643 & ENS de Cachan

Plan of the talk

1. State explosion problem.
2. Parameterized complexity.
3. Parameterized Turing machine problems.
4. Parameterized reachability problems.
5. Parameterized logical model-checking problems.
6. Parameterized behavioral equivalence problems.

Symbolic model-checking

- Model-checking: $\mathcal{M} \models \phi$?
- Symbolic model-checking: $\mathcal{M} \models \phi$?
  - with $\mathcal{M}$ represented succinctly (not in extension);
  - symbolic algorithms have no explicit representation of the state space of $\mathcal{M}$.
- In practice, composition of subsystems is natural (by synchronization of actions/variables/clocks).
- Examples of succinct representation:
  - $\mathcal{M} = \mathcal{M}_1 \times \cdots \times \mathcal{M}_k$ synchronized product.
  - Graphs represented as OBDDs.

Succinct makes complex

- Graph Accessibility Problem (GAP)
  - is NLOGSPACE-complete [Jones 75].
  - is PSPACE-complete with graphs represented as OBDDs [Feigenbaum et al 98].

- Finite automaton intersection problem
  - $L(\mathcal{A}_1 \cap \mathcal{A}_2) = \emptyset$? is NLOGSPACE-complete.
  - $L(\mathcal{A}_1 \cap \cdots \cap \mathcal{A}_k) = \emptyset$? is PSPACE-complete (even with deterministic automata)

- Succinct representation may cause an increase of complexity.

Verification of non-flat systems

Logic	$\mathcal{M} \models \phi$?	$\mathcal{M}_1 \times \cdots \times \mathcal{M}_k \models \phi$?
LTL	PSPACE-complete	PSPACE-complete
CTL	P-complete	PSPACE-complete
CTL*	PSPACE-complete	PSPACE-complete
μ-cal.	in NP $\cap$ coNP	EXPTIME-complete

See e.g., [Rabinovich 97], [Esparza 98], [Kupferman et al. 00].

In practice, the source of intractability is the size of the model, not the size of the property.

Time complexity

Logic	$\mathcal{M} \models \phi$?
LTL	$2^{\mathcal{O}(\|\phi\|)} \times \|\mathcal{M}\|$
CTL	$\mathcal{O}(\|\phi\| \times \|\mathcal{M}\|)$
CTL*	$2^{\mathcal{O}(\|\phi\|)} \times \|\mathcal{M}\|$
μ-calculus	$\mathcal{O}((\|\phi\| \times \|\mathcal{M}\|)^{\|\phi\|})$

- With $\mathcal{M} = \mathcal{M}_1 \times \cdots \times \mathcal{M}_k$, $|\mathcal{M}| = |\mathcal{M}_1| \times \cdots \times |\mathcal{M}_k|$.
- Size of the input product model: $n = \Sigma_i |\mathcal{M}_i|$.
- $|\mathcal{M}| \in \mathcal{O}(n^k)$ and $|\mathcal{M}| \in \mathcal{O}(2^n)$.

Behavioral equivalences

Bisimulation is a typical example.

- $\mathcal{M}, s \stackrel{?}{\sim} \mathcal{M}', s'$ is P-complete [Balcàzar et al 92].
- $\mathcal{M}_1 \times \cdots \times \mathcal{M}_k, \bar{s} \stackrel{?}{\sim} \mathcal{M}'_1 \times \cdots \times \mathcal{M}'_k, \bar{s}'$ is EXPTIME-complete. See e.g.,
  - [Jategaonkar & Meyer 96]
  - [Harel et al 97]
  - [Rabinovich 97]
  - [Laroussinie & Schnoebelen 00]

Any hope to tame intractability?

The state explosion problem seems inescapable in the classical worst-case complexity paradigm.

How Downey & Fellows'
parameterized complexity framework
can cope with it?

A basic problem

Can $\mathcal{M}_1 \times \cdots \times \mathcal{M}_k \models \phi$ be solved in time
$\mathcal{O}(f(k) \times p(|\phi| + \Sigma_i |\mathcal{M}_i|))$ with f recursive & p polynomial?

Parameterized complexity

- Primary framework for problem analysis and algorithm design.
- Still a worst-case complexity paradigm.
- Analyses of problems in e.g.
  - graph theory, see e.g. [Downey & Fellows 99],
  - database queries [Papamiditriou & Yannakakis 99],
  - logic programming [Lonc & Truszczyński 02],
  - model-checking for first-order logic [Flum & Grohe 01],
  - infinite games [Björklund et al 03],
  - verification of non-flat systems [DLS02],
  - etc.

A few basic definitions

Parameterized language: L subset of $\Sigma^* \times \mathbb{N}$.

kth slice: $L_k = \{\langle x, k\rangle \in \Sigma^* \times \mathbb{N} : \langle x, k\rangle \in L\}$.

x: main part $\qquad$ k: parameter.

Assumption: k varies less than the size of x.

Fixed-parameter tractable: L is FPT, $\overset{\text{def}}{\Leftrightarrow}$ there exist a recursive function $f : \mathbb{N} \mapsto \mathbb{N}$ and a constant $c \in \mathbb{N}$ such that the question $\langle x, k\rangle \in L$ can be solved in time

$$f(k) \times |x|^c.$$

$f(k)$ as a factor not as an exponent.

$f(k) = 2^{2^{2^k}}$ is allowed.

Parameterized m-reduction (I)

$L \leq_{\mathrm{m}}^{\mathrm{fp}} L'$: $\overset{\text{def}}{\Leftrightarrow}$ there exist recursive total functions

- $f_1 : k \mapsto k'$,
- $f_2 : k \mapsto k''$,
- $f_3 : \langle x, k \rangle \mapsto x'$, and
- a constant $c \in \mathbb{N}$

such that

- $\langle x, k \rangle \mapsto x'$ is computable in time $k''|x|^c$, and
- $\langle x, k \rangle \in L$ iff $\langle x', k' \rangle \in L'$.

Parameterized m-reduction (II)

- Classical reductions carry less structure than parameterized reductions.
- $L \leq_{\mathrm{m}}^{\mathrm{fp}} L'$: each kth slice of L is reduced to the $f_1(k)$th slice of L'.
- Adding parameters to a problem makes it easier in the parameterized sense: $L(k,k') \leq_{\mathrm{m}}^{\mathrm{fp}} L(k)$.
- $[X]^{\mathrm{FPT}} = \{L : L \leq_{\mathrm{m}}^{\mathrm{fp}} L', \text{ for some } L' \in X\}$.
  (X set of parameterized languages)
- FPT is closed under m-reductions.

A non-parameterized reduction (I)

- WEIGHTED CNF SATISFIABILITY

  Instance: a propositional formula ϕ in CNF;

  Parameter: integer k;

  Question: Does ϕ have a satisfying valuation such that exactly k variables are set to true?

- WEIGHTED 3CNF SAT. defined as WEIGHTED CNF SAT. except each clause in ϕ has at most 3 literals.

- SAT $\leq_m^P$ 3SAT but what about

  WEIGHTED CNF SAT. $\leq_{\mathrm{m}}^{\mathrm{fp}}$ WEIGHTED 3CNF SAT.?

A non-parameterized reduction (II)

- $\phi = C_1 \wedge \cdots \wedge C_n$ with C_i of length l_i.
- $f(\phi)$ in 3CNF obtained from ϕ (by renaming of pairs of literals) with $v \models \phi$ implies $v' \models f(\phi)$ such that v is of weight k implies v' is of weight $g(k, l_1, \ldots, l_n)$.
- To be a parameterized reduction, the weight of v' should only depend on k.

A parameterized reduction

INDEPENDENT SET

Instance: a graph $G = \langle V, E \rangle$;

Parameter: k;

Question: Is there $V' \subseteq V$ of cardinality k such that for all $u, v \in V'$, $\langle u, v \rangle \notin E$?

CLIQUE

Instance: a graph $G = \langle V, E \rangle$;

Parameter: k;

Question: Is there $V' \subseteq V$ of cardinality k such that for all $u, v \in V'$, $\langle u, v \rangle \in E$?

$\langle V, E \rangle, k \longmapsto \langle V, (V \times V) \setminus E \rangle, k$.

Hierarchies of classes

- W[1]-hardness of L: first evidence that L is likely not to be FPT.

- XP: $L \in$ XP $\overset{\text{def}}{\Leftrightarrow}$ for every k, L_k is in P.
  Languages tractable "by the slice".

$$\mathrm{FPT} \subseteq \overbrace{\mathrm{W}[1] \subseteq \mathrm{W}[2] \subseteq \cdots \subseteq \mathrm{W}[\mathrm{SAT}] \subseteq \mathrm{W}[\mathrm{P}]}^{\text{originally defined with decision circuits}} \subseteq$$

$$\subseteq \underbrace{\mathrm{AW}[1] \subseteq \mathrm{AW}[\mathrm{SAT}] \subseteq \mathrm{AW}[\mathrm{P}]}_{\text{defined with PARAMETERIZED QBFSAT}} \subseteq \mathrm{XP}$$

- Few problems complete for each class below:

$$\mathrm{AW}[1] \;=\; \mathrm{AW}[*] \;=\; \bigcup_t \mathrm{AW}[t], \quad \mathrm{AW}[\mathrm{SAT}], \quad \mathrm{AW}[\mathrm{P}].$$

A definition of W[t]

$$\exists\, x_{11} \cdots \exists\, x_{1k_1}\, \forall\, x_{21} \cdots \forall\, x_{2k_2}\ \cdots Q\, x_{t1} \cdots Q\, x_{tk_t} \phi$$

- ϕ quantifier-free formula built over atomic formulae of the form $x = y$ and $R(x_1, \ldots, x_r)$,
- $Q = \forall$ if t is even, $Q = \exists$ otherwise,

$\Sigma_{t,u}$: Σ_t + all quantifier blocks after the leading $\exists$ block have length $\leq u$.

W[t] and model-checking problems

- P-MC(GRAPH,$\Sigma_{t,u}$)

  Instance: a graph $G = \langle V, E \rangle$ and $\phi \in \Sigma_{t,u}$;

  Parameter: $|\phi|$;

  Question: $G \models \phi$?

- **Theorem.** [Chen & Flum 2003] W[t] = [{P-MC(GRAPH,$\Sigma_{t,u}$) : $u \geq 1$}]$^{\mathrm{FPT}}$

- Other parameterized classes can be characterized by other model-checking problems.

Example - VERTEX COVER

- PARAMETERIZED VERTEX COVER

  Instance: a graph $G = \langle V, E \rangle$;

  Parameter: k;

  Question: Is there $V' \subseteq V$ with $|V'| \leq k$ such that for every $\langle u, v \rangle \in E$, either $u \in V'$ or $v \in V'$?

- VERTEX COVER is NP-complete but

  Theorem. [Balasubramanian et al 98]
  PARAMETERIZED VERTEX COVER is in FPT and can be solved in time $\mathcal{O}((53/40)^k \times k^2 + k \times n)$.

Example - INDEPENDENT SET

- INDEPENDENT SET is NP-complete.

- **Theorem.** PARAMETERIZED INDEPENDENT SET is W[1]-complete.

- INDEPENDENT SET with graphs represented as OBDDs is NEXPTIME-complete [Feigenbaum et al 98].

Time as a parameter in TMs

- SHORT NDTM COMPUTATION

  Instance: a single-tape non-deterministic Turing machine M and a positive integer k (unary);

  Parameter: k;

  Question: Is there a computation of M on the empty string input that reaches a final accepting state in at most k steps?

- SHORT NDTM COMPUTATION is W[1]-complete [Downey et al 94].

- SHORT DTM COMPUTATION is FPT.

- The multi-tape version of SHORT NDTM COMPUTATION is W[2]-complete [Cesati 03].

SHORT ATM COMPUTATION

- **Theorem.** [DLS02] SHORT ATM COMPUTATION is AW[1]-complete.

  $\longrightarrow$ very high in the hierarchy

- Other problems with ATMs complete for classes of the W/AW hierarchies can be found in [Chen & Flum 03, Chen & Flum & Grohe 03].

- We show fp-equivalence with PARAMETERIZED QBFSAT$_t$.

An AW[1]-complete problem

- PARAMETERIZED QBFSAT$_t$

  Instance: $\psi = \exists^{=k_1} X_1 \forall^{=k_2} X_2 \ldots \forall^{=k_{2p}} X_{2p} \phi$

  ϕ positive Boolean combination of literals with at most t alternations of $\wedge$ and $\vee$;

  Parameter: $\langle k_1, \ldots, k_{2p} \rangle$;

  Question: Is ψ true?

  $\exists^{=k_i} X_i$ is interpreted by “does there exist an valuation of weight k_i over X_i such that . . . ”.
  $\forall^{=k_i} X_i$ is interpreted by “for all valuations of weight k_i over X_i, . . . ”.

- **Theorem.** [Downey & Fellows 99] PARAMETERIZED QBFSAT$_t$ is AW[1]-complete $\forall t \geq 1$.

- $AW[*] = AW[1] = AW[t]$ for all $t \geq 2$.

Reduction to SHORT ATM COMP.

- $\psi = \exists^{=k_1} X_1 \forall^{=k_2} X_2 \ldots \forall^{=k_{2p}} X_{2p} \phi$.

- Construction of the ATM M_ψ.

  M_ψ picks $k_1 + \cdots + k_{2p}$ variables in $X_1 \cup \cdots \cup X_{2p}$.

  Structure of ϕ reflected by the transition table of M_ψ.

  Universal states encode both $\forall^{=k_i}$ and conjunctions.

  Existential states encode both $\exists^{=k_i}$ and disjunctions.

- M_ψ answers in time $\mathcal{O}(k + t)$, i.e. $\mathcal{O}(k)$.

Space as a parameter in TMs

- COMPACT NDTM COMPUTATION

  Instance: a single-tape non-deterministic Turing machine M and a positive integer k;

  Question: Is there a computation of M on the empty string input that reaches a final accepting state using at most k work tape squares?

- COMPACT NDTM COMPUTATION is AW[SAT]-hard [Chen & Flum & Grohe 03].

- **Theorem.** COMPACT ATM COMPUTATION is XP-complete.

PARAMETERIZED PEBBLE GAME (I)

PARAMETERIZED PEBBLE GAME

Instance: A pebble game $\langle N, R, S, T \rangle$;

Parameter: $|S|$;

Question: Does the player I has winning strategy?

N: set of nodes
S: set of initial nodes
$T \in N$: terminal node
$R \subseteq N^3$: set of moves

Move: $\overset{x}{\blacksquare} \quad \overset{y}{\blacksquare} \quad \overset{z}{\square} \Rightarrow \overset{x}{\square} \quad \overset{y}{\blacksquare} \quad \overset{z}{\blacksquare}$ if $R(x, y, z)$.

Player I wins if he can reach T or if Player II cannot move.

PARAMETERIZED PEBBLE GAME *(II)*

Theorem. [Adachi & Iwata & Kasai 79]
PARAMETERIZED PEBBLE GAME is XP-complete.

The reduction showing PEBBLE GAME is EXPTIME-hard turns out to show also that

$$\text{COMPACT ATM COMP.} \leq_{\mathrm{m}}^{\mathrm{fp}} \text{PAR. PEBBLE GAME.}$$

PAR. PEBBLE GAME *(III)*

- PARAMETERIZED PEBBLE GAME $\leq^{\mathrm{fp}}_{\mathrm{m}}$ COMPACT ATM COMPUTATION.

  $PG = \langle N, R, S, T \rangle$; $|S| = k$.

- Construction of the ATM M_{PG}.

  Alphabet: N. k work-tape squares.

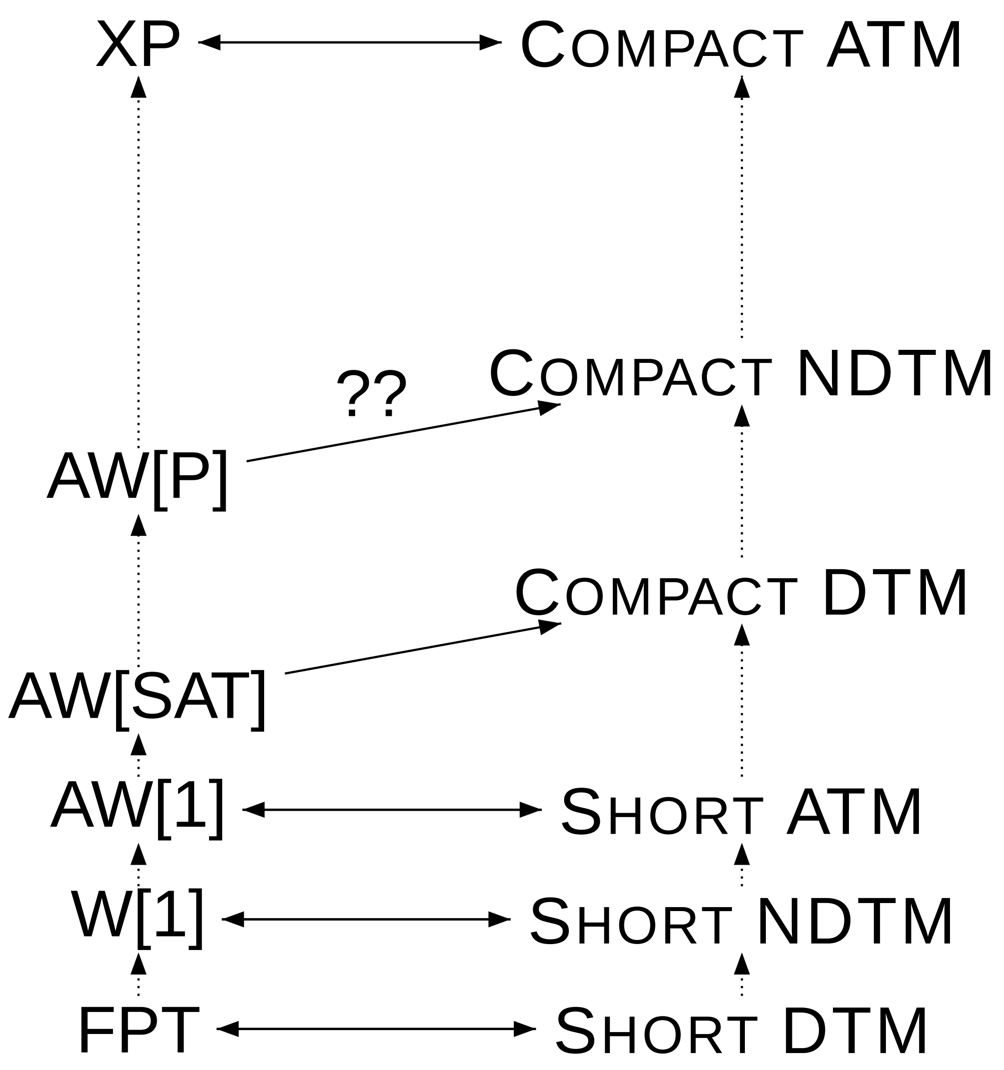
  Moves of Player I emulated by existential states.

  Moves of Player II emulated by universal states.

  R and S encoded in the transition table.

- $|M_{PG}|$ is in $\mathcal{O}(|PG|)$ and $k' = k$.

Parameterized classes and TM pbs



LTSs

- Labeled transition system (LTS): $\mathcal{A} = \langle Q, \Sigma, \rightarrow \rangle$.
- $\rightarrow \subseteq Q \times \Sigma \times Q$.
- $|\mathcal{A}| = |Q| + |\Sigma| + |\rightarrow|$.
- Product LTS $\mathcal{A}_1 \times \cdots \times \mathcal{A}_n$ with set of states $\Pi_{i=1}^{n} Q_i$ and alphabet $\bigcup_{i=1}^{k} \Sigma_i$.

Synchronization protocols

Strong synchronization

all components move at the same time:

$\langle s_1, \ldots, s_k \rangle \xrightarrow{a}_{\mathrm{str}} \langle t_1, \ldots, t_k \rangle$ iff $s_i \xrightarrow{a}_i t_i$ for all $i = 1, \ldots, k$.

Binary synchronization

two components synchronize while the rest does not move.

$\langle s_1, \ldots, s_k \rangle \xrightarrow{a}_{\mathrm{bin}} \langle t_1, \ldots, t_k \rangle$ iff there exist i and j ($i \neq j$) s.t. $s_i \xrightarrow{a}_i t_i$ and $s_j \xrightarrow{a}_j t_j$ while $s_l = t_l$ for all $l \notin \{i, j\}$.

Parameterized Exact Reachability

Reachability problems are fundamental in model-checking.

Exact Reachability (EXACT-REACH)

Instance: k LTSs $\mathcal{A}_1, \cdots, \mathcal{A}_k$,
two configurations $\bar{s}$ and $\bar{t}$ of $\mathcal{A}_1 \times \cdots \times \mathcal{A}_k$;

Parameter: k;

Question: $\bar{s} \xrightarrow{*} \bar{t}$?

Parameterized Local Reachability

Local Reachability (LOCAL-REACH)

Instance: k LTSs $\mathcal{A}_1, \cdots, \mathcal{A}_k$,
sets $F_1, \ldots, F_k$ of states with $F_i \subseteq Q_i$,
a configuration $\bar{s}$ of $\mathcal{A}_1 \times \cdots \times \mathcal{A}_k$;

Parameter: k;

Question: Does $\bar{s} \xrightarrow{*} \bar{t}$ for some $\bar{t} \in \bar{F}$
where $\bar{F} = F_1 \times \cdots \times F_k$?

Parameterized Repeated Reachability

Repeated Reachability (REP-REACH)

Instance: k LTSs $\mathcal{A}_1, \cdots, \mathcal{A}_k$,
sets $F_1, \ldots, F_k$ of states with $F_i \subseteq Q_i$,
a configuration $\bar{s}$ of $\mathcal{A}_1 \times \cdots \times \mathcal{A}_k$;

Parameter: k;

Question: Does $\bar{s} \xrightarrow{*} \bar{t} \xrightarrow{+} \bar{t}$ for some $\bar{t} \in \bar{F}$
where $\bar{F} = F_1 \times \cdots \times F_k$?

(Büchi acceptance condition)

Parameterized Fair Reachability

Fair Reachability (FAIR-REACH)

Instance: k LTSs $\mathcal{A}_1, \cdots, \mathcal{A}_k$,

sets $(F_i^j)_{i=1,\ldots,k}^{j=1,\ldots,p}$ with $F_i^j \subseteq Q_i$ for all i, j,

a configuration $\bar{s}$ of $\mathcal{A}_1 \times \cdots \times \mathcal{A}_k$.

For all j, we write $\bar{F^j}$ for $F_1^j \times \cdots \times F_k^j$.

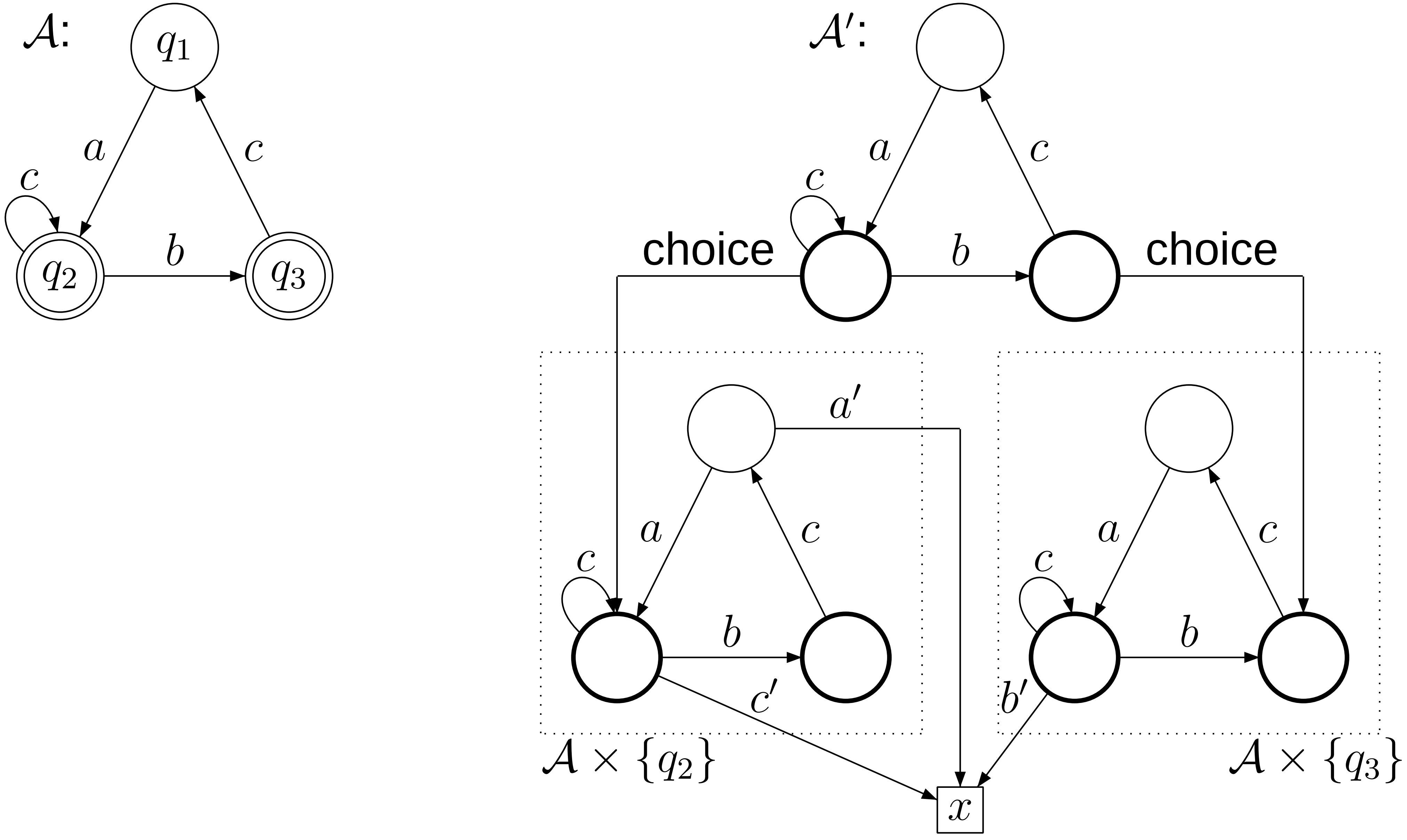
Parameter: k;

Question: Does $\bar{s} \xrightarrow{*} \bar{t_1} \xrightarrow{*} \bar{t_2} \ldots \xrightarrow{*} \bar{t_p} \xrightarrow{+} \bar{t_1}$ for some $\bar{t_1}, \ldots, \bar{t_p} \in \bar{F^1}, \ldots, \bar{F^p}$?

Equivalence

- **Theorem.** The four parameterized reachability problems are fp-equivalent.
- k-$*$-REACH: any of the four problems.
- By way of example, we sketch the construction to show k-REP-REACH $\leq_{\mathrm{m}}^{\mathrm{fp}}$ k-EXACT-REACH:

Sketch of the proof (I)



Sketch of the proof (II)

Equivalence between

1. $\bar{s} = \langle q_1, \ldots, q_k \rangle \xrightarrow{*} \bar{t} \xrightarrow{+} \bar{t}$ in $\mathcal{A}_1 \times \cdots \times \mathcal{A}_k$;
2. $\langle q_1^0, \ldots, q_k^0 \rangle \xrightarrow{*}\xrightarrow{\text{choice}} \langle f_1^{j_1}, \ldots, f_k^{j_k} \rangle \xrightarrow{+} \langle x_1, \ldots, x_k \rangle$ in $\mathcal{A}'_1 \times \cdots \times \mathcal{A}'_k$;
3. $\langle q_1^0, \ldots, q_k^0 \rangle \xrightarrow{*} \langle x_1, \ldots, x_k \rangle$.

$\bar{t} = \langle f_{1,j_1}, \ldots, f_{k,j_k} \rangle \in F_1 \times \cdots \times F_k$.

Cost of the reduction

- $|\mathcal{A}'_i|$ in $\mathcal{O}((|F_i|+1) \times |\mathcal{A}_i|)$.
- $k' = k$.
- $|\Sigma'| = 2 \times |\Sigma| + 1$.
- $n' \in \mathcal{O}(n^2)$.
- Simpler reductions exist but we want also to preserve determinism.

fp-equivalence (I)

Theorem. k-$*$-REACH is fp-equivalent to COMPACT NDTM COMPUTATION.

Proof sketch of

$$\text{COMPACT NDTM COMPUTATION} \leq^{\text{fp}}_{\text{m}} k\text{-LOCAL-REACH}.$$

With an NDTM M and an integer k we associate a product $\mathcal{A}_1 \times \cdots \times \mathcal{A}_k \times \mathcal{A}_{\text{state}} \times \mathcal{A}_{\text{head}}$ of $k+2$ LTSs that emulate the behaviour of M on a k-bounded tape.

- each $\mathcal{A}_i$ stores the current contents of the i-th tape square,
- $\mathcal{A}_{\text{state}}$ stores the current control-state of M,
- $\mathcal{A}_{\text{head}}$ stores the position of the TM head.

fp-equivalence (II)

- Synchronization on labels of the form $\langle t, i\rangle$ that stand for "rule t of M is fired while head is in position i".
- Successful acceptance by M is directly encoded as a local reachability criterion.
- Finally we translated our instance to a k-LOCAL-REACH instance with $k' = k + 2$ and $n' = O(kn^2)$.
- See also [Kozen 77] and [Papadimitriou 94] for the PSPACE-hardness proof of reachable deadlock for a system of communicating processes.

Robustness of the equivalence

Variants fp-equivalent to k-$*$-REACH:

Binary synchronization:

k-$*$-REACH$_{bin}$ $\quad$ k, Σ-$*$-REACH$_{bin}$

Bounded size alphabet:

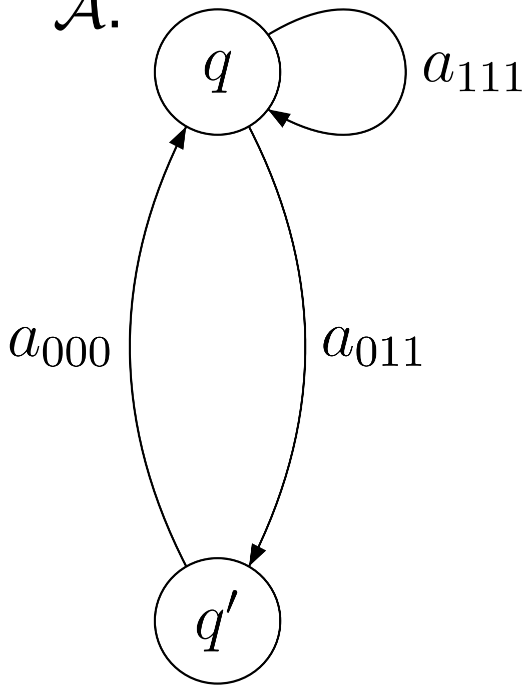
k, Σ-$*$-REACH $\quad$ k-$*$-REACH$_{|\Sigma|=2}$

Determinism:

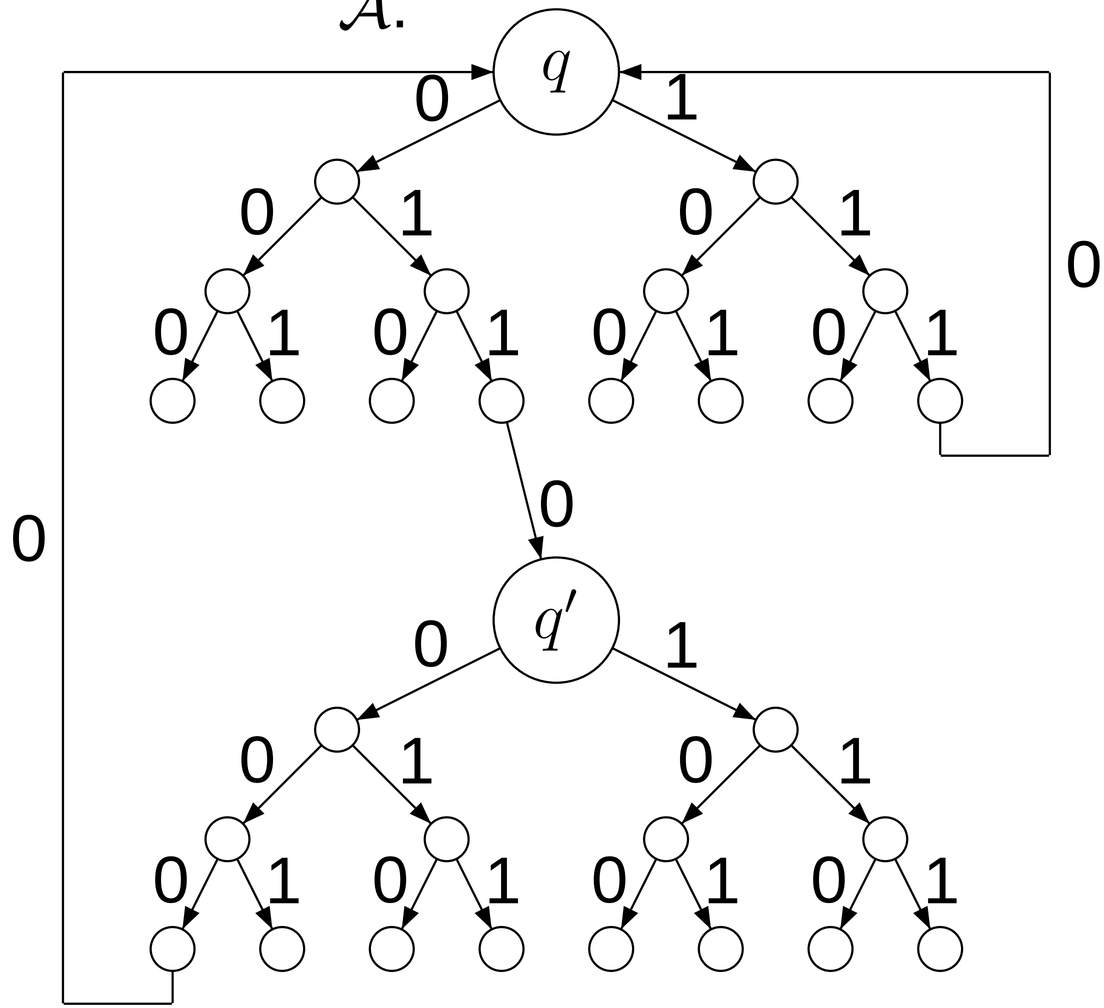
k, Σ-$*$-REACH$_{det}$ $\quad$ k-$*$-REACH$_{|\Sigma|=2,det}$

Bounding $|\Sigma|$

$\mathcal{A}$:



$\widehat{\mathcal{A}}$:



$q \xrightarrow{a_{000}} q'$ iff $q \xrightarrow{0000} q'$.

Parameterized temporal logic pbs.

- **Kripke structure** $\mathcal{M} = \langle \mathcal{A}, m \rangle$
  $\mathcal{A}$ LTS, $m \subseteq Q \times AP$.
  $\langle \mathcal{A}_1, m_1 \rangle \times \cdots \times \langle \mathcal{A}_k, m_k \rangle = \langle \mathcal{A}_1 \times \cdots \times \mathcal{A}_k, \bigoplus_i m_i \rangle$

- Sometimes, the labels are used only for the synchronization and not in the product models.

- **Parameterized model checking for logic L (MC$_L$)**

  Instance: Kripke structures $\mathcal{M}_1, \cdots, \mathcal{M}_k$,
  a configuration $\bar{s}$,
  an L-formula ϕ;

  Parameter: $k, |\phi|$;

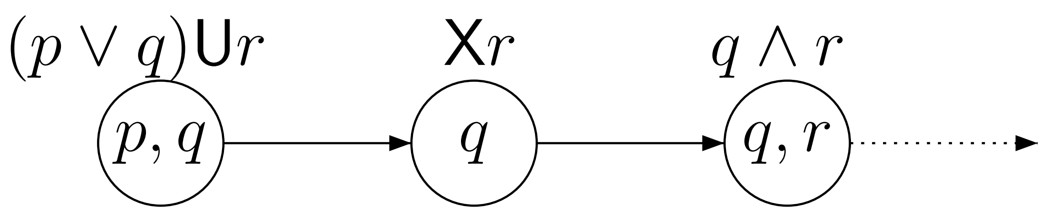
  Question: $\mathcal{M}_1 \times \cdots \times \mathcal{M}_k, \bar{s} \models \phi$?

LTL

- Linear-time temporal logic for the specification of critical systems.

$$\phi := \mathrm{p} \mid \neg\phi \mid \phi \wedge \phi' \mid \mathsf{X}\phi \mid \phi \mathsf{U} \phi'.$$

- Models: $\sigma : \mathbb{N} \rightarrow 2^{AP}$.
  Satisfiability relation: $\sigma, i \models \phi$



- Model-checking: $\mathcal{M}, s \models \phi$?
  Is there a path σ starting at s such that $\sigma, 0 \models \phi$?

Par. model checking for LTL

- **Theorem.** k, ϕ-MC$_{\mathrm{LTL}}$ is fp-equivalent to COMPACT NDTM COMPUTATION (and hence is AW[SAT]-hard).
- COMPACT NDTM COMPUTATION $\leq^{\mathrm{fp}}_{\mathrm{m}}$ k, ϕ-MC$_{\mathrm{LTL}}$ because LTL can express reachability questions.
- k, ϕ-MC$_{\mathrm{LTL}}$ $\leq^{\mathrm{fp}}_{\mathrm{m}}$ COMPACT NDTM COMPUTATION reduces to a repeated reachability question on $\mathcal{M}_1 \times \cdots \times \mathcal{M}_k \times \mathcal{B}_\phi$.

W[1]-completeness

LTL0: poor fragment of LTL that cannot express reachability.

$$\phi := \mathrm{p} \mid \phi \vee \phi' \mid \mathsf{X}\phi.$$

Theorem. k, ϕ-MC$_{\mathrm{LTL0}}$ is W[1]-complete, even with only using a single atomic proposition.

Modal μ-calculus

- **Theorem.** k, ϕ-MC$_\mu$ is XP-complete.

  Writing n for $\sum_i |\mathcal{M}_i|$, k, ϕ-MC$_\mu$ can be solved in time $\mathcal{O}\big((|\phi|.n^k)^{|\phi|}\big)$.

- XP-hardness is proved by a reduction from non-flat bisimilarity. Equivalence between
  - $\mathcal{A}$ and $\mathcal{B}$ are bisimilar;
  - $\mathcal{A} \parallel \mathcal{B}' \models \nu X. \bigwedge_{a\in\Sigma}([a]\langle a'\rangle X \wedge [a']\langle a\rangle X)$.
    $\mathcal{A} \parallel \mathcal{B}'$ interleaved product with $\mathcal{B}'$ obtained from $\mathcal{B}$ by renaming the actions $a \in \Sigma$ by a'.

- Non-flat bisimilarity is XP-hard already when $|\Sigma| = 2$.
  $\rightarrow$ we can bound the size of the μ-formula and have an fp-reduction.

HML

$$\phi ::= \mathrm{p} \;\mid\; \phi \vee \phi' \;\mid\; \phi \wedge \phi' \;\mid\; \Box\phi \;\mid\; \Diamond\phi.$$

- **Theorem.** k, ϕ-MC$_{\mathrm{HML}}$ is AW[1]-complete.
- Idea of the proof: k, ϕ-MC$_{\mathrm{HML}}$ is fp-equivalent to SHORT ATM COMPUTATION.
- Use of the standard correspondence between $\Box$ and $\Diamond$ and the behaviour of the ATMs with univ. states and exist. states, resp.

Computation Tree Logic CTL

- CTL can express reachability questions:
- **Theorem.** COMPACT NDTM COMPUTATION $\leq_{\mathrm{m}}^{\mathrm{fp}} k, \phi$-MC$_{\mathrm{CTL}}$.
- Hence k, ϕ-MC$_{\mathrm{CTL}}$ is AW[SAT]-hard.
- **Open question**: Do we have k, ϕ-MC$_{\mathrm{CTL}} \leq_{\mathrm{m}}^{\mathrm{fp}}$ COMPACT NDTM COMPUTATION?

Parameterized bisimulation

Parameterized Bisimulation (BISIM)

Instance: $2k$ LTSs $\mathcal{A}_1, \cdots, \mathcal{A}_k, \mathcal{A}'_1, \cdots, \mathcal{A}'_k$,
a configuration $\bar{s}$ of $\mathcal{A}_1 \times \cdots \times \mathcal{A}_k$,
a configuration $\bar{s'}$ of $\mathcal{A}'_1 \times \cdots \times \mathcal{A}'_k$.

Question: Is $\langle \mathcal{A}_1 \times \cdots \times \mathcal{A}_k, \bar{s} \rangle$ (strongly) bisimilar to
$\langle \mathcal{A}'_1 \times \cdots \times \mathcal{A}'_k, \bar{s'} \rangle$?

Similar definition for other behavioral equivalence R between trace inclusion $\subseteq_{\mathrm{tr}}$ and bisimulation.

XP-complete problems

- **Theorem.** k-BISIM is XP-complete.
- k-BISIM is in XP since bisimilarity of flat systems is in P.
- XP-hardness is by observing that the reduction in the proof of Theorem 4.1 in [Laroussinie & Schnoebelen 00] can be seen as an fp-reduction from COMPACT ATM COMPUTATION to k-BISIM.
- **Theorem.** k-BISIM and k-BISIM$_{|\Sigma|=2}$ are fp-equivalent.

Other behavioral equivalences

- **Theorem.** For any relation R lying between the simulation preorder and bisimilarity, k-R-CHECKING is XP-hard.

- Consequence of [Laroussinie & Schnoebelen 00].

- Another hardness result:

  Theorem. For any relation R lying between trace inclusion and bisimilarity, coCOMPACT NDTM COMPUTATION is fp-reducible to k-R-CHECKING, i.e. the problem of checking whether $\langle \mathcal{A}_1 \times \cdots \times \mathcal{A}_k, \bar{s}\rangle R \langle \mathcal{A}'_1 \times \cdots \times \mathcal{A}'_k, \bar{s'}\rangle$.

Sketch of the proof

Reduction of $\overline{k\text{-Exact-Reach}}$ to k-R-Checking.

$\mathcal{A}_1, \ldots, \mathcal{A}_k$, $\bar{s}$, $\bar{t}$ instance of k-Exact-Reach where $\bar{t} = \langle t_1, \ldots, t_k \rangle$.

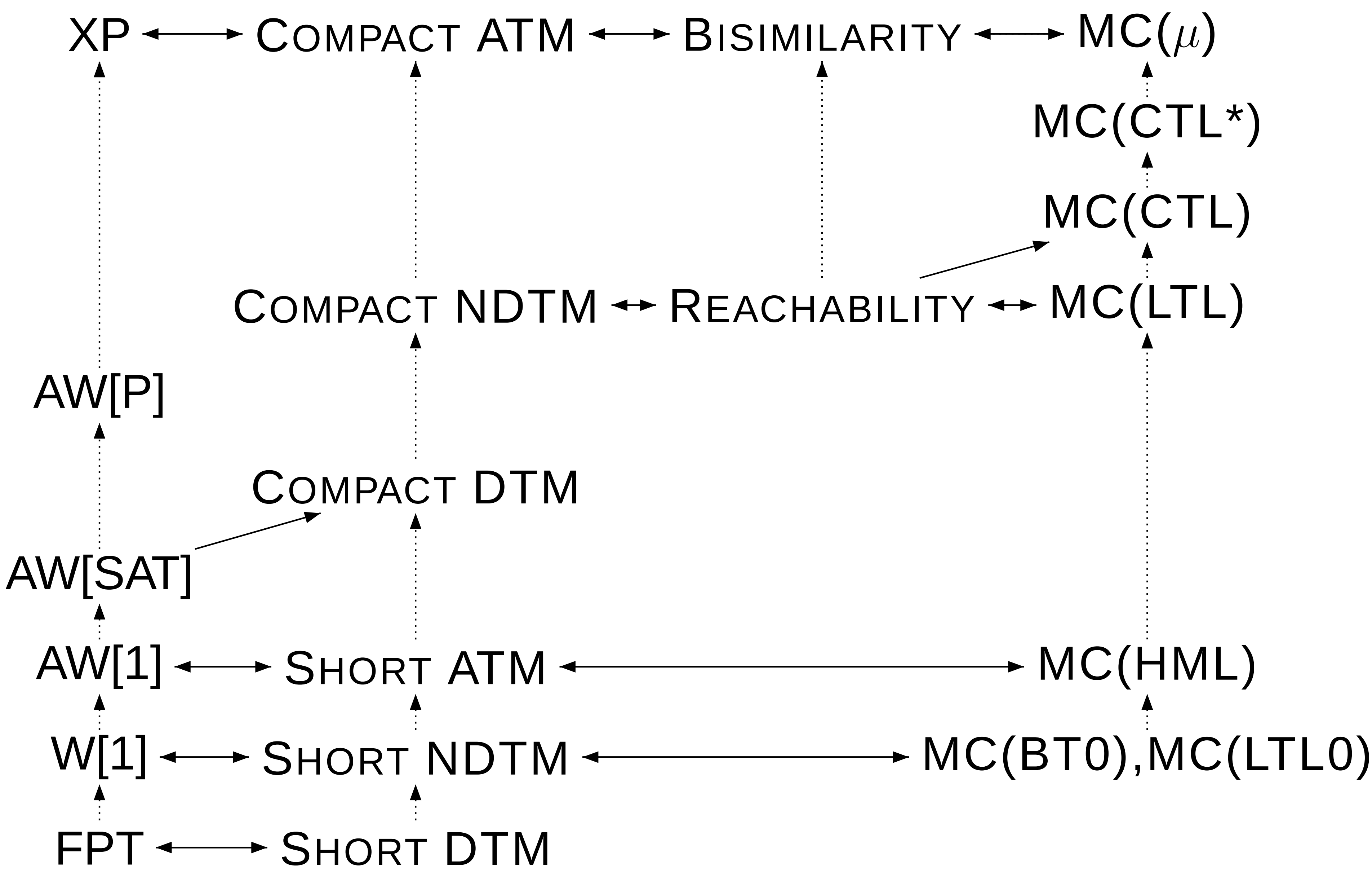
$\mathcal{A}'_i$: $\mathcal{A}_i$ + a loop $t_i \xrightarrow{\#} t_i$, $\#$ new label.

$\mathcal{S} = \mathcal{A}_1 \times \cdots \times \mathcal{A}_k$, $\mathcal{S}' = \mathcal{A}'_1 \times \cdots \times \mathcal{A}'_k$

(1) $\langle \mathcal{S}, \bar{s} \rangle \sim \langle \mathcal{S}', \bar{s} \rangle$ iff (2) $\langle \mathcal{S}', \bar{s} \rangle \subseteq_{\mathrm{tr}} \langle \mathcal{S}, \bar{s} \rangle$ iff (3) not $\bar{s} \xrightarrow{*} \bar{t}$ in $\mathcal{S}$.

Consequently, for $\sim \subseteq R \subseteq \subseteq_{\mathrm{tr}}$, $\langle \mathcal{S}, \bar{s} \rangle R \langle \mathcal{S}', \bar{s} \rangle$ iff not $\bar{s} \xrightarrow{*} \bar{t}$.

Summary


XP
COMPACT ATM
BISIMILARITY
MC(μ)
MC(CTL*)
MC(CTL)
COMPACT NDTM
REACHABILITY
MC(LTL)
AW[P]
COMPACT DTM
AW[SAT]
AW[1]
SHORT ATM
MC(HML)
W[1]
SHORT NDTM
MC(BT0),MC(LTL0)
FPT
SHORT DTM

Some concluding remarks

- Parameterized complexity framework is not yet in a stable condition. (see e.g. the introduction of the class MINI[1]).
- There are plenty of complexity issues related to verification problems in this framework (timed automata, Rabin automata, etc ...).
- Many problems from formal verification can be naturally parameterized but how parameterized complexity can be used to induce improvements in practice?
(mainly dark side presented during this talk)