PSPACE-Hardness of Strong Bisimilarity for BPP

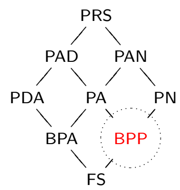
Jiri Srba, BRICS Aalborg

30.11 – 1.12 2005
PhD Course at FIRST Graduate School, IT University

BPP - Basic Parallel Processes

Basic Parallel Processes (BPP)
$(1, \mathcal{P})$-PRS

Rule type:
$X \stackrel{a}{\longrightarrow} X \| Y \| Z$
$X \stackrel{a}{\longrightarrow} \epsilon$



- a basic model of purely parallel programs
- fragment of CCS without restriction, relabelling and communication
- equivalent to communication free subclass of Petri nets

Example

Let $Const = \{Q_1, Q_2, \ldots, Q_k\}$ and $Act = \{q_1, q_2, \ldots, q_k\}$.

$$Q_j \stackrel{q_j}{\longrightarrow} Q_j \qquad \text{for all } j,\ 1 \le j \le k$$

Let $i_1, \ldots, i_\ell \in \{1, 2, \ldots, k\}$ and $j_1, \ldots, j_m \in \{1, 2, \ldots, k\}$. Now

$$Q_{i_1} \| \cdots \| Q_{i_\ell} \sim Q_{j_1} \| \cdots \| Q_{j_m}$$

if and only if

$$\{i_1, \ldots, i_\ell\} = \{j_1, \ldots, j_m\}.$$

E.g.: $Q_1 \| Q_2 \| Q_2 \sim Q_2 \| Q_1$

Summary of Results for BPP

- Language equivalence is undecidable [Hüttel'94].
- Strong bisimilarity is decidable [Christensen, Hirshfeld, Moller'93], even in PSPACE [Jančar'03].
- We will argue how to show PSPACE-hardness [Srba'02].

QSAT — a PSPACE-Complete Problem

Quantified Satisfiability (QSAT) or also Quantified Boolean formula (QBF) problem is PSPACE-complete.

Problem:	QSAT
Instance:	A natural number $n > 0$ and a Boolean formula ϕ in conjunctive normal form with Boolean variables $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$.
Question:	Is $\exists x_1 \forall y_1 \exists x_2 \forall y_2 \ldots \exists x_n \forall y_n . \phi$ true?

Example:
$\exists x_1 \forall y_1 \exists x_2 \forall y_2.\ (x_1 \vee \neg y_1 \vee y_2) \wedge (\neg x_1 \vee y_1 \vee y_2) \wedge (x_1 \vee y_1 \vee y_2 \vee \neg y_2)$

Reduction Idea

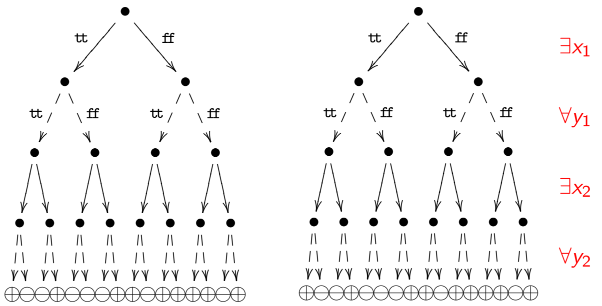
For a QSAT formula C we construct a BPP system with two processes X and X' such that:

C is true

if and only if

$X \sim X'$

Bisimulation Game



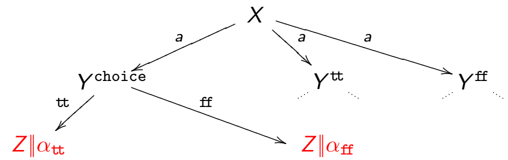
Problems:

- the $\xrightarrow{tt}$ and $\xrightarrow{ff}$ arrows
- exponential blow up in the size

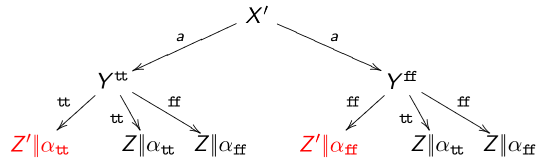
Reduction from QSAT to $\sim$ of BPP

- We present a construction enabling the defender to force the attacker to perform a certain move (Defender's Choice).
- We show a way how to remember (encode) and check satisfied clauses.

Defender's Choice Technique



Can this be simplified?



How to Represent Clauses

Let us fix a QSAT formula C:

$$C \equiv \exists x_1 \forall y_1 \exists x_2 \forall y_2 \ldots \exists x_n \forall y_n.\ C_1 \wedge C_2 \wedge \ldots \wedge C_k$$

New process constants $Q_1, \ldots, Q_k$ such that for all j, $1 \leq j \leq k$:

$$Q_j \xrightarrow{q_j} Q_j$$

Example:
Satisfied clauses C_1, C_3 and C_4 are represented by $Q_1 \| Q_3 \| Q_4$.

How to Remember Satisfied Clauses

$$C \equiv \exists x_1 \forall y_1 \exists x_2 \forall y_2 \ldots \exists x_n \forall y_n.\ C_1 \wedge C_2 \wedge \ldots \wedge C_k$$

Let

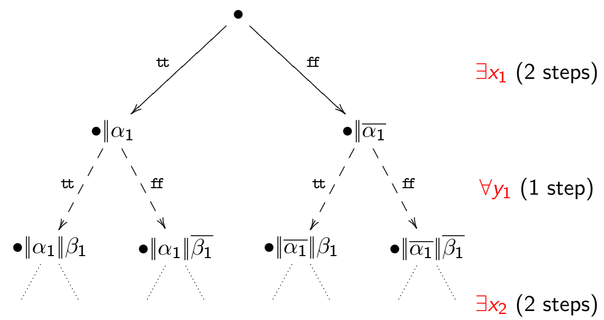
$\alpha_i \equiv Q_{i_1} \| Q_{i_2} \| \cdots \| Q_{i_\ell}$ such that x_i occurs positively in $C_{i_1}, C_{i_2}, \ldots, C_{i_\ell}$

$\overline{\alpha_i} \equiv Q_{i_1} \| Q_{i_2} \| \cdots \| Q_{i_\ell}$ such that x_i occurs negatively in $C_{i_1}, C_{i_2}, \ldots, C_{i_\ell}$

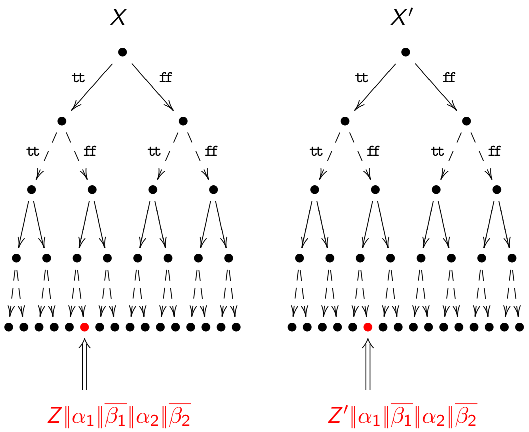
$\beta_i \equiv Q_{i_1} \| Q_{i_2} \| \cdots \| Q_{i_\ell}$ such that y_i occurs positively in $C_{i_1}, C_{i_2}, \ldots, C_{i_\ell}$

$\overline{\beta_i} \equiv Q_{i_1} \| Q_{i_2} \| \cdots \| Q_{i_\ell}$ such that y_i occurs negatively in $C_{i_1}, C_{i_2}, \ldots, C_{i_\ell}$.

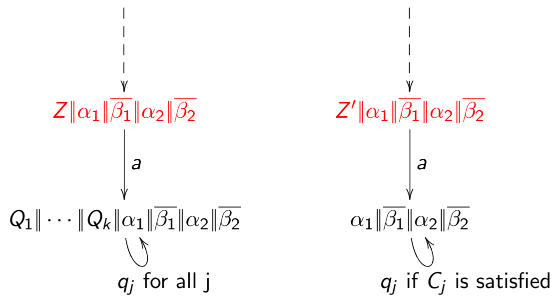
Remembering Clauses



Generation Phase from X and X'



Checking Clauses



$Z \xrightarrow{a} Q_1\|Q_2\|\cdots\|Q_k$ $\qquad$ $Z' \xrightarrow{a} \epsilon$

Strong Bisimilarity on BPP is PSPACE-Complete

Theorem

Strong bisimilarity on BPP is PSPACE-hard.

Theorem

Strong bisimilarity on BPP is PSPACE-complete.