Algorithms for Model Checking (2IW55)

Lecture 11
Parity games
Background material:
Chapter 3 of "An experimental study of algorithms and optimisations for parity games, with an application to Boolean Equation Systems",
J.J.A. Keiren

Jeroen Keiren
(jkeiren@win.tue.nl)
http://www.win.tue.nl/~jkeiren
HG 6.81

Parity games

Today: verification problem represented by parity games:

- graph game
- total graph
- two players: $\Diamond$ and $\Box$ (Even and Odd)
- vertices:
  - integer priority $\mathsf{p}(v)$
  - owned by one player

Playing the game:

- token on vertex
- player does step to successor vertex if token is on vertex owned by him
- play: infinite sequence of steps

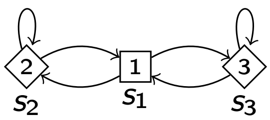
Parity games (definition)

Definition (Parity game)

A parity game Γ is a four tuple $(V, E, p, (V_\diamond, V_\Box))$ where

- (V, E) is a directed graph
- V a set of vertices
- E a total edge relation
- $p : V \to \mathbb{N}$ a priority function
- $(V_\diamond, V_\Box)$ a partitioning of V, i.e. $V = V_\diamond \cup V_\Box$ and $V_\diamond \cap V_\Box = \emptyset$

Parity game (example)



$$
\begin{array}{lcl}
V_\diamond & = & \{s_2, s_3\} \\
V_\Box & = & \{s_1\} \\
p & = & \{s_1 \mapsto 1, s_2 \mapsto 2, s_3 \mapsto 3\}
\end{array}
$$

Motivation

- BES can blow up exponentially (see e.g. Mader, section 6.4.2)
- Semantics of BES hard to understand
- Alternative model:
  - additional insights
  - other algorithms
  - graph model more intuitive and easier to understand
  - strong link with BES
- Algorithms still exponential

Winning a parity game

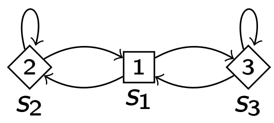
Definition (Winner)

Let:

- $\pi = v_1, v_2, v_3, \ldots$ be a play
- $\inf(\pi)$ be the set of priorities occurring infinitely often in π

Play π is winning for player $\Diamond$ iff $\min(\inf(\pi))$ is even

Winning a parity game (example)



- Play $s_1 s_2^\omega$ won by player $\Diamond$;
- Play $(s_1 s_2 s_1 s_3)^\omega$ won by player $\Box$.

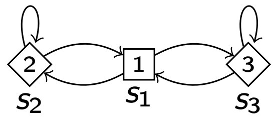
Strategies

Definition (Strategy)

A strategy for $\bigcirc$ is a partial function $\varrho_{\bigcirc} : V^* \times V_{\bigcirc} \to V$ that decides the vertex the token is played to based on the history of visited vertices.

- A play $\pi = v_1, v_2, v_3, \ldots$ is consistent with strategy $\varrho_{\bigcirc}$ for $\bigcirc$ iff every $v_i \in \pi$ such that $v_i \in V_{\bigcirc}$ is immediately followed by $v_{i+1} = \varrho_{\bigcirc}(v_1, \ldots, v_i)$.

Strategy (example)



- Consider strategy $\varrho_\Box$ that, from s_1 plays token to s_2 if s_1 has been visited an even number of times, and to s_3 otherwise.
- What if $\varrho_\Diamond$ always plays token from s_2 to s_2?

Winning

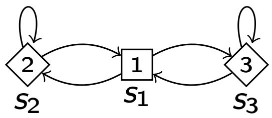
Definition (Winning strategy)

Strategy $\varrho_\bigcirc$ is a winning strategy for $\bigcirc$ from set $W \subseteq V$ if every play starting from a vertex in W, consistent with $\varrho_\bigcirc$ is winning for $\bigcirc$.

Goal of solving parity games: determine unique partitioning $(W_\Diamond, W_\Box)$ of V such that:

- player $\Diamond$ has winning strategy from $W_\Diamond$
- player $\Box$ has winning strategy from $W_\Box$

Winning strategy (example)



- $\varrho_\diamond(\dots, s_2) = s_2$
- $\varrho_\Box(\dots, s_1) = s_3$
- $\varrho_\diamond(\dots, s_3) = \begin{cases} s_1 & \text{if number of occurrences of } s_3 \text{ is prime} \\ s_3 & \text{otherwise} \end{cases}$

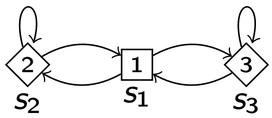
Memoryless strategies

Theorem
For finding winning strategies it suffices to look at memoryless (also history free) strategies.

Memoryless strategy is function $\varrho_\bigcirc : V_\bigcirc \to V$, such that:

- vertex v_i always gets the same successor v_{i+1}
- independent of path by which v_i is reached.

Memoryless strategy (example)



Let $\varrho_\diamond(s_2) = s_2$, $\varrho_\diamond(s_3) = s_1$, and $\varrho_\Box(s_1) = s_3$.

- $\varrho_\diamond$ is winning from $\{s_2\}$
- $\varrho_\Box$ is winning from $\{s_1, s_3\}$

Boolean Equation Systems

A Boolean expression is defined by:

$$f ::= X \mid \text{true} \mid \text{false} \mid f \wedge f \mid f \vee f$$

A Boolean equation is an equation of the form

$$\sigma X = f \quad \text{for } \sigma \in \{\nu, \mu\}$$

A Boolean Equation System (BES) is a sequence of Boolean quations:

$$\mathcal{E} ::= \varepsilon \mid (\sigma X = f)\mathcal{E}$$

BES (example)

$$
\begin{aligned}
\mu X &= X \wedge (Y \vee Z) \\
\nu Y &= W \vee (X \wedge Y) \\
\mu Z &= \text{false} \\
\mu W &= Z \vee (Z \vee W)
\end{aligned}
$$

Notation

Rank:

- natural number
- lowest rank alway 0 or 1
- rank(X) indicates in which block of like-signed equations X occurs
- rank(X) is odd iff X is defined in a μ-equation

Operand:

- $\wedge$, $\vee$ or $\perp$
- op(X) indicates top-level boolean operator of equation for X

Rank/Op (definition)

Let $\mathcal{E}$ be a BES, $X \in \mathsf{bnd}(\mathcal{E})$.

$$
\begin{array}{lcl}
\mathsf{rank}(X) & = & \mathsf{rank}_\nu(X, \mathcal{E}) \\
\mathsf{rank}_\sigma(X, (\sigma X = f)\mathcal{E}) & = & 0 \\
\mathsf{rank}_\sigma(X, (\sigma' X = f)\mathcal{E}) & = & 1 \text{ if } \sigma \neq \sigma' \\
\mathsf{rank}_\sigma(X, (\sigma Y = f)\mathcal{E}) & = & \mathsf{rank}_\sigma(X, \mathcal{E}) \\
\mathsf{rank}_\sigma(X, (\sigma' Y = f)\mathcal{E}) & = & 1 + \mathsf{rank}_{\sigma'}(X, \mathcal{E}) \text{ if } \sigma \neq \sigma'
\end{array}
$$

$$
\begin{array}{lcl}
\mathsf{op}(X) & = & \mathsf{op}(X, \mathcal{E}) \\
\mathsf{op}(X, \mathcal{E}(\sigma X = f)\mathcal{F}) & = & \mathsf{op}(f) \\
\mathsf{op}(f \wedge g) & = & \wedge \\
\mathsf{op}(f \vee g) & = & \vee \\
\mathsf{op}(X) & = & \perp \\
\mathsf{op}(\mathsf{true}) & = & \perp \\
\mathsf{op}(\mathsf{false}) & = & \perp
\end{array}
$$

Rank/Op (example)

rank(_)	op(_)			
(1)	$\wedge$	μX	$=$	$X \wedge (Y \vee Z)$
(2)	$\vee$	νY	$=$	$W \vee (X \wedge Y)$
(3)	$\perp$	μZ	$=$	false
(3)	$\vee$	μW	$=$	$Z \vee (Z \vee W)$

Standard Recursive Form

A BES is in Standard Recursive Form (SRF) if all right hand sides of Boolean Equations adhere to the following syntax:

$$f := X \mid \bigvee F \mid \bigwedge F$$

- X is a proposition variable
- F is a non-empty set of proposition variables

Observe that:

- all BESs can be transformed into an equivalent BES in SRF
- this transformation can be done in polynomial time

Translation to SRF

Let $\mathcal{E}$ be a BES.

$$\begin{array}{lcl} SRF(\varepsilon) & = & \varepsilon \\ SRF((\sigma X = f)\mathcal{E}) & = & SRF(\sigma X = f)SRF(\mathcal{E}) \end{array}$$

Translation of a single equation to SRF:

$$SRF(\sigma X = f) = \sigma X = f \text{ if } \mathsf{op}(f) = \bot$$

$$SRF(\sigma X = f \wedge g)$$

$$= \begin{cases} \sigma X = f \wedge g & \text{if } \vee \notin \mathsf{ops}(f), \mathsf{ops}(g) \\ (\sigma X = X_f \wedge g)SRF(\sigma X_f = f) & \text{if } \vee \in \mathsf{ops}(f), \vee \notin \mathsf{ops}(g) \\ (\sigma X = f \wedge X_g)SRF(\sigma X_g = g) & \text{if } \vee \notin \mathsf{ops}(f), \vee \in \mathsf{ops}(g) \\ (\sigma X = X_f \wedge X_g)SRF(\sigma X_f = f)SRF(\sigma X_g = g) & \text{if } \vee \in \mathsf{ops}(f), \vee \in \mathsf{ops}(g) \end{cases}$$

where $\vee \in \mathsf{ops}(f)$ iff there is a subformula f' of f s.t. $\mathsf{op}(f') = \vee$.
Likewise for $SRF(\sigma X = f \vee g)$

true and false can be removed by replacing all occurrences of true by X_{true}, false by X_{false}, and appending the equations $(\nu X_{\mathsf{true}} = X_{\mathsf{true}})(\mu X_{\mathsf{false}} = X_{\mathsf{false}})$

Transformation to SRF (example)

Consider the following BES:

$$\begin{aligned}\mu X &= X \wedge (Y \vee Z)\\ \nu Y &= W \vee (X \wedge Y)\\ \mu Z &= \text{false}\\ \mu W &= Z \vee (Z \vee W)\end{aligned}$$

This corresponds to the following BES in SRF:

$$\begin{aligned}\mu X &= X \wedge X'\\ \mu X' &= Y \vee Z\\ \nu Y &= W \vee Y'\\ \nu Y' &= X \wedge Y\\ \mu Z &= X_{\text{false}}\\ \mu W &= Z \vee (Z \vee W)\\ \nu X_{\text{true}} &= X_{\text{true}}\\ \mu X_{\text{false}} &= X_{\text{false}}\end{aligned}$$

Parity games vs BES

Definition (Parity game to BES)

Let $(V, E, p, (V_\diamond, V_\Box))$ be a parity game.
The corresponding closed BES in SRF contains the following equations:

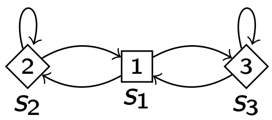
$$\begin{cases}\sigma X_v = \bigwedge\{X_{v'} \mid (v, v') \in E\} & \text{if } v \in V_\Box\\ \sigma X_v = \bigvee\{X_{v'} \mid (v, v') \in E\} & \text{if } v \in V_\diamond\end{cases}$$

where:

- $\sigma = \mu$ if $p(v)$ is odd, $\sigma = \nu$ otherwise
- X_v occurs before X_u in the BES if $p(v) < p(u)$

Theorem

Solution to X_v is true $\Leftrightarrow$ player $\diamond$ has winning strategy from v



Corresponds to the following BES:

$$\begin{aligned}
\mu X_{s_1} &= X_{s_2} \wedge X_{s_3} \\
\nu X_{s_2} &= X_{s_2} \vee X_{s_1} \\
\mu X_{s_3} &= X_{s_1} \vee X_{s_3}
\end{aligned}$$

Let $\mathcal{E}$ be a BES, then

- bnd($\mathcal{E}$): variables occurring at the lhs of an equation in $\mathcal{E}$;
- occ($\mathcal{E}$) variables occurring at the rhs of an equation in $\mathcal{E}$;
- occ(f) are all variables occurring in formula f.

Definition (Dependency graph)

Let $\mathcal{E}$ be a BES. Its dependency graph $\mathcal{G}_{\mathcal{E}}$ is defined as (V, E), where:

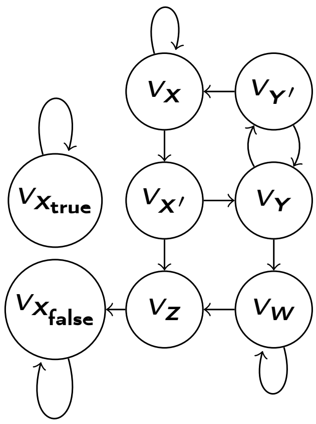
- $V = \{V_X \mid X \in \text{bnd}(\mathcal{E})\}$
- $(V_X, V_Y) \in E$ iff there is $\sigma X = f$ in $\mathcal{E}$ with $Y \in \text{occ(f)}$

Dependency graph (example)

Consider the following BES:

$$
\begin{array}{lcl}
\mu X & = & X \wedge X' \\
\mu X' & = & Y \vee Z \\
\nu Y & = & W \vee Y' \\
\nu Y' & = & X \wedge Y \\
\mu Z & = & X_{\mathsf{false}} \\
\mu W & = & Z \vee (Z \vee W) \\
\nu X_{\mathsf{true}} & = & X_{\mathsf{true}} \\
\mu X_{\mathsf{false}} & = & X_{\mathsf{false}}
\end{array}
$$

Its dependency graph is:



BES vs parity game

Definition (BES to parity game)

Let $\mathcal{E}$ be a closed BES in SRF. This corresponds to the parity game $\Gamma = (V, E, p, (V_\diamond, V_\Box))$, where

- (V, E) is the dependency graph $\mathcal{G}_\mathcal{E}$ of $\mathcal{E}$,
- $p(V_X) = \text{rank}(X)$ for all variables $X \in \text{bnd}(\text{E})$,
- $V_\Box = \{V_X \mid \text{op}(X) = \wedge\}$, so all conjunctive equations are assigned to $V_\Box$, and
- $V_\diamond = V \setminus V_\Box$, all other equations are assigned to $V_\diamond$.

Theorem

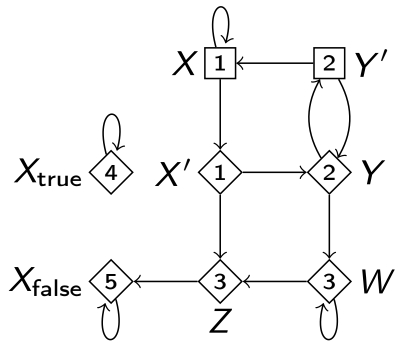
Player $\diamond$ has winning strategy from $V_X \Leftrightarrow$ the solution of X is true

BES vs parity game (example)

Consider the following BES:

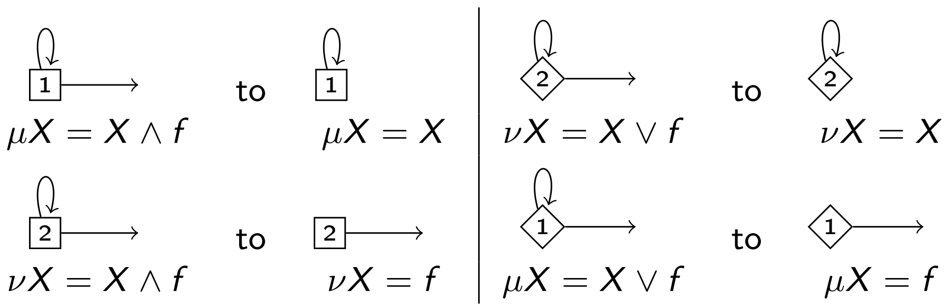
$$
\begin{array}{lcl}
\mu X & = & X \wedge X' \\
\mu X' & = & Y \vee Z \\
\nu Y & = & W \vee Y' \\
\nu Y' & = & X \wedge Y \\
\mu Z & = & X_{\mathsf{false}} \\
\mu W & = & Z \vee (Z \vee W) \\
\nu X_{\mathsf{true}} & = & X_{\mathsf{true}} \\
\mu X_{\mathsf{false}} & = & X_{\mathsf{false}}
\end{array}
$$

Its parity game is:



Transformations on parity games

Self-loop elimination

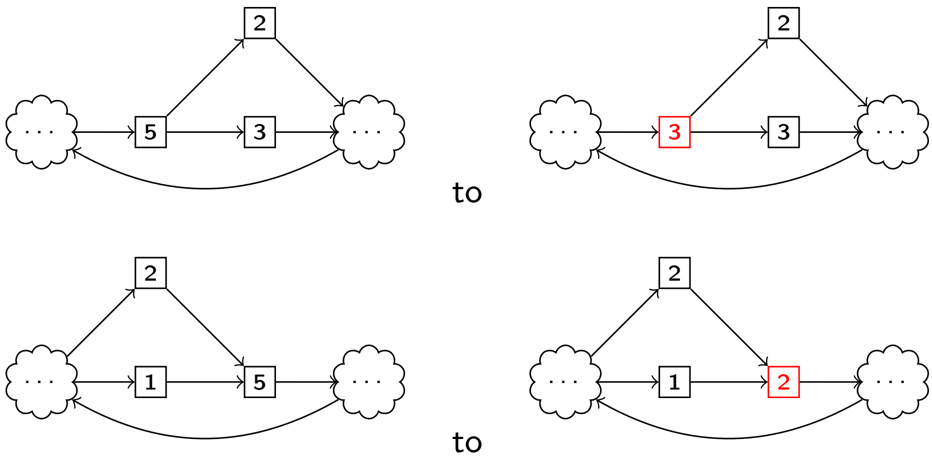


Priority compaction

In case priority 4 does not occur in the parity game. Evenness must be preserved!

Transformations on parity games

Priority propagation



Corresponds to re-ordering of equations in BES, which is generally unsafe!

Bisimulation

Definition (Bisimilarity of vertices)

Let $G = (V, E, \mathrm{p}, (V_\Diamond, V_\Box))$ be a parity game. Let R be a symmetric relation. R is a bisimulation relation if $v \, R \, v'$ implies

- $v \in V_\Diamond \Leftrightarrow v' \in V_\Diamond$
- $\mathrm{p}(v) = \mathrm{p}(v')$
- $v \to w$ implies $\exists w'$ such that $v' \to w'$ and $w \, R \, w'$

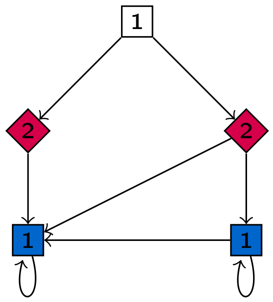
Vertices v and v' are bisimilar ($v \equiv v'$) iff there exists a bisimulation relation R such that $v \, R \, v'$.

Theorem

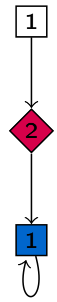
$v \equiv v'$ implies that v and v' are won by the same player

Bisimilarity (example)

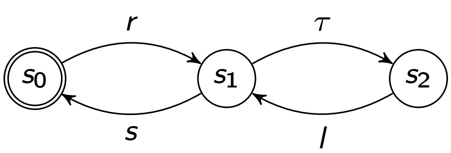
Original



Minimal bisimilar parity game



Exercise



Consider the following modal μ-calculus formula f:

$$\phi \equiv \nu X.\mu Y.(([r]X \wedge [s]X \wedge (\nu Z.\langle \neg s \rangle Z)) \vee ([r]Y \wedge [s]Y))$$

- Translate the model checking question $M \models f$ to a BES.
- Transform the resulting BES into a parity game.
- Determine the winner from vertex $V_{X_{s_0}}$.
- Provide winning strategy for this player from $V_{X_{s_0}}$.

Outlook

Summary:

- Parity games
- Relation to BES
- Simplifications

Next week:

- Recursive algorithm