Algorithms for Model Checking (2IW55)

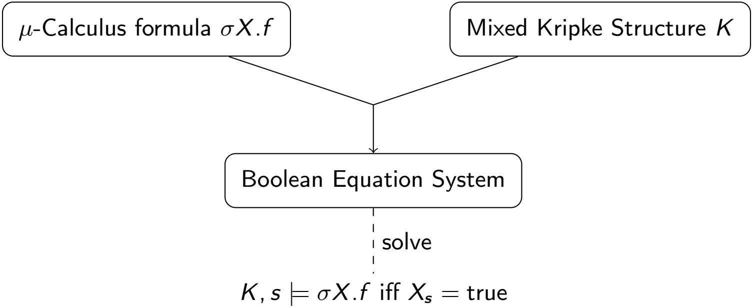
Lecture 6
Parity games

Background material: Chapter 3 of
J.J.A. Keiren, *An experimental study of algorithms and optimisations for parity games, with an application to Boolean Equation Systems*, MSc thesis, 2009

Tim Willemse
(timw@win.tue.nl)
http://www.win.tue.nl/∼timw
MF 7.073

TU/e Technische Universiteit Eindhoven University of Technology

Outline



- Model checking mu-calculus = solving BES
- Solving BESs conceptually simpler than model checking mu-calculus . still exponential
- BESs are more elementary than mu-calculus . . . . still: fixpoints
- Fixpoints can be understood through an infinite game . . . . Parity games

The arena:

- total graph
- two players: ◇ (Even) and □ (Odd)
- each vertex:
  - has a non-negative priority $p(v)$
  - is owned by one player
- objective: win as many vertices as possible

Definition (Parity game)

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

- (V, E) is a directed graph
- V a set of vertices partitioned into $V_\diamond$ and $V_\Box$
  - $V_\diamond$: vertices owned by player $\diamond$
  - $V_\Box$: vertices owned by player $\Box$
- E a total edge relation
- $\mathrm{p} : V \to \mathbb{N}$ a priority function

Rules of the game:

Rules of the game:

1. place a token on some vertex v
2. owner of the vertex v moves token to successor vertex v'
3. Repeat step 2

Rules of the game:

1. place a token on some vertex v
2. owner of the vertex v moves token to successor vertex v'
3. Repeat step 2

Play: infinite sequence of vertices visited by token

Parity games

Rules of the game:

1. place a token on some vertex v
2. owner of the vertex v moves token to successor vertex v'
3. Repeat step 2

Play: infinite sequence of vertices visited by token

Definition (Winner of a play)

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

Play π is winning for player $\Diamond$ iff $\min(\inf(\pi))$ is even. Likewise for player $\Box$/odd.

Definition (Strategy)

A strategy for player $\Diamond$ (similarly for $\Box$) is a partial function $\varrho_\Diamond : V^* \times V_\Diamond \to V$

- $v_1 \dots v_n \in V^*$ . . . . sequence of visited vertices (history)
- $v_n \in V_\Diamond$ . . . . vertex owned by $\Diamond$
- $\varrho_\Diamond(v_1 \dots v_{n-1}, v_n) \in \{v \mid (v_n, v) \in E\}$ . . . . rule for moving token from v_n

Definition (Strategy)

A strategy for player $\Diamond$ (similarly for $\Box$) is a partial function $\varrho_\Diamond : V^* \times V_\Diamond \to V$

- $v_1 \dots v_n \in V^*$ .... sequence of visited vertices (history)
- $v_n \in V_\Diamond$ .... vertex owned by $\Diamond$
- $\varrho_\Diamond(v_1 \dots v_{n-1}, v_n) \in \{v \mid (v_n, v) \in E\}$ .... rule for moving token from v_n

Definition (Consistent plays)

- Let $\pi = v_1 v_2 v_3 \dots$ be an infinite play
- Let $\varrho_\bigcirc$ be a strategy for player $\bigcirc \in \{\Diamond, \Box\}$
- π is consistent with $\varrho_\bigcirc$ iff whenever $\varrho_\bigcirc(v_1 \dots v_{i-1}, v_i)$ is defined, then it is v_{i+1}

$\mathrm{Play}_{\varrho_\bigcirc}(v)$ is the set of all plays starting in v that are consistent with $\varrho_\bigcirc$

Definition (Winning strategy)

- $\bigcirc \in \{\Diamond, \Box\}$
- $\varrho_{\bigcirc}$ is a strategy for $\bigcirc$

$\varrho_{\bigcirc}$ is a winning strategy from v if every play in $\mathsf{Play}_{\varrho_{\bigcirc}}(v)$ is winning for $\bigcirc$.

Technische Universiteit Eindhoven University of Technology

Definition (Winning strategy)

- $\bigcirc \in \{\Diamond, \Box\}$
- $\varrho_{\bigcirc}$ is a strategy for $\bigcirc$

$\varrho_{\bigcirc}$ is a winning strategy from v if every play in $\mathsf{Play}_{\varrho_{\bigcirc}}(v)$ is winning for $\bigcirc$.

Player $\bigcirc$ wins the vertices in W if from all vertices $v \in W$ she has a winning strategy $\varrho_{\bigcirc}$.

Definition (Winning strategy)

- $\bigcirc \in \{\Diamond, \Box\}$
- $\varrho_{\bigcirc}$ is a strategy for $\bigcirc$

$\varrho_{\bigcirc}$ is a winning strategy from v if every play in $\mathsf{Play}_{\varrho_{\bigcirc}}(v)$ is winning for $\bigcirc$.

Player $\bigcirc$ wins the vertices in W if from all vertices $v \in W$ she has a winning strategy $\varrho_{\bigcirc}$.

Natural questions

- Is there always at least one player that can win a vertex?
- Is there a unique winner for each vertex?
- Can the winning strategies be of a particular shape or not?
- Can we compute the winning sets $W_{\Diamond}$ and $W_{\Box}$?

Theorem (Positional determinacy)

Player ○ wins a vertex w iff she has a memoryless strategy that is winning from w

Theorem (Positional determinacy)

Player $\bigcirc$ wins a vertex w iff she has a memoryless strategy that is winning from w

Strategy $\varrho_{\bigcirc}: V^* \times V_{\bigcirc} \to V$ is memoryless (also *history free*) if:

for all histories $\lambda\ v, \lambda'\ v \in V^+$ for which $\varrho_{\bigcirc}$ is defined, we have $\varrho_{\bigcirc}(\lambda, v) = \varrho_{\bigcirc}(\lambda', v)$

Theorem (Positional determinacy)

Player $\bigcirc$ wins a vertex w iff she has a memoryless strategy that is winning from w

Strategy $\varrho_{\bigcirc}{:}V^* \times V_{\bigcirc} \to V$ is memoryless (also *history free*) if:

for all histories $\lambda\ v, \lambda'\ v \in V^+$ for which $\varrho_{\bigcirc}$ is defined, we have $\varrho_{\bigcirc}(\lambda, v) = \varrho_{\bigcirc}(\lambda', v)$

Consequences:

- we can drop the history and consider strategies $\varrho_{\bigcirc}{:}V_{\bigcirc} \to V$
- there are only a finite number of memoryless strategies

Outline

Boolean Equation Systems

Recall Boolean equation systems:

- Boolean expressions: $f, g ::= X \mid \text{true} \mid \text{false} \mid f \wedge g \mid f \vee g$
- Boolean equation system: $\mathcal{E} ::= \varepsilon \mid (\mu X = f)\ \mathcal{E} \mid (\nu X = f)\ \mathcal{E}$

Boolean Equation Systems

Recall Boolean equation systems:

- Boolean expressions: $f, g ::= X \mid \text{true} \mid \text{false} \mid f \wedge g \mid f \vee g$
- Boolean equation system: $\mathcal{E} ::= \varepsilon \mid (\mu X = f)\ \mathcal{E} \mid (\nu X = f)\ \mathcal{E}$

Lemma ("Tseitin" transformation)

For all Y bound in $\mathcal{E}_0, \mathcal{E}_1$ or $Y = X$:

$$[\mathcal{E}_0\ (\sigma X = f \wedge g)\ \mathcal{E}_1]\eta(Y) = [\mathcal{E}_0\ (\sigma X = f \wedge X')\ (\sigma' X' = g)\ \mathcal{E}_1]\eta(Y)$$

Note: likewise for f, likewise for $f \vee g$

Recall Boolean equation systems:

- Boolean expressions: $f, g ::= X \mid \text{true} \mid \text{false} \mid f \wedge g \mid f \vee g$
- Boolean equation system: $\mathcal{E} ::= \varepsilon \mid (\mu X = f)\ \mathcal{E} \mid (\nu X = f)\ \mathcal{E}$

Lemma ("Tseitin" transformation)

For all Y bound in $\mathcal{E}_0, \mathcal{E}_1$ or $Y = X$:

$$[\![\mathcal{E}_0\ (\sigma X = f \wedge g)\ \mathcal{E}_1]\!]\eta(Y) = [\![\mathcal{E}_0\ (\sigma X = f \wedge X')\ (\sigma' X' = g)\ \mathcal{E}_1]\!]\eta(Y)$$

Note: likewise for f, likewise for $f \vee g$

Lemma (Constant elimination)

For all Y bound in $\mathcal{E}$:

$$[\![\mathcal{E}]\!]\eta(Y) = [\![\mathcal{E}[\mathit{true} := X_{\mathit{true}}]\ (\nu X_{\mathit{true}} = X_{\mathit{true}})]\!]\eta(Y)$$

Note: similarly for false (with $\mu X_{\text{false}} = X_{\text{false}}$)

Definition (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

Definition (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 a BES in SRF preserving the solution
- how: repeatedly use "Tseitin" transformation and constant elimination
- the total transformation can be done in polynomial time

TU/e Technische Universiteit Eindhoven University of Technology

Definition (Blocks and ranks)

- a μ-block is a BES of μ-signed equations; likewise: ν-block
- let $\mathcal{E} = \mathcal{B}_1 \cdots \mathcal{B}_n$ for blocks $\mathcal{B}_1, \ldots, \mathcal{B}_n$
- Assume for all i, signs of blocks $\mathcal{B}_i$ and $\mathcal{B}_{i+1}$ differ

$$\text{for all } (\sigma X = f) \in \mathcal{B}_i,\ \text{rank}(X) = \begin{cases} i & \text{if } \mathcal{B}_1 \text{ is } \mu\text{-block} \\ i-1 & \text{otherwise} \end{cases}$$

Technische Universiteit Eindhoven University of Technology

Definition (Blocks and ranks)

- a μ-block is a BES of μ-signed equations; likewise: ν-block
- let $\mathcal{E} = \mathcal{B}_1 \cdots \mathcal{B}_n$ for blocks $\mathcal{B}_1, \ldots, \mathcal{B}_n$
- Assume for all i, signs of blocks $\mathcal{B}_i$ and $\mathcal{B}_{i+1}$ differ

$$\text{for all } (\sigma X = f) \in \mathcal{B}_i,\ \text{rank}(X) = \begin{cases} i & \text{if } \mathcal{B}_1 \text{ is } \mu\text{-block} \\ i-1 & \text{otherwise} \end{cases}$$

Observe:

- $\text{rank}(X) = \text{rank}(Y)$ if both X and Y occur in the same block
- $\text{rank}(X)$ is odd iff X is defined in a μ-equation

Outline

Boolean equation systems and Parity games correspond

Let $G = (V, E, p, (V_\diamond, V_\Box))$ be a parity game

Definition (Parity game to BES)

Define the BES $\mathcal{E}_G$ as follows:

- equations $(\sigma_v X_v = \bigwedge\{X_w \mid (v, w) \in E\})$ for vertices $v \in V_\Box$
- equations $(\sigma_v X_v = \bigvee\{X_w \mid (v, w) \in E\})$ for vertices $v \in V_\diamond$
- $\sigma_v = \mu$ if $p(v)$ is odd, $\sigma_v = \nu$ otherwise
- ensure $\text{rank}(X_v) \leq \text{rank}(X_u)$ if $p(v) < p(u)$

Boolean equation systems and Parity games correspond

Let $G = (V, E, p, (V_\diamond, V_\Box))$ be a parity game

Definition (Parity game to BES)

Define the BES $\mathcal{E}_G$ as follows:

- equations $(\sigma_v X_v = \bigwedge\{X_w \mid (v, w) \in E\})$ for vertices $v \in V_\Box$
- equations $(\sigma_v X_v = \bigvee\{X_w \mid (v, w) \in E\})$ for vertices $v \in V_\diamond$
- $\sigma_v = \mu$ if $p(v)$ is odd, $\sigma_v = \nu$ otherwise
- ensure $\text{rank}(X_v) \leq \text{rank}(X_u)$ if $p(v) < p(u)$

Theorem

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

Let $\mathcal{E}$ be a closed BES in SRF.

Definition (BES to parity game)

Define a parity game $G_{\mathcal{E}} = (V, E, p, (V_\diamond, V_\Box))$ as follows:

- $v_X \in V$ iff there is an equation for X in $\mathcal{E}$
- $(v_X, v_Y) \in E$ iff propositional variable Y occurs in f in $\sigma X = f$
- $p(v_X) = \text{rank}(X)$ for all equations $(\sigma X = f)$ in $\mathcal{E}$
- $v_X \in V_\Box$ iff the equation for X is of the form $(\sigma X = \bigwedge F)$
- $V_\diamond = V \setminus V_\Box$

Boolean equation systems and Parity games correspond

Let $\mathcal{E}$ be a closed BES in SRF.

Definition (BES to parity game)

Define a parity game $G_{\mathcal{E}} = (V, E, p, (V_\Diamond, V_\Box))$ as follows:

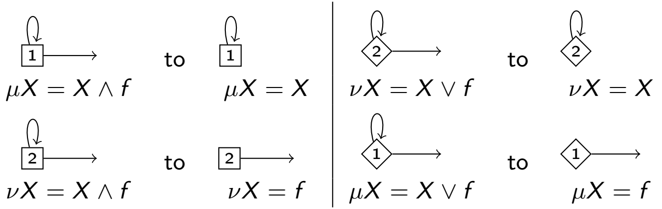
- $v_X \in V$ iff there is an equation for X in $\mathcal{E}$
- $(v_X, v_Y) \in E$ iff propositional variable Y occurs in f in $\sigma X = f$
- $p(v_X) = \text{rank}(X)$ for all equations $(\sigma X = f)$ in $\mathcal{E}$
- $v_X \in V_\Box$ iff the equation for X is of the form $(\sigma X = \bigwedge F)$
- $V_\Diamond = V \setminus V_\Box$

Theorem

Player $\Diamond$ has winning strategy from v_X $\Leftrightarrow$ the solution of X is true

Outline

Self-loop elimination



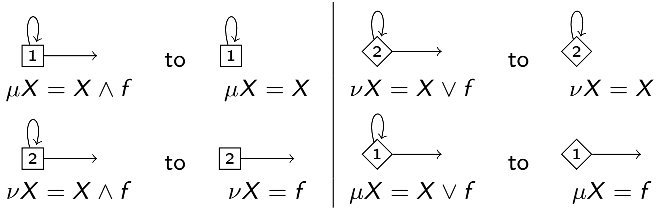
$\mu X = X \wedge f$ to $\mu X = X$

$\nu X = X \vee f$ to $\nu X = X$

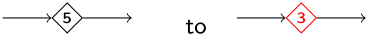
$\nu X = X \wedge f$ to $\nu X = f$

$\mu X = X \vee f$ to $\mu X = f$

Self-loop elimination



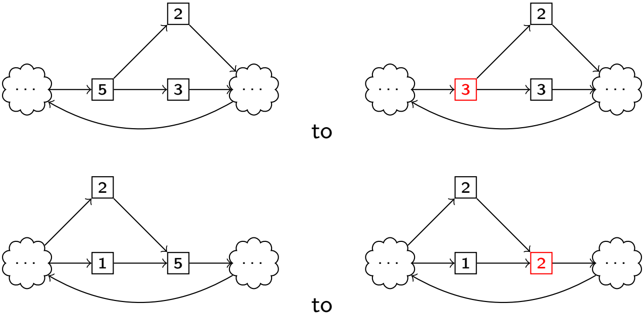
Priority compaction



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

Simplifying parity games

Priority propagation



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

Summary

- Computing winners in parity games $=$ solving BESs
- Reduction parity games $\leftrightarrow$ BESs is polynomial
- Operational interpretation of fixpoints:
  - μ-fixpoint: odd priorities; can only be won by $\diamond$ if it ensures stretches are finite
  - ν-fixpoint: even priorities; benign for player $\diamond$
- Simplifications
- No algorithm yet . . . . but

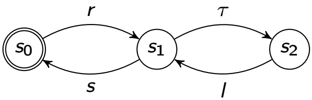
Summary

- Computing winners in parity games = solving BESs
- Reduction parity games $\leftrightarrow$ BESs is polynomial
- Operational interpretation of fixpoints:
  - μ-fixpoint: odd priorities; can only be won by $\Diamond$ if it ensures stretches are finite
  - ν-fixpoint: even priorities; benign for player $\Diamond$
- Simplifications
- No algorithm yet . . . . but

Next week:

- Recursive algorithm

Outline



Consider the following modal μ-calculus formula f:

$$\nu X.([r]X \wedge ((\nu Y.\langle\tau\rangle Y \vee \langle l\rangle Y) \vee (\mu Z.(([l]Z \wedge [s]Z) \vee \langle s\rangle \mathrm{true}))))$$

- Translate the model checking question $M \models f$ to a BES.
- Transform the resulting BES into a parity game.
- Determine whether f holds in s_0 by solving the obtained parity game, and
- provide a winning strategy that justifies this solution.