Algorithms for Model Checking (2IMF35)

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 6.073

Outline

Parity games

μ-Calculus formula $\sigma X.f$

Mixed Kripke Structure K

Boolean Equation System

solve

$K, s \models \sigma X.f$ iff $X_s = \text{true}$

- 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

Parity games

The arena:

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

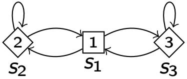
Technische Universiteit Eindhoven University of Technology

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

Parity game (example)



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

Rules of the game:

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

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

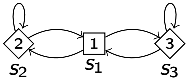
Play: infinite sequence of vertices visited by token

Definition (Winner of a play)

- Let $\pi = v_1 v_2 v_3 \dots$ 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.

Example: winner of a play/winning strategy



Examples of winners of a play:

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

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 $\varrho_\Diamond : V^* \times V_\Diamond \to V$

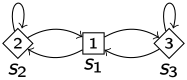
- $v_1 \dots v_n \in V^*$ .... sequence of visited vertices (history)
- $v_n \in V_\Diamond$ .... vertex owned by $\Diamond$
- $\varrho_\Diamond(v_1 \dots v_{n-1}, v_n) \in \{v \mid (v_n, v) \in E\}$ .... rule for moving token from v_n

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}

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

Strategy (example)



- possible strategy $\varrho_\Box$: play token from s_1 to s_2 if s_1 has been visited an even number of times, and to s_3 otherwise
- possible strategy $\varrho_\Diamond$ always plays token from s_2 to s_2

Examples of winning strategies:

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

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 $\bigcirc$.

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 $\varrho_\bigcirc$.

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 $\varrho_{\bigcirc}$.

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

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

Technische Universiteit Eindhoven University of Technology

Theorem (Positional determinacy)

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

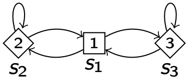
Strategy $\varrho_\bigcirc : V^* \times V_\bigcirc \to V$ is memoryless (also *history free*) if:

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

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 $\{s_1, s_3\}$

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

Technische Universiteit Eindhoven University of Technology

Boolean Equation Systems

Recall Boolean equation systems:

- Boolean expressions: $f, g ::= X \mid \mathsf{true} \mid \mathsf{false} \mid f \wedge g \mid f \vee g$
- 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: $f, g ::= X \mid \mathsf{true} \mid \mathsf{false} \mid f \wedge g \mid f \vee g$
- 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 $\mu X_{\mathsf{false}} = X_{\mathsf{false}}$)

Technische Universiteit Eindhoven University of Technology

BES (example)

Consider the following BES:

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

This corresponds to the following BES in SRF:

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

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

Technische Universiteit Eindhoven University of Technology

Boolean Equation Systems

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

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

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

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

Observe:

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

Rank examples

rank(_)

$$
\begin{array}{llll}
(1) & \mu X & = & X \wedge (Y \vee Z) \\
(2) & \nu Y & = & W \vee (X \wedge Y) \\
(3) & \mu Z & = & \mathsf{false} \\
(3) & \mu W & = & Z \vee (Z \vee W)
\end{array}
$$

rank(_)

$$
\begin{array}{llll}
(1) & \mu X & = & X \wedge X' \\
(1) & \mu X' & = & Y \vee Z \\
(2) & \nu Y & = & W \vee Y' \\
(2) & \nu Y' & = & X \wedge Y \\
(3) & \mu Z & = & X_{\mathsf{false}} \\
(3) & \mu W & = & Z \vee (Z \vee W) \\
(3) & \mu X_{\mathsf{false}} & = & X_{\mathsf{false}}
\end{array}
$$

Outline

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 $\mathrm{rank}(X_v) \leq \mathrm{rank}(X_u)$ if $p(v) < p(u)$

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

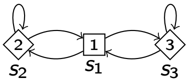
Definition (Parity game to BES)

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 $\mathrm{rank}(X_v) \leq \mathrm{rank}(X_u)$ if $p(v) < p(u)$

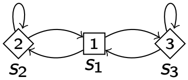
Theorem

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



2
1
3
s_2
s_1
s_3

Parity game to BES example



Corresponds to the following BES:

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

Assume $\mathcal{E}$ is a closed BES in SRF from hereon, unless indicated otherwise.

Lemma

There is a conjunctive BES in SRF $\mathcal{E}'$ constructed from $\mathcal{E}$ by replacing each disjunctive equation $\sigma X_i = \bigvee F_i$ with $\sigma X_i = Y$ for $Y \in F_i$ such that:

$$[\mathcal{E}] = [\mathcal{E}']$$

In the same vein, there is a disjunctive BES in SRF that has the same solution as $\mathcal{E}$.

Parity game to BES intuition

Definition (μ-dominated lasso)

A μ-dominated lasso starting in some X_1 is a finite sequence $X_1 \; X_2 \cdots X_n$, such that:

- We have $X_{i+1} \in F_i$ for $\sigma_i X_i = \bigwedge F_i$ or $\sigma_i X_i = \bigvee F_i$
- We have $X_n \in X_j$ for some $1 \leq j \leq n$.
- $\min\{\text{rank}(X_i) \mid j \leq i \leq n\}$ is odd.

Lemma

Assume $\mathcal{E}$ is conjunctive. Then:

$$[\![\mathcal{E}]\!](X) = \textit{false iff there is a } \mu\textit{-dominated lasso starting in } X$$

Parity game to BES intuition

Theorem

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

Proof.

- $\Leftarrow$
  - Assume player $\diamond$ has a winning strategy ϱ from vertex v.
  - Let $\mathcal{E}$ be the BES obtained from the parity game.
  - Construct $\mathcal{E}'$ from $\mathcal{E}$ by replacing every disjunctive equation as follows:

$$(\sigma X_u = \bigvee F) \text{ becomes } (\sigma X_u = X_{\varrho(u)})$$

  - Towards a contradiction, suppose $[E'](X_v) = \text{false}$
  - Then there must be a μ-dominated lasso starting in X_v
  - But that means that the lowest rank on the lasso is odd
  - Hence, by the transformation, there must be an infinite path in the parity game on which the lowest priority is odd
  - Hence, ϱ is not winning for $\diamond$. Contradiction
- $\Rightarrow$
  - Dually, assume $\square$ has a winning strategy and prove $[\mathcal{E}](X_v) = \text{false}$.

$\square$

Technische Universiteit Eindhoven University of Technology

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 $\sigma X = f$
- $p(v_X) = \mathrm{rank}(X)$ 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 $\sigma X = f$
- $p(v_X) = \mathrm{rank}(X)$ 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

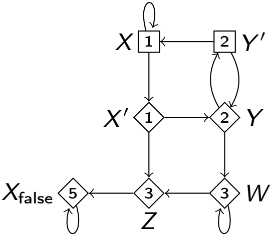
Technische Universiteit Eindhoven University of Technology

BES vs parity game (example)

Consider the following BES:

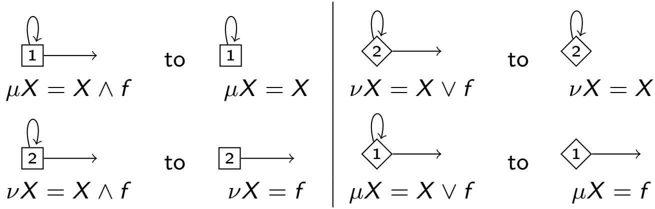
$$
\begin{array}{lcl}
\mu X & = & X \wedge X' \\
\mu X' & = & Y \vee Z \\
\nu Y & = & W \vee Y' \\
\nu Y' & = & X \wedge Y \\
\mu Z & = & X_{\textsf{false}} \\
\mu W & = & Z \vee (Z \vee W) \\
\mu X_{\textsf{false}} & = & X_{\textsf{false}}
\end{array}
$$

Its parity game is:



Outline

Self-loop elimination



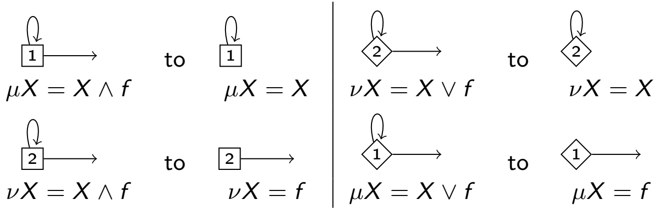
$\mu X = X \wedge f$ to $\mu X = X$

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

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

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

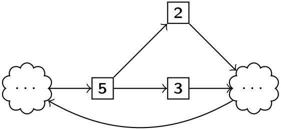
Self-loop elimination



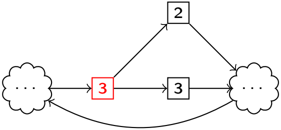
Priority compaction

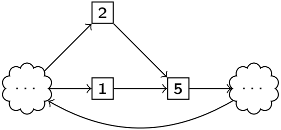
In case priority 4 does not occur in the parity game. Evenness must be preserved!

Priority propagation

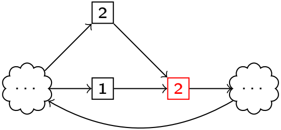


to





to



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

Outline

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

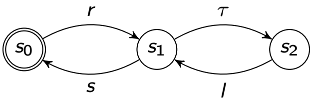
- Computing winners in parity games = solving BESs
- Reduction parity games $\leftrightarrow$ BESs is polynomial
- Operational interpretation of fixpoints:
  - μ-fixpoint: odd priorities; can only be won by $\Diamond$ if it ensures stretches are finite
  - ν-fixpoint: even priorities; benign for player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

Next week:

- Recursive algorithm

Outline

Exercise



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.