Reactive Synthesis

Lecture 7

Swen Jacobs and Martin Zimmermann
(Saarland University)

Plan for Today

Have fun!

Have fun!

My kind of fun:

- Infinite games in infinite arenas
- An undetermined game

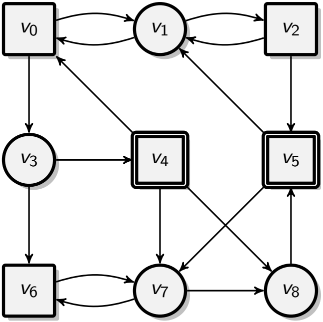
Recap: Attractors

- The *controlled predecessor* $\mathrm{CPre}_0(R)$ of R is defined as

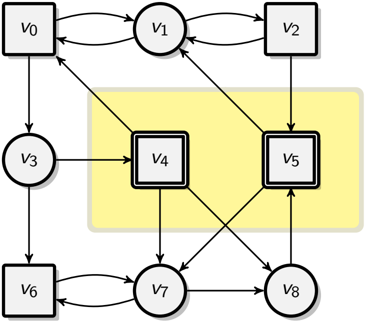
$$\mathrm{CPre}_0(R) = \{v \in V_0 \mid v' \in R \text{ for some successor } v' \text{ of } v\} \cup \{v \in V_1 \mid v' \in R \text{ for all successors } v' \text{ of } v\}.$$

- The *(Player 0) attractor* $\mathrm{Attr}_0(R)$ of R is defined as
  - $\mathrm{Attr}_0^0(R) = R$,
  - $\mathrm{Attr}_0^{n+1}(R) = \mathrm{Attr}_0^n(R) \cup \mathrm{CPre}_0(\mathrm{Attr}_0^n(R))$, and
  - $\mathrm{Attr}_0(R) = \bigcup_{n \in \mathbb{N}} \mathrm{Attr}_0^n(R)$.

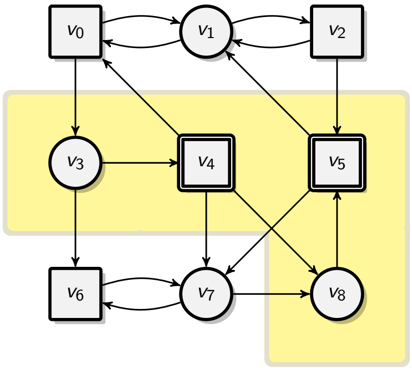
Recap: Attractors



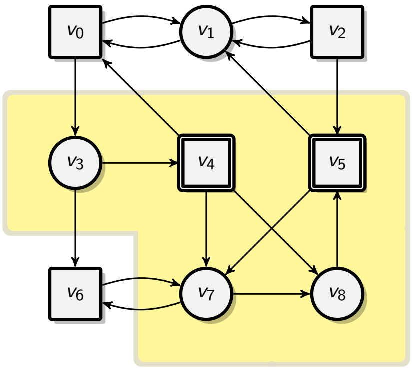
Recap: Attractors



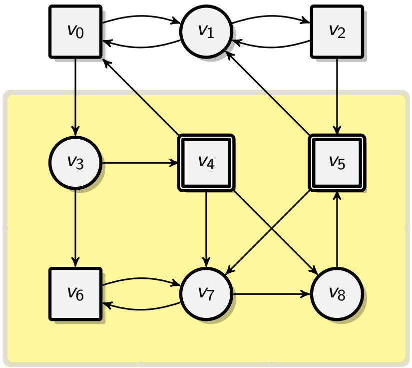
Recap: Attractors



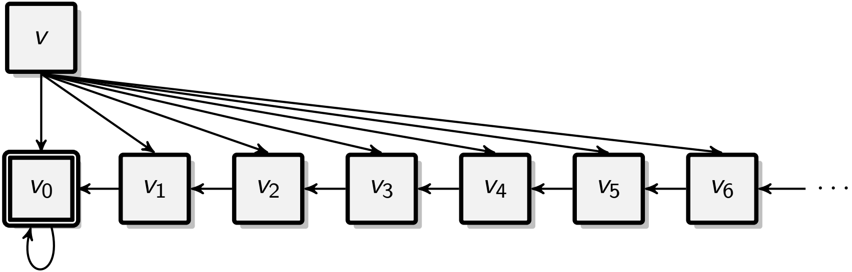
Recap: Attractors



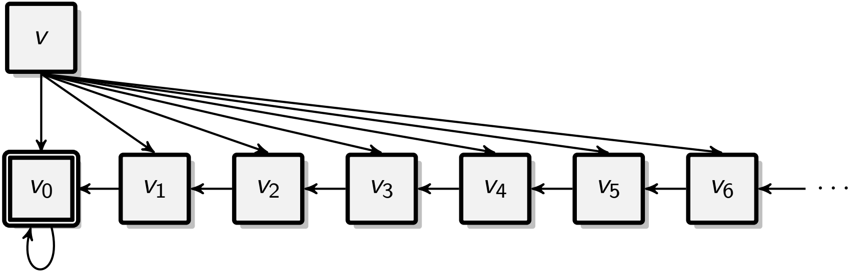
Recap: Attractors



A Problem

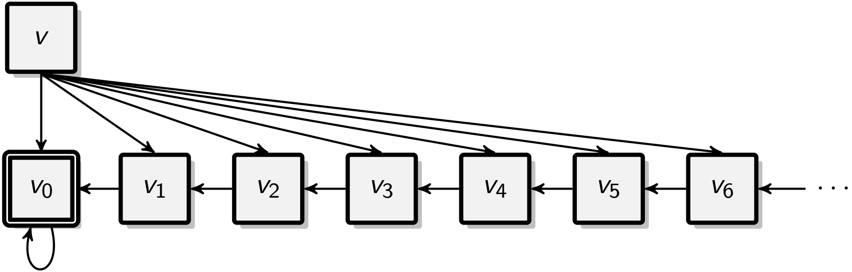


A Problem



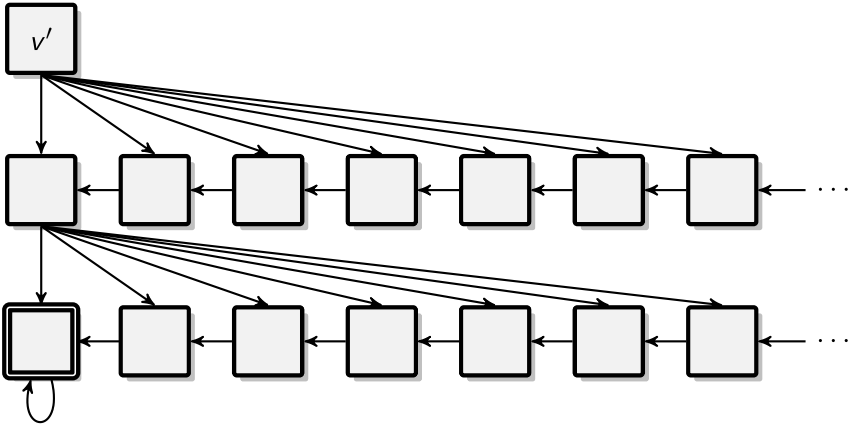
- We have $\mathrm{Attr}_0^n(\{v_0\}) = \{v_j \mid j \leq n\}$ for every $n \in \mathbb{N}$.
- Hence, $v \notin \mathrm{Attr}_0(\{v_0\}) = \bigcup_{n \in \mathbb{N}} \mathrm{Attr}_0^n(\{v_0\}) = \{v_j \mid j \in \mathbb{N}\}$.
- But, v is in Player 0's winning region.

A Problem

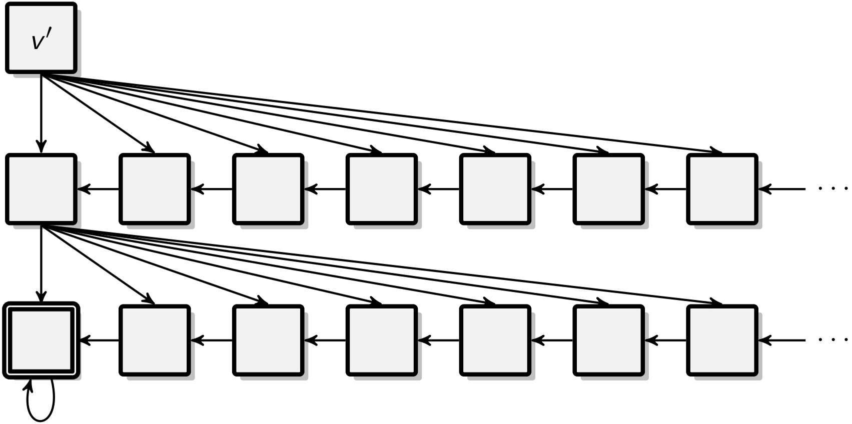


- We have $\mathrm{Attr}_0^n(\{v_0\}) = \{v_j \mid j \leq n\}$ for every $n \in \mathbb{N}$.
- Hence, $v \notin \mathrm{Attr}_0(\{v_0\}) = \bigcup_{n\in\mathbb{N}} \mathrm{Attr}_0^n(\{v_0\}) = \{v_j \mid j \in \mathbb{N}\}$.
- But, v is in Player 0's winning region.
- Solution: apply CPre_0 to $\bigcup_{n\in\mathbb{N}} \mathrm{Attr}_0^n(\{v_0\})$.

Pushing It Further

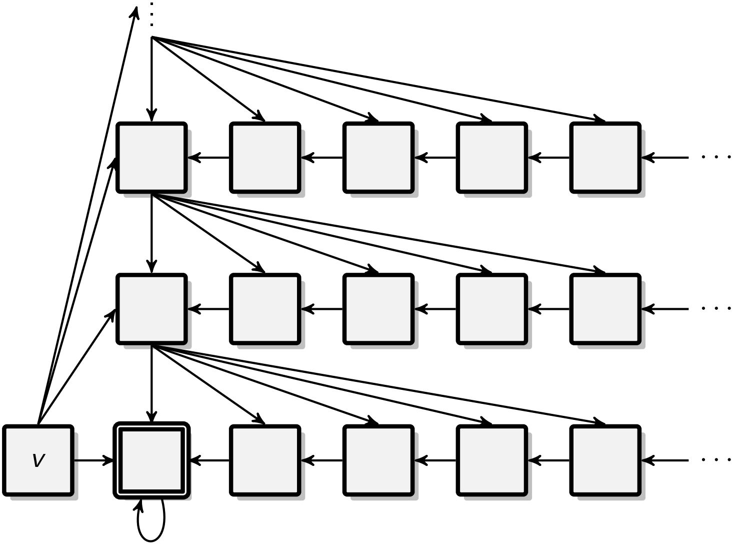


Pushing It Further



- Applying CPre_0 to $\bigcup_{n\in\mathbb{N}} \mathrm{Attr}_0^n(\{v_0\})$ repeatedly adds all vertices in the second row (one in each stage).. but not v'.
- Thus, again take the union over all smaller stages and then apply CPre_0 to add v'.

And Even Further



The Solution

There is a tool to implement this process: Ordinal Numbers

The Solution

There is a tool to implement this process: Ordinal Numbers

Warm-up: Natural numbers a la von Neumann.

Define $0 = \emptyset$ and $n + 1 = n \cup \{n\}$,

The Solution

There is a tool to implement this process: Ordinal Numbers

Warm-up: Natural numbers a la von Neumann.

Define $0 = \emptyset$ and $n + 1 = n \cup \{n\}$, i.e.,

- $0 = \emptyset$,

The Solution

There is a tool to implement this process: Ordinal Numbers

Warm-up: Natural numbers a la von Neumann.

Define $0 = \emptyset$ and $n + 1 = n \cup \{n\}$, i.e.,

- $0 = \emptyset$,
- $1 = 0 \cup \{0\} = \{\emptyset\}$,

The Solution

There is a tool to implement this process: Ordinal Numbers

Warm-up: Natural numbers a la von Neumann.

Define $0 = \emptyset$ and $n + 1 = n \cup \{n\}$, i.e.,

- $0 = \emptyset$,
- $1 = 0 \cup \{0\} = \{\emptyset\}$,
- $2 = 1 \cup \{1\} = \{\emptyset, \{\emptyset\}\}$,

The Solution

There is a tool to implement this process: Ordinal Numbers

Warm-up: Natural numbers a la von Neumann.

Define $0 = \emptyset$ and $n + 1 = n \cup \{n\}$, i.e.,

- $0 = \emptyset$,
- $1 = 0 \cup \{0\} = \{\emptyset\}$,
- $2 = 1 \cup \{1\} = \{\emptyset, \{\emptyset\}\}$,
- $3 = 2 \cup \{2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$,

The Solution

There is a tool to implement this process: Ordinal Numbers

Warm-up: Natural numbers a la von Neumann.

Define $0 = \emptyset$ and $n + 1 = n \cup \{n\}$, i.e.,

- $0 = \emptyset$,
- $1 = 0 \cup \{0\} = \{\emptyset\}$,
- $2 = 1 \cup \{1\} = \{\emptyset, \{\emptyset\}\}$,
- $3 = 2 \cup \{2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$,
- $4 = 3 \cup \{3\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}$,

The Solution

There is a tool to implement this process: Ordinal Numbers

Warm-up: Natural numbers a la von Neumann.

Define $0 = \emptyset$ and $n + 1 = n \cup \{n\}$, i.e.,

- $0 = \emptyset$,
- $1 = 0 \cup \{0\} = \{\emptyset\}$,
- $2 = 1 \cup \{1\} = \{\emptyset, \{\emptyset\}\}$,
- $3 = 2 \cup \{2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$,
- $4 = 3 \cup \{3\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}$,

Note

1. $n + 1 = \{0, 1, \ldots, n\}$, i.e., set membership $\in$ coincides with the natural order $\leq$ (which is a well-order).
2. Every element of n is also a subset of n.

Well-orders

Definition

Let $\leq$ be a total order on some set S.

Well-orders

Definition

Let $\leq$ be a total order on some set S.

1. Let $S' \subseteq S$. An element $\ell \in S$ is a least element of S', if $\ell \in S'$ and $\ell \leq s$ for every $s \in S'$.

Well-orders

Definition

Let $\leq$ be a total order on some set S.

1. Let $S' \subseteq S$. An element $\ell \in S$ is a least element of S', if $\ell \in S'$ and $\ell \leq s$ for every $s \in S'$.
2. $\leq$ is a *well-order*, if every subset of S has a least element.

Well-orders

Definition

Let $\leq$ be a total order on some set S.

1. Let $S' \subseteq S$. An element $\ell \in S$ is a least element of S', if $\ell \in S'$ and $\ell \leq s$ for every $s \in S'$.
2. $\leq$ is a *well-order*, if every subset of S has a least element.

Examples

- $\leq$ on $\mathbb{N}$ is a well-order.

Well-orders

Definition

Let $\leq$ be a total order on some set S.

1. Let $S' \subseteq S$. An element $\ell \in S$ is a least element of S', if $\ell \in S'$ and $\ell \leq s$ for every $s \in S'$.
2. $\leq$ is a *well-order*, if every subset of S has a least element.

Examples

- $\leq$ on $\mathbb{N}$ is a well-order.
- $0 \preceq 2 \preceq 4 \preceq \cdots 1 \preceq 3 \preceq 5 \preceq \cdots$ is another well-order on $\mathbb{N}$.

Well-orders

Definition

Let $\leq$ be a total order on some set S.

1. Let $S' \subseteq S$. An element $\ell \in S$ is a least element of S', if $\ell \in S'$ and $\ell \leq s$ for every $s \in S'$.
2. $\leq$ is a *well-order*, if every subset of S has a least element.

Examples

- $\leq$ on $\mathbb{N}$ is a well-order.
- $0 \preceq 2 \preceq 4 \preceq \cdots 1 \preceq 3 \preceq 5 \preceq \cdots$ is another well-order on $\mathbb{N}$.
- $\leq$ on $\mathbb{Z}$ is not a well-order, as the negative integers have no least element.

Well-orders

Definition

Let $\leq$ be a total order on some set S.

1. Let $S' \subseteq S$. An element $\ell \in S$ is a least element of S', if $\ell \in S'$ and $\ell \leq s$ for every $s \in S'$.
2. $\leq$ is a *well-order*, if every subset of S has a least element.

Examples

- $\leq$ on $\mathbb{N}$ is a well-order.
- $0 \preceq 2 \preceq 4 \preceq \cdots 1 \preceq 3 \preceq 5 \preceq \cdots$ is another well-order on $\mathbb{N}$.
- $\leq$ on $\mathbb{Z}$ is not a well-order, as the negative integers have no least element.
- $0 \preceq 1 \preceq 2 \preceq \cdots - 1 \preceq -2 \preceq \cdots$ is a well-order on $\mathbb{Z}$.

Well-orders

Definition

Let $\leq$ be a total order on some set S.

1. Let $S' \subseteq S$. An element $\ell \in S$ is a least element of S', if $\ell \in S'$ and $\ell \leq s$ for every $s \in S'$.
2. $\leq$ is a *well-order*, if every subset of S has a least element.

Examples

- $\leq$ on $\mathbb{N}$ is a well-order.
- $0 \preceq 2 \preceq 4 \preceq \cdots 1 \preceq 3 \preceq 5 \preceq \cdots$ is another well-order on $\mathbb{N}$.
- $\leq$ on $\mathbb{Z}$ is not a well-order, as the negative integers have no least element.
- $0 \preceq 1 \preceq 2 \preceq \cdots - 1 \preceq -2 \preceq \cdots$ is a well-order on $\mathbb{Z}$.
- $\mathbb{Q}$ can be well-ordered, e.g., using a bijection to $\mathbb{N}$.

Well-orders

Definition

Let $\leq$ be a total order on some set S.

1. Let $S' \subseteq S$. An element $\ell \in S$ is a least element of S', if $\ell \in S'$ and $\ell \leq s$ for every $s \in S'$.
2. $\leq$ is a *well-order*, if every subset of S has a least element.

Examples

- $\leq$ on $\mathbb{N}$ is a well-order.
- $0 \preceq 2 \preceq 4 \preceq \cdots 1 \preceq 3 \preceq 5 \preceq \cdots$ is another well-order on $\mathbb{N}$.
- $\leq$ on $\mathbb{Z}$ is not a well-order, as the negative integers have no least element.
- $0 \preceq 1 \preceq 2 \preceq \cdots - 1 \preceq -2 \preceq \cdots$ is a well-order on $\mathbb{Z}$.
- $\mathbb{Q}$ can be well-ordered, e.g., using a bijection to $\mathbb{N}$.
- What about well-ordering $\mathbb{R}$?

von Neumann Ordinals

Definition

A set S is an ordinal if, and only if, it is well-ordered by $\in$ and if every element of S is also a subset of S.

von Neumann Ordinals

Definition

A set S is an ordinal if, and only if, it is well-ordered by $\in$ and if every element of S is also a subset of S.

Examples

Recall: $0 = \emptyset$ and $n + 1 = n \cup \{n\}$.

von Neumann Ordinals

Definition

A set S is an ordinal if, and only if, it is well-ordered by $\in$ and if every element of S is also a subset of S.

Examples

Recall: $0 = \emptyset$ and $n + 1 = n \cup \{n\}$.

- Every n is an ordinal.

von Neumann Ordinals

Definition

A set S is an ordinal if, and only if, it is well-ordered by $\in$ and if every element of S is also a subset of S.

Examples

Recall: $0 = \emptyset$ and $n + 1 = n \cup \{n\}$.

- Every n is an ordinal.
- $\omega = \{0, 1, 2, \ldots\}$ is an ordinal.

von Neumann Ordinals

Definition

A set S is an ordinal if, and only if, it is well-ordered by $\in$ and if every element of S is also a subset of S.

Examples

Recall: $0 = \emptyset$ and $n + 1 = n \cup \{n\}$.

- Every n is an ordinal.
- $\omega = \{0, 1, 2, \ldots\}$ is an ordinal.
- $\omega + 1 = \omega \cup \{\omega\} = \{0, 1, 2, \ldots, \omega\}$ is an ordinal.

von Neumann Ordinals

Definition

A set S is an ordinal if, and only if, it is well-ordered by $\in$ and if every element of S is also a subset of S.

Examples

Recall: $0 = \emptyset$ and $n + 1 = n \cup \{n\}$.

- Every n is an ordinal.
- $\omega = \{0, 1, 2, \ldots\}$ is an ordinal.
- $\omega + 1 = \omega \cup \{\omega\} = \{0, 1, 2, \ldots, \omega\}$ is an ordinal.
- $\omega + 2 = \omega + 1 \cup \{\omega + 1\} = \{0, 1, 2, \ldots, \omega, \omega + 1\}$.

von Neumann Ordinals

Definition

A set S is an ordinal if, and only if, it is well-ordered by $\in$ and if every element of S is also a subset of S.

Examples

Recall: $0 = \emptyset$ and $n + 1 = n \cup \{n\}$.

- Every n is an ordinal.
- $\omega = \{0, 1, 2, \ldots\}$ is an ordinal.
- $\omega + 1 = \omega \cup \{\omega\} = \{0, 1, 2, \ldots, \omega\}$ is an ordinal.
- $\omega + 2 = \omega + 1 \cup \{\omega + 1\} = \{0, 1, 2, \ldots, \omega, \omega + 1\}$.
- $\omega + \omega = \{0, 1, 2, \ldots, \omega, \omega + 1, \omega + 2, \ldots\}$ is an ordinal, typically denoted as $\omega \cdot 2$.

Back to Attractors

There are three types of ordinals:

1. $0 = \emptyset$.
2. Successor ordinals of the form $\alpha \cup \{\alpha\}$, denoted as $\alpha + 1$.
3. Limit ordinals, i.e., those that are not zero and not successor ordinals, e.g., ω and $\omega \cdot 2$.

Back to Attractors

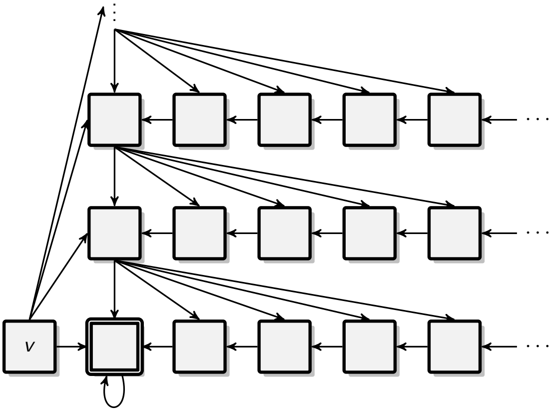
There are three types of ordinals:

1. $0 = \emptyset$.
2. Successor ordinals of the form $\alpha \cup \{\alpha\}$, denoted as $\alpha + 1$.
3. Limit ordinals, i.e., those that are not zero and not successor ordinals, e.g., ω and $\omega \cdot 2$.

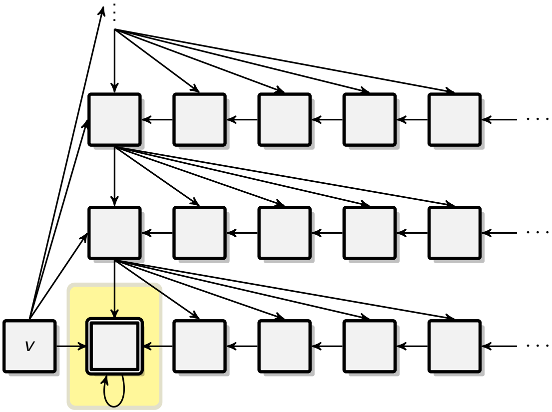
Given a (possibly infinite) arena $\mathcal{A} = (V, V_0, V_1, E)$ and $R \subseteq V$ define

- $\mathrm{Attr}_0^0(R) = R$,
- $\mathrm{Attr}_0^{\alpha+1}(R) = \mathrm{Attr}_0^{\alpha}(R) \cup \mathrm{CPre}_0(\mathrm{Attr}_0^{\alpha}(R))$ for a successor ordinal $\alpha + 1$, and
- $\mathrm{Attr}_0^{\alpha}(R) = \bigcup_{\alpha' < \alpha} \mathrm{Attr}_0^{\alpha'}(R)$ for a limit ordinal α.

Back to the Example

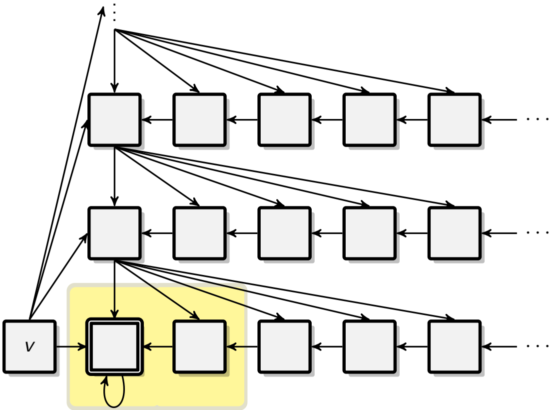


Back to the Example



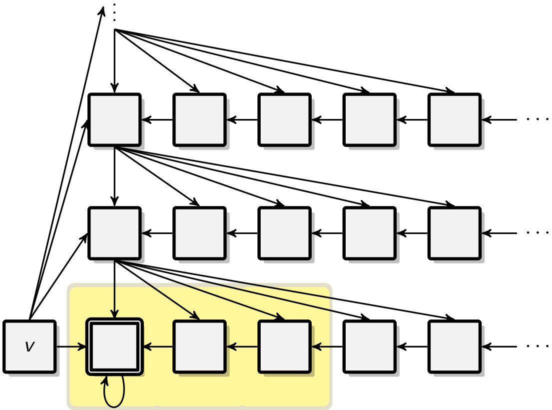
$$\mathrm{Attr}_0^0(\{v_0\})$$

Back to the Example



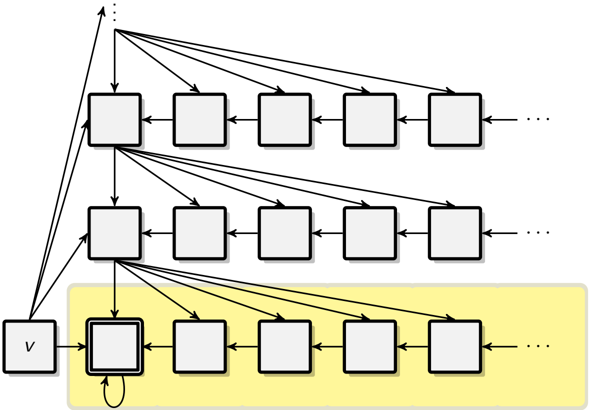
$$\mathrm{Attr}_0^1(\{v_0\})$$

Back to the Example



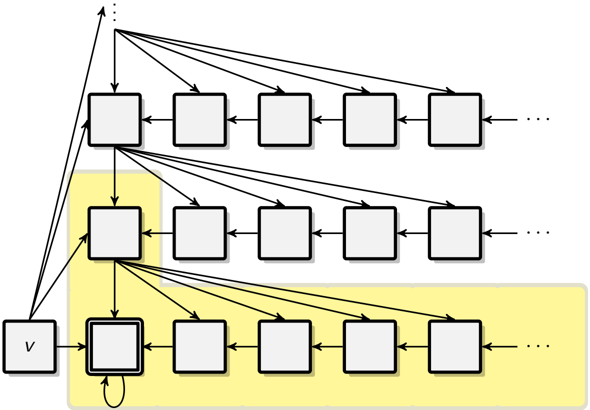
$$\mathrm{Attr}_0^2(\{v_0\})$$

Back to the Example



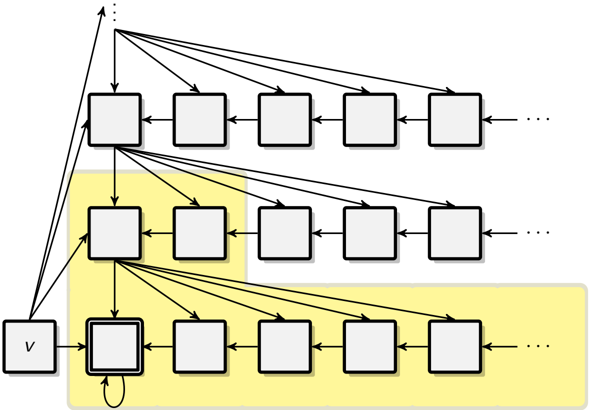
$$\mathrm{Attr}_0^{\omega}(\{v_0\})$$

Back to the Example



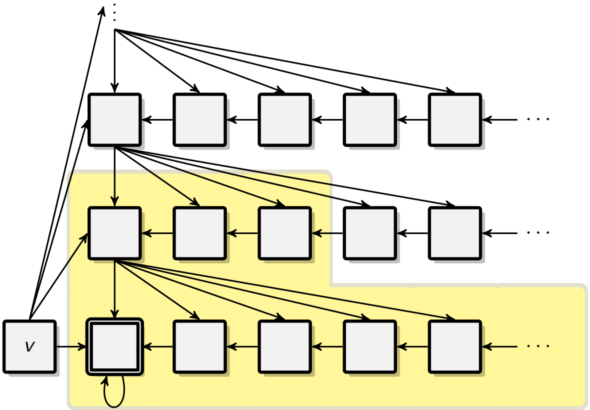
$$\mathrm{Attr}_0^{\omega+1}(\{v_0\})$$

Back to the Example



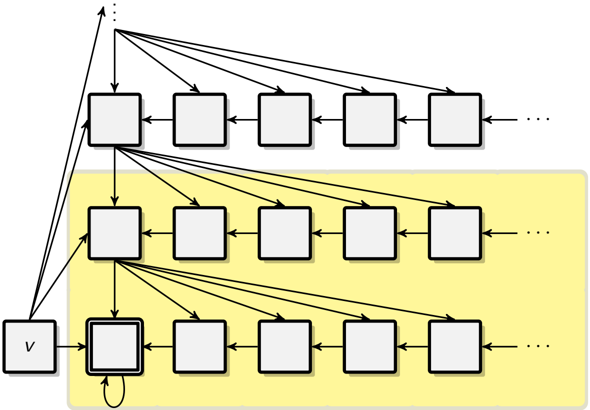
$$\mathrm{Attr}_0^{\omega+2}(\{v_0\})$$

Back to the Example

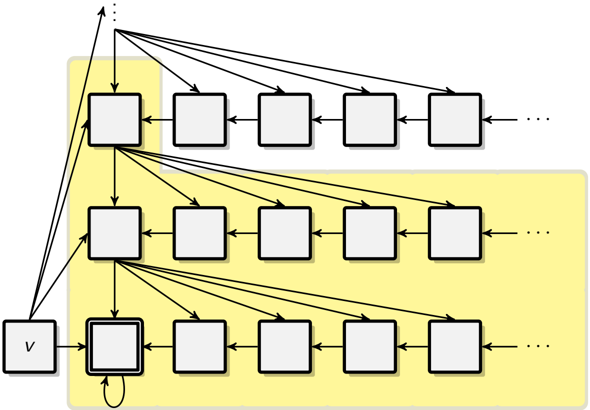


$$\mathrm{Attr}_0^{\omega+3}(\{v_0\})$$

Back to the Example

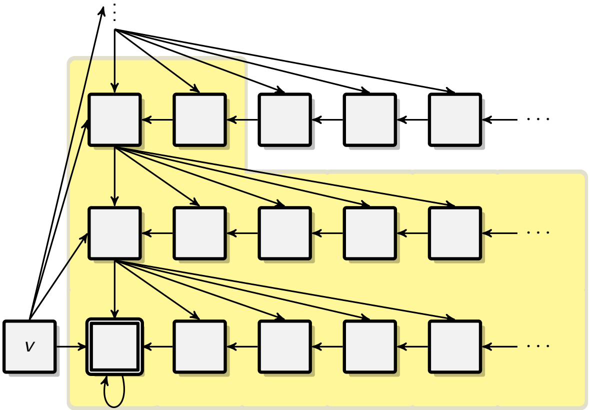


$$\mathrm{Attr}_0^{\omega\cdot 2}(\{v_0\})$$



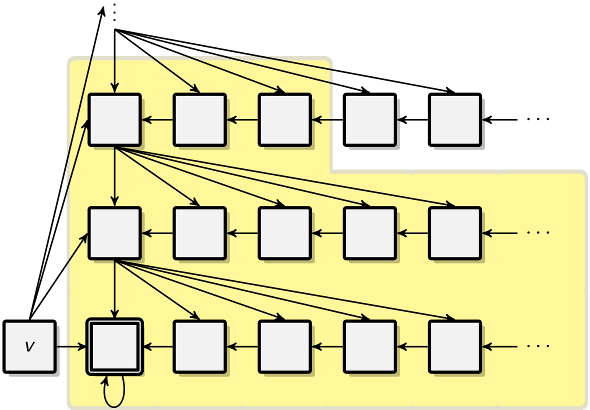
$$\mathrm{Attr}_0^{\omega\cdot 2+1}(\{v_0\})$$

Back to the Example



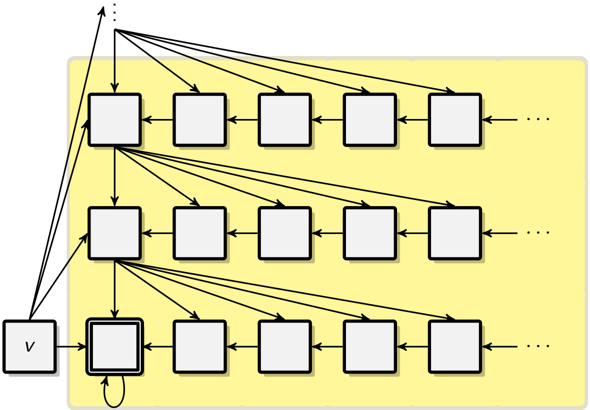
$$\mathrm{Attr}_0^{\omega\cdot 2+2}(\{v_0\})$$

Back to the Example



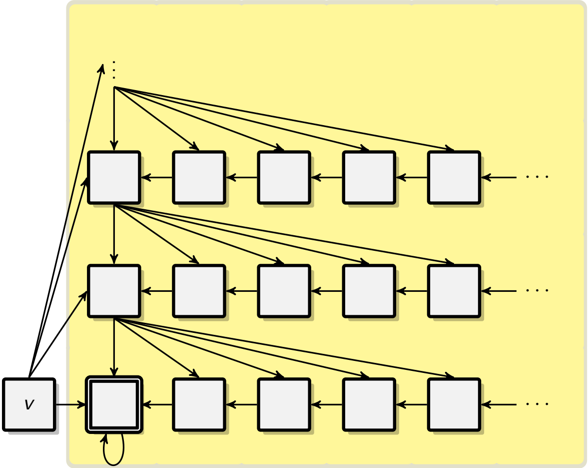
$$\mathrm{Attr}_0^{\omega\cdot 2+3}(\{v_0\})$$

Back to the Example



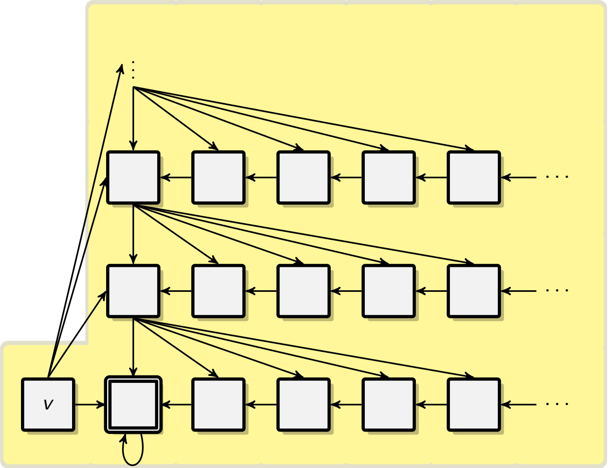
$$\mathrm{Attr}_0^{\omega\cdot 3}(\{v_0\})$$

Back to the Example



$$\mathrm{Attr}_0^{\omega^2}(\{v_0\})$$

Back to the Example



$$\mathrm{Attr}_0^{\omega^2+1}(\{v_0\})$$

Theorem

For every (possibly infinite) reachability game $\mathcal{G} = (\mathcal{A}, \textsc{Reach}(R))$*, there is an ordinal* α *such that*

$$\mathrm{Attr}_0^{\alpha}(R) = W_0(\mathcal{G}).$$

Have fun!

My kind of fun:

- Infinite games in infinite arenas
- An undetermined game

Chomp

- There is a (rectangular) chocolate bar with $m \times n$ pieces.
- A move consists of taking a piece and all others that are to the right and above.
- The players move in alternation, starting with Player 0.
- The player who takes the bottom-left piece loses.
- This description can be formalized as a reachability game.

Let's Play

Let's Play


Milka
PLAYER 0'S TURN

Let’s Play


PLAYER 0'S TURN

Let's Play

Let's Play

Let's Play

Let's Play

Strategy Stealing

Claim

Player 0 has a winning strategy for every bar (unless $m = n = 1$).

Strategy Stealing

Claim

Player 0 has a winning strategy for every bar (unless $m = n = 1$).

- Assume Player 1 has a winning strategy.
- Look how this strategy reacts to Player 0 only taking the top-right piece in the first move.
- Let Player 0 use this strategy from the beginning.
- This is winning for Player 0, which is a contradiction.
- As Chomp is determined, this means Player 0 must have a winning strategy.

Strategy Stealing

Claim

Player 0 has a winning strategy for every bar (unless $m = n = 1$).

- Assume Player 1 has a winning strategy.
- Look how this strategy reacts to Player 0 only taking the top-right piece in the first move.
- Let Player 0 use this strategy from the beginning.
- This is winning for Player 0, which is a contradiction.
- As Chomp is determined, this means Player 0 must have a winning strategy.

Note

- The proof is non-constructive..
- .. winning strategy only known for special cases $n \times n$, $2 \times n$, and $n \times 2$ (try to find them).

Hamming Distance

In the following: $\mathbb{B} = \{0, 1\}$

Definition

For $x = x_0 x_1 x_2 \cdots$ and $y = y_0 y_1 y_2 \cdots$ in $\mathbb{B}^\omega$, the *Hamming distance* between x and y is defined as

$$\mathrm{hd}(x, y) = |\{n \in \mathbb{N} \mid x_n \neq y_n\}| \in \mathbb{N} \cup \{\infty\}.$$

Example

- $\mathrm{hd}(0101101000 \cdots,$
  $1010100000 \cdots) = 5$
- $\mathrm{hd}(1010101010 \cdots,$
  $0101010101 \cdots) = \infty$
- $\mathrm{hd}(1010101010 \cdots,$
  $1111111111 \cdots) = \infty.$

Definition

A function $f\colon \mathbb{B}^\omega \to \mathbb{B}$ is an *infinite XOR function*, if $hd(x, y) = 1$ implies $f(x) \neq f(y)$ for all $x, y \in \mathbb{B}^\omega$.

Infinite XOR Functions

Definition

A function $f\colon \mathbb{B}^\omega \to \mathbb{B}$ is an *infinite XOR function*, if $hd(x, y) = 1$ implies $f(x) \neq f(y)$ for all $x, y \in \mathbb{B}^\omega$.

Example

Infinite XOR Functions

Definition

A function $f : \mathbb{B}^\omega \to \mathbb{B}$ is an *infinite XOR function*, if $hd(x, y) = 1$ implies $f(x) \neq f(y)$ for all $x, y \in \mathbb{B}^\omega$.

Example

I have none.. we will come back to this later.

Infinite XOR Functions

Definition

A function $f\colon \mathbb{B}^\omega \to \mathbb{B}$ is an *infinite XOR function*, if $hd(x, y) = 1$ implies $f(x) \neq f(y)$ for all $x, y \in \mathbb{B}^\omega$.

Example

I have none.. we will come back to this later.

Theorem

There exists an infinite XOR function.

Proof

Define $x \sim y$ if $\mathrm{hd}(x, y) < \infty$.

Remark

$x \sim y \Leftrightarrow$ there are $n \in \mathbb{N}$ and $z \in \mathbb{B}^\omega$ with

$$x = x_0 \cdots x_n z \qquad \textit{and} \qquad y = y_0 \cdots y_n z.$$

Proof

Define $x \sim y$ if $\mathrm{hd}(x, y) < \infty$.

Remark

$x \sim y \Leftrightarrow$ there are $n \in \mathbb{N}$ and $z \in \mathbb{B}^\omega$ with

$$x = x_0 \cdots x_n z \qquad \text{and} \qquad y = y_0 \cdots y_n z.$$

Lemma

$\sim$ is an equivalence relation.

Proof.

1. Reflexitivity: trivial, as $\mathrm{hd}(x, x) = 0 < \infty$.
2. Symmetry: trivial, as $\mathrm{hd}(x, y) = \mathrm{hd}(y, x)$.
3. Transitivity: apply the previous remark. □

Proof

- Let $S \subseteq \mathbb{B}^\omega$ be a set that contains exactly one element from each $\sim$-equivalence class.
- Hence, for every $x \in \mathbb{B}^\omega$, let $r(x)$ denote the unique element in S with $x \sim r(x)$.
- Define $f(x) = \mathrm{hd}(x, r(x))$ mod 2.
- This is well-defined, since $\mathrm{hd}(x, r(x)) \in \mathbb{N}$ for all $x \in \mathbb{B}^\omega$.

Proof

- Let $S \subseteq \mathbb{B}^\omega$ be a set that contains exactly one element from each $\sim$-equivalence class.
- Hence, for every $x \in \mathbb{B}^\omega$, let $r(x)$ denote the unique element in S with $x \sim r(x)$.
- Define $f(x) = \mathrm{hd}(x, r(x))$ mod 2.
- This is well-defined, since $\mathrm{hd}(x, r(x)) \in \mathbb{N}$ for all $x \in \mathbb{B}^\omega$.

Claim: f is an infinite XOR function.

Proof

Fix $x = x_0 x_1 x_2 \cdots$ and $y = y_0 y_1 y_2 \cdots$ with $\mathrm{hd}(x, y) = 1$.

- W.l.o.g., $x = w0z$ and $y = w1z$ for some $w \in \mathbb{B}^*$ and $z \in \mathbb{B}^\omega$.
- We have $x \sim y$ and thus $r(x) = r(y) =: r = r_0 r_1 r_2 \cdots$.

Proof

Fix $x = x_0 x_1 x_2 \cdots$ and $y = y_0 y_1 y_2 \cdots$ with $\mathrm{hd}(x, y) = 1$.

- W.l.o.g., $x = w0z$ and $y = w1z$ for some $w \in \mathbb{B}^*$ and $z \in \mathbb{B}^\omega$.
- We have $x \sim y$ and thus $r(x) = r(y) =: r = r_0 r_1 r_2 \cdots$.
- Let $D_x = \{n \mid x_n \neq r_n\}$ and $D_y = \{n \mid y_n \neq r_n\}$.
- $D_x \setminus \{|w|\} = D_y \setminus \{|w|\}$, as x and y only differ at position $|w|$.

Proof

Fix $x = x_0 x_1 x_2 \cdots$ and $y = y_0 y_1 y_2 \cdots$ with $\mathrm{hd}(x, y) = 1$.

- W.l.o.g., $x = w0z$ and $y = w1z$ for some $w \in \mathbb{B}^*$ and $z \in \mathbb{B}^\omega$.
- We have $x \sim y$ and thus $r(x) = r(y) =: r = r_0 r_1 r_2 \cdots$.
- Let $D_x = \{n \mid x_n \neq r_n\}$ and $D_y = \{n \mid y_n \neq r_n\}$.
- $D_x \setminus \{|w|\} = D_y \setminus \{|w|\}$, as x and y only differ at position $|w|$.
- As $x_{|w|} \neq y_{|w|}$, exactly one of the sets contains $|w|$, say D_y.
- Thus, $|D_y| = |D_x| + 1$.

Proof

Fix $x = x_0 x_1 x_2 \cdots$ and $y = y_0 y_1 y_2 \cdots$ with $\mathrm{hd}(x, y) = 1$.

- W.l.o.g., $x = w0z$ and $y = w1z$ for some $w \in \mathbb{B}^*$ and $z \in \mathbb{B}^\omega$.
- We have $x \sim y$ and thus $r(x) = r(y) =: r = r_0 r_1 r_2 \cdots$.
- Let $D_x = \{n \mid x_n \neq r_n\}$ and $D_y = \{n \mid y_n \neq r_n\}$.
- $D_x \setminus \{|w|\} = D_y \setminus \{|w|\}$, as x and y only differ at position $|w|$.
- As $x_{|w|} \neq y_{|w|}$, exactly one of the sets contains $|w|$, say D_y.
- Thus, $|D_y| = |D_x| + 1$.

Hence,

$$f(x) = \mathrm{hd}(x, r) \bmod 2 = |D_x| \bmod 2$$

and

$$f(y) = \mathrm{hd}(y, r) \bmod 2 = |D_y| \bmod 2 = (|D_x| + 1) \bmod 2,$$

i.e., $f(x) \neq f(y)$.

The Game $\mathcal{G}_f$

- Fix some infinite XOR function f.
- We define a game $\mathcal{G}_f$ between Player 0 and Player 1. For the sake of simplicity, it is not played in an arena, but the players pick sequences of bits in alternation.

The Game $\mathcal{G}_f$

- Fix some infinite XOR function f.
- We define a game $\mathcal{G}_f$ between Player 0 and Player 1. For the sake of simplicity, it is not played in an arena, but the players pick sequences of bits in alternation.

Example

The Game $\mathcal{G}_f$

- Fix some infinite XOR function f.
- We define a game $\mathcal{G}_f$ between Player 0 and Player 1. For the sake of simplicity, it is not played in an arena, but the players pick sequences of bits in alternation.

Example

1100

The Game $\mathcal{G}_f$

- Fix some infinite XOR function f.
- We define a game $\mathcal{G}_f$ between Player 0 and Player 1. For the sake of simplicity, it is not played in an arena, but the players pick sequences of bits in alternation.

Example

1100 0

The Game $\mathcal{G}_f$

- Fix some infinite XOR function f.
- We define a game $\mathcal{G}_f$ between Player 0 and Player 1. For the sake of simplicity, it is not played in an arena, but the players pick sequences of bits in alternation.

Example

1100 0 000000110000

The Game $\mathcal{G}_f$

- Fix some infinite XOR function f.
- We define a game $\mathcal{G}_f$ between Player 0 and Player 1. For the sake of simplicity, it is not played in an arena, but the players pick sequences of bits in alternation.

Example

1100 0 000000110000 1100101

The Game $\mathcal{G}_f$

- Fix some infinite XOR function f.
- We define a game $\mathcal{G}_f$ between Player 0 and Player 1. For the sake of simplicity, it is not played in an arena, but the players pick sequences of bits in alternation.

Example

1100 0 000000110000 1100101 1

The Game $\mathcal{G}_f$

- Fix some infinite XOR function f.
- We define a game $\mathcal{G}_f$ between Player 0 and Player 1. For the sake of simplicity, it is not played in an arena, but the players pick sequences of bits in alternation.

Example

1100 0 000000110000 1100101 1 100000

The Game $\mathcal{G}_f$

- Fix some infinite XOR function f.
- We define a game $\mathcal{G}_f$ between Player 0 and Player 1. For the sake of simplicity, it is not played in an arena, but the players pick sequences of bits in alternation.

Example

1100 0 000000110000 1100101 1 100000 $\cdots$

The Game $\mathcal{G}_f$

- Fix some infinite XOR function f.
- We define a game $\mathcal{G}_f$ between Player 0 and Player 1. For the sake of simplicity, it is not played in an arena, but the players pick sequences of bits in alternation.

Example

winner: Player $f($ 1100 0 000000110000 1100101 1 100000 $\cdots$ $)$

The Game $\mathcal{G}_f$

- Fix some infinite XOR function f.
- We define a game $\mathcal{G}_f$ between Player 0 and Player 1. For the sake of simplicity, it is not played in an arena, but the players pick sequences of bits in alternation.

Example

winner: Player $f($ 1100 0 000000110000 1100101 1 100000 $\cdots$ $)$

- Formally, $\mathcal{G}_f$ is played in rounds $n = 0, 1, 2, \ldots$.
- In round n, first Player 0 picks $w_{2n} \in \mathbb{B}^+$, then Player 1 picks $w_{2n+1} \in \mathbb{B}^+$.
- Play $w_0, w_1, w_2, \ldots$ is won by Player $f(w_0 w_1 w_2 \cdots)$.

There are Undetermined Games

Theorem

Let f be an infinite XOR function. No player has a winning strategy for $\mathcal{G}_f$.

Proof Idea

Strategy stealing:

- For every strategy τ of Player 1, we construct two counter strategies σ and σ' that mimic τ.
- The only difference between σ and σ' is that one starts by playing a 0, the other by playing a 1.
- The remainder of the plays resulting from playing σ and σ' against τ are equal.
- Hence, their Hamming distance is 1 and one of the plays is won by Player 0.
- Thus, τ is not a winning strategy.

Proof Idea

Strategy stealing:

- For every strategy τ of Player 1, we construct two counter strategies σ and σ' that mimic τ.
- The only difference between σ and σ' is that one starts by playing a 0, the other by playing a 1.
- The remainder of the plays resulting from playing σ and σ' against τ are equal.
- Hence, their Hamming distance is 1 and one of the plays is won by Player 0.
- Thus, τ is not a winning strategy.

The argument showing that Player 0 has no winning strategy is similar.

Proof

Let τ be a strategy for Player 1 in $\mathcal{G}_f$. We show that τ is not winning by constructing counter strategies σ and σ' as above.

Proof

Let τ be a strategy for Player 1 in $\mathcal{G}_f$. We show that τ is not winning by constructing counter strategies σ and σ' as above.

Proof

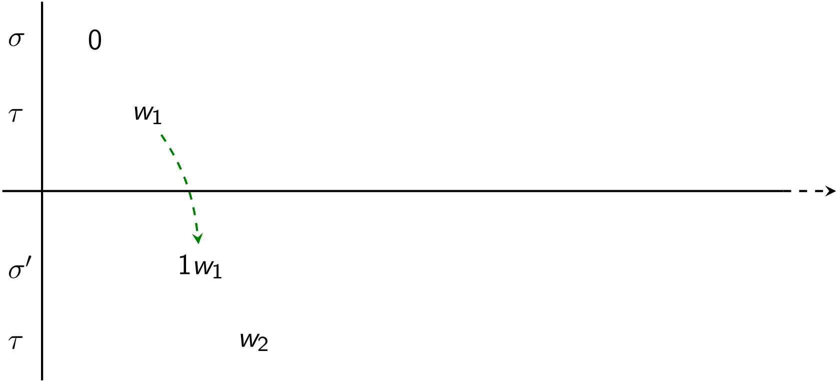
Let τ be a strategy for Player 1 in $\mathcal{G}_f$. We show that τ is not winning by constructing counter strategies σ and σ' as above.

Proof

Let τ be a strategy for Player 1 in $\mathcal{G}_f$. We show that τ is not winning by constructing counter strategies σ and σ' as above.

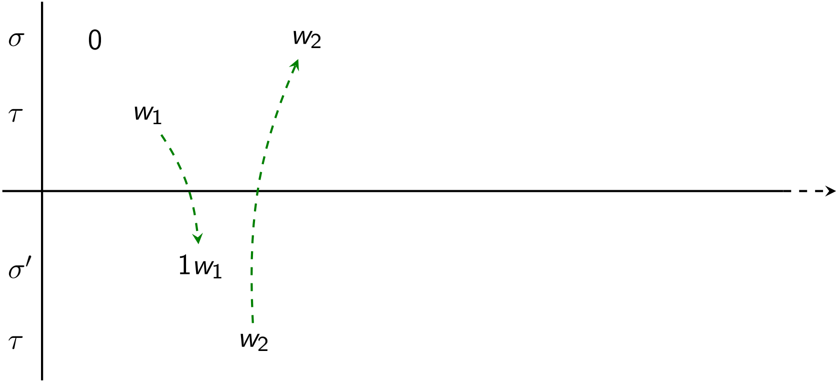
Proof

Let τ be a strategy for Player 1 in $\mathcal{G}_f$. We show that τ is not winning by constructing counter strategies σ and σ' as above.



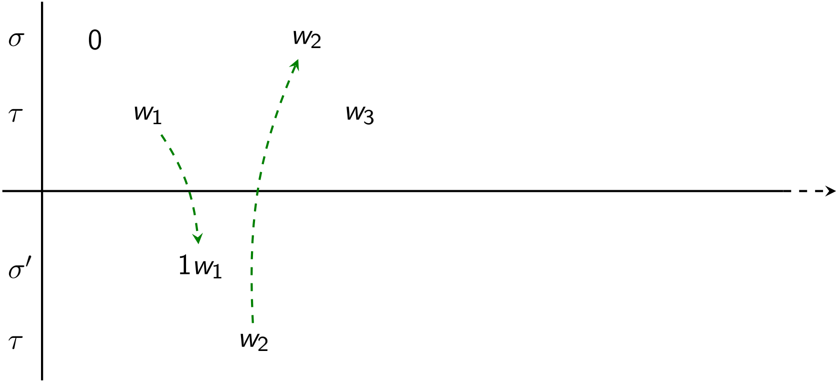
Proof

Let τ be a strategy for Player 1 in $\mathcal{G}_f$. We show that τ is not winning by constructing counter strategies σ and σ' as above.



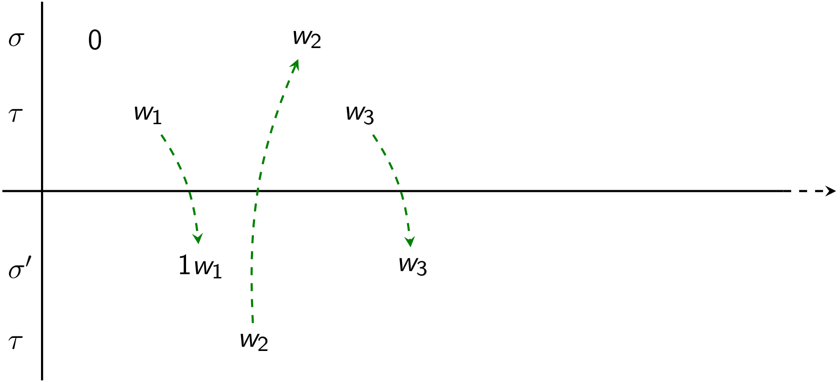
Proof

Let τ be a strategy for Player 1 in $\mathcal{G}_f$. We show that τ is not winning by constructing counter strategies σ and σ' as above.



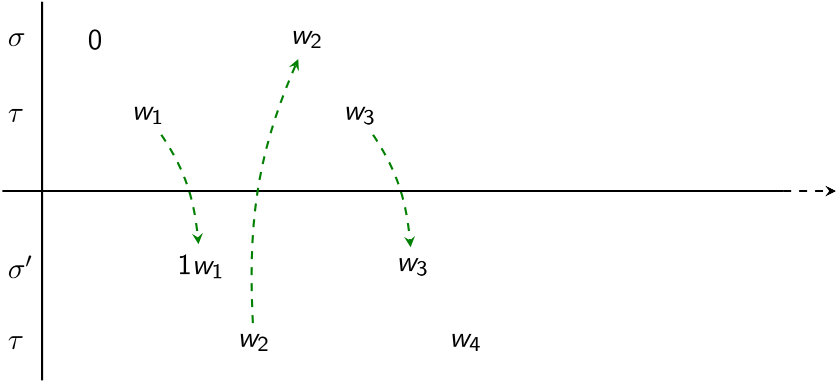
Proof

Let τ be a strategy for Player 1 in $\mathcal{G}_f$. We show that τ is not winning by constructing counter strategies σ and σ' as above.



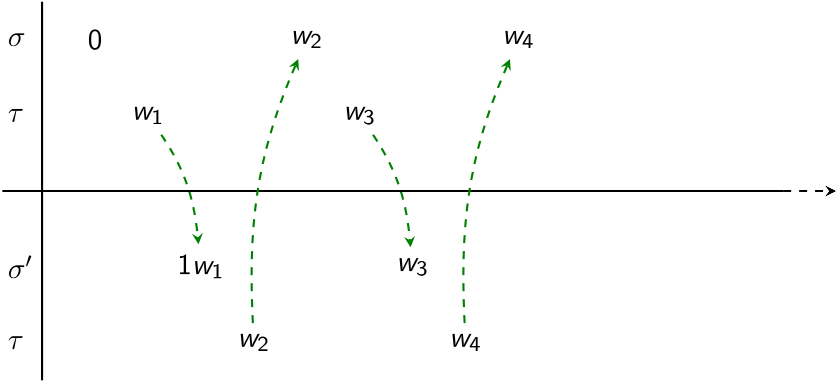
Proof

Let τ be a strategy for Player 1 in $\mathcal{G}_f$. We show that τ is not winning by constructing counter strategies σ and σ' as above.



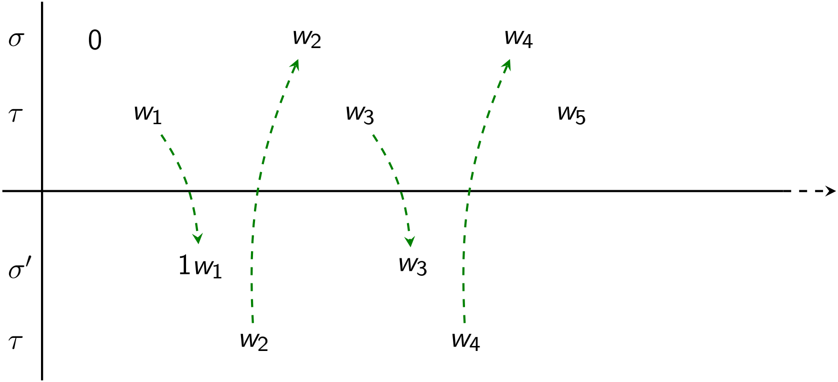
Proof

Let τ be a strategy for Player 1 in $\mathcal{G}_f$. We show that τ is not winning by constructing counter strategies σ and σ' as above.



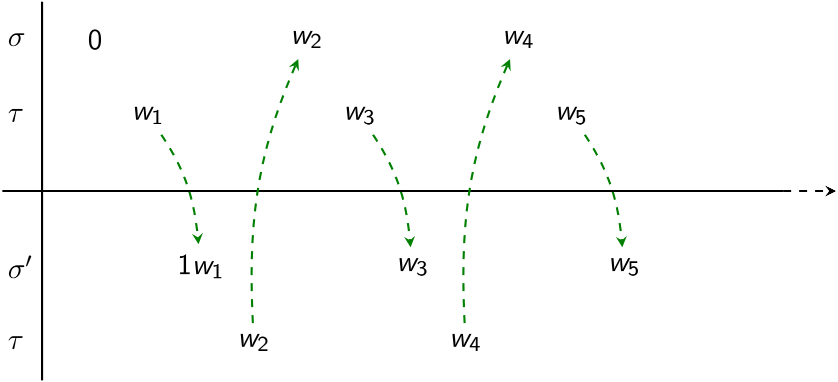
Proof

Let τ be a strategy for Player 1 in $\mathcal{G}_f$. We show that τ is not winning by constructing counter strategies σ and σ' as above.



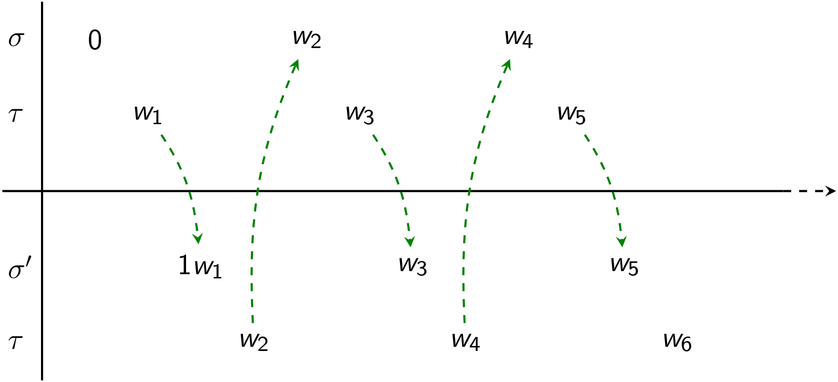
Proof

Let τ be a strategy for Player 1 in $\mathcal{G}_f$. We show that τ is not winning by constructing counter strategies σ and σ' as above.



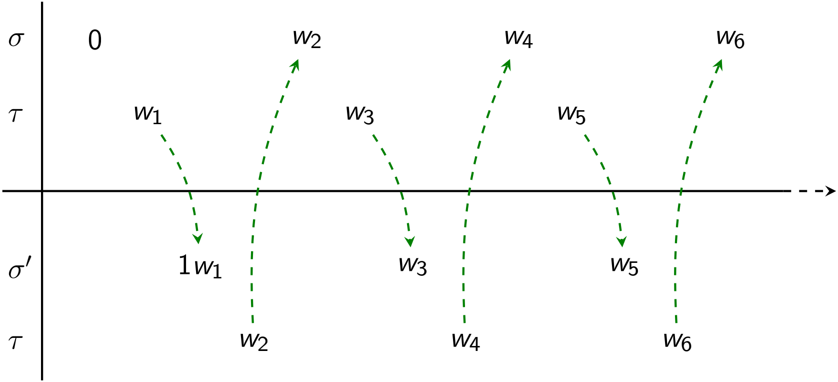
Proof

Let τ be a strategy for Player 1 in $\mathcal{G}_f$. We show that τ is not winning by constructing counter strategies σ and σ' as above.



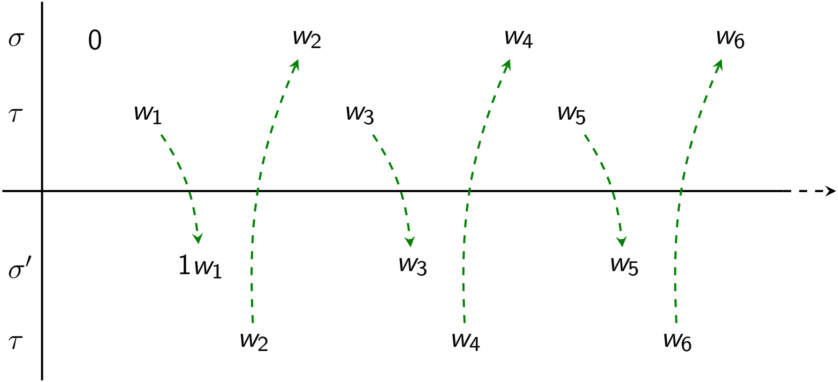
Proof

Let τ be a strategy for Player 1 in $\mathcal{G}_f$. We show that τ is not winning by constructing counter strategies σ and σ' as above.



Proof

Let τ be a strategy for Player 1 in $\mathcal{G}_f$. We show that τ is not winning by constructing counter strategies σ and σ' as above.



Consider the resulting plays: they differ only at their first position. Hence, Player 0 wins one of them. So, τ is not winning.

Proof

Let σ be a strategy for Player 0 in $\mathcal{G}_f$. We show that σ is not winning by constructing counter strategies τ and τ' as above.

Proof

Let σ be a strategy for Player 0 in $\mathcal{G}_f$. We show that σ is not winning by constructing counter strategies τ and τ' as above.

Proof

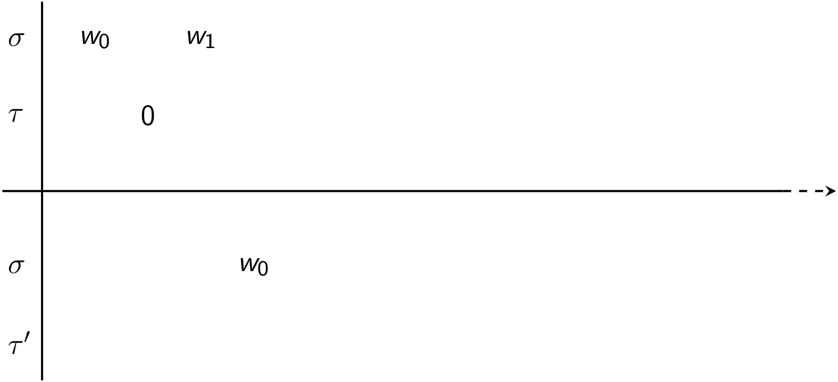
Let σ be a strategy for Player 0 in $\mathcal{G}_f$. We show that σ is not winning by constructing counter strategies τ and τ' as above.

Proof

Let σ be a strategy for Player 0 in $\mathcal{G}_f$. We show that σ is not winning by constructing counter strategies τ and τ' as above.

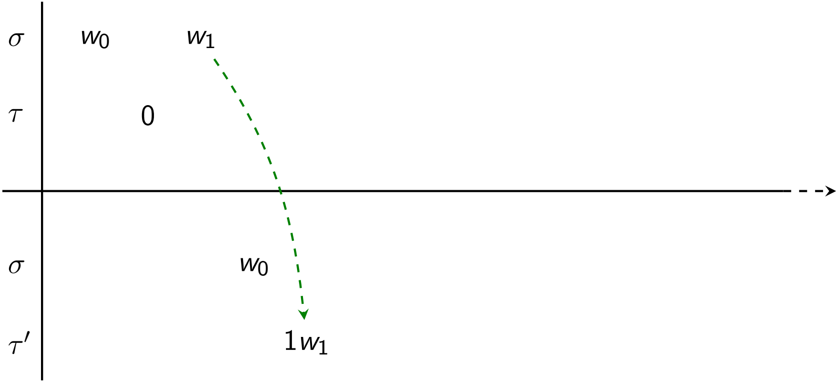
Proof

Let σ be a strategy for Player 0 in $\mathcal{G}_f$. We show that σ is not winning by constructing counter strategies τ and τ' as above.



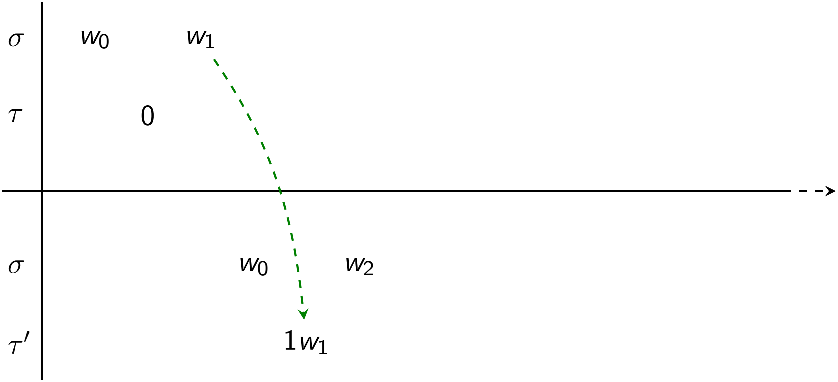
Proof

Let σ be a strategy for Player 0 in $\mathcal{G}_f$. We show that σ is not winning by constructing counter strategies τ and τ' as above.



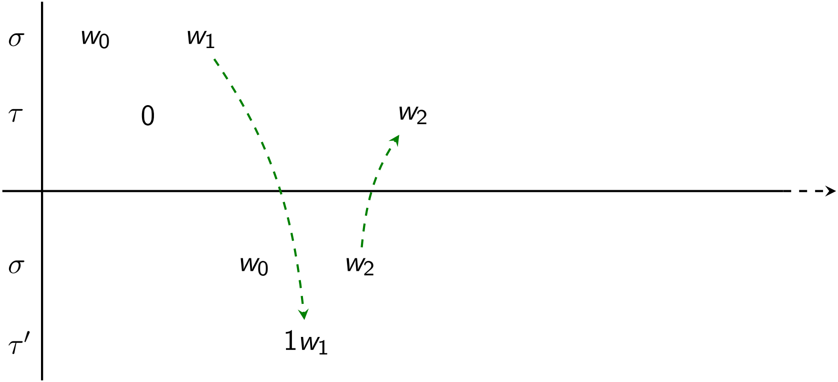
Proof

Let σ be a strategy for Player 0 in $\mathcal{G}_f$. We show that σ is not winning by constructing counter strategies τ and τ' as above.



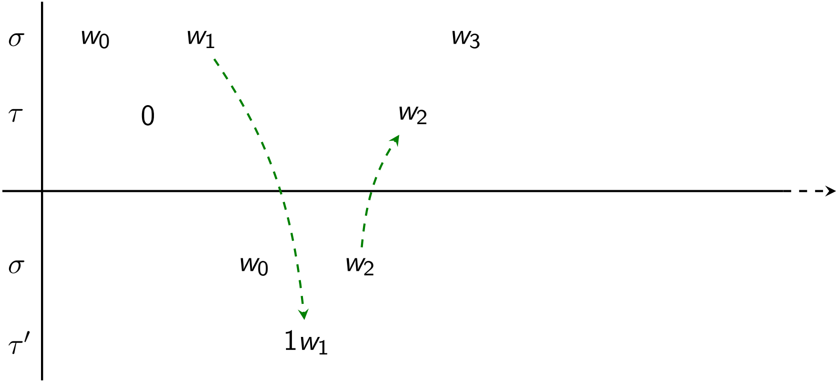
Proof

Let σ be a strategy for Player 0 in $\mathcal{G}_f$. We show that σ is not winning by constructing counter strategies τ and τ' as above.



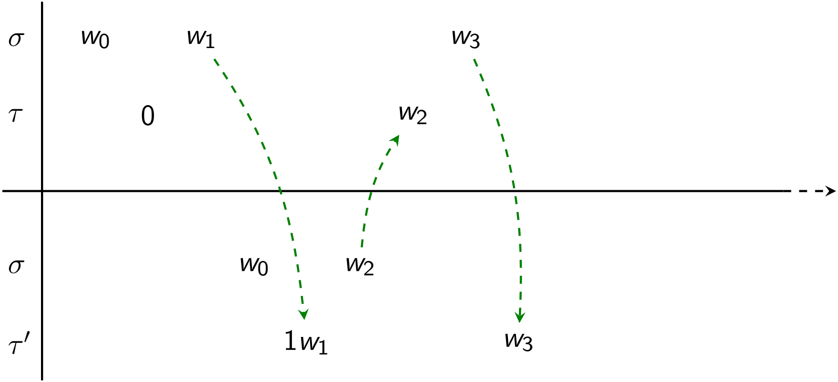
Proof

Let σ be a strategy for Player 0 in $\mathcal{G}_f$. We show that σ is not winning by constructing counter strategies τ and τ' as above.



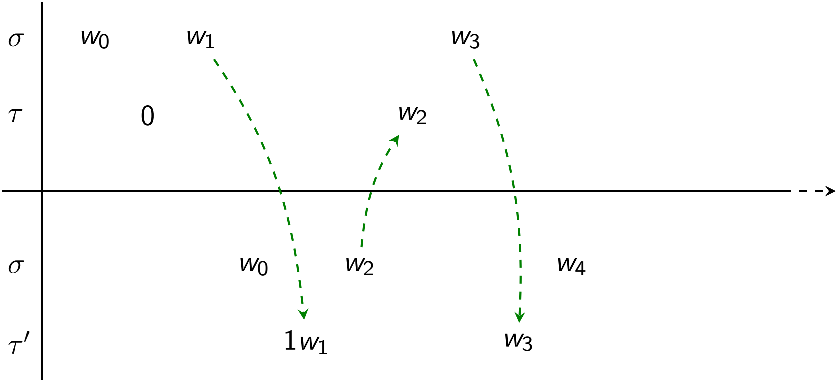
Proof

Let σ be a strategy for Player 0 in $\mathcal{G}_f$. We show that σ is not winning by constructing counter strategies τ and τ' as above.



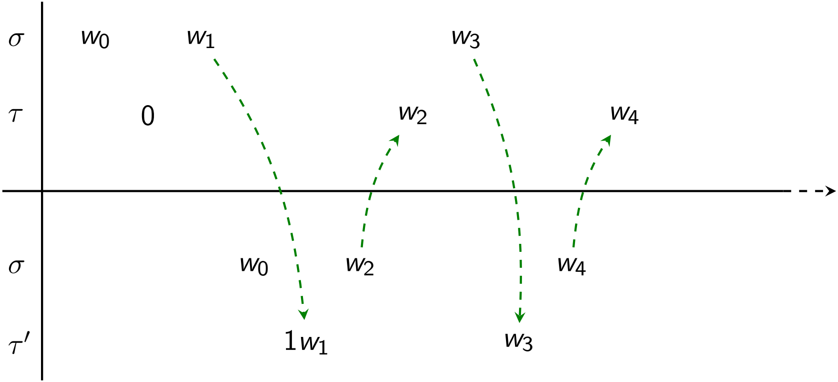
Proof

Let σ be a strategy for Player 0 in $\mathcal{G}_f$. We show that σ is not winning by constructing counter strategies τ and τ' as above.



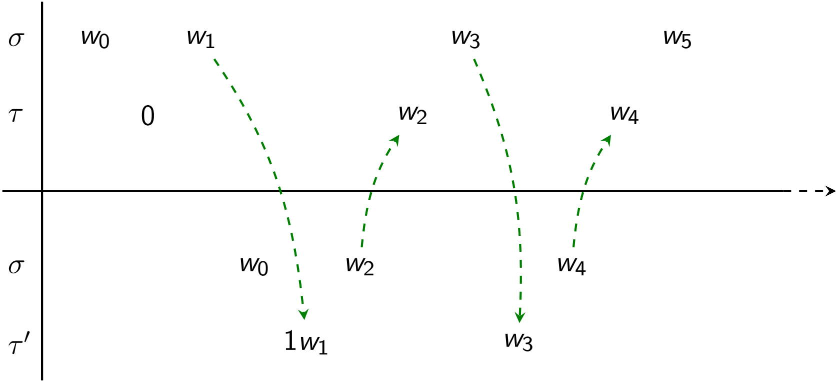
Proof

Let σ be a strategy for Player 0 in $\mathcal{G}_f$. We show that σ is not winning by constructing counter strategies τ and τ' as above.



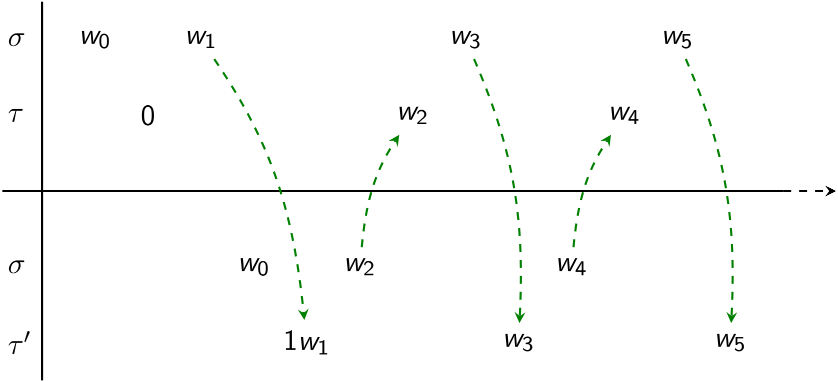
Proof

Let σ be a strategy for Player 0 in $\mathcal{G}_f$. We show that σ is not winning by constructing counter strategies τ and τ' as above.



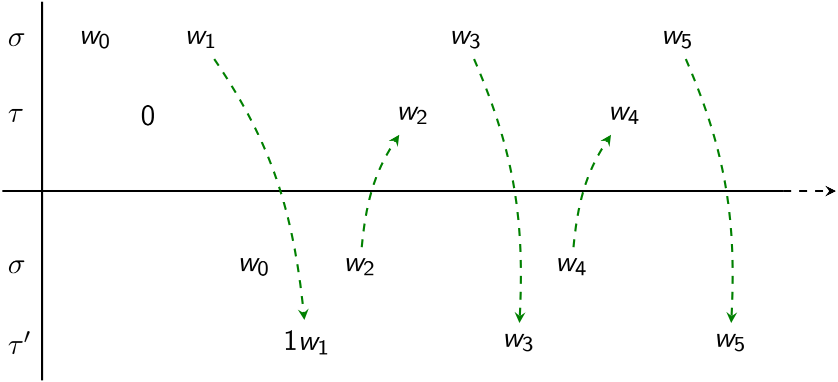
Proof

Let σ be a strategy for Player 0 in $\mathcal{G}_f$. We show that σ is not winning by constructing counter strategies τ and τ' as above.



Proof

Let σ be a strategy for Player 0 in $\mathcal{G}_f$. We show that σ is not winning by constructing counter strategies τ and τ' as above.



Consider the resulting plays: they differ only at their first position. Hence, Player 1 wins one of them. So, σ is not winning.

Set Theory

- Recall that we constructed f by picking S such that it contains exactly one element of each $\sim$-equivalence class.
- This seems innocuous, but requires the *axiom of choice*.

  For every family $(S_i)_{i \in I}$ of nonempty sets there exists an indexed family $(x_i)_{i \in I}$ of elements such that $x_i \in S_i$ for every $i \in I$.

Set Theory

- Recall that we constructed f by picking S such that it contains exactly one element of each $\sim$-equivalence class.
- This seems innocuous, but requires the *axiom of choice*.

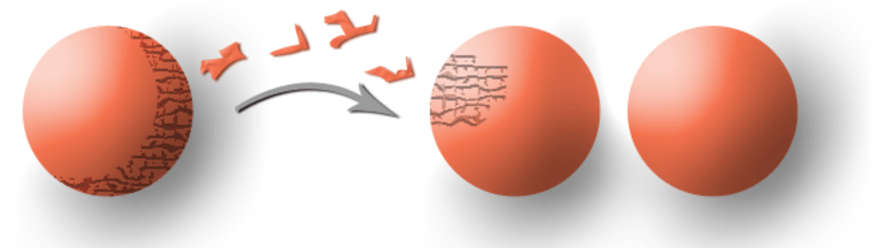
  For every family $(S_i)_{i \in I}$ of nonempty sets there exists an indexed family $(x_i)_{i \in I}$ of elements such that $x_i \in S_i$ for every $i \in I$.

The following statements are equivalent to the axion of choice:

1. The cartesian product of a collection of non-empty sets is non-empty.
2. *Well-ordering principle*: Every set can be well-ordered.
3. *Zorn's Lemma*: Every non-empty partially ordered set in which every chain (i.e., totally ordered subset) has an upper bound contains at least one maximal element.

Consequences of the Axion of Choice

The Banach-Tarski paradox:



"Doubling of a sphere, as per the Banach-Tarski Theorem" by Sean Kelly (CC BY-SA 3.0)

You can decompose a ball into five pieces and reassemble them into two balls of the same size by just moving and rotating these pieces.

Parting Words

The Axiom of Choice is obviously true, the well-ordering principle obviously false, and who can tell about Zorn's lemma? *(Jerry L. Bona)*

Parting Words

The Axiom of Choice is obviously true, the well-ordering principle obviously false, and who can tell about Zorn's lemma? *(Jerry L. Bona)*

Merry Christmas and a happy new year