Games for discrete-time Markov chain and their application to verification

Shota Nakagawa

The University of Tokyo

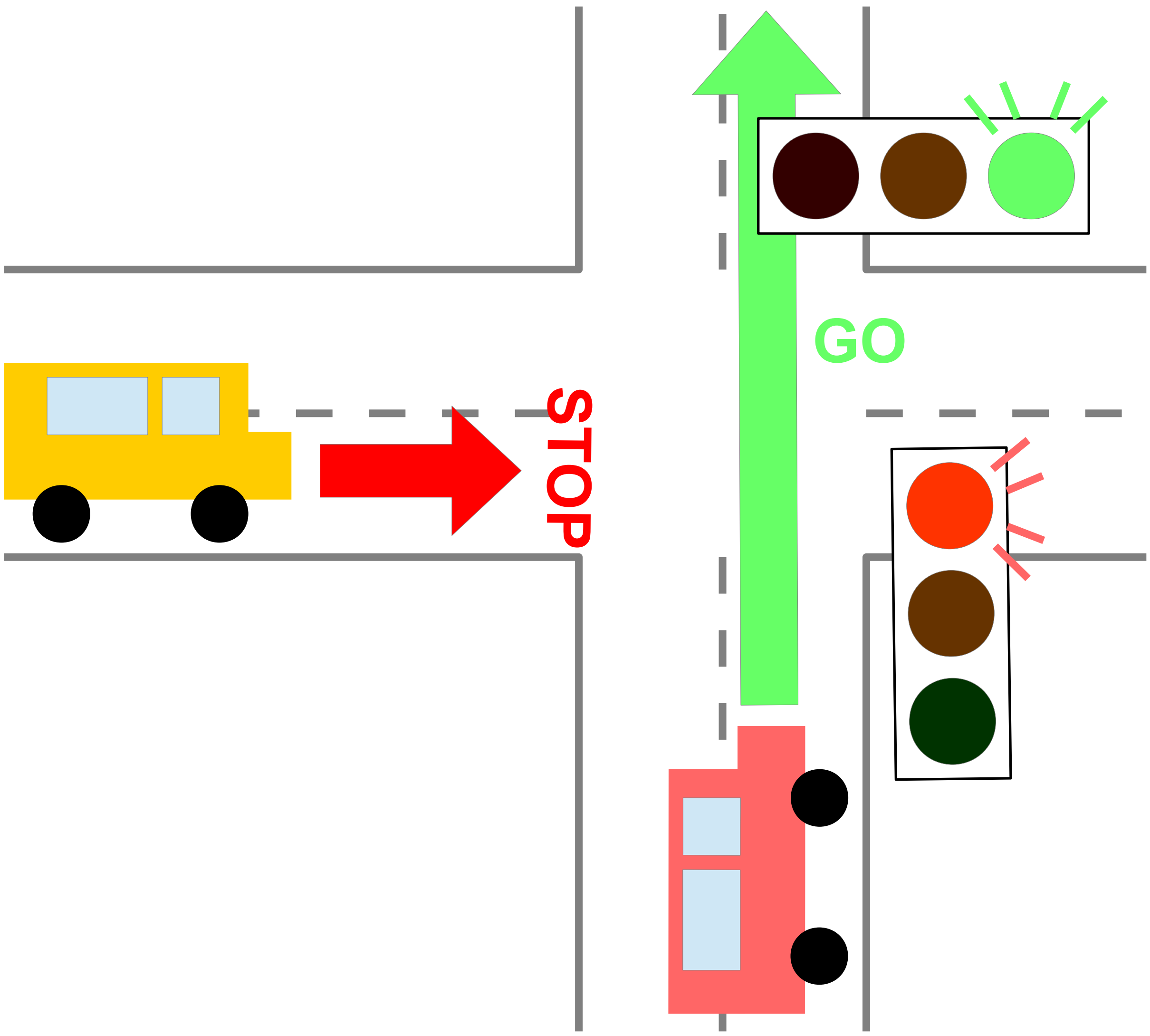
Outline

- What model-checking is
- Applications of GTP to model-checking
  - Fairness theorem
  - Simulation
- Conclusion and future work

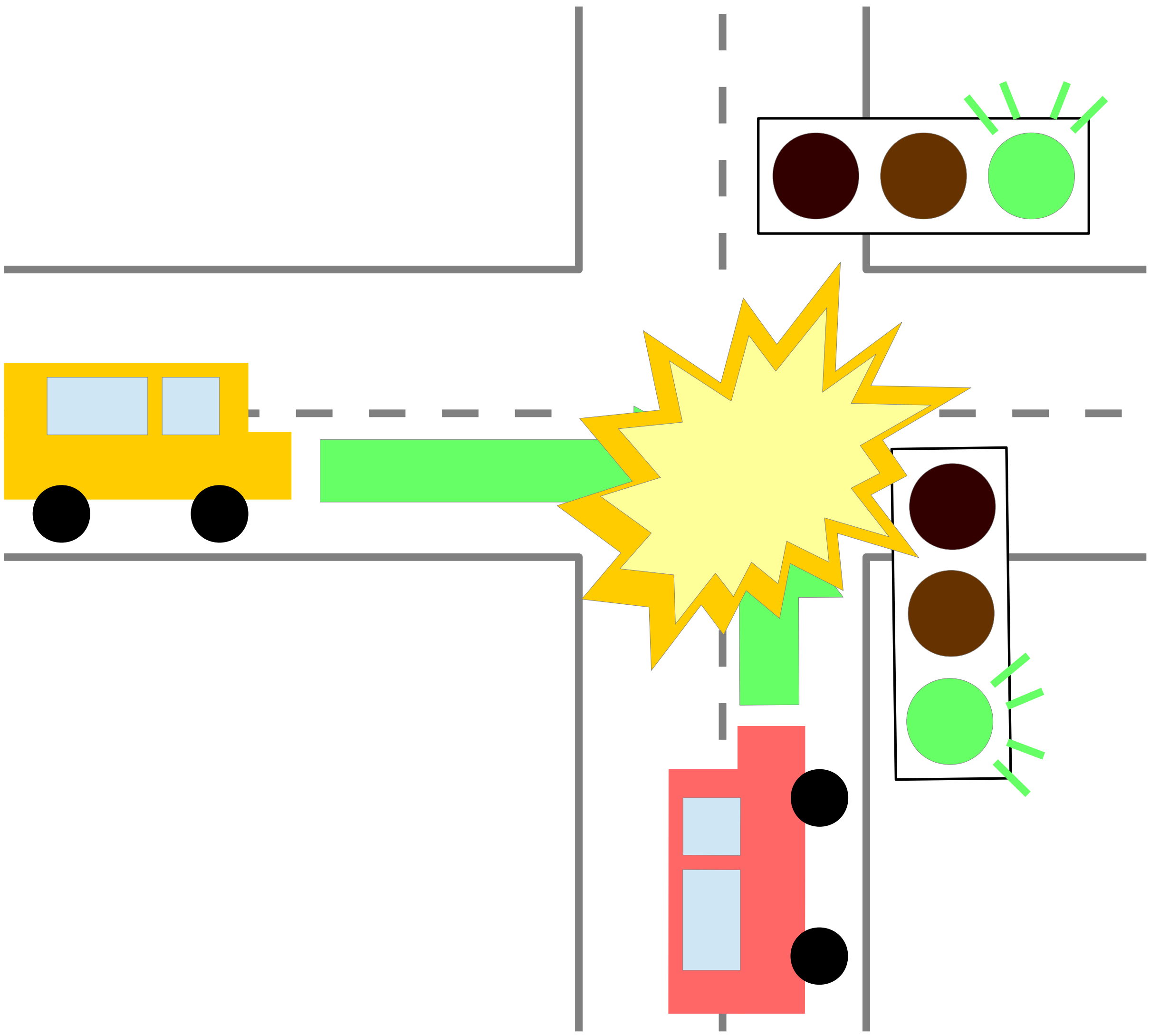
Outline

- What model-checking is
- Applications of GTP to model-checking
  - Fairness theorem
  - Simulation
- Conclusion and future work

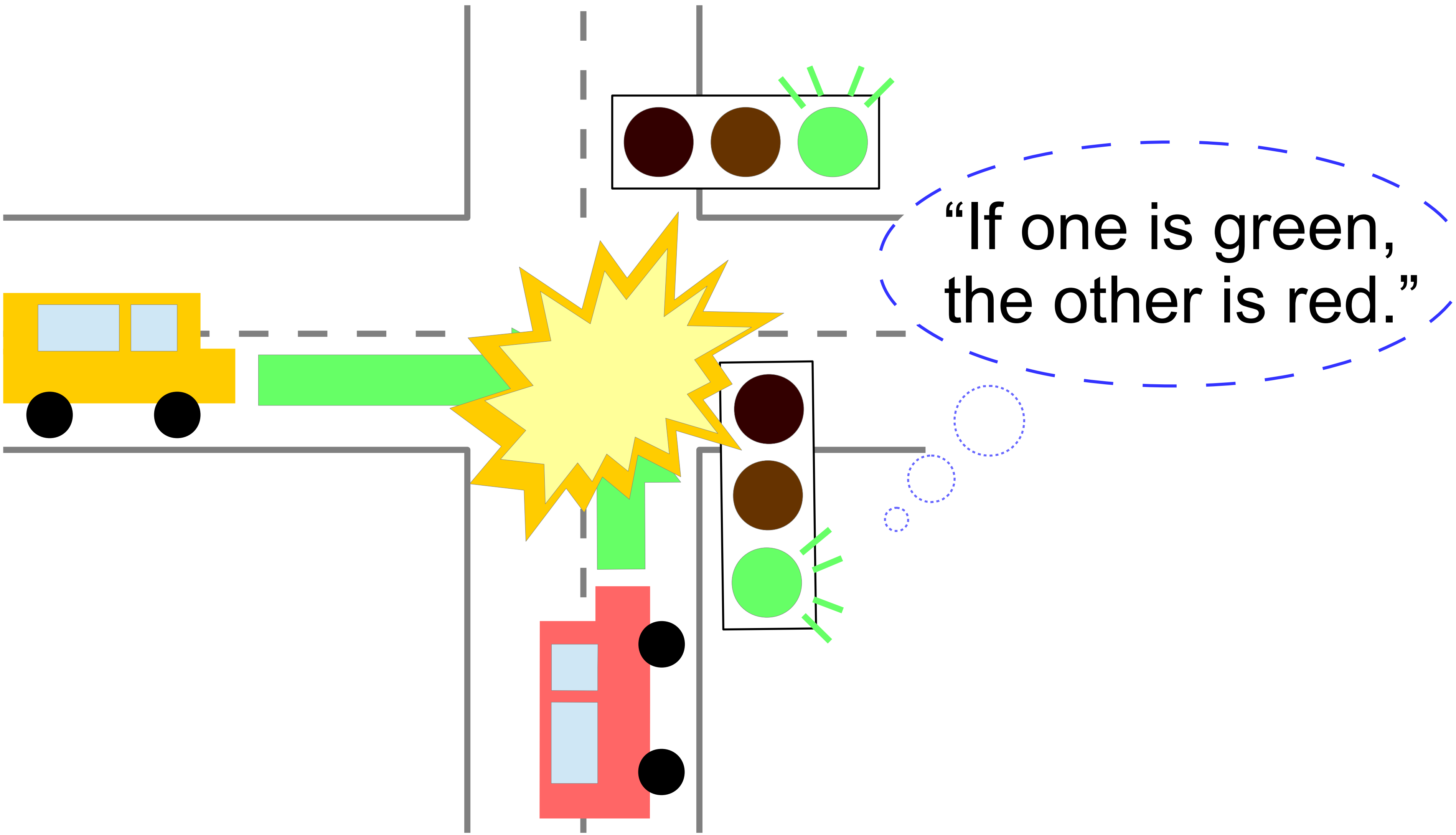
Example: Traffic Lights



Example: Traffic Lights



Example: Traffic Lights

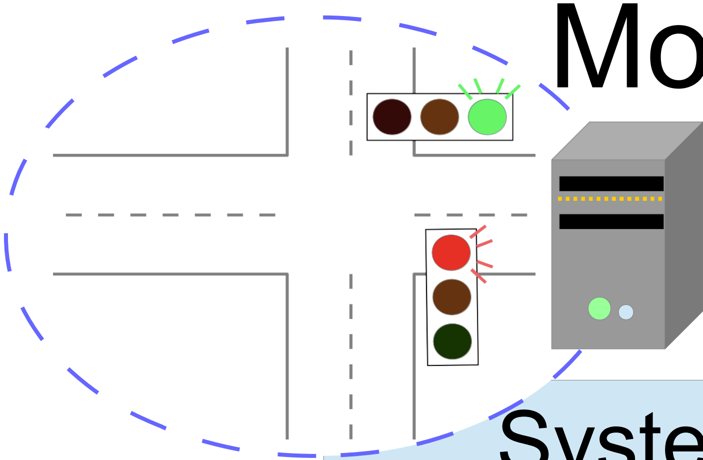


Model-Checking

System

Specification

Model-Checking

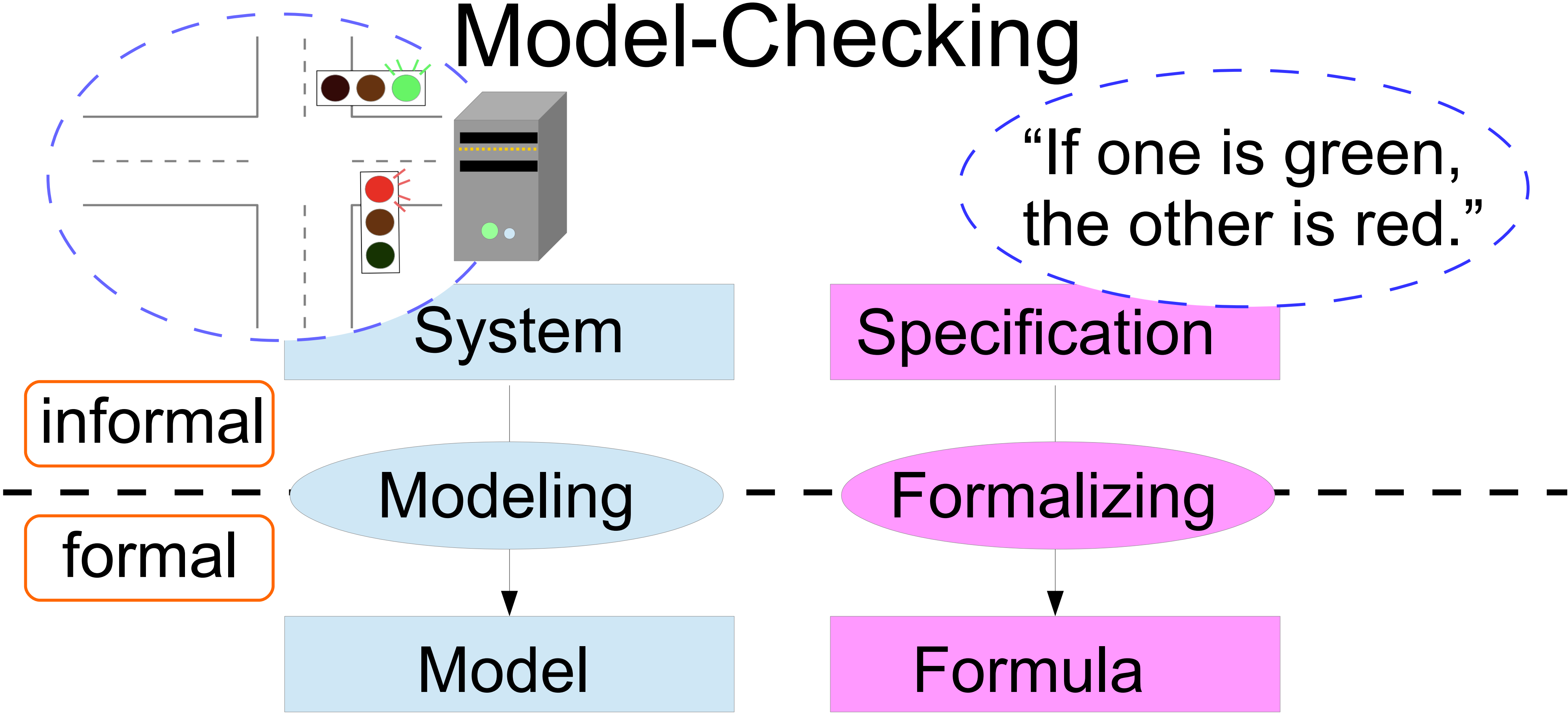


System

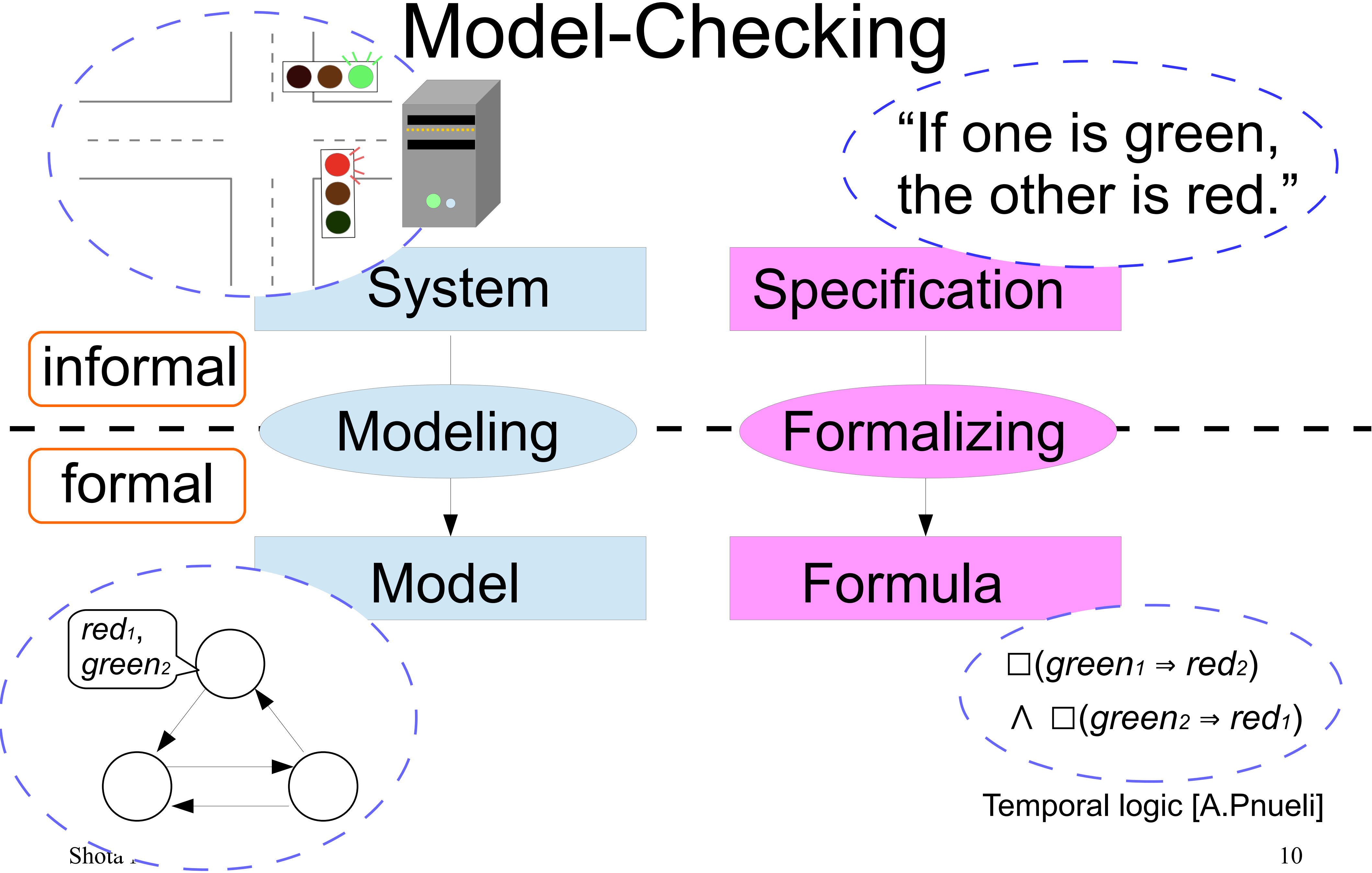
Specification

"If one is green, the other is red."

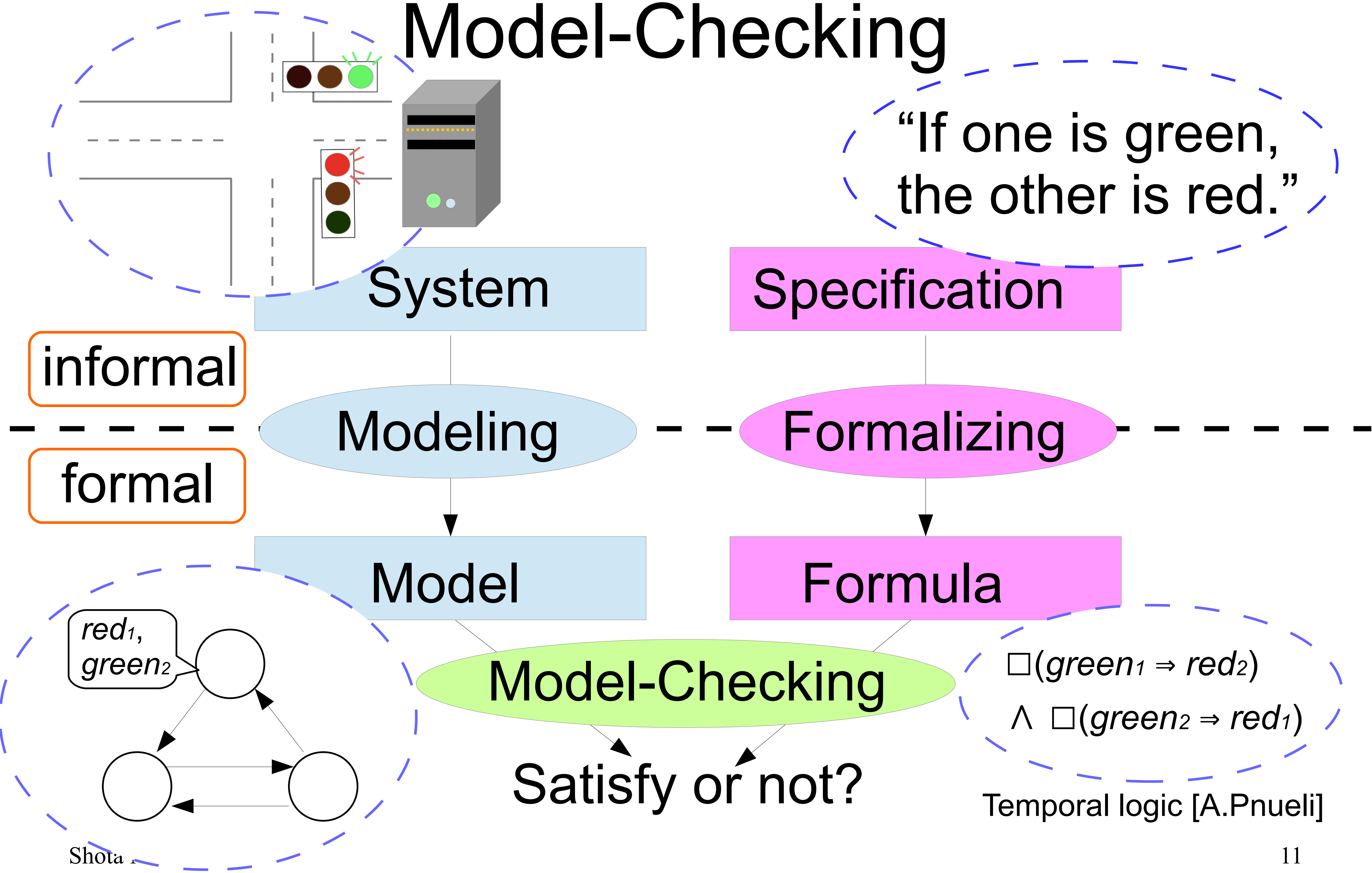
Model-Checking



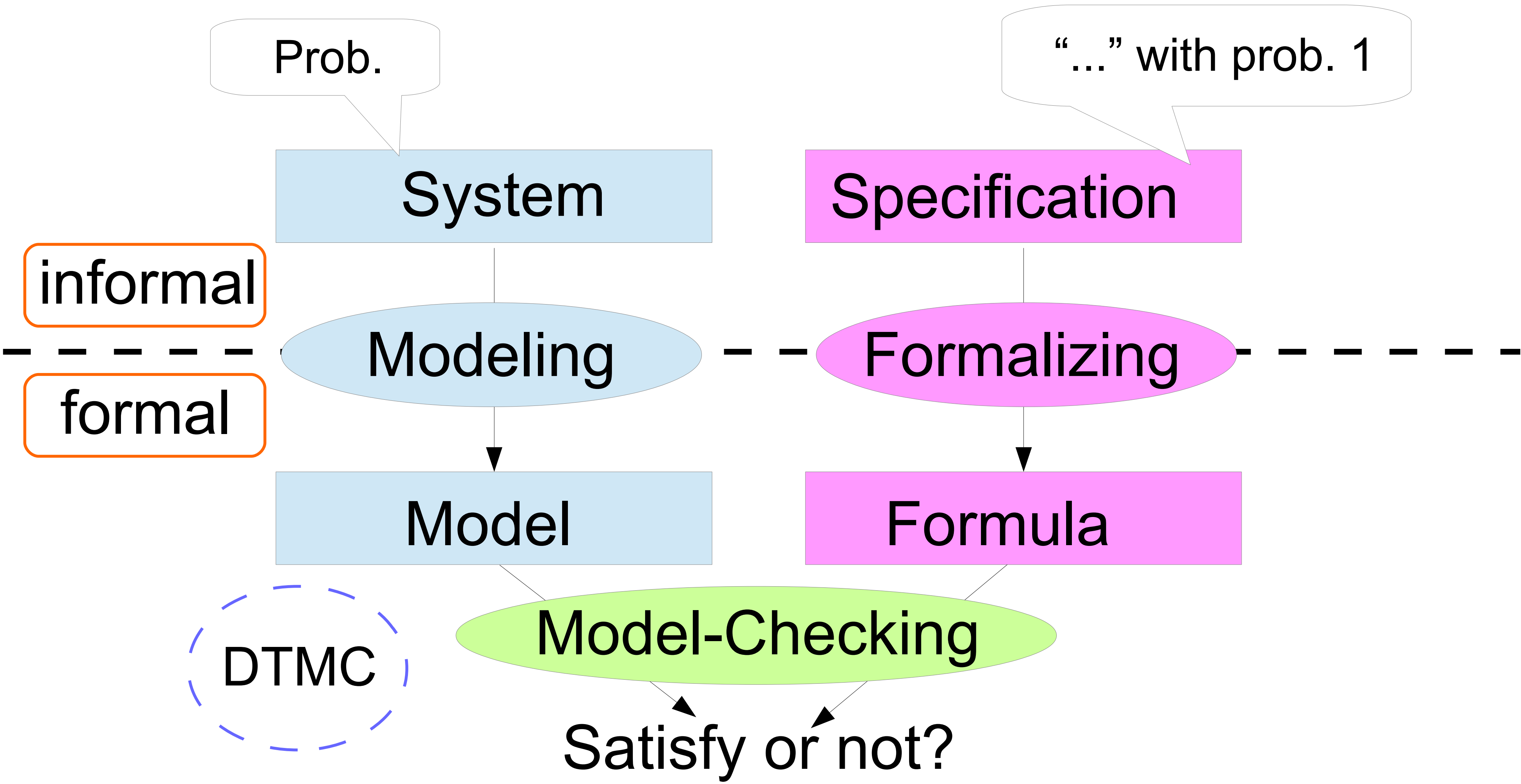
Model-Checking



Model-Checking



Probabilistic Model-Checking



Discrete-Time Markov Chain

- As a random process

Def.
A (finite or countable) state space S and
random variables $X_1, X_2, X_3, \ldots$ such that
$$\Pr(X_{n+1} = s \mid X_1 = s_1, \ldots, X_n = s_n) = \Pr(X_2 = s \mid X_1 = s_n)$$

Discrete-Time Markov Chain

- As a random process

Def.
A (finite or countable) state space S and
random variables $X_1, X_2, X_3, \ldots$ such that
$$\Pr(X_{n+1} = \mathrm{s} \mid X_1 = \mathrm{s}_1, \ldots, X_n = \mathrm{s}_n) = \Pr(X_2 = \mathrm{s} \mid X_1 = \mathrm{s}_n)$$

- As a transition system

Def.
A pair (S, P) of
- a (finite or countable) state space S and
- a stochastic matrix $\mathrm{P} : \mathrm{S}\times\mathrm{S} \to [0,1]$ (transition)

- Connection between two definitions: $\mathrm{P}(\mathrm{s},\mathrm{s}') = \Pr(X_2 = \mathrm{s}' \mid X_1 = \mathrm{s})$

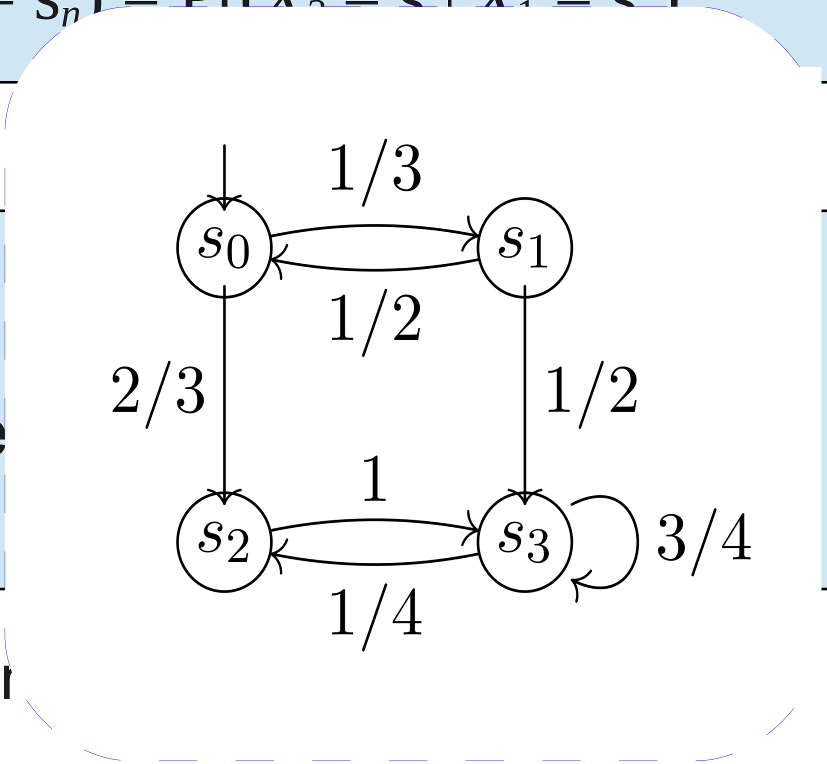
Discrete-Time Markov Chain

- As a random process

Def.
A (finite or countable) state space S and random variables $X_1, X_2, X_3, \ldots$ such that
$\Pr(X_{n+1} = s \mid X_1 = s_1, \ldots, X_n = s_n) = \Pr(X_2 = s \mid X_1 = s_n)$

- As a transition system

Def.
A pair (S, P) of
- a (finite or countable) state
- a stochastic matrix P : S×S



- Connection between two definitio

Outline

- What model-checking is
- Applications of GTP to model-checking
  - Fairness theorem
  - Simulation
- Conclusion and future work

Applications to model-checking

- Connection between GTP and model-checking
  - One step of transitions ⇔ One round of games.
  -

Applications to model-checking

- Connection between GTP and model-checking
  - One step of transitions ⇔ One round of games.
  -
- Long term goals
  - Get efficient model-checking algorithms, models or expressions of specifications
  -

Applications to model-checking

- Connection between GTP and model-checking
  - One step of transitions ⇔ One round of games.
  -
- Long term goals
  - Get efficient model-checking algorithms, models or expressions of specifications
  -
- In my BSc thesis
  - Formulate DTMC in terms of GTP and
  - Give proofs of some known theorems by using GTP

Game for DTMC

Parameter: $S, P, x_0 \in S$

Protocol:

$K_0 := 1.$

FOR $n = 1, 2, \ldots$:

Skeptic announces a function $f_n \colon S \to \mathbb{R}$.

Reality announces $x_n \in \{s \in S \mid P(x_{n-1}, s) > 0\}$.

$K_n := K_{n-1} + f_n(x_n) - \sum_{s \in S} f_n(s) P(x_{n-1}, s)$.

Game for DTMC

Parameter: $S, P, x_0 \in S$

Protocol:

$K_0 := 1.$

FOR $n = 1, 2, \ldots$:

Skeptic announces a function f_n: $S \to \mathbb{R}$.

Reality announces $x_n \in \{s \in S \mid P(x_{n-1}, s) > 0\}$.

$K_n := K_{n-1} + f_n(x_n) - \sum_{s \in S} f_n(s) P(x_{n-1}, s)$.

Skeptic bets $f_n(s)$ for "s will be the next state."

Outline

- What model-checking is
- Applications of GTP to model-checking
  - Fairness theorem
  - Simulation
- Conclusion and future work

Fairness Theorem

Thm. If a state t can be reached from a state s,

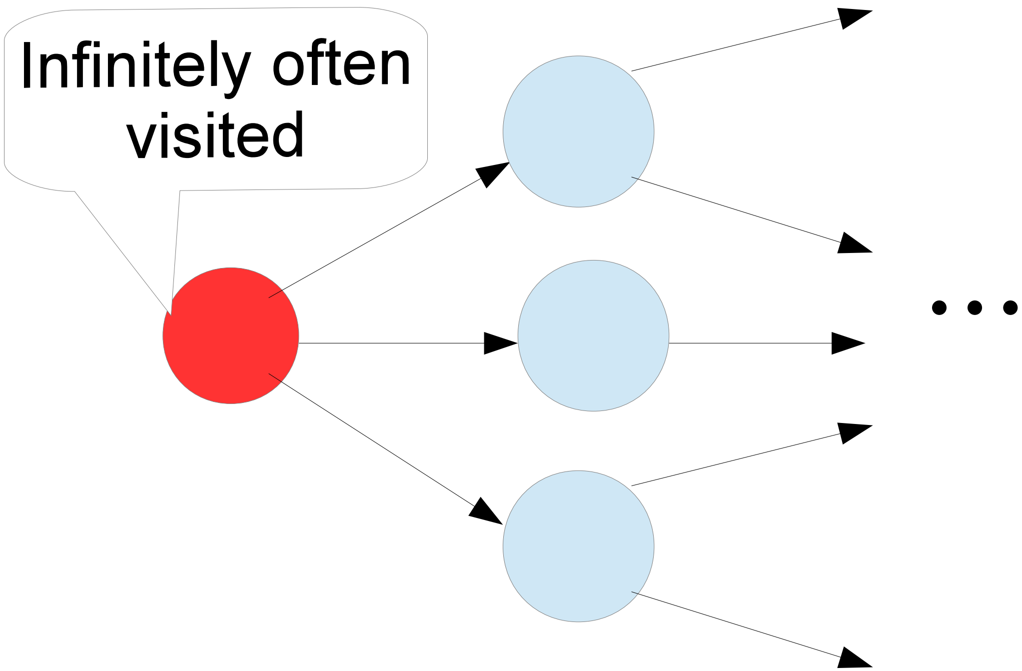
$$Pr(\Box\Diamond s \Rightarrow \Box\Diamond t) = 1.$$

s is visited
Infinitely often

Fairness Theorem

Thm. If a state t can be reached from a state s,

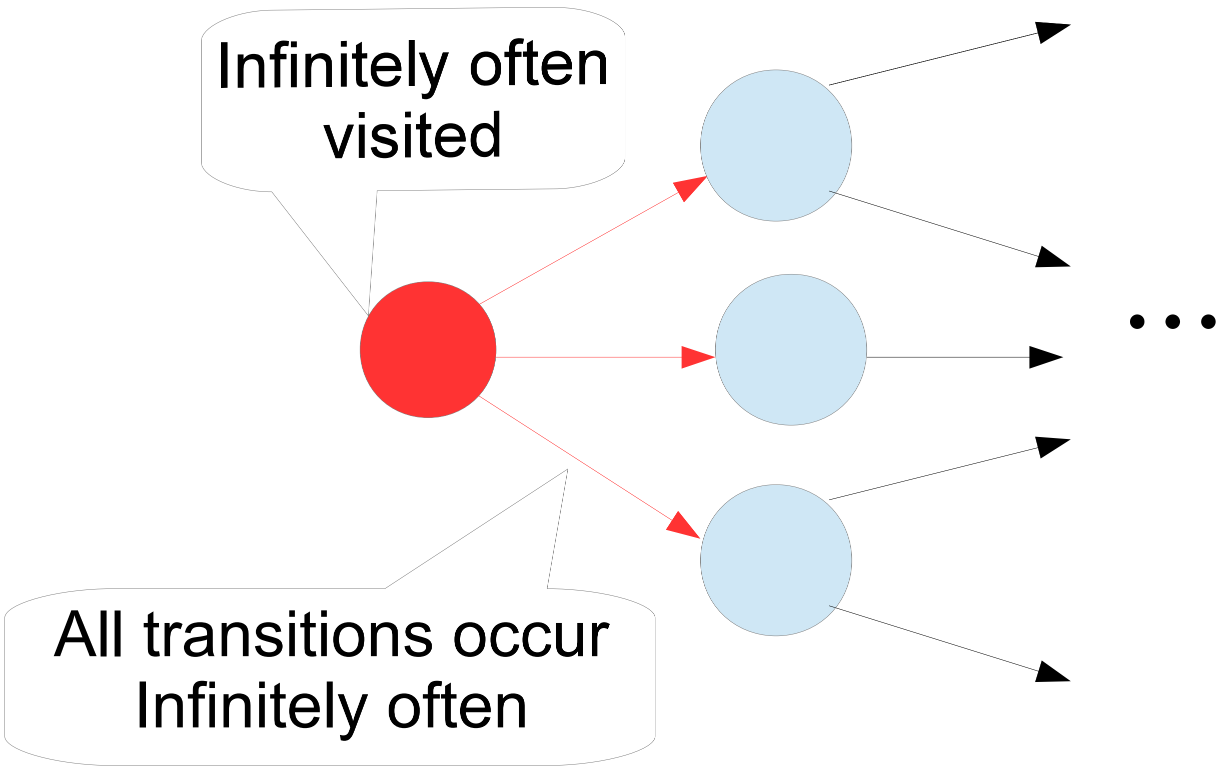
$$\Pr(\Box\Diamond s \Rightarrow \Box\Diamond t) = 1.$$



Fairness Theorem

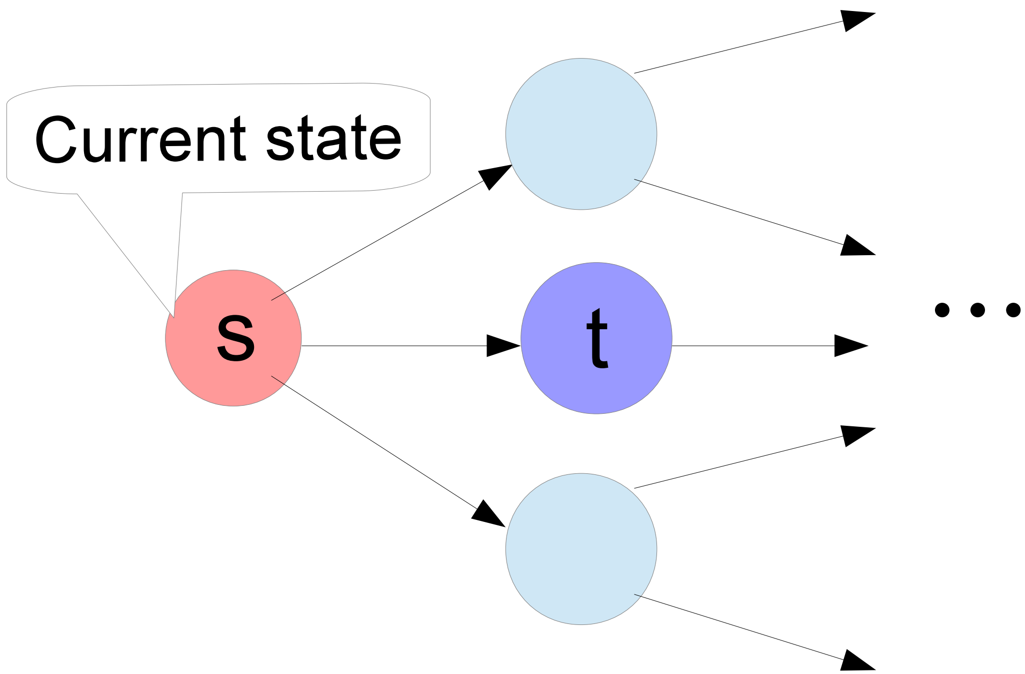
Thm. If a state t can be reached from a state s,

$$\Pr(\Box\Diamond s \Rightarrow \Box\Diamond t) = 1.$$



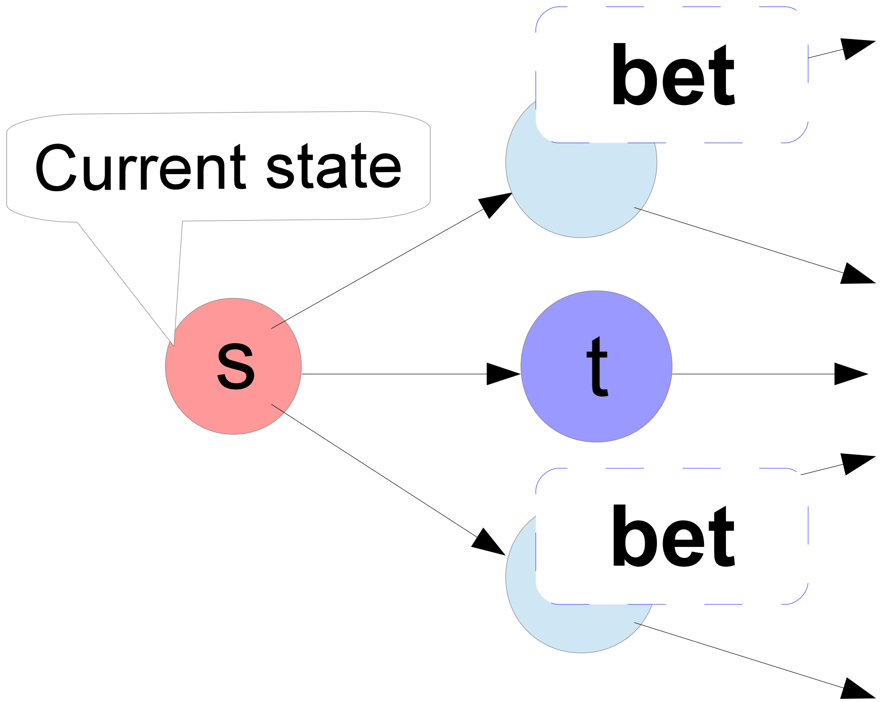
Strategy of Skeptic

- Aim: Pr(□◇s ∧ ¬□◇t) = 0 (complementary event.)
- In case that P(s,t) > 0,



Strategy of Skeptic

- Aim: Pr(□◇s ∧ ¬□◇t) = 0 (complementary event.)
- In case that P(s,t) > 0,



- Skeptic bets on all states except for t
- s is visited infinitely often and t is visited only finitely often ⇒ Skeptic wins

• • •

Outline

- What model-checking is
- Applications of GTP to model-checking
  - Fairness theorem
  - Simulation
- Conclusion and future work

Simulation

- Probabilistic variant [R. Segala and N. Lynch, 1995]

Def. (weight function)

Let μ and ν be distributions on S_1 and S_2, respectively.
A function $\delta : S_1 \times S_2 \to [0,1]$ is a weight function for μ and ν w.r.t. $R \subseteq S_1 \times S_2$ if:

- for each $s \in S_1$, $\sum_{s' \in S_2} \delta(s, s') = \mu(s)$,
- for each $s' \in S_2$, $\sum_{s \in S_1} \delta(s, s') = \nu(s')$, and
- if $\delta(s, s') > 0$ then $(s, s') \in R$.

Simulation

- Probabilistic variant [R. Segala and N. Lynch, 1995]

Def. (simulation)

$R \subseteq S_1 \times S_2$ is a simulation between $D_1 = (S_1, P_1)$ and $D_2 = (S_2, P_2)$
$\Leftrightarrow$ there exists a weight function δ_{s_1,s_2} for $P(s_1, -)$ and $P(s_2, -)$ w.r.t. R for each $(s_1, s_2) \in R$.

Thm.

$R \subseteq S_1 \times S_2$ is a simulation between $D_1 = (S_1, P_1)$ and $D_2 = (S_2, P_2)$
$\Rightarrow \forall (s_1, s_2) \in R.\ Pr^{D_1}(s_1 \models E) \leq Pr^{D_2}(s_2 \models E{\uparrow_R})$

Simulation

- Two games: G_1 for (S_1, P_1) and G_2 for (S_2, P_2)

- Suppose that there exists a weight function δ_{s_1,s_2} for $P(s_1, -)$ and $P(s_2, -)$ w.r.t. R.
  - Skeptic's move f^1 in G_1 can be constructed from a weight function δ_{s_1,s_2} and Skeptic's move f^2 in G_2:

$$f^1(s) = \sum_{s' \in S_2} \delta_{s_1,s_2}(s, s')\, f^2(s') \,/\, P(s_1, s)$$

  - $\forall s_1' \in S_1.\ \exists s_2' \in S_2.\ (s_1, s_2) \in R \wedge$

$$f^1(s_1') - \sum_{s \in S_1} f^1(s) P_1(s_1, s) \geqq f^2(s_2') - \sum_{s' \in S_2} f^2(s') P_2(s_2, s')$$

Outline

- What model-checking is
- Applications of GTP to model-checking
  - Fairness theorem
  - Simulation
- Conclusion and future work

Conclusion

- Application of GTP to model-checking
  - Formulation of DTMC in terms of GTP
  - Give proofs of some known theorems by using GTP

Future work

- Formulate other models
  - Markov decision process (which have both probabilistic and non-deterministic behavior)
- Use GTP and get model-checking algorithms, models or expressions of specifications

References

- E.M. Clarke, O. Grumberg, and D.A. Peled. Model Checking. MIT Press, 1999
- Christel Baier and Joost-Pieter Katoen. Principles of Model Checking. MIT Press, 2007.
- Shota Nakagawa. Games for Discrete-time Markov Chain and Their Application to Verification. BSc thesis, University of Tokyo, 2014.