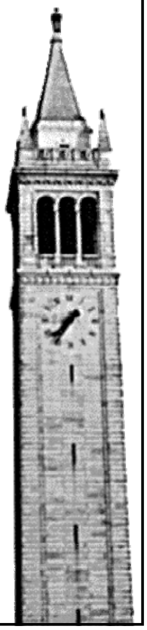
Hybrid Systems Theory

Edited and Presented by
Thomas A. Henzinger, Co-PI
UC Berkeley

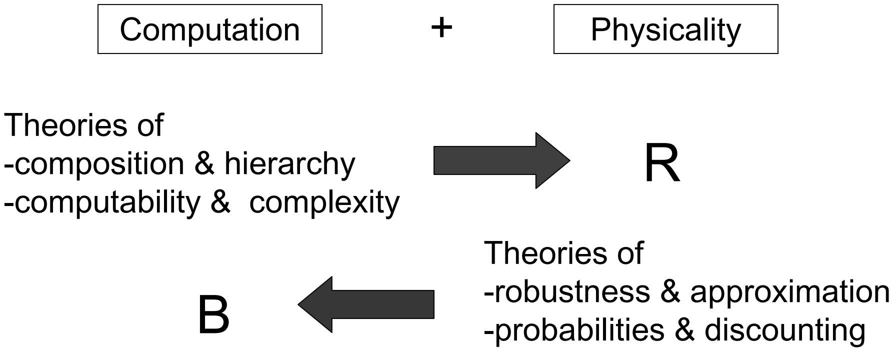
Chess Review
November 18, 2004
Berkeley, CA

Chess



Formal Foundation for Embedded Systems

needs to combine



Computation + Physicality

Theories of
-composition & hierarchy
-computability & complexity

R

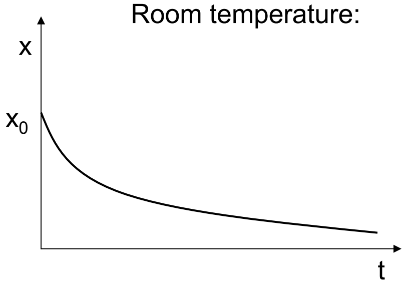
Theories of
-robustness & approximation
-probabilities & discounting

B

Continuous Dynamical Systems

State space: R^n
Dynamics: initial condition + differential equations

Room temperature: $x(0) = x_0$
$x'(t) = -K \cdot x(t)$

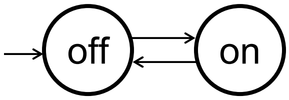


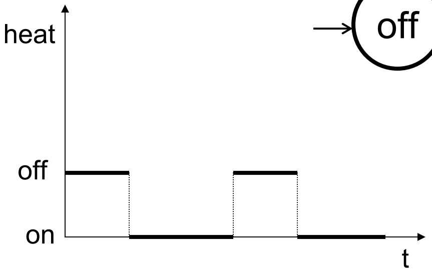
Analytic complexity.

Discrete Transition Systems

State space: B^m
Dynamics: initial condition + transition relation

Heater:

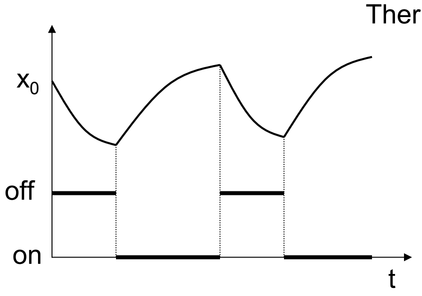




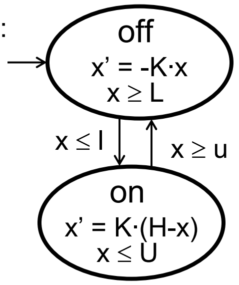
Combinatorial complexity.

Hybrid Automata

State space: $B^m \times R^n$
Dynamics: initial condition + transition relation + differential equations



Thermostat:



Four Problems with Hybrid Automata

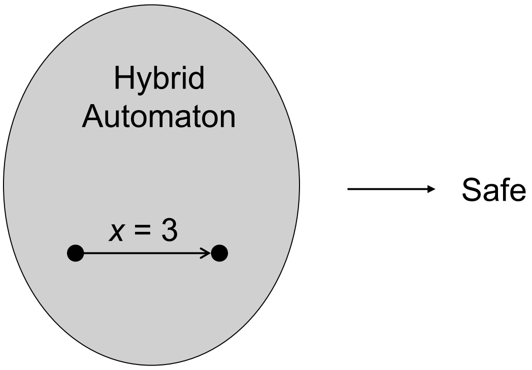
1 Robustness

2 Uncertainty

3 Compositionality

4 Computationality

The Robustness Issue

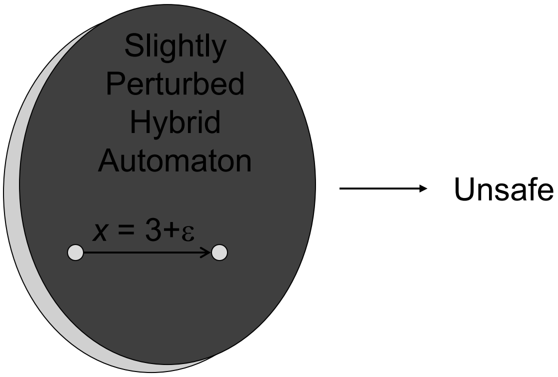


Hybrid Automaton

$x = 3$

Safe

The Robustness Issue



Slightly Perturbed Hybrid Automaton

$x = 3+\varepsilon$

Unsafe

Robust Hybrid Automata

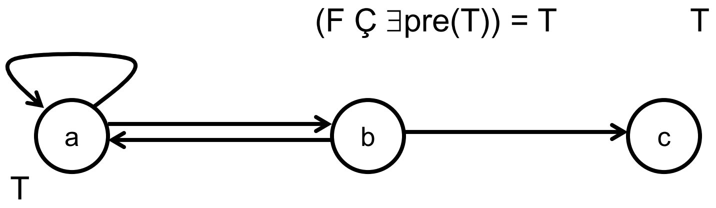
value(Model,Property): States → B

⇓

value(Model,Property): States → R

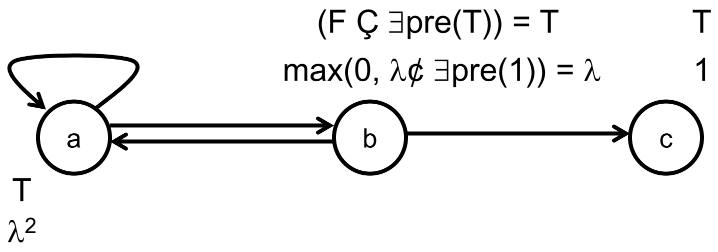
Semantics: de Alfaro, H, Majumdar [ICALP 03]
Computation: de Alfaro, Faella, H, Majumdar, Stoelinga [TACAS 04]
Metrics on models: Chatterjee et al. [submitted]

Boolean-valued Reachability



∃ ◇ c … True or False

Real-valued Reachability



∃ ◇ c … True or False

∃ $◇_\lambda$ c … between 0 and 1

discount factor 0 < λ < 1

Robust Hybrid Automata

Continuity Theorem:

If discountedBisimilarity(m_1,m_2) > 1 - ε,
then |discountedValue(m_1,p) - discountedValue(m_2,p)| < f(ε).

Further Advantages of Discounting:

-approximability because of geometric convergence (avoids non-termination of verification algorithms)

-applies also to probabilistic systems and to games (enables reasoning under uncertainty, and control)

Four Problems with Hybrid Automata

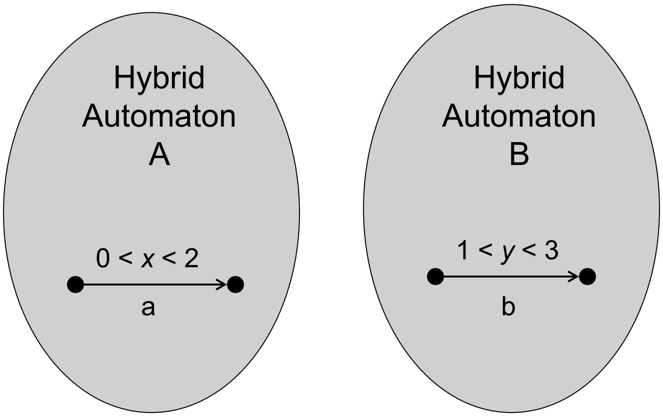
1 Robustness

2 Uncertainty

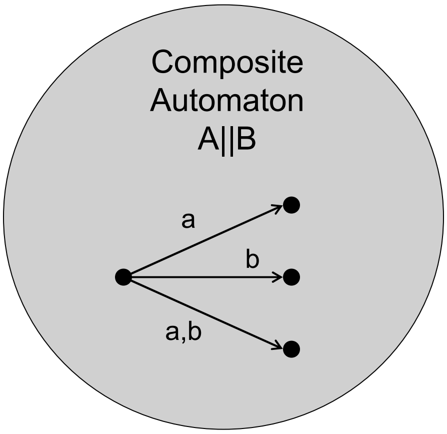
3 Compositionality

4 Computationality

The Uncertainty Issue



The Uncertainty Issue

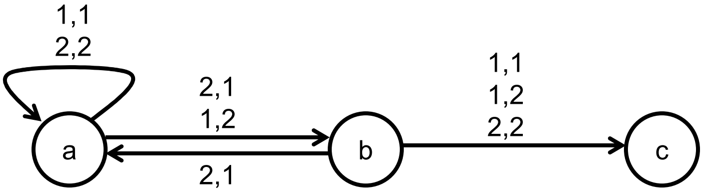


more likely

less likely

impossible

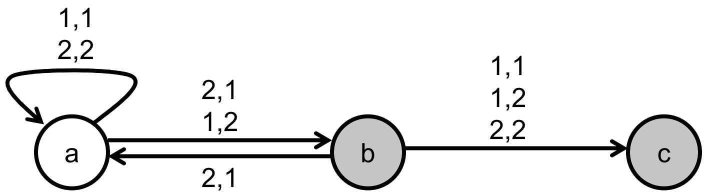
Concurrent Games



player "left"
player "right"

-for modeling component-based systems (“interfaces”)
-for strategy synthesis (“control”)

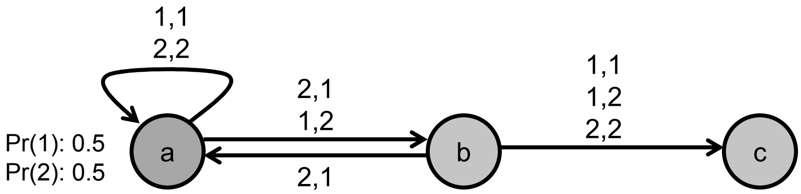
Concurrent Games



$\exists_{\text{left}} \forall_{\text{right}} \diamond c$ … player "left" has a deterministic strategy to reach c

$$\boxed{(\mu X)\ (c \vee \exists_{\text{left}} \forall_{\text{right}}\ \text{pre}(X))}$$

Concurrent Games



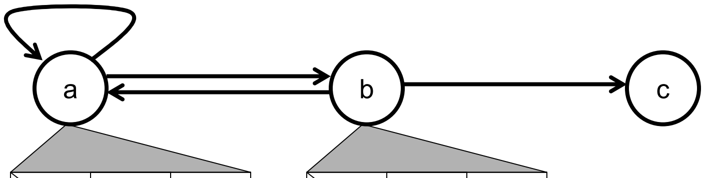
$\exists_{\text{left}} \forall_{\text{right}} \diamond c$ … player "left" has a deterministic strategy to reach c

$\cancel{\exists}_{\text{left}} \cancel{\forall}_{\text{right}} \diamond c$ … player "left" has a randomized strategy to reach c

$$\boxed{(\mu X)\ (c \vee \cancel{\exists}_{\text{left}} \cancel{\forall}_{\text{right}}\ \text{pre}(X))}$$

Stochastic Games

Probability with which player "left" can reach c ?

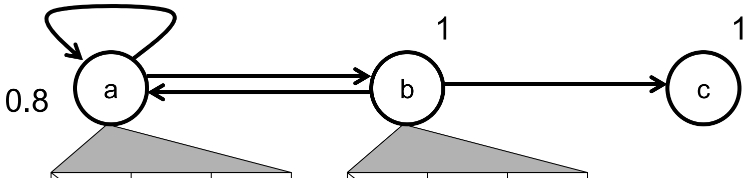


right left	1	2
1	a: 0.6 b: 0.4	a: 0.5 b: 0.5
2	a: 0.1 b: 0.9	a: 0.2 b: 0.8

right left	1	2
1	a: 0.0 c: 1.0	a: 0.0 c: 1.0
2	a: 0.7 b: 0.3	a: 0.0 b: 1.0

Stochastic Games

Probability with which player "left" can reach c ?



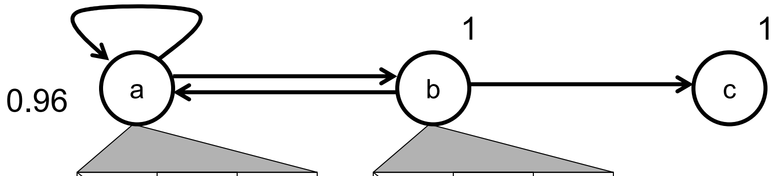
right left	1	2
1	a: 0.6 b: 0.4	a: 0.5 b: 0.5
2	a: 0.1 b: 0.9	a: 0.2 b: 0.8

right left	1	2
1	a: 0.0 c: 1.0	a: 0.0 c: 1.0
2	a: 0.7 b: 0.3	a: 0.0 b: 1.0

$$(\mu X)\ \max(c, \exists_{\text{left}} \forall_{\text{right}}\ \mathrm{pre}(X))$$

Stochastic Games

Probability with which player "left" can reach c ?



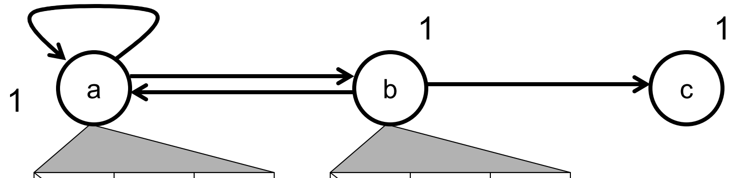
right left	1	2
1	a: 0.6 b: 0.4	a: 0.5 b: 0.5
2	a: 0.1 b: 0.9	a: 0.2 b: 0.8

right left	1	2
1	a: 0.0 c: 1.0	a: 0.0 c: 1.0
2	a: 0.7 b: 0.3	a: 0.0 b: 1.0

$$(\mu X) \max(c, \exists_{\text{left}} \forall_{\text{right}} \text{pre}(X))$$

Stochastic Games

Probability with which player "left" can reach c ?



right left	1	2
1	a: 0.6 b: 0.4	a: 0.5 b: 0.5
2	a: 0.1 b: 0.9	a: 0.2 b: 0.8

right left	1	2
1	a: 0.0 c: 1.0	a: 0.0 c: 1.0
2	a: 0.7 b: 0.3	a: 0.0 b: 1.0

Limit gives correct answer: de Alfaro, Majumdar [JCSS 04]
coNP Å NP computation: Chatterjee, de Alfaro, H [submitted]

Four Problems with Hybrid Automata

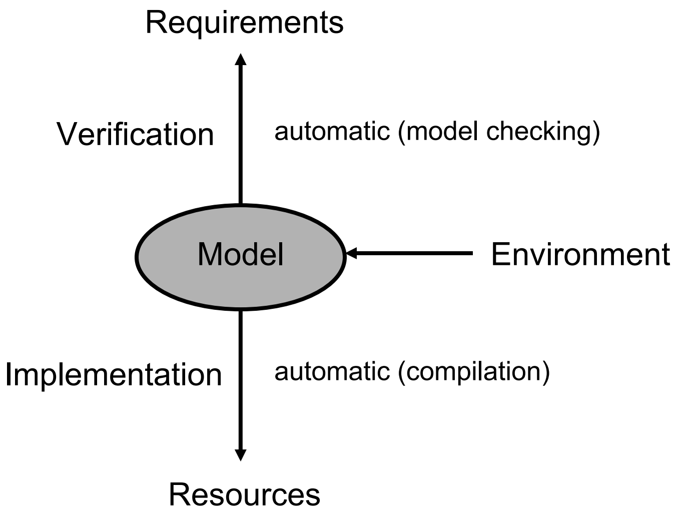
1 Robustness

2 Uncertainty

3 Compositionality

4 Computationality

The Compositionality Issue



Requirements

Verification

automatic (model checking)

Model

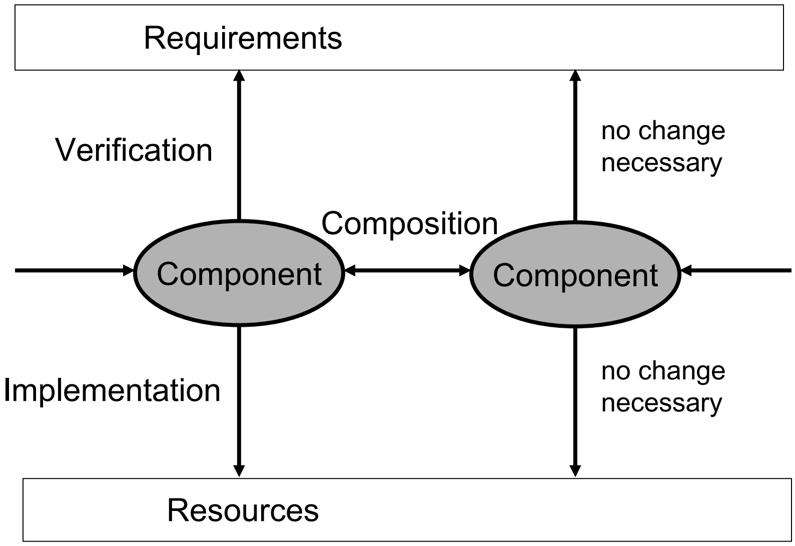
Environment

Implementation

automatic (compilation)

Resources

The Compositionality Issue



Requirements

Verification

no change necessary

Composition

Component

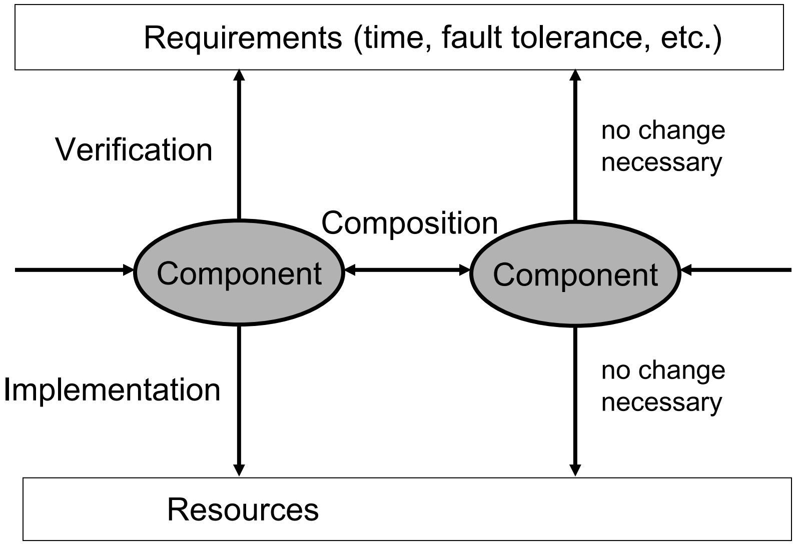
Component

Implementation

no change necessary

Resources

The Compositionality Issue



Requirements (time, fault tolerance, etc.)

Verification

no change necessary

Composition

Component

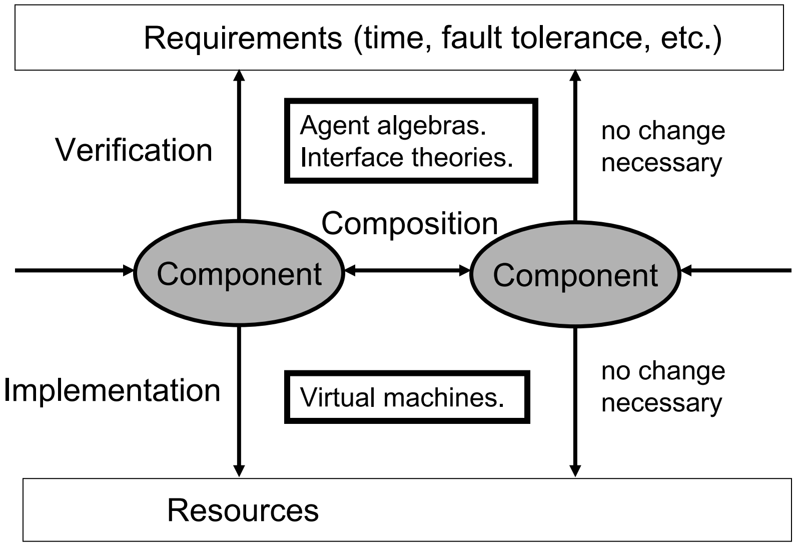
Component

Implementation

no change necessary

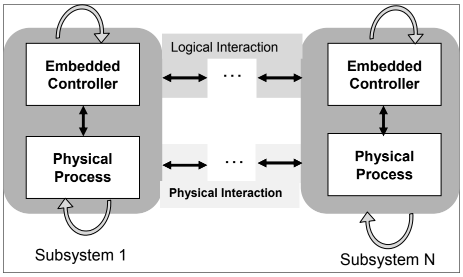
Resources

The Compositionality Issue



Heterogeneous Compositional Modeling

Consider hybrid system made up of interacting distributed subsystems:



- Physical subsystems coupled through a backbone
- Each unit includes ECDs that implement the control, monitoring, and fault diagnosis tasks
- Subsystem interactions at two levels:
  - physical – energy-based
  - logical – information based, facilitated by LANs

  Levels are not independent.

Question: *How does one systematically model the interactions between the subsystems efficiently while avoiding the computational complexity of generating global hybrid models?*

Implications: reachability analysis, design, control, and fault diagnosis

Four Problems with Hybrid Automata

1 Robustness

2 Uncertainty

3 Compositionality

4 Computationality

The Computationality Issue

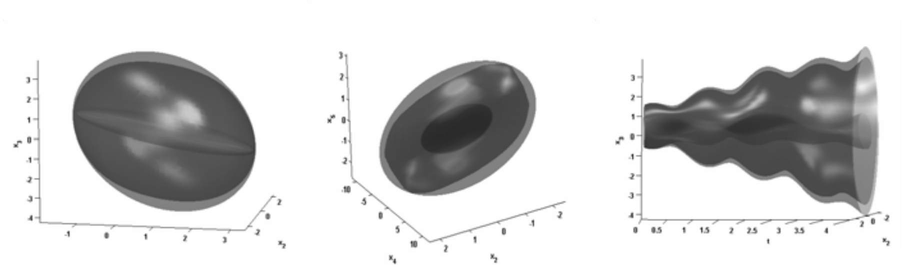
Reach Set Computation:

system $\dot{x}(t) = A(t)x(t) + B(t)u(t)$
control $u(t) \in \mathcal{P}(t)$, initial state $x(t_0) \in \mathcal{X}^0$

Find reach set $\mathcal{X}(t, t_0, X^0)$ of all states that can be reached at time *t* starting in $\mathcal{X}^0$ at t_0 using open loop control *u(t).*

Ellipsoidal Toolbox

- Calculation of reach sets using ellipsoidal approximation algorithms
- Visualization of their 3D projections



www.eecs.berkeley.edu/~akurzhan/ellipsoids

Putting It All Together

1 Robustness

2 Uncertainty

3 Compositionality

4 Computationality

Classification of 2-Player Games

- Zero-sum games: complementary payoffs.
- Non-zero-sum games: arbitrary payoffs.

1,-1	0,0
-1,1	2,-2

3,1	1,0
3,2	4,2

Classical Notion of Rationality

Nash equilibrium: none of the players gains by deviation.

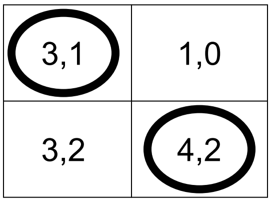
(row, column)

3,1	1,0
3,2	4,2

Classical Notion of Rationality

Nash equilibrium: none of the players gains by deviation.

(row, column)

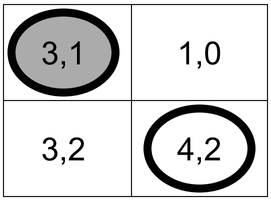


3,1	1,0
3,2	4,2

New Notion of Rationality

Nash equilibrium: none of the players gains by deviation.
Secure equilibrium: none hurts the opponent by deviation.

(row, column)



3,1	1,0
3,2	4,2

Secure Equilibria

- Natural notion of rationality for component systems:
  - First, a component tries to meet its spec.
  - Second, a component may obstruct the other components.
- For Borel specs, there is always unique maximal secure equilibrium.

Borel Games on State Spaces

Synthesis:

- Zero-sum game controller versus plant.
- Control against all plant behaviors.

Verification:

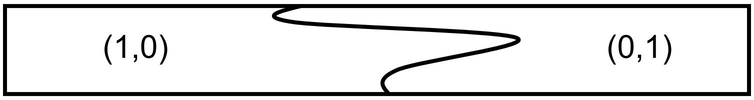
- Non-zero-sum specs for components.
- Components may behave adversarially, but without threatening their own specs.

Borel Games on State Spaces

- Zero-sum games:
  - Complementary objectives: ϕ_2 = : ϕ_1.
  - Possible payoff profiles (1,0) and (0,1).
- Non-zero-sum games:
  - Arbitrary objectives ϕ_1, ϕ_2.
  - Possible payoff profiles (1,1), (1,0), (0,1), and (0,0).

Zero-Sum Borel Games

- Winning:
  - Winning-1 states s: (9 σ) (8 π) $\Omega^{\sigma,\pi}(s)$ 2 ϕ_1.
  - Winning-2 states s: (9 π) (8 σ) $\Omega^{\sigma,\pi}(s)$ 2 ϕ_2.
- Determinacy:
  - Every state is winning-1 or winning-2.
  - Borel determinacy [Martin 75].
  - Memoryless determinacy for parity games [Emerson/Jutla 91].



Secure Equilibria

- Secure strategy profile (σ,π) at state s:

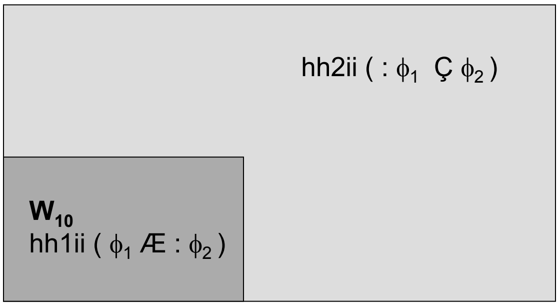
  $(8\ \pi') (\ v_1^{\sigma,\pi'}(s) < v_1^{\sigma,\pi}(s)\ )\ \ v_2^{\sigma,\pi'}(s) < v_2^{\sigma,\pi}(s)\ )$
  $(8\ \sigma') (\ v_2^{\sigma',\pi}(s) < v_2^{\sigma,\pi}(s)\ )\ \ v_1^{\sigma',\pi}(s) < v_1^{\sigma,\pi}(s)\ )$

- A secure profile (σ,π) is a contract:
  if the player-1 deviates to lower player-2's payoff,
  her own payoff decreases as well, and vice versa.

- Secure equilibrium:
  secure strategy profile that is also a Nash equilibrium.

State Space Partition

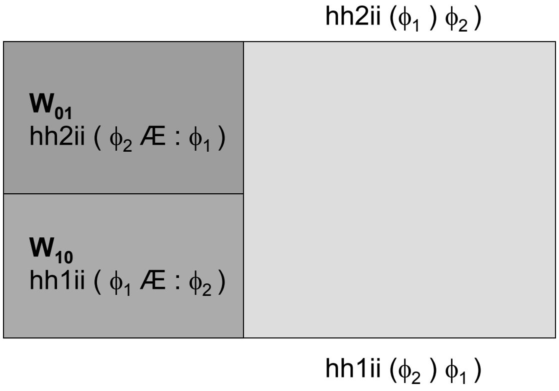
Computing the Partition



hh2ii (: ϕ_1 Ç ϕ_2)

$\mathbf{W_{10}}$
hh1ii (ϕ_1 Æ : ϕ_2)

Computing the Partition



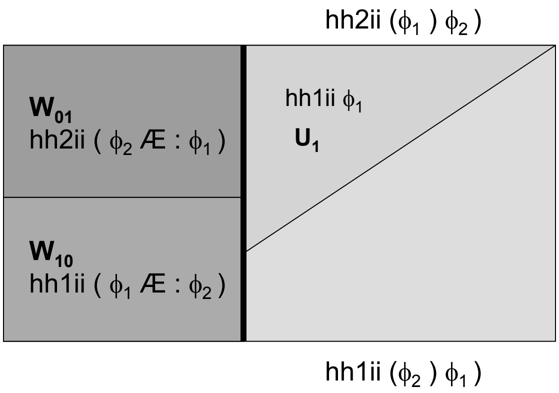
hh2ii (ϕ_1) ϕ_2)

$\mathbf{W_{01}}$
hh2ii (ϕ_2 Æ : ϕ_1)

$\mathbf{W_{10}}$
hh1ii (ϕ_1 Æ : ϕ_2)

hh1ii (ϕ_2) ϕ_1)

Computing the Partition



hh2ii (ϕ_1) ϕ_2)

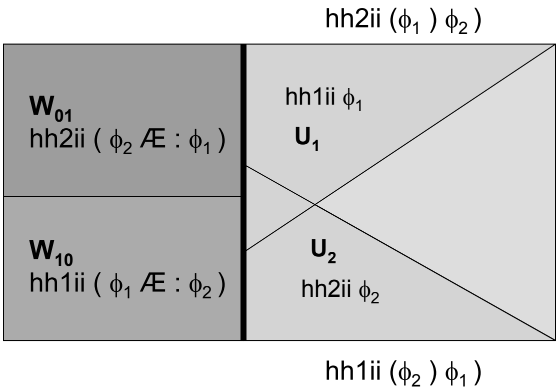
W_{01}
hh2ii (ϕ_2 Æ : ϕ_1)

W_{10}
hh1ii (ϕ_1 Æ : ϕ_2)

hh1ii ϕ_1
U_1

hh1ii (ϕ_2) ϕ_1)

Computing the Partition



hh2ii (ϕ_1) ϕ_2)

W_{01}
hh2ii (ϕ_2 Æ : ϕ_1)

W_{10}
hh1ii (ϕ_1 Æ : ϕ_2)

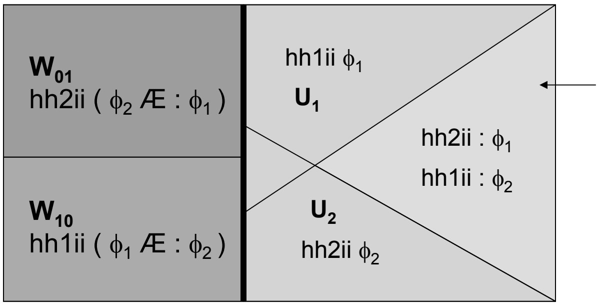
hh1ii ϕ_1
U_1

U_2
hh2ii ϕ_2

hh1ii (ϕ_2) ϕ_1)

Computing the Partition

hh2ii (ϕ_1) ϕ_2)



W_{01}
hh2ii (ϕ_2 Æ : ϕ_1)

W_{10}
hh1ii (ϕ_1 Æ : ϕ_2)

hh1ii ϕ_1
U_1

hh2ii : ϕ_1
hh1ii : ϕ_2

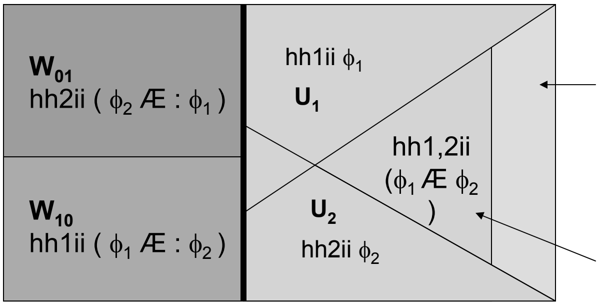
U_2
hh2ii ϕ_2

hh1ii (ϕ_2) ϕ_1)

Threat strategies
σ_T, π_T

Computing the Partition

hh2ii (ϕ_1) ϕ_2)



W_{01}
hh2ii (ϕ_2 Æ : ϕ_1)

W_{10}
hh1ii (ϕ_1 Æ : ϕ_2)

hh1ii ϕ_1
U_1

hh1,2ii
(ϕ_1 Æ ϕ_2
)

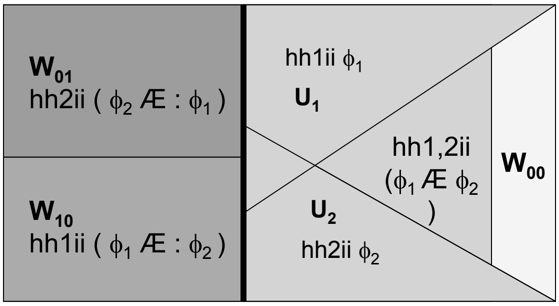
U_2
hh2ii ϕ_2

hh1ii (ϕ_2) ϕ_1)

hh1ii : ϕ_2
hh2ii : ϕ_1
Threat strategies
σ_T, π_T

Cooperation strategies
σ_C, π_C

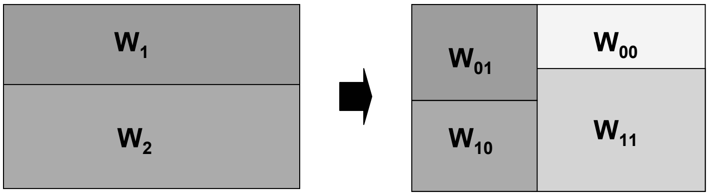
Computing the Partition



Generalization of Determinacy

Zero-sum games: ϕ_2 = :ϕ_1

Non-zero-sum games: ϕ_1, ϕ_2



Application: Compositional Verification

$$\begin{array}{l} P_1 \; 2 \; \mathbf{W_1} \; (\phi_1) \\ P_2 \; 2 \; \mathbf{W_2} \; (\phi_2) \\ \phi_1 \; \text{Æ} \; \phi_2 \;) \; \phi \\ \hline \\ P_1||P_2 \; {}^2 \; \phi \end{array}$$

Application: Compositional Verification

$$\begin{array}{l} P_1 \; 2 \; \mathbf{W_1} \; (\phi_1) \\ P_2 \; 2 \; \mathbf{W_2} \; (\phi_2) \\ \phi_1 \; \text{Æ} \; \phi_2 \;) \; \phi \\ \hline \\ P_1||P_2 \; {}^2 \; \phi \end{array}$$

$$\begin{array}{l} P_1 \; 2 \; (\mathbf{W_{10}} \; \mathbf{[} \; \mathbf{W_{11}}) \; (\phi_1) \\ P_2 \; 2 \; (\mathbf{W_{01}} \; \mathbf{[} \; \mathbf{W_{11}}) \; (\phi_2) \\ \phi_1 \; \text{Æ} \; \phi_2 \;) \; \phi \\ \hline \\ P_1||P_2 \; {}^2 \; \phi \end{array}$$

$\mathbf{W_1 \; ½ \; W_{10} \; [\; W_{11}}$

$\mathbf{W_2 \; ½ \; W_{01} \; [\; W_{11}}$

An assume/guarantee rule.

Related In-Depth Talks

Roberto Passerone (11:50 am):

-semantics of hybrid systems

Aaron Ames (12:10 pm):

-stochastic approximation of hybrid systems

-a categorical theory of hybrid systems

Related Posters

Robust Hybrid Systems:

Blowing up Hybrid Systems (Aaron Ames)
Quantitative Verification (Vinayak Prabhu)

Compositional Hybrid Systems:

Rich Interface Theories (Arindam Chakrabarti)

Stochastic Hybrid Systems:

Stochastic Games (Krishnendu Chatterjee)

Computational Hybrid Systems:

Computation of Reach Sets (Alex Kurzhansky)