Model Predictive Control from Signal Temporal Logic Specifications: A Case Study

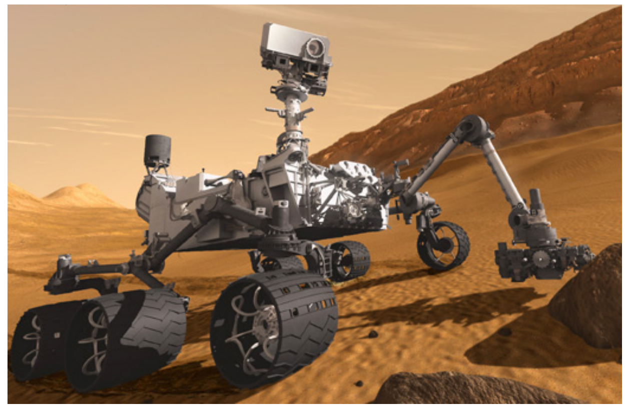
Vasu Raman[1]
Alexandre Donzé[2] and Mehdi Maasoumy[2]

[1]California Institute of Technology
[2]University of California at Berkeley

CyPhy
14 April 2014

Modern Cyber-Physical Systems

Caltech DUC vehicle



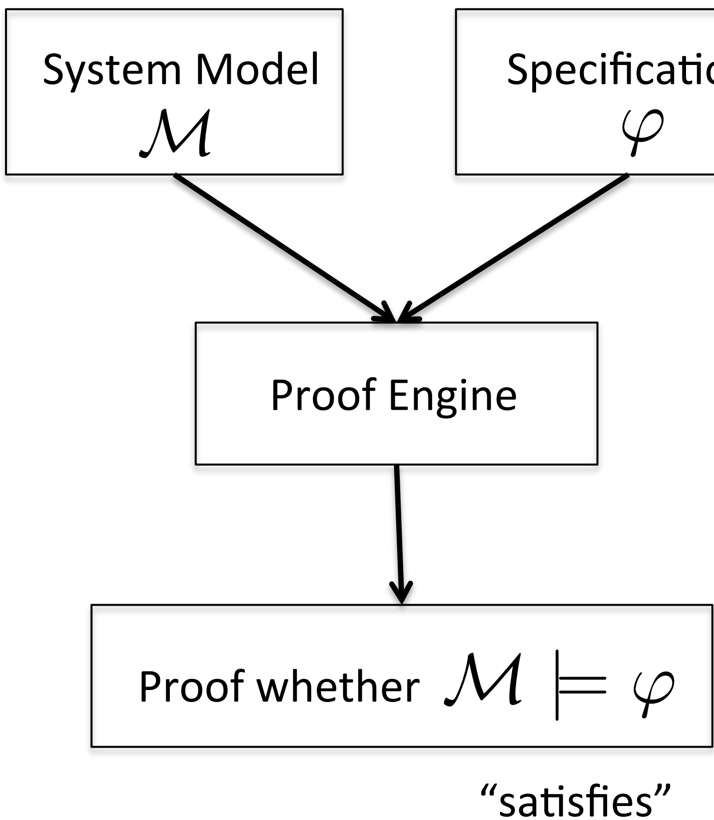
NASA/JPL-Caltech Rover

Smart Grid
(automationfederation.org)

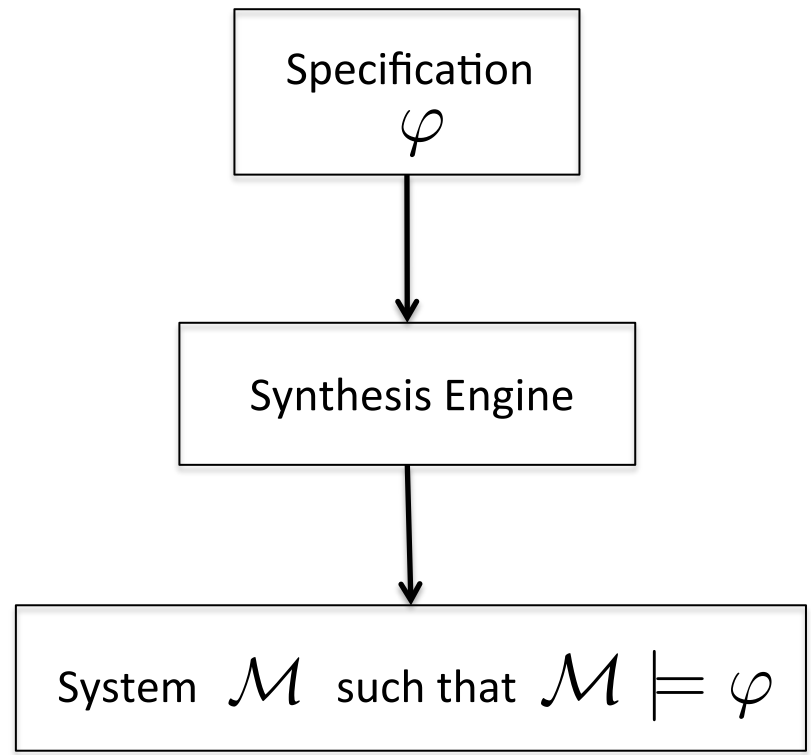
- Operate **autonomously**
- Fulfill **complex** requirements
- Easy to **specify** and **enforce** guarantees

Formal Methods: Two Perspectives

Verification



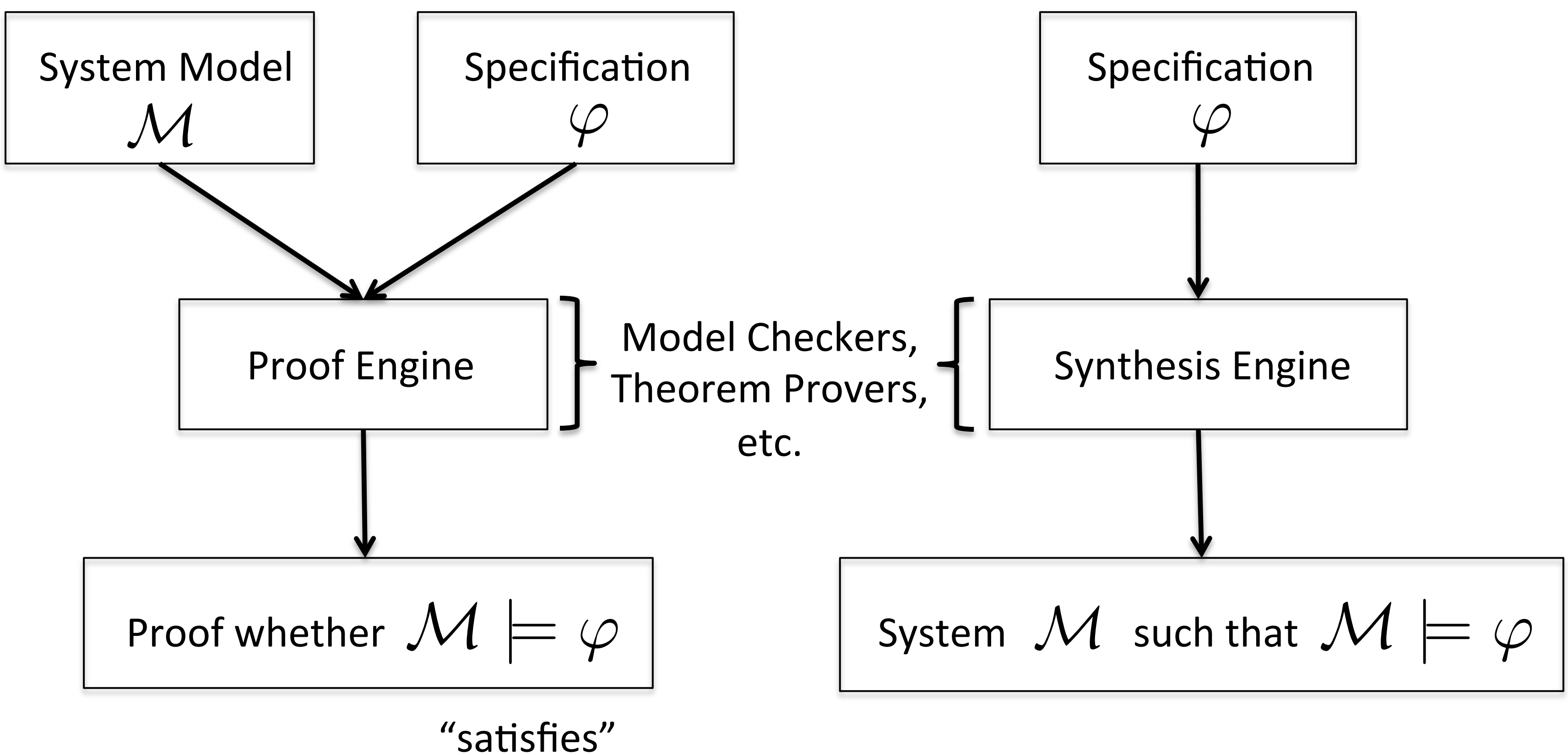
Synthesis



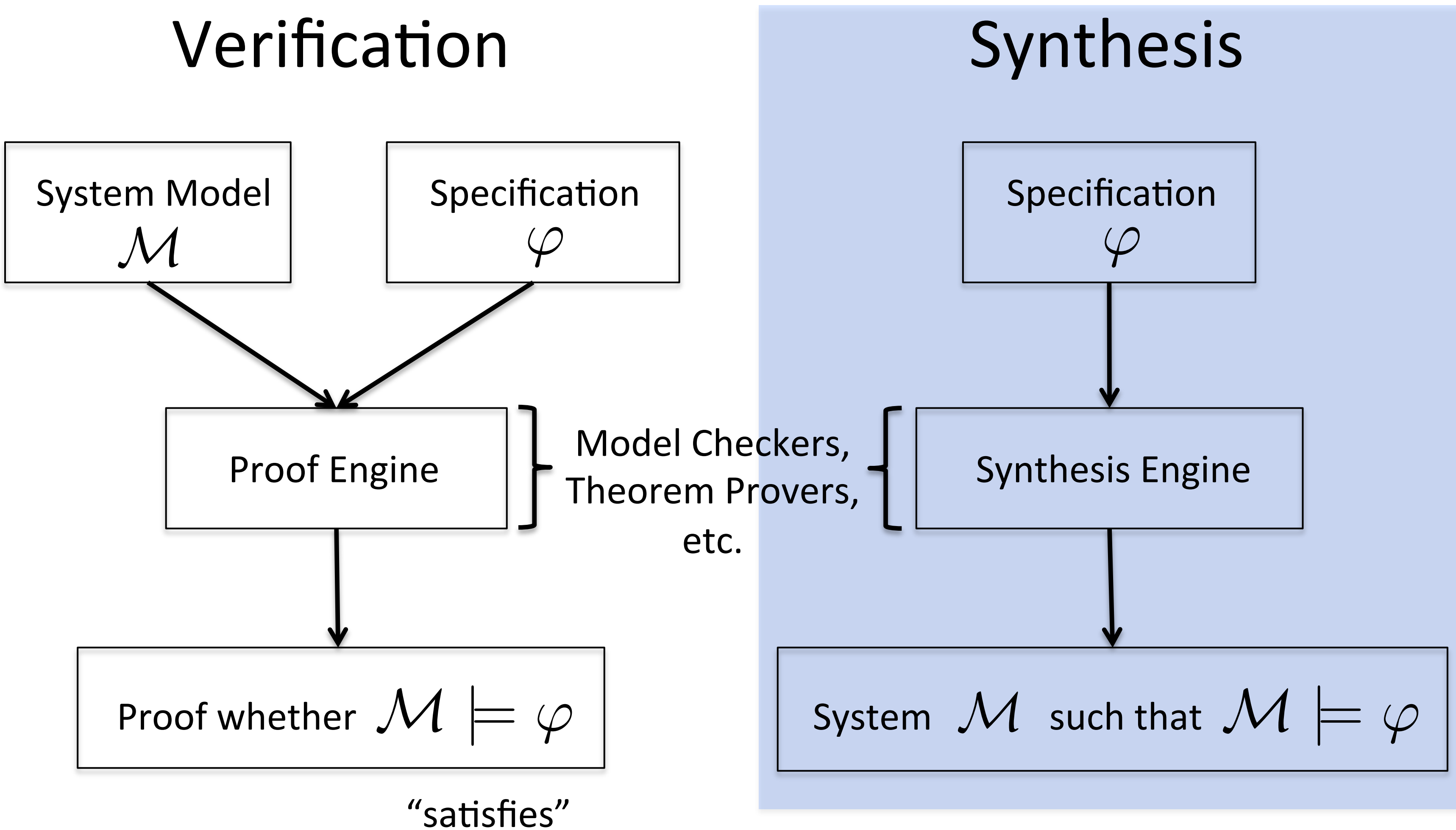
Formal Methods: Two Perspectives

Verification

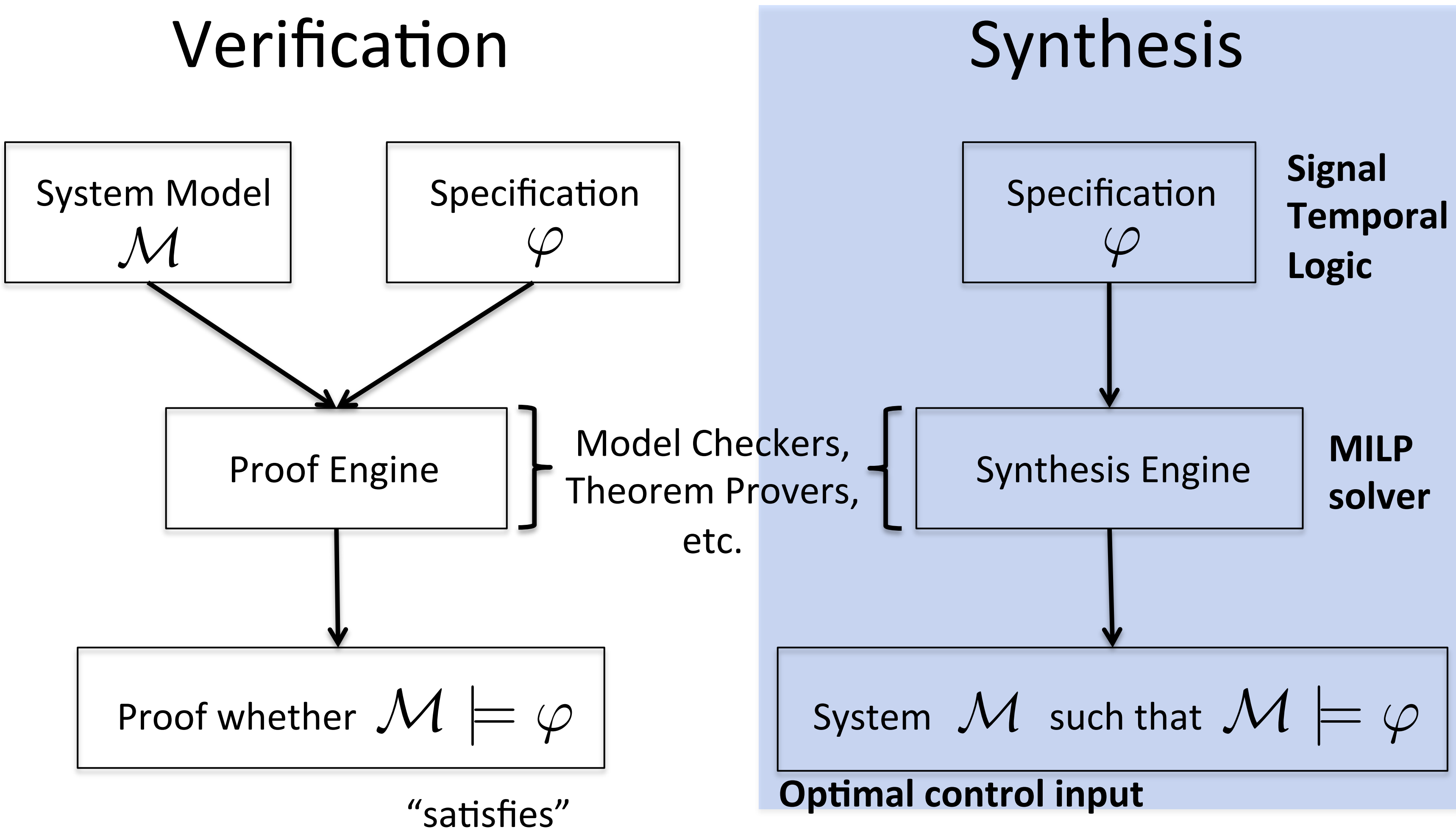
Synthesis



Formal Methods: Two Perspectives



Formal Methods: Two Perspectives



Temporal Logic Synthesis for CPS (Related Work)

- Robotics
  - Kress-Gazit, Fainekos and Pappas, ICRA 2007
  - Kloetzer and Belta, TAC 2008
  - Karaman and Frazzoli, CDC 2009
  - Bhatia, Kavraki and Vardi, ICRA 2010
- Autonomous Cars
  - Wongpiromsarn, Topcu and Murray, HSCC 2010
- Aircraft Electric Power Systems
  - Nuzzo et al, IEEE Access 2013

Temporal Logic Synthesis for CPS (what is lacking?)

- Usually requires **discrete abstraction**
  - "If temperature falls below 20°C, get it back above 20°C in the next time step"

$$\square(\text{T\_less\_than\_20} \implies \bigcirc(\neg \text{T\_less\_than\_20}))$$

Temporal Logic Synthesis for CPS (what is lacking?)

- Temporal duration is often **cumbersome**
  - "Infinitely often visit A and no more than 5 time steps later visit B"

$$\Box\Diamond(A \wedge \bigcirc B \vee \bigcirc\bigcirc B \vee \bigcirc\bigcirc\bigcirc B \vee \bigcirc\bigcirc\bigcirc\bigcirc B \vee \bigcirc\bigcirc\bigcirc\bigcirc\bigcirc B)$$

  - "All visits to A and B should be no more than 5.1s apart"

$$\Box(A \implies \Diamond(\mathrm{clock\_less\_than\_5.1} \wedge B))$$

Signal Temporal Logic (STL)

- Continuous predicates: $\mu(\mathbf{x}) > 0$
- Boolean Operators: $\wedge, \vee, \implies, \neg$
- Bounded Temporal Operators:

$\Box_{[a,b]}\varphi$ $\Diamond_{[a,b]}\varphi$ $\varphi_1 \, \mathcal{U}_{[a,b]} \, \varphi_2$

φ holds at all $t \in [a,b]$ φ holds at some $t \in [a,b]$

- Synthesis undecidable for dense time
  - We'll restrict to discrete time (but continuous systems)

Signal Temporal Logic (STL)

Syntax

$$\varphi ::= \mu \mid \neg\mu \mid \varphi \wedge \psi \mid \varphi \vee \psi \mid \Box_{[a,b]}\ \psi \mid \varphi\, \mathcal{U}_{[a,b]}\ \psi$$

$$\mu \equiv \mu(\mathbf{x}) > 0$$

Semantics

$$\begin{array}{lcl}
(\mathrm{x}, t) \models \mu & \Leftrightarrow & \mu(\mathrm{x}(t)) > 0 \\
(\mathrm{x}, t) \models \neg\mu & \Leftrightarrow & \neg((\mathrm{x}, t) \models \mu) \\
(\mathrm{x}, t) \models \varphi \wedge \psi & \Leftrightarrow & (\mathrm{x}, t) \models \varphi \wedge (\mathrm{x}, t) \models \psi \\
(\mathrm{x}, t) \models \varphi \vee \psi & \Leftrightarrow & (\mathrm{x}, t) \models \varphi \vee (\mathrm{x}, t) \models \psi \\
(\mathrm{x}, t) \models \Box_{[a,b]}\, \varphi & \Leftrightarrow & \forall t' \in [t+a, t+b], (\mathrm{x}, t') \models \varphi \\
(\mathrm{x}, t) \models \varphi\, \mathcal{U}_{[a,b]}\ \psi & \Leftrightarrow & \exists t' \in [t+a, t+b] \text{ s.t. } (\mathrm{x}, t') \models \psi \\
 & & \wedge \forall t'' \in [t, t'], (\mathrm{x}, t'') \models \varphi.
\end{array}$$

Vasu Raman (Caltech)

Examples

- If temperature falls below 20°C, get it back above 20°C within 5 time steps

$$\square(\mathrm{T\_less\_than\_20} \implies \bigcirc(\neg \mathrm{T\_less\_than\_20}))$$

- Infinitely often visit A and no more than five time steps later visit B

$$\square\Diamond(A \wedge \bigcirc B \vee \bigcirc\bigcirc B \vee \bigcirc\bigcirc\bigcirc B \vee \bigcirc\bigcirc\bigcirc\bigcirc B \vee \bigcirc\bigcirc\bigcirc\bigcirc\bigcirc B)$$

- All visits to A and B should be no more than 5.1 seconds steps apart

$$\square(A \implies \Diamond(\mathrm{clock\_less\_than\_5.1} \wedge B))$$

Examples

- If temperature falls below 20°C, get it back above 20°C within 5 time steps

$$\Box(T < 20 \implies \Diamond_{[0,5]}(T > 20))$$

- Infinitely often visit A and no more than five time steps later visit B

$$\Box\Diamond(A \wedge \Diamond_{[0,5]} B)$$

- All visits to A and B should be no more than 5.1 seconds steps apart

$$\Box(A \implies \Diamond_{[0,5.1]} B)$$

Optimal Control Synthesis from STL

Given:

Discrete time continuous system $x_{t+1} = f(x_t, u_t)$

STL specification φ

Initial state x_0

Cost function J on runs of the system

Compute:

$$\arg\min_{\mathbf{u}} \quad J(\mathbf{x}(x_0, \mathbf{u}), \mathbf{u})$$
$$\text{s.t. } \mathbf{x}(x_0, \mathbf{u}) \models \varphi$$

Model Predictive Control from STL

Given:

Discrete time continuous system $x_{t+1} = f(x_t, u_t)$

STL specification φ

Initial state x_0

Cost function J on runs of the system

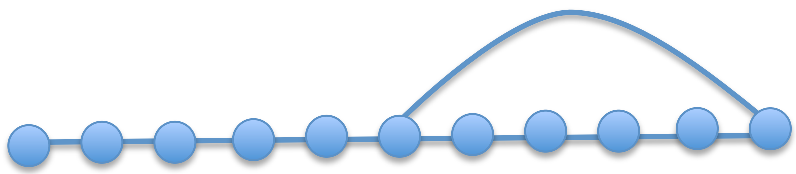
Horizon H

Compute:

$$\arg\min_{\mathbf{u}_t^H} \quad J(\mathbf{x}^H(x_t, \mathbf{u}_t^H), \mathbf{u}_t^H)$$
$$\text{s.t. } \mathbf{x}(x_0, \mathbf{u}) \models \varphi,$$

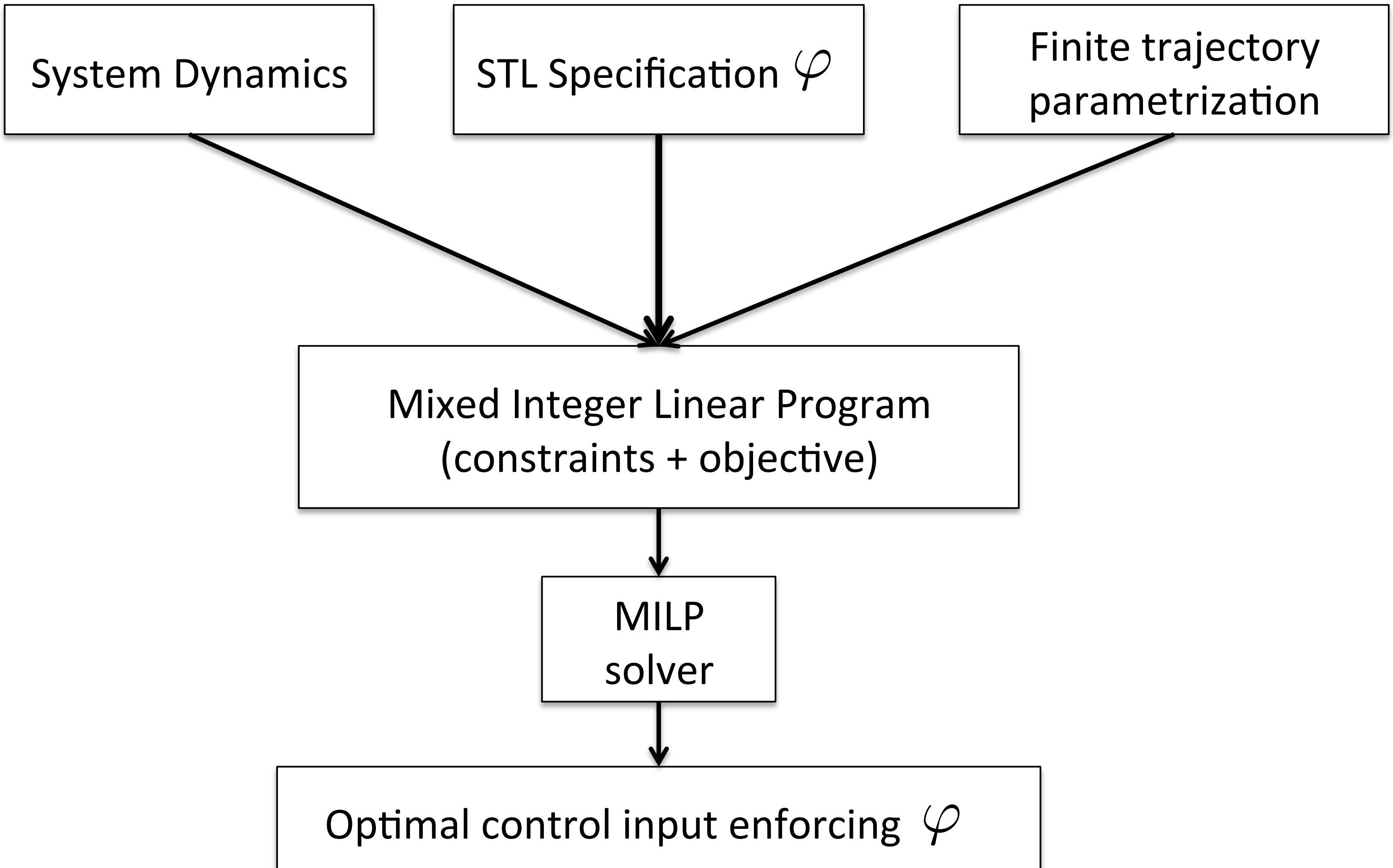
Finite Trajectory Parametrization

- Lasso-shaped parametrization for infinite executions



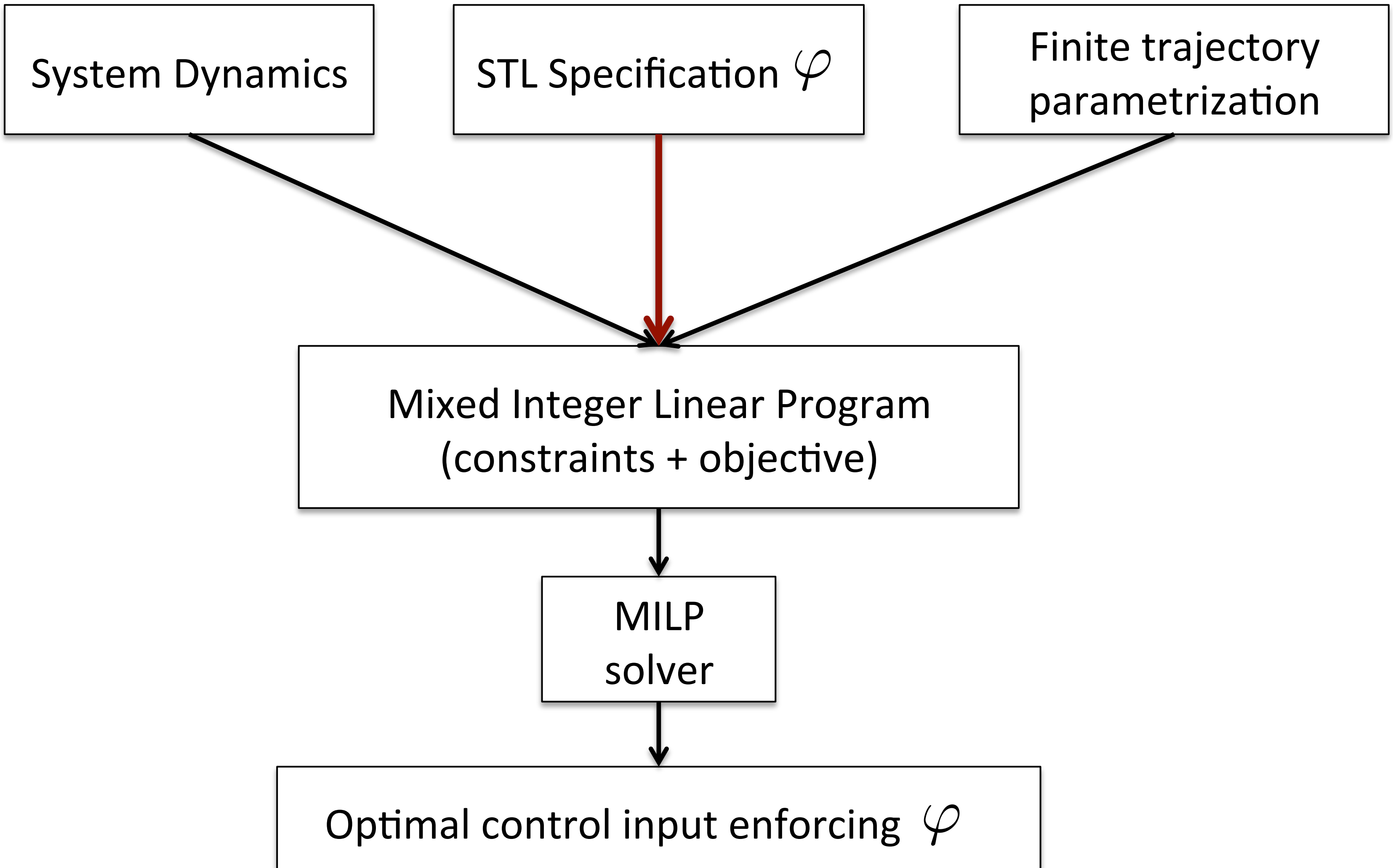
- Common approach in Bounded Model Checking

STL Synthesis for Control (Overview)



Raman et al, in submission (2014)

STL Synthesis for Control (Overview)



STL to MILP constraints

Given a formula ψ with subformulas denoted by φ

Introduce z_t^{φ}

Constrained such that $z_t^{\varphi} = 1 \Leftrightarrow (\mathbf{x}, t) \models \varphi$

Enforce $z_0^{\psi} = 1$

Recursively generate the MILP constraints corresponding to z_0^{ψ}.

STL to MILP constraints

Given a formula ψ with subformulas denoted by φ

Predicates

$$\begin{aligned} \mu(x_t) &\leq M_t z_t^{\mu} + \epsilon_t \\ -\mu(x_t) &\leq M_t(1 - z_t^{\mu}) - \epsilon_t \end{aligned}$$

Conjunction
$\psi = \wedge_{i=1}^{m} \varphi_i$

$$z_t^{\psi} \leq z_t^{\varphi_i}, i = 1, ..., m,$$
$$z_t^{\psi} \geq 1 - m + \sum_{i=1}^{m} z_t^{\varphi_i}$$

Disjunction
$\psi = \vee_{i=1}^{m} \varphi_i$

$$z_t^{\psi} \geq z_t^{\varphi_i}, i = 1, ..., m,$$
$$z_t^{\psi} \leq \sum_{i=1}^{m} z_t^{\varphi_i}$$

STL to MILP constraints

Given a formula ψ with subformulas denoted by φ

Always

$\psi = \Box_{[a,b]}\,\varphi$

$$a_t^N = \min(t+a, N),\ \ b_t^N = \min(t+b, N)$$

$$z_t^{\psi} = \vee_{i=a_t^N}^{b_t^N} z_i^{\varphi} \wedge (\vee_{j=1}^{N} l_j \wedge \wedge_{i=j+\hat{a}_t^N}^{j+\hat{b}_t^N} z_i^{\varphi})$$

Eventually

$\psi = \Diamond_{[a,b]}\,\varphi$

$$z_t^{\psi} = \wedge_{i=a_t^N}^{b_t^N} z_i^{\varphi} \wedge (\vee_{j=1}^{N} l_j \wedge \wedge_{i=j+\hat{a}_t^N}^{j+\hat{b}_t^N} z_i^{\varphi})$$

Until

$\psi = \varphi_1\ \mathcal{U}_{[a,b]}\ \varphi_2$

$$\varphi_1\ \mathcal{U}_{[a,b]}\ \varphi_2 = \Box_{[0,a]}\,\varphi_1 \wedge \Diamond_{[a,b]}\,\varphi_2 \wedge \Diamond_{[a,a]}(\varphi_1\ \mathcal{U}\ \varphi_2)$$

Quantitative Semantics for STL

- How much can we **vary the signal** and still satisfy φ
- Robustness function $\rho^{\varphi} : \mathcal{X} \times \mathbb{N} \rightarrow \mathbb{R}$

$$(\mathbf{x}, t) \models \varphi \equiv \rho^{\varphi}(\mathbf{x}, t) > 0$$

$$\begin{aligned}
\rho^{\mu}(\mathrm{x}, t) &= \mu(\mathrm{x}(t)) \\
\rho^{\neg\mu}(\mathrm{x}, t) &= -\mu(\mathrm{x}(t)) \\
\rho^{\varphi \wedge \psi}(\mathrm{x}, t) &= \min(\rho^{\varphi}(\mathrm{x}, t), \rho^{\psi}(\mathrm{x}, t)) \\
\rho^{\varphi \vee \psi}(\mathrm{x}, t) &= \max(\rho^{\varphi}(\mathrm{x}, t), \rho^{\psi}(\mathrm{x}, t)) \\
\rho^{\Box_{[a,b]}\, \varphi}(\mathrm{x}, t) &= \min_{t' \in [t+a, t+b]} \rho^{\varphi}(\mathrm{x}, t') \\
\rho^{\varphi\ \mathcal{U}_{[a,b]}\ \psi}(\mathrm{x}, t) &= \max_{t' \in [t+a, t+b]} (\min(\rho^{\psi}(\mathrm{x}, t'), \\
&\qquad \min_{t'' \in [t, t']} \rho^{\varphi}(\mathrm{x}, t'')))
\end{aligned}$$

Quantitative Semantics for STL

- How much can we **vary the signal** and still satisfy φ
- Robustness function $\rho^{\varphi} : \mathcal{X} \times \mathbb{N} \to \mathbb{R}$

$$(\mathbf{x}, t) \models \varphi \equiv \rho^{\varphi}(\mathbf{x}, t) > 0$$

- Examples: $\mu_1 \equiv x - 3 > 0 \quad \varphi = \Box_{[0,2]}\mu_1$

$$\rho^{\mu_1}(x, 0) = x(0) - 3$$
$$\rho^{\mu_1 \wedge \mu_2}(x, t) = \min(\rho^{\mu_1}, \rho^{\mu_2})$$
$$\rho^{\varphi}(x, t) = \min_{t \in [0,2]} \rho^{\mu_1}(x, t) = \min_{t \in [0,2]} x(t) - 3$$

Maximally Robust Synthesis from STL

Given:

Discrete time continuous system $x_{t+1} = f(x_t, u_t)$

STL specification φ

Initial state x_0

Robustness function $\rho^{\varphi} : \mathcal{X} \times \mathbb{N} \to \mathbb{R}$

Compute:

$$\arg\max_{\mathbf{u}} \quad \rho^{\varphi}(x_0, 0)$$
$$\text{s.t.} \ \ \mathbf{x}(x_0, \mathbf{u}) \models \varphi$$

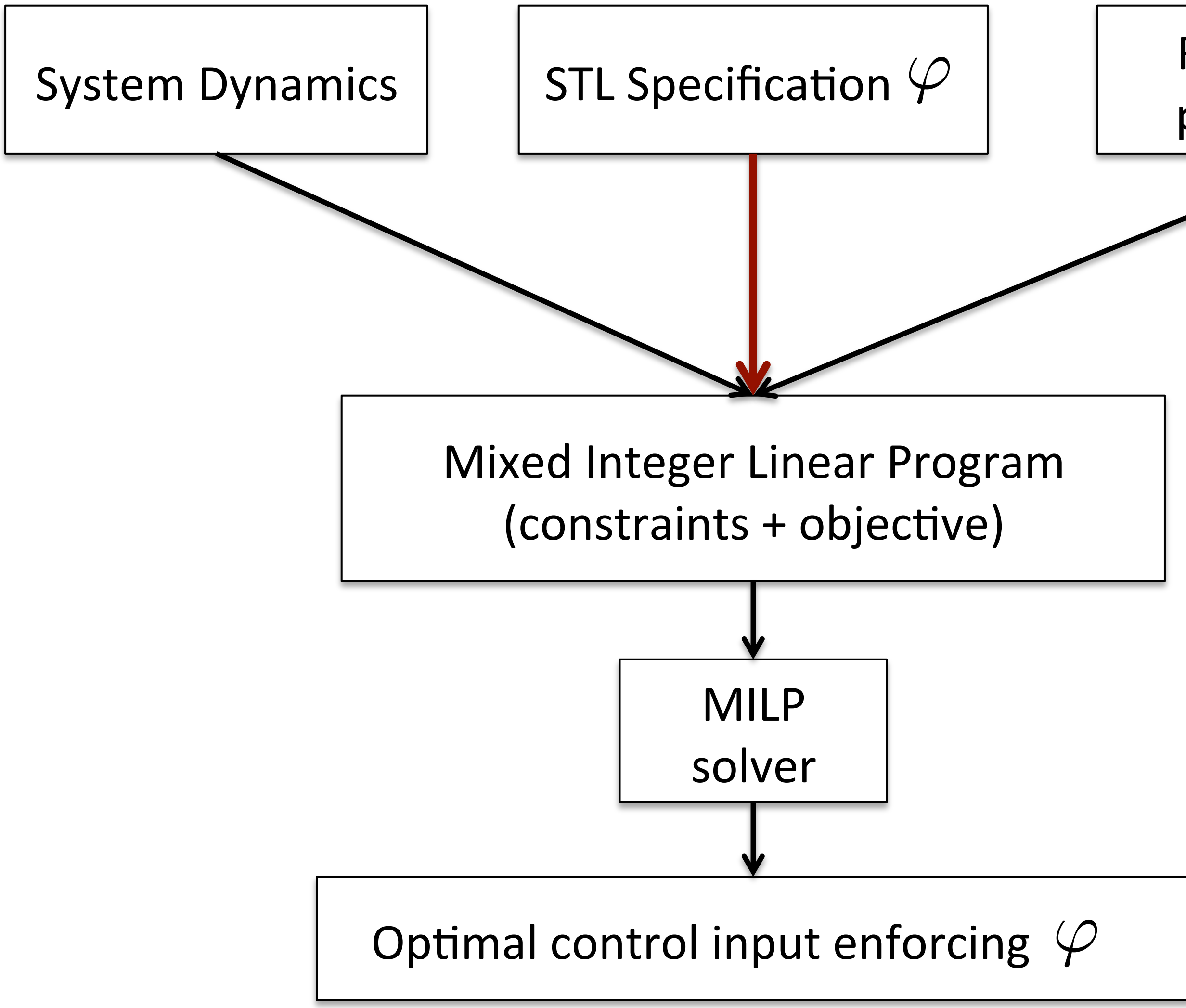
STL to MILP constraints

Given a formula ψ with subformulas denoted by φ

	Boolean encoding	Robustness encoding
Introduce	z_t^φ	r_t^φ
Constrained such that	$z_t^\varphi = 1 \Leftrightarrow (\mathbf{x}, t) \models \varphi$	$r_t^\varphi > 0 \Leftrightarrow (\mathbf{x}, t) \models \varphi$ In fact, $r_t^\varphi = \rho^\varphi(\mathbf{x}, t)$
Enforce	$z_0^\psi = 1$	$r_0^\psi > 0$

Recursively generate the MILP constraints corresponding to z_0^ψ or r_0^ψ

STL Synthesis for Control (Overview)



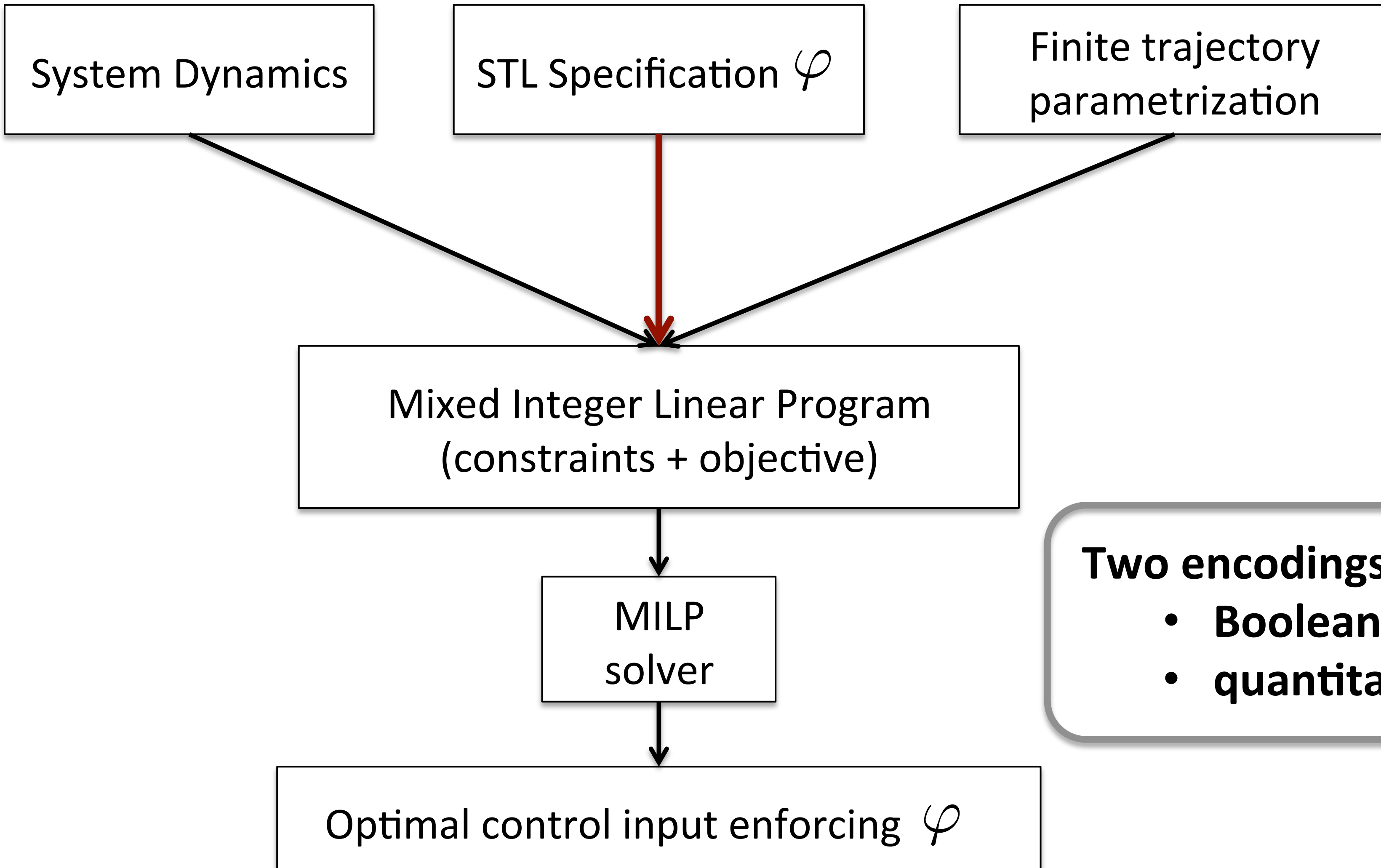
Two encodings:

- **Boolean**
- **quantitative**

Vasu Raman (Caltech)

Raman et al, in submission (2014)

STL Synthesis for Control (Overview)



Two encodings:

- **Boolean**
- **quantitative**

This is open loop…what about model predictive control?

MPC/Receding Horizon Control
(for **bounded** formulas)

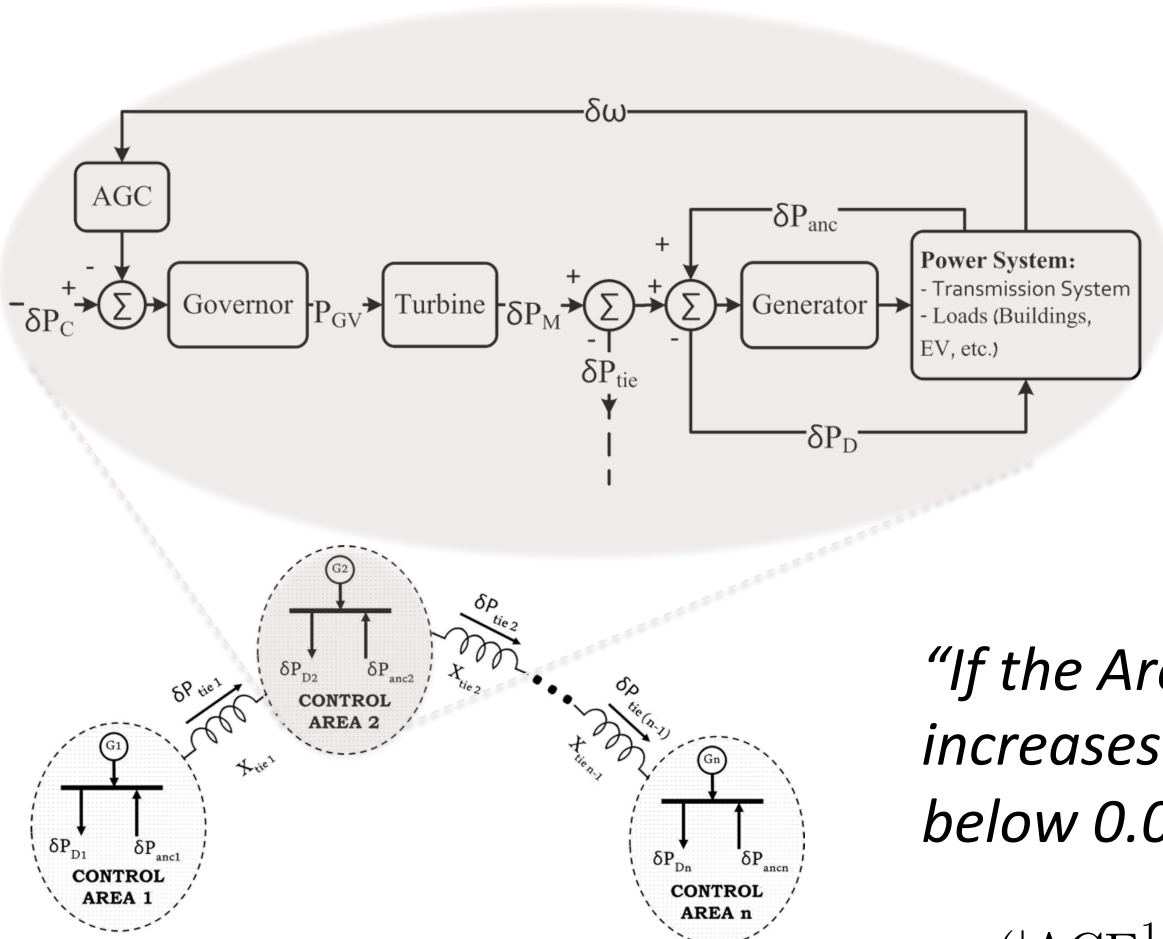
- Pick *H* based on φ
  - conservative bound on trajectory length to decide satisfiability
  - e.g. for $\Box_{[0,10]} \Diamond_{[1,6]} \varphi$ use $H \geq 10 + 6 = 16$

- Open-loop synthesis at each time step
  - STL constraints apply on the length-*H* prefix

- Store history of states and inputs
  - ensures φ is satisfied over the length-*H* prefix

- Extends to certain unbounded formulas
  - e.g. $\varphi = \Box(\varphi_{MPC})$ for bounded φ_{MPC}.

Example: Grid regulation



Controlling ancillary service power flow for grid frequency regulation

Minimize control input

subject to

"If the Area Control Error (ACE) increases above 0.01, it will decrease below 0.01 within τ time steps"

$$\varphi_t = \neg(|\mathrm{ACE}^1| < .01)) \Rightarrow (\Diamond_{[0,\tau]}(|\mathrm{ACE}^1| < .01)$$
$$\wedge\, (\neg(|\mathrm{ACE}^2| < .01)) \Rightarrow (\Diamond_{[0,\tau]}(|\mathrm{ACE}^2| < .01)$$

Example: Grid regulation

$$\min_{U_{\text{anc}}[k]} \quad J(\text{ACE}, U_{\text{anc}}) + ||x[k+H] - x_{\text{ref}}||_Q$$

$$\text{s.t.} \quad x[k+j+1] = Ax[k+j] + B_2 u_{\text{anc}}[k+j] + Ed[k+j]$$

Dynamics

$$\underline{u}_{\text{anc}} \leq u_{\text{anc}}[k+j] \leq \overline{u}_{\text{anc}}$$

$$|u_{\text{anc}}[k+j+1] - u_{\text{anc}}[k+j]| \leq \lambda$$

$$x[k+H] \in \mathcal{X}[H]$$

$$x[k] \models \varphi$$

Specification

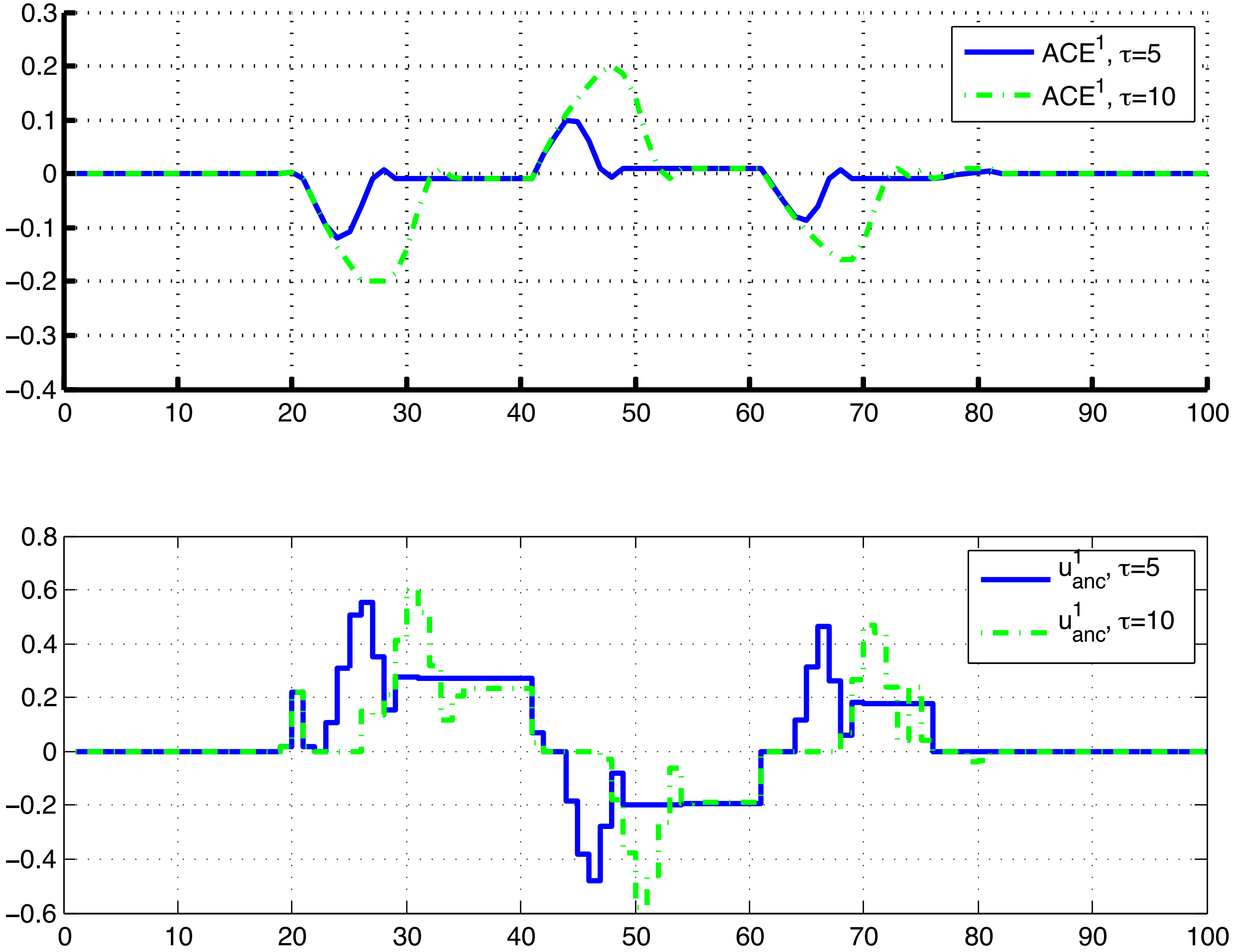
$$J(ACE, U_{\text{anc}}) = \|U_{\text{anc}}\|_{\ell_2} = \sum_{i=1}^{2} \sum_{j=0}^{H-1} (U^i_{\text{anc}}[k+j])^2$$

$$\varphi = \Box(\varphi_t)$$

$$\varphi_t = \neg(|\text{ACE}^1| < .01)) \Rightarrow (\Diamond_{[0,\tau]}(|\text{ACE}^1| < .01) \wedge(\neg(|\text{ACE}^2| < .01)) \Rightarrow (\Diamond_{[0,\tau]}(|\text{ACE}^2| < .01)$$

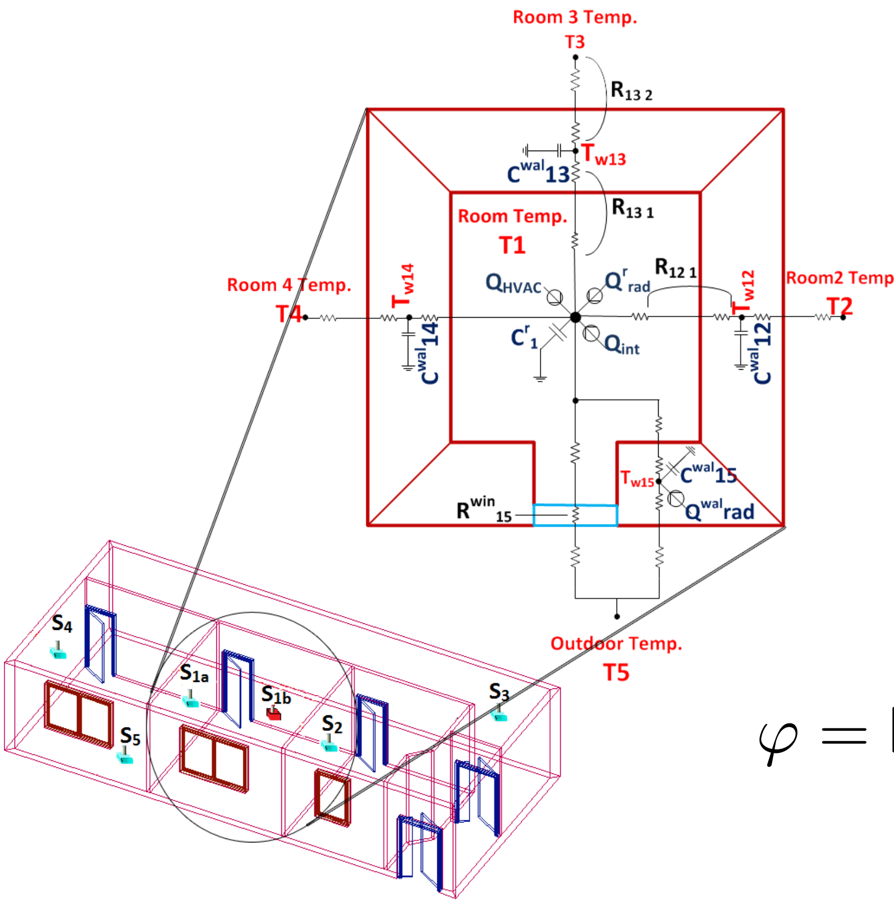
Raman et al, in submission (2014)

Example: Grid regulation



Raman et al, in submission (2014)

Example: HVAC system



Minimize the input (total air flow)

subject to

"If the occupancy of a room is > 0, the temperature should be above the comfort level"

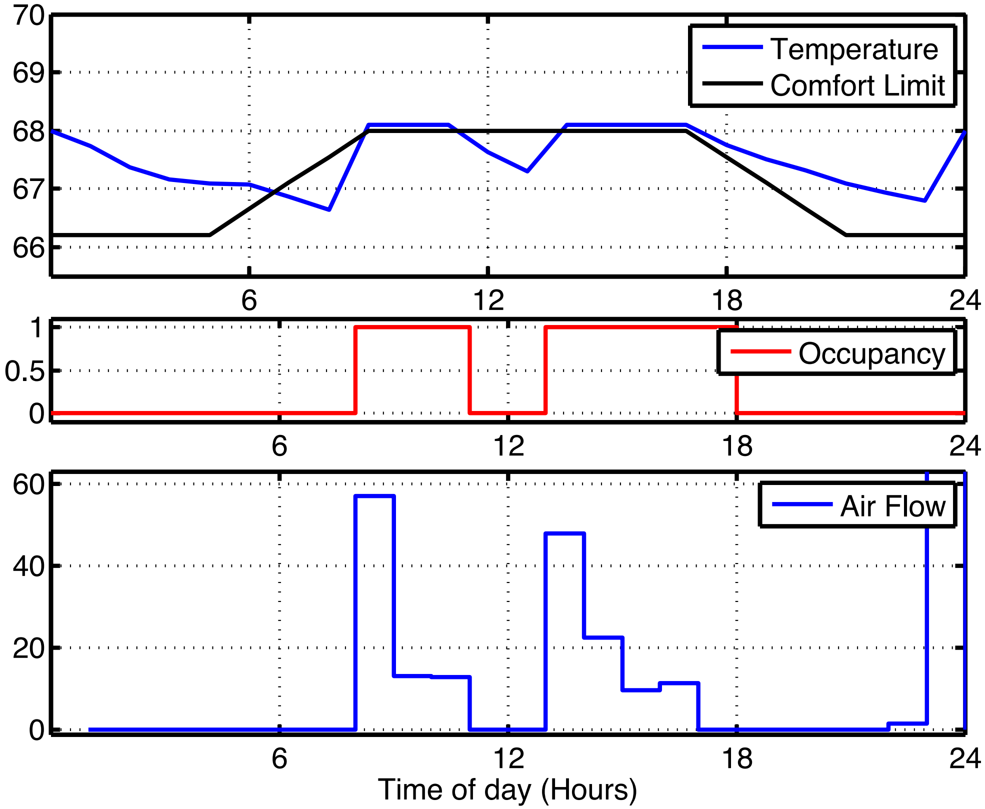
$$\varphi = \Box_{[0,H]}((\mathrm{occ}_t > 0) \Rightarrow (T_t > T_t^{\mathrm{conf}}))$$

Vasu Raman (Caltech)

Raman et al, in submission (2014)

Example: HVAC system

$$\varphi = \square_{[0,H]}((\mathrm{occ}_t > 0) \Rightarrow (T_t > T_t^{\mathrm{conf}}))$$



$$\min_{\vec{u}_t} \sum_{k=0}^{H-1} \|u_{t+l}\| \text{ s.t.}$$

$$x_{t+k+1} = f(x_{t+k}, u_{t+k}, d_{t+k}),$$

$$x_t \models \varphi$$

$$u_{t+k} \in \mathcal{U}_{t+k}, \; k = 0, \ldots, H-1$$

Raman et al, in submission (2014)

Future Work

- Receding Horizon framework for unbounded STL properties
  - ties to online monitoring of STL properties
  - formalize connection with reactive synthesis

- Contract-based framework for specifying and designing components (e.g. of the smart-grid) and their interactions

Thank You!

Model Predictive Control from Signal Temporal Logic Specifications: A Case Study

Vasu Raman[1]

Alexandre Donzé[2] and Mehdi Maasoumy[2]

[1]California Institute of Technology

[2]University of California at Berkeley

Email: vasu@caltech.edu