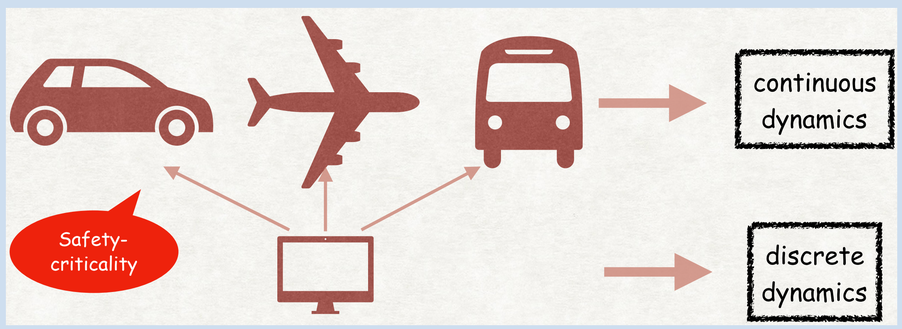
Stochastic Optimization based Hybrid System Falsification

Zhenya Zhang
zhangzy@nii.ac.jp
National Institute of Informatics, Tokyo, Japan
The Graduate University for Advanced Studies (SOKENDAI), Hayama, Japan

Quality assurance of Cyber-Physical Systems



Why falsification?

- Verification based on system exploration is infeasible because of infinite state space.
- Testing which aims at a counterexample refuting the specification is more suited.

The advantages of falsification:

- Aims at one counterexample, much easier and more feasible than verification.
- Be able to handle black-box model, no need to know the dynamics.
- Rely on optimization techniques, more intelligent than random sampling.

Falsification problem

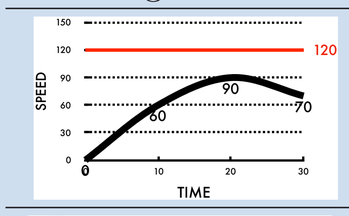
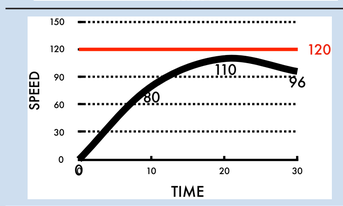
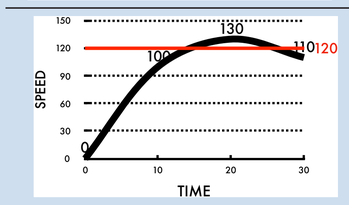
Falsification problem is defined as follows:

- **Given:** a *Simulink* model $\mathcal{M}$ or other black box, and a *specification* φ in Signal Temporal Logic (STL)
- **Answer:** *error input*, i.e., an input signal $\mathbf{u}$ such that the corresponding output $\mathcal{M}(\mathbf{u})$ violates φ

$$\xrightarrow{\mathbf{u}} \boxed{\mathcal{M}} \xrightarrow{\mathcal{M}(\mathbf{u}) \\ \not\models \varphi\,?}$$

Signal Temporal Logic (STL)

STL is used for formalizing system requirements, like safety or comfort concerns
E.g., $\varphi \equiv \square_{[0,30]}(speed[t] < 120)$

signal $\mathbf{w}$	$\mathbf{w} \models \varphi$	$[\![\mathbf{w}, \varphi]\!]$
	TRUE	30
	TRUE	10
	FALSE	-10

Optimization approach

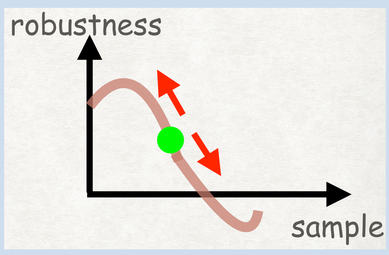
Objective function:

$$\min_{\mathbf{u}} [\![\mathcal{M}(\mathbf{u}), \varphi]\!]$$

Constraints:

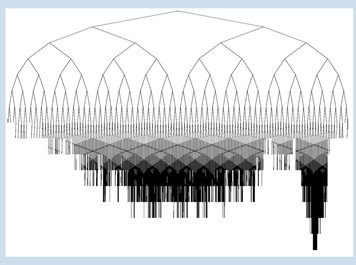
- $\mathbf{u}$ is bounded
- Constraints from domain knowledge.

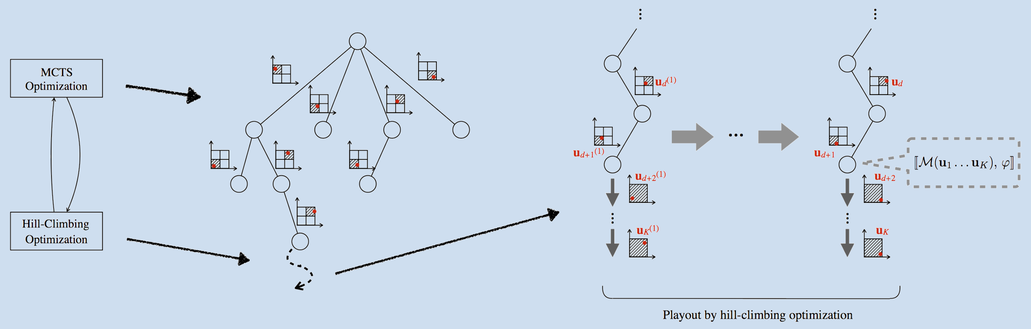
"Hill-climbing" Optimization



- Make use of the history sampling.
- Derivative free.
- Successful applications:
  - Breach (CMA-ES, NM, etc.)
  - S-TaLiRo (SA, etc.)

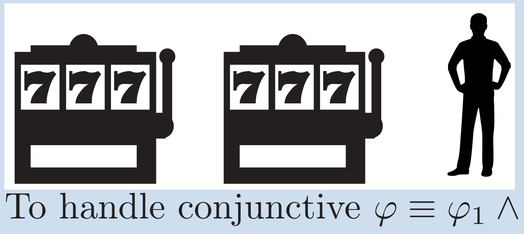
Work 1: Monte Carlo Tree Search for Global Optimum





- Time-staging. Divide the time bound into K intervals to find a sequence $\mathbf{u}_1, \ldots, \mathbf{u}_K$.
- Node expansion. Use a *partitioning* of the input space $I_1 \times \cdots \times I_M$ as the children set A.
- Child selection. Define that $reward = 1 - \frac{R(wa)}{\max_{w' \in \mathcal{T}} R(w')}$, and apply UCB1 algorithm $\arg\max_{a \in A} \left(reward + c\sqrt{\frac{2 \ln N(w)}{N(wa)}} \right)$ to select the best child.
- Simulation. Apply optimization solvers in the selected sub-region sequence with time budget.
- Backpropagation. Update the reward of parent if the newly computed reward is better.

Work 2: Multi-armed Bandits for Boolean Connectives



$$[\![\mathbf{w}, f(x_1, \cdots, x_n) > 0]\!] := f\big(\mathbf{w}(0)(x_1), \cdots, \mathbf{w}(0)(x_n)\big)$$
$$[\![\mathbf{w}, \bot]\!] := -\infty \qquad [\![\mathbf{w}, \neg\varphi]\!] := -[\![\mathbf{w}, \varphi]\!]$$
$$[\![\mathbf{w}, \varphi_1 \wedge \varphi_2]\!] := [\![\mathbf{w}, \varphi_1]\!] \sqcap [\![\mathbf{w}, \varphi_2]\!] \qquad [\![\mathbf{w}, \varphi_1 \vee \varphi_2]\!] := [\![\mathbf{w}, \varphi_1]\!] \sqcup [\![\mathbf{w}, \varphi_2]\!]$$
$$[\![\mathbf{w}, \varphi_1 \,\mathcal{U}_I\, \varphi_2]\!] := \bigsqcup_{t \in I \cap [0,T]} \big([\![\mathbf{w}^t, \varphi_2]\!] \sqcap \bigsqcap_{t' \in [0,t)} [\![\mathbf{w}^{t'}, \varphi_1]\!] \big)$$

To handle conjunctive $\varphi \equiv \varphi_1 \wedge \varphi_2$

- It suffices to falsify either $[\![\mathcal{M}(\mathbf{u}), \varphi_1]\!]$ or $[\![\mathcal{M}(\mathbf{u}), \varphi_2]\!]$
- Apply algorithms for MAB, such as UCB1, ϵ-greedy, to alternatively optimize $[\![\mathcal{M}(\mathbf{u}), \varphi_1]\!]$ and $[\![\mathcal{M}(\mathbf{u}), \varphi_2]\!]$
- The reward is defined as
$$\frac{\mathsf{max\text{-}rb}(i, k-1) - \mathsf{last\text{-}rb}(i, k-1)}{\mathsf{max\text{-}rb}(i, k-1)}$$

To handle disjunctive $\varphi \equiv \varphi_1 \vee \varphi_2$:

- In this case, it is not sufficient to falsify only $[\![\mathcal{M}(\mathbf{u}), \varphi_1]\!]$ or $[\![\mathcal{M}(\mathbf{u}), \varphi_2]\!]$
- $[\![\mathcal{M}(\mathbf{u}), \varphi_i]\!]_S$ is defined as $\mathcal{S} = \{\, t \in I \cap [0,T] \mid [\![\mathcal{M}(\mathbf{u}^t), \varphi_{\bar{i}}]\!] < 0 \,\}$
- Similarly, we apply MAB algorithms to alternatively optimize $[\![\mathcal{M}(\mathbf{u}), \varphi_1]\!]_S$ and $[\![\mathcal{M}(\mathbf{u}), \varphi_2]\!]_S$
- The reward is defined accordingly.

Case Study 1

$\varphi \equiv \square_{[0,30]}(rpm < 4770 \vee \square_{[0,1]}(rpm > 600))$
Comment The property states that when the RPM is over 4770, it should not drop drastically to 600 within 1 second.
Comparison with Breach

	FR	time (s)
Breach	3/10	75.5
P.A.	9/10	384.4

Discussion For the falsification rate, our proposed approach is better than Breach; for the time consumption, our approach takes longer than Breach, which is reasonable since MCTS takes more efforts on exploration.

Case Study 2

$\varphi \equiv \square_{[0,30]}(gear[t] = 4 \rightarrow speed[t] > 35)$
Comment The property states that when the gear is 4, the speed of the car should not be too slow, say, below 35.
Comparison with Breach

	FR	time (s)
Breach	11/30	28.9
P.A.	29/30	41.7

Discussion Breach here suffers from the problem in Work 2, since it can falsify the property within short time, but not very often. The proposed approach solves the problem and thus increase the falsification rate.

References

- Zhang, Z., Ernst, G., Sedwards, S., Arcaini, P., & Hasuo, I. (2018). Two-layered falsification of hybrid systems guided by monte carlo tree search. International Conference on Embedded Software (EMSOFT 2018). Published in a special issue of IEEE Trans. on CAD of Integrated Circuits and Systems.
- Zhang, Z., Hasuo, I., Arcaini, P. (2019). Multi-Armed Bandits for Boolean Connectives in Hybrid System Falsification. 31st International Conference on Computer-Aided Verification (CAV) 2019.

Acknowledgements

This work is supported by ERATO HASUO Metamathematics for Systems Design Project (No. JPMJER1603), Japan Science and Technology Agency.