Semi-formal Validation of Cyber-Physical Systems

Thao Dang [2]

Collaborators: Arvind Adimoolam [1], Alexandre Donzé [3], James Kapinski [4], Xiaoqing Jin [5]

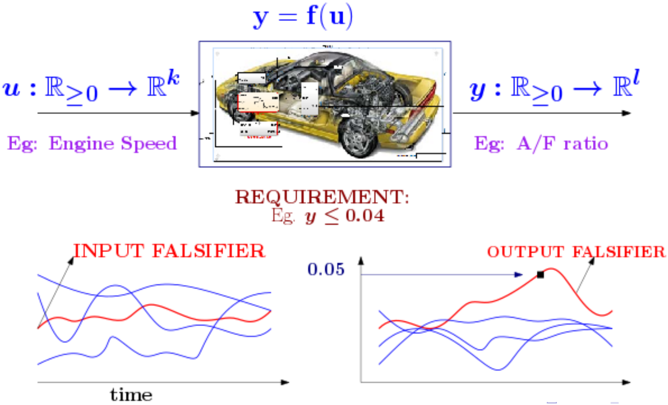
[1,2]VERIMAG/ [2]CNRS
Grenoble, France

[3]Decyphir, Inc, France

Toyota Motors North America R&D, USA.

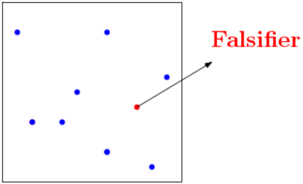
Semi-formal Validation of CPS - Testing with Quantitative Guarantees

- **Falsification**: Find input signal so that output violates requirement.
- **Coverage**: measure to evaluate testing quality. When no bug is found, this allows quantifying the "correctness degree" of the system.



Validation of CPS

- CPS models: Specification of Input-Output function f can be highly complex. Eg. [Differential Equations + Automata + Look-up tables + Delays + Control Programs].
- Black-box systems: Testing with knowing a model f of the system under test, i.e. only by sampling input signals.



Robustness - Quantitative Guarantee

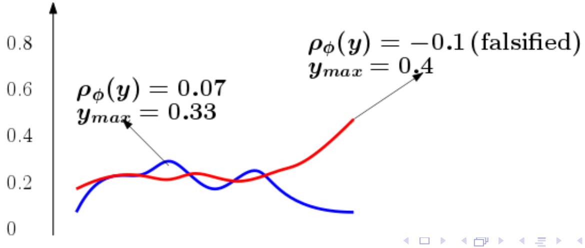
- Quantitative semantics: A function ρ measures extent of satisfifaction of a formal specification ϕ by output y.

$$\boldsymbol{y \rightarrow \rho_\phi(y)}$$

- Robustness of STL formulas. Eg, given $\phi : \square(y \leq 0.04)$,

$$\rho_\phi(y) = max_{t\geq 0} 0.4 - y(t)$$

- $(\text{Robustness} < 0) \Rightarrow$ Falsified.



Robustness

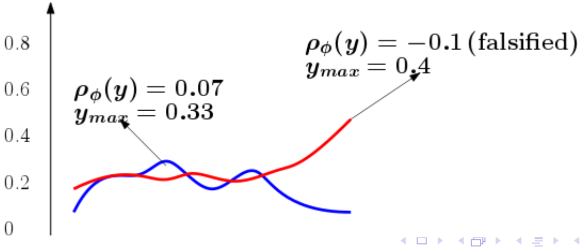
- Quantitative semantics: A function ρ measures extent of satisfifaction of a formal specification ϕ by output y.

$$\boldsymbol{y \rightarrow \rho_\phi(y)}$$

- Robustness of STL formulas. Eg, given $\phi : \Box(y \leq 0.04)$,

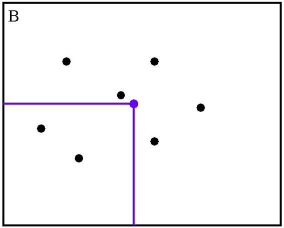
$$\rho_\phi(y) = max_{t \geq 0} 0.04 - y(t)$$

- (Robustness < 0) $\Rightarrow$ Falsified.



Coverage - Star Discrepancy

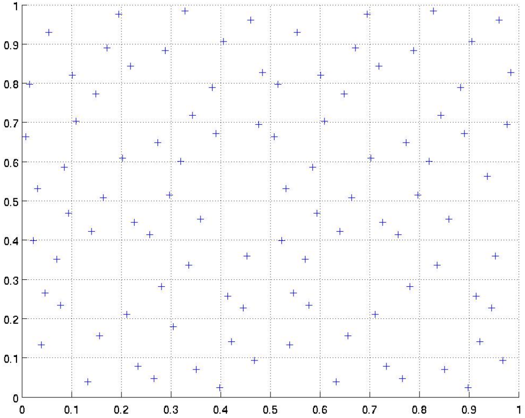
Star Discrepancy



- Let P be a **set of k points** inside $B = [l_1, L_1] \times \ldots \times [l_n, L_n]$.
- **Local discrepancy**: $D(P, J) = |\frac{\#(P, J)}{k} - \frac{vol(J)}{vol(B)}|$. Example:

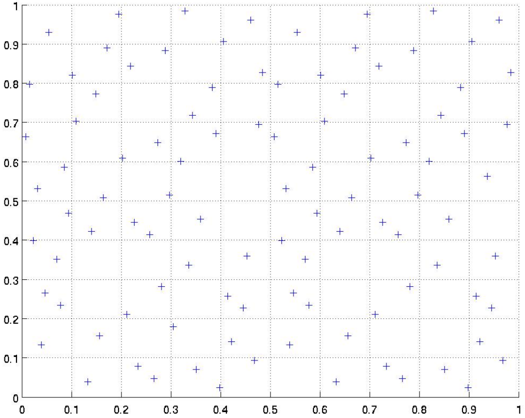
  $D(P, \mathbf{J}) = |\frac{\mathbf{2}}{\mathbf{7}} - \frac{\mathbf{1}}{\mathbf{4}}|$
- **Discrepancy**: supremum of local discrepancy values of all sub-boxes

Coverage - Star Discrepancy



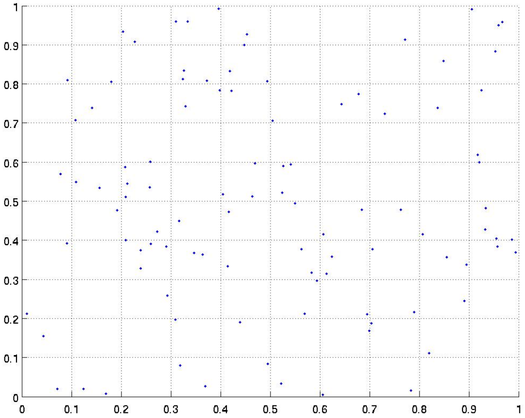
Faure sequence of 100 points. Its star discrepancy value is 0.048.

Coverage - Star Discrepancy



Halton sequence of 100 points. The star discrepancy value is 0.05.

Coverage - Star Discrepancy

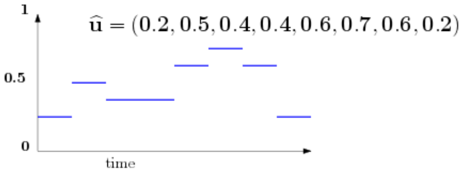


Sequence of 100 points generated by a **pseudo-random function in the C library**. Its star discrepancy value is 0.1.

From Points to Signals

- Actual input signal space is INFINITE DIMENSIONAL, but we may search on a Finite Dimensional Space.
- For example, a uniform step signal in a bounded time horizon can be represented by a finite set of parameters.

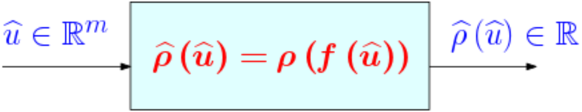
$$u \to \widehat{u} \in \mathbb{R}^m$$



- Extension to signals satisfying some temporal properties (STL)

Falsification as Optimization

1. Define new robustness function on parametrized input space.



2. Falsification:

$$\min_{\widehat{u} \in (S \subset \mathbb{R}^m)} \widehat{\rho}_\phi(\widehat{u}) < 0$$

Testing as Optimization

1. Define new robustness function on the parametrized input space.

$$\widehat{u} \in \mathbb{R}^m \longrightarrow \boxed{\widehat{\rho}\left(\widehat{u}\right) = \rho\left(f\left(\widehat{u}\right)\right)} \longrightarrow \widehat{\rho}\left(\widehat{u}\right) \in \mathbb{R}$$

2. Falsification:

$$\min_{\widehat{u} \in (S \subset \mathbb{R}^m)} \widehat{\rho}_\phi\left(\widehat{u}\right) < 0$$

3. Good coverage over input signal space or state space

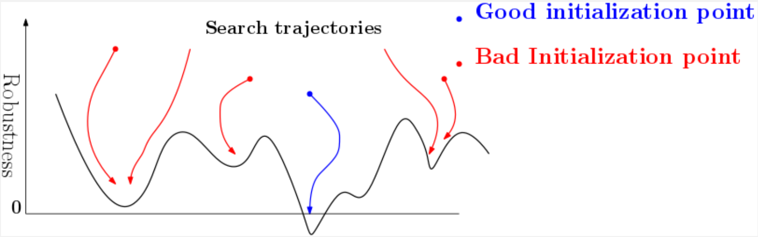
Testing as Optimization

- **Randomized** exploration, inspired by probabilistic **motion planning** techniques **RRT** (Random Rapidly-Exploring Trees) in robotics. **Guided** by coverage criteria
- **Classification + black-box search**

Sensitivity to Initial search Conditions

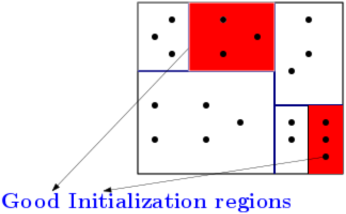
- Common black-box search approaches Bias Sampling towards local optimum, generally called *stochastic local search techniques.* Eg. Simulated Annealing, CMA-ES, Nelder-Mead, etc.

- Local Search Effectiveness is Sensitive to Initial conditions.



Problem: Find good Initialization Conditions

1. Global search: Find well separated regions of search space that are likely to contain a falsifier.



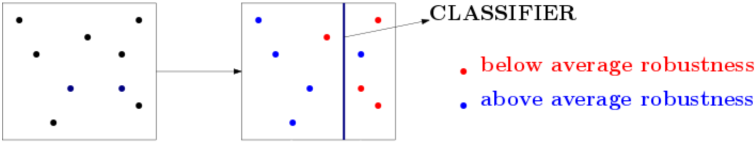
2. Initialize local search with promising initialization conditions based on above analysis.

Overview of global search

- STATISTICAL CLASSIFICATION $+$ BIASED SAMPLING.

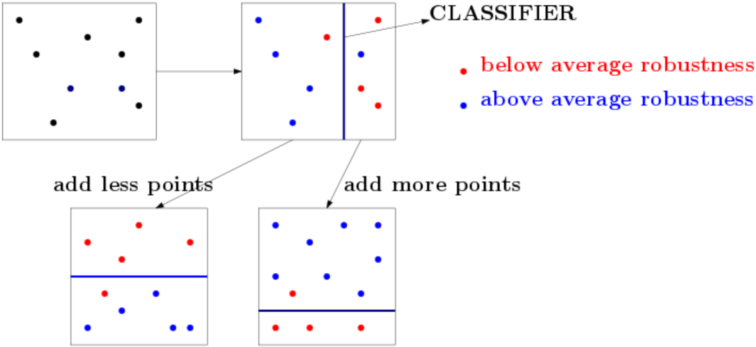
Overview of global search

- STATISTICAL CLASSIFICATION + BIASED SAMPLING.



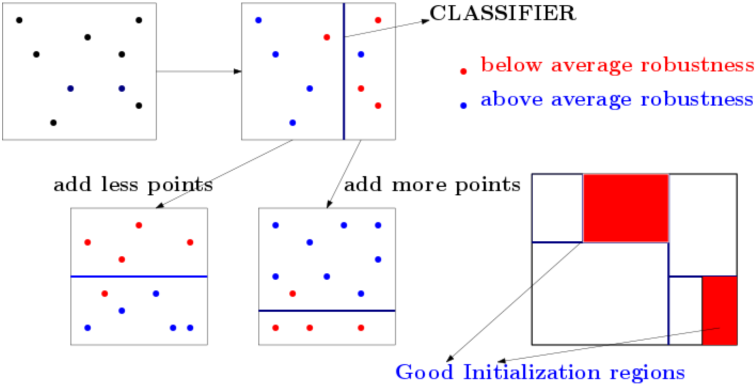
Overview of global search

- STATISTICAL CLASSIFICATION + BIASED SAMPLING.



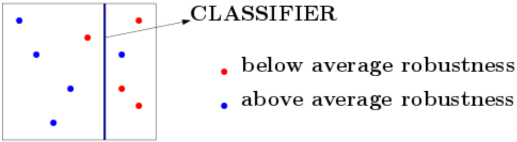
Overview of global search

- STATISTICAL CLASSIFICATION + BIASED SAMPLING.



Classification

1. Use Axis Aligned Hyperplane for best possible separation of points BELOW and ABOVE Average Robustness μ.



2. Criteria for separation: Minimize misclassification error, like Soft Margin Support Vector machines (SVM).

$$error(d, r) = \min_{p \in \{0,1\}} \sum_{x \in S} p\left(\rho(x) - \mu\right)(x_d - r)$$

$d \in \{1, \ldots, m\}$: axis along which classifier is aligned, $r \in [a_d, b_d]$: position of classifier, S: set of points, μ: average robustness.

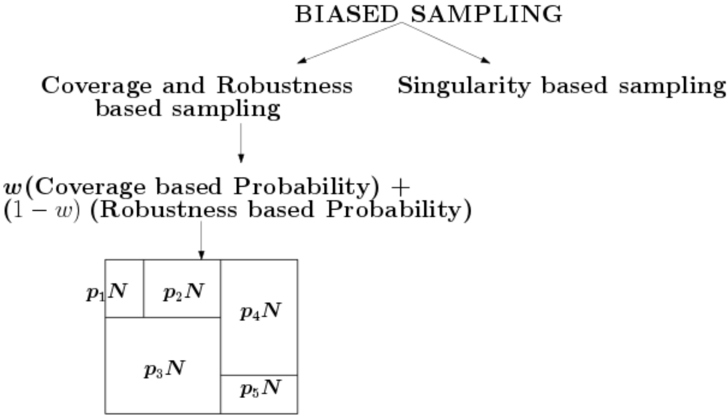
Biased Sampling

BIASED SAMPLING

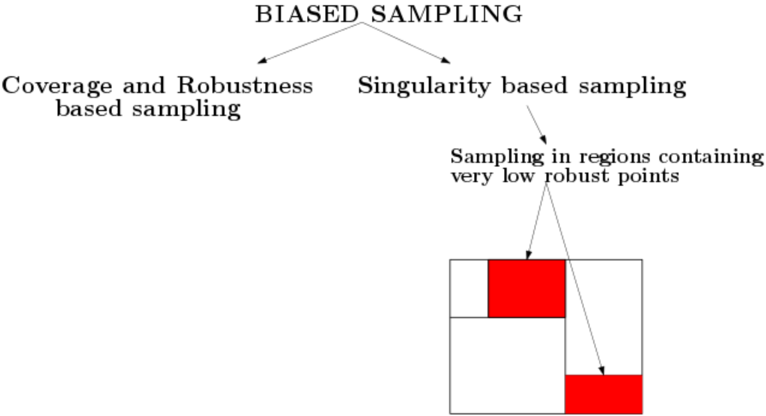
Coverage and Robustness based sampling

Singularity based sampling

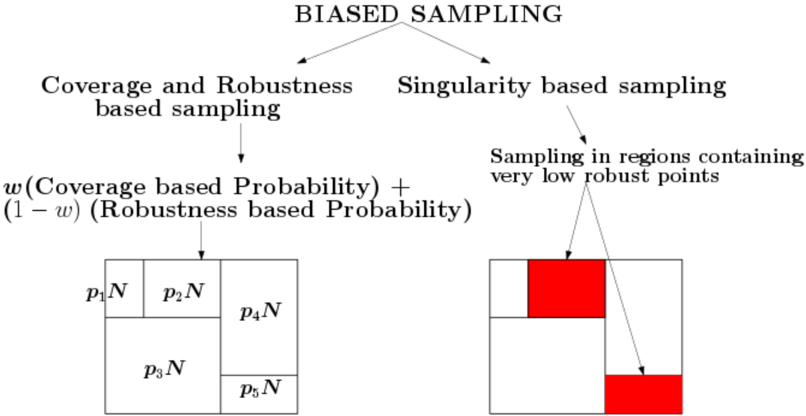
Biased Sampling



Biased Sampling



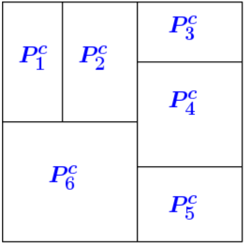
Biased Sampling



Coverage based Probability distribution

- Let h_i denote coverage in rectangle R_i.
- Coverage based probability:

$$\boldsymbol{P_i^c = \frac{(1 - h_i)}{\sum_{i=1}^{K}(1 - h_i)}}$$



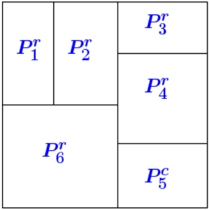
Robustness based Probability distribution

- Given set of samples S_i in rectangle R_i, the expected reduction below average robustness:

$$\lambda_i = \frac{1}{|S_i|} \sum_{x \in S_i} \max(\mu_i - \rho(x), 0)$$

- Expected reduced robustness below average: $\theta_i = \mu_i - \lambda_i$
- So, we heuristically determine a robustness based probability distribution as

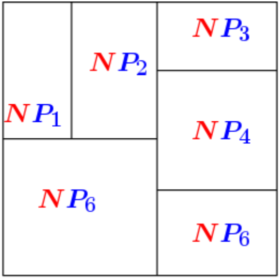
$$P_r^i = \frac{\frac{1}{\theta_i}}{\sum_{j=1}^{K} \frac{1}{\theta_j}}$$



Weighted Probabilistic Sampling

- User defined Weight $w \in [0, 1]$.
- Weighted coverage and robustness based probability and distribute N samples accordingly.

$$P_i = wP_i^c + (1 - w)P_i^r$$



Singular samples

Very low robustness samples: Singular samples.

- Given γ: Vector of lowest robust values in different rectangles.
- μ_γ: Average of elements of γ. λ_γ: Average deviation below μ_γ.

Definition

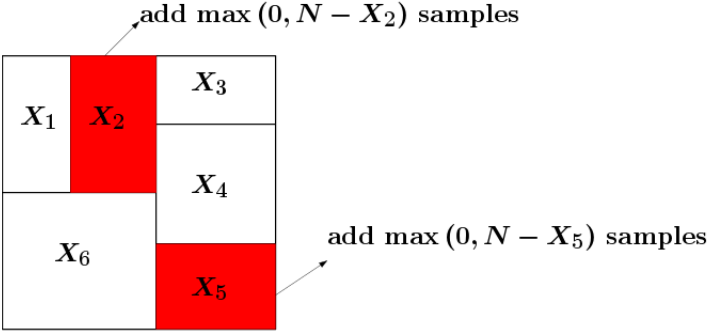
A point $x \in \bigcup_{i=1}^{k} S_i$ for which $\rho(x) \leq max\,(\mu_\gamma - 3\lambda_\gamma, \lambda_\gamma)$ is called a singular sample.

Reason: For a normal distribution, less than 15% samples are singular.

Singularity based sampling

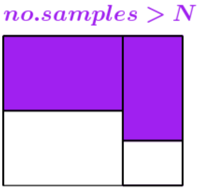
Given N: User defined threshold no. samples for Classification,

- If R_i has a singular sample and contains total X_i samples, then add $\max(0, N - X_i)$ samples.



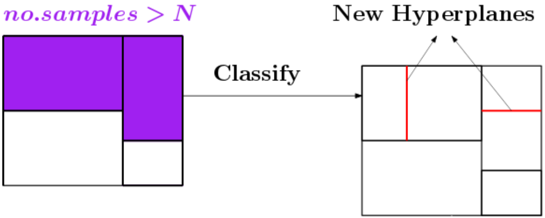
One Iteration of Global Search

Given N: User define threshold no. samples for classification.



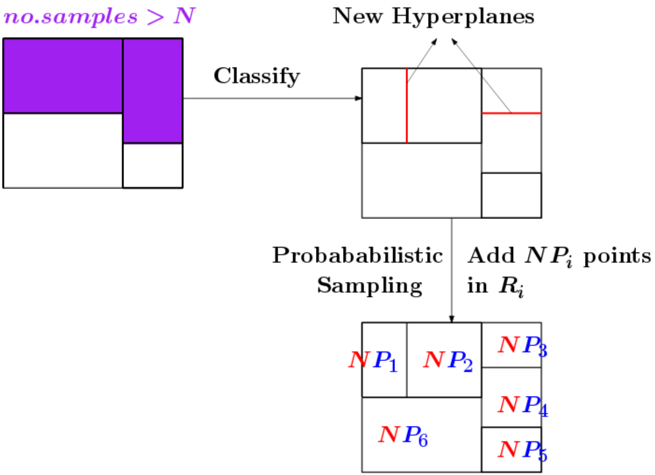
One Iteration of Global Search

Given N: User define threshold no. samples for classification.



One Iteration of Global Search

Given N: User define threshold no. samples for classification.



One Iteration of Global Search

Given N: User define threshold no. samples for classification.

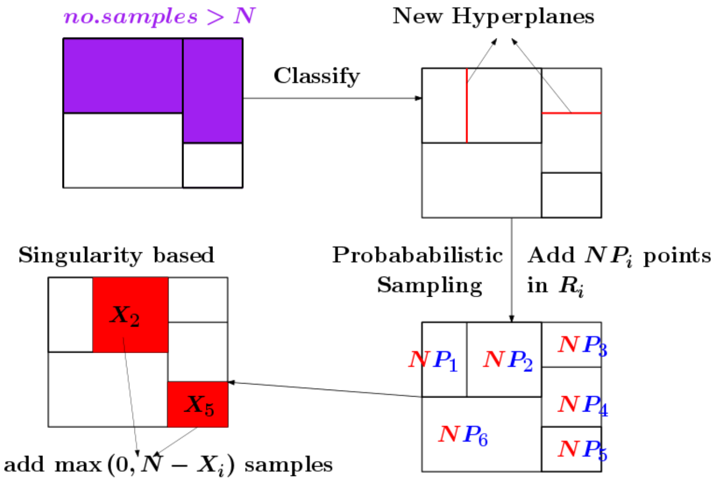
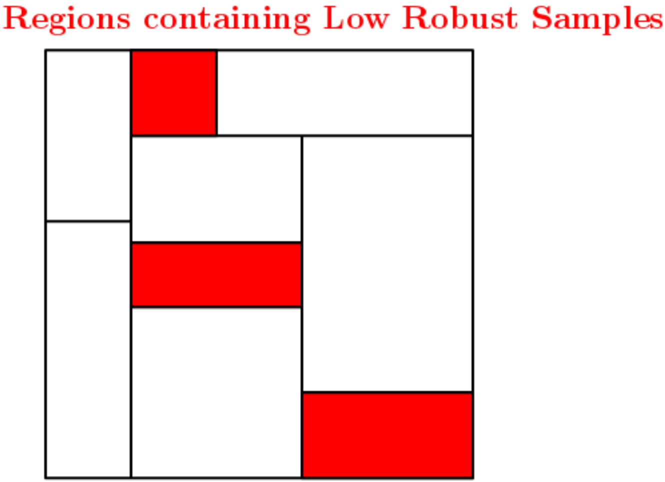


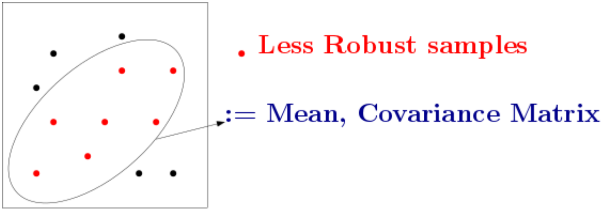
Illustration of Final Subdivision



CMA-ES local search

CMA-ES: Covariance Matrix Adaptive Evolutionary Search.

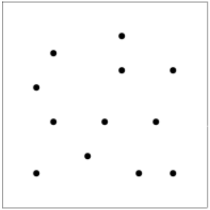
- *Procedure*: Update Mean and Covariance Matrix of Normally Distributed Samples in each iteration, based on Less Robust Samples.



CMA-ES local search

CMA-ES: Covariance Matrix Adaptive Evolutionary Search.

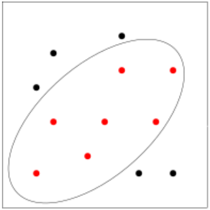
- *Procedure*: Update Mean and Covariance Matrix of Normally Distributed Samples in each iteration, based on Less Robust Samples.



CMA-ES local search

CMA-ES: Covariance Matrix Adaptive Evolutionary Search.

- *Procedure*: Update Mean and Covariance Matrix of Normally Distributed Samples in each iteration, based on Less Robust Samples.

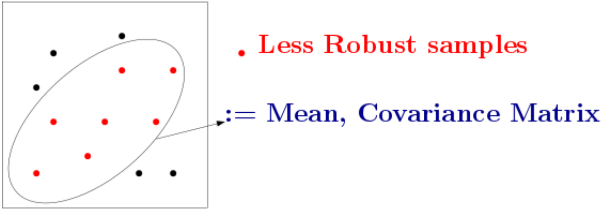


• Less Robust samples

CMA-ES local search

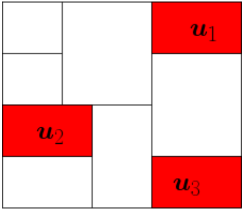
CMA-ES: Covariance Matrix Adaptive Evolutionary Search.

- *Procedure*: Update Mean and Covariance Matrix of Normally Distributed Samples in each iteration, based on Less Robust Samples.



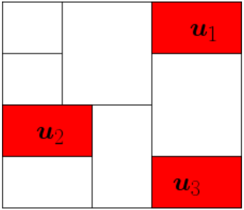
Combine Global and CMA-ES Local search

- Use Global Search to Find good Initial Mean and Covariance Matrix for CMAES search.



Combine Global and CMA-ES Local search

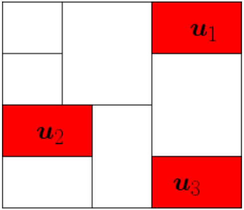
- Use Global Search to Find good Initial Mean and Covariance Matrix for CMAES search.



1. Initialize Mean with each of the Lowest Robust Points in promising regions.

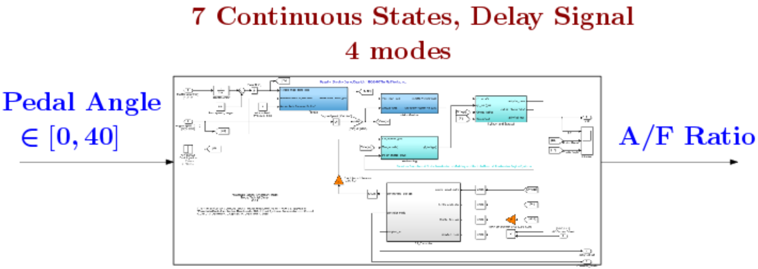
Combine Global and CMA-ES Local search

- Use Global Search to Find good Initial Mean and Covariance Matrix for CMAES search.



1. Initialize Mean with each of the Lowest Robust Points in promissing regions.
2. Initialize Mean and Covariance Matrix as that of the Mean and Covariance of Lowest Robust Points in promissing regions.

Example: Automatic Powertrain Control System

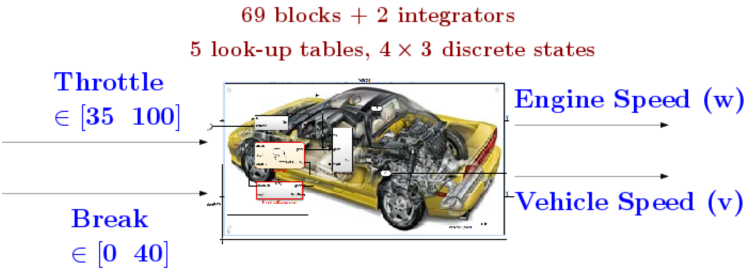


- **Requirement:** $\Box_{[5,10]} (\eta < 0.5)$.
- **Parametrization.** Pedal Angle Signal: 10 control points.
- **Dimension of Search Space:** 10.

Experimental results: PTC benchmark

Solver	Seed	Computation time (secs)	Falsification
Hyperplane classification + CMA-ES-Breach	0	2891	✓
	5000	2364	✓
	10000	2101	✓
	15000	2271	✓
CMA-ES-Breach	0	T.O (5000)	
	5000	T.O. (5000)	
	10000	T.O. (5000)	
	15000	T.O. (5000)	
Grid based random sampling	0	T.O. (5000)	
	5000	T.O. (5000)	
	10000	3766	✓
	15000	268	✓
Global Nelder-Mead-Breach		T.O. (5000)	✓
S-TaLiRo (Simulated Annealing)		4481	✓

Example: Automatic Transmission



- **Requirement.** $\phi = \neg\left(\left(\Diamond_{[0,10]} v > 50\right) \wedge \left(\Box w \leq 2520\right)\right)$
- **Parametrization.** Throttle: 7 Control Points, Break: 3 Control Points.
- **Dimension of Search Space.** 7+3=10.

Experimental Results: Automatic Transmission

Solver	Seed	Computation time (secs)	Falsification
Hyperplane classification + CMA-ES-Breach	0	996	✓
	5000	1382	✓
	10000	1720	✓
	15000	1355	✓
CMA-ES-Breach	0	T.O (2000)	
	5000	1302	✓
	10000	T.O. (2000)	
	15000	1325	✓
Grid based random sampling	0	T.O. (2000)	
	5000	T.O. (2000)	
	10000	T.O. (2000)	
	15000	T.O. (2000)	
Global Nelder-Mead-Breach		T.O. (2000)	
S-TaLiRo (Simulated Annealing)		T.O. (2000)	

Experiment: Industrial Example

Current-Air flow dynamics of an Automative Fuel Control system.

Solver	Seed	Computation time (sec.)	Falsification
Hyperplane classification + CMA-ES-Breach (Cell partition: A)†	1	406	✓
	2	1383	✓
	3	T.O.	
	4	794	✓
Hyperplane classification + CMA-ES-Breach (Cell partition: B)†	1	409	✓
	2	T.O.	
	3	T.O.	
	4	T.O.	
CMA-ES Breach†	1	314	✓
	2	1418	
	3	T.O.	
	4	1316	✓
Uniform random† sampling	1	396	✓
	2	786	✓
	3	2241	✓
	4	T.O.	
S-TaLiRo (Simulated Annealing)‡ sampling	1	310	✓
	2	T.O.	
	3	671	✓
	4	T.O.	
Global Nelder-Mead-Breach†		1501	✓

Concluding remarks

1. Other applications under investigation: biological systems modelling
2. More coverage measures (entropy,...)

Thank You!