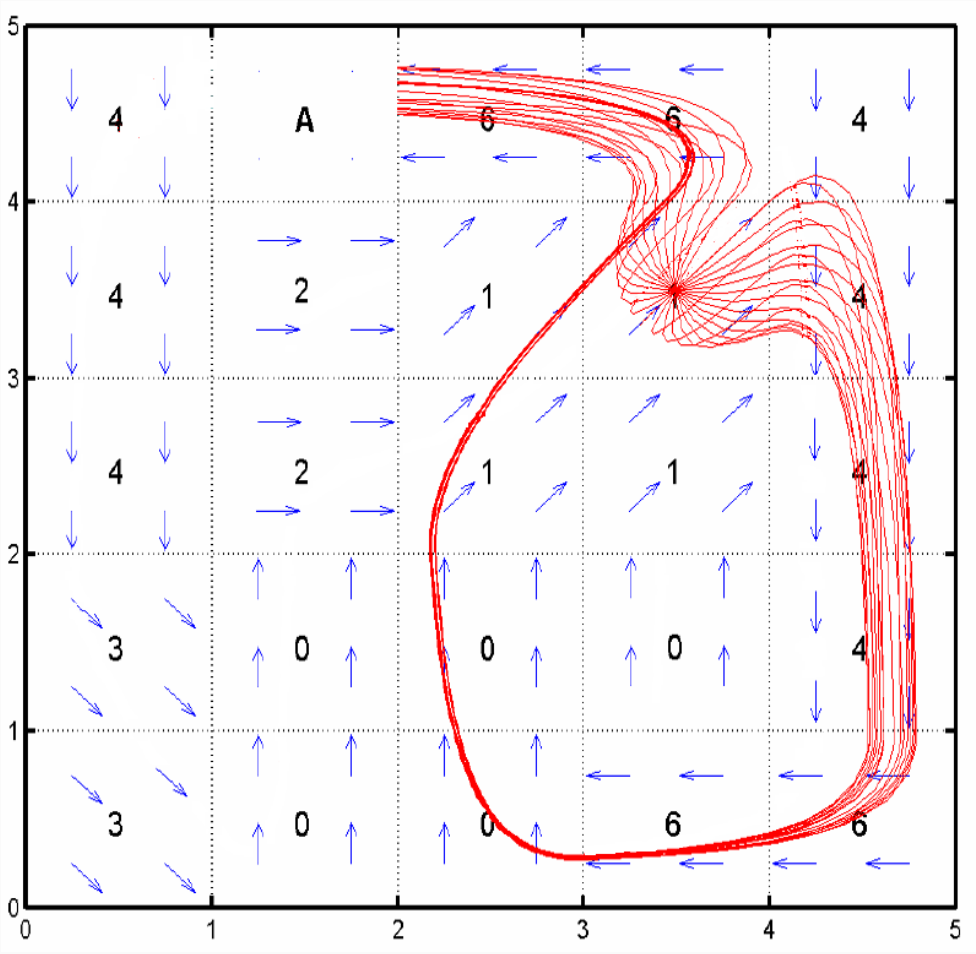
Guided Search for Hybrid Systems

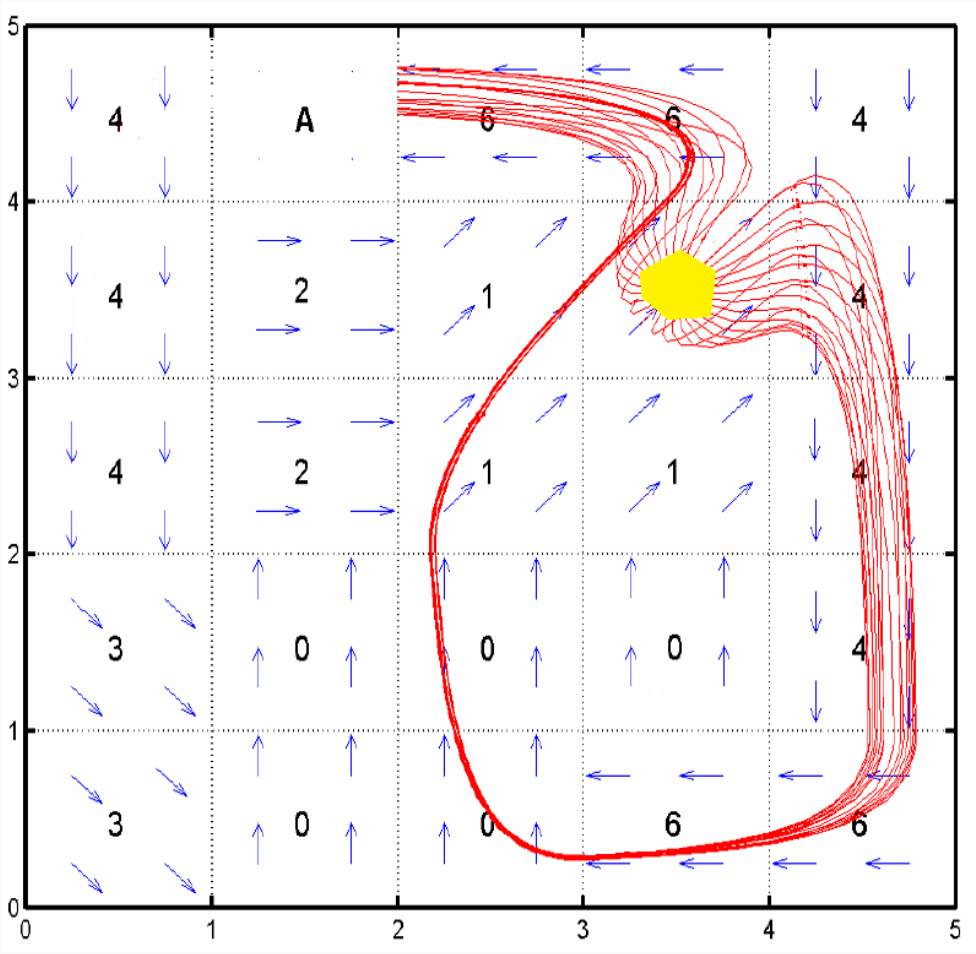
Sergiy Bogomolov

A. Donzé, G. Frehse, R. Grosu, T. Johnson,
H. Ladan, A. Podelski, M. Wehrle

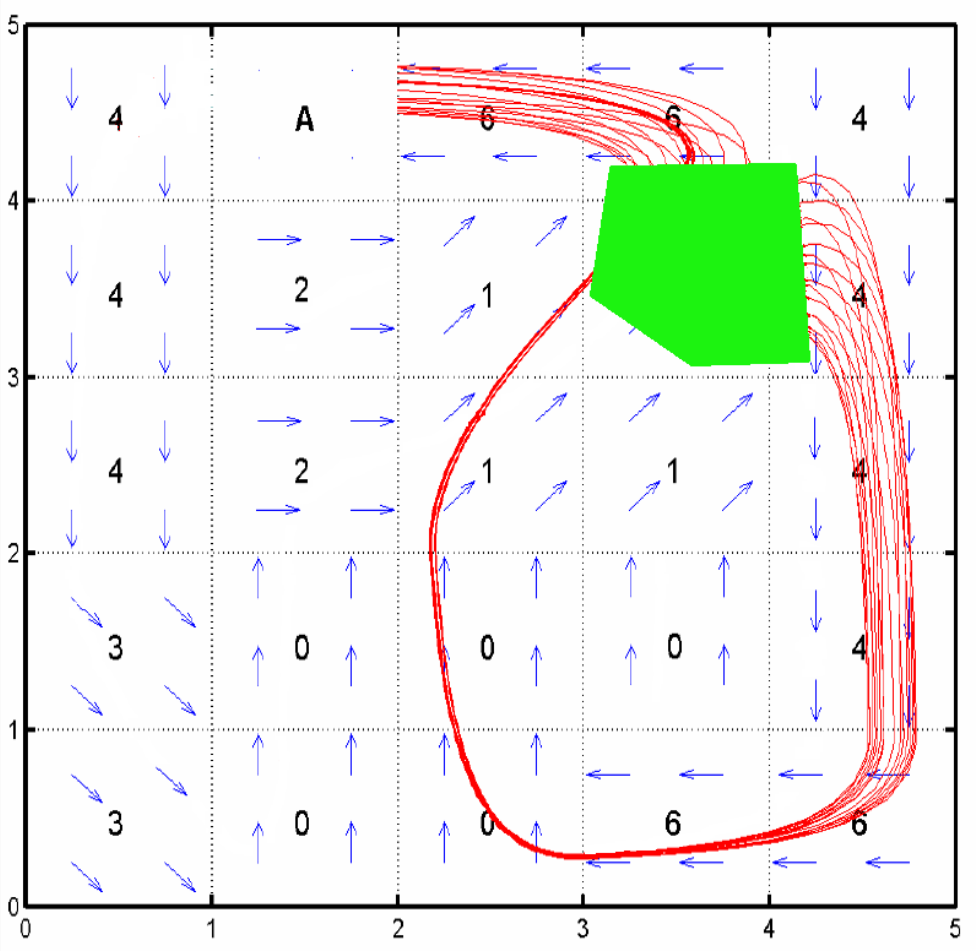
NAV Example



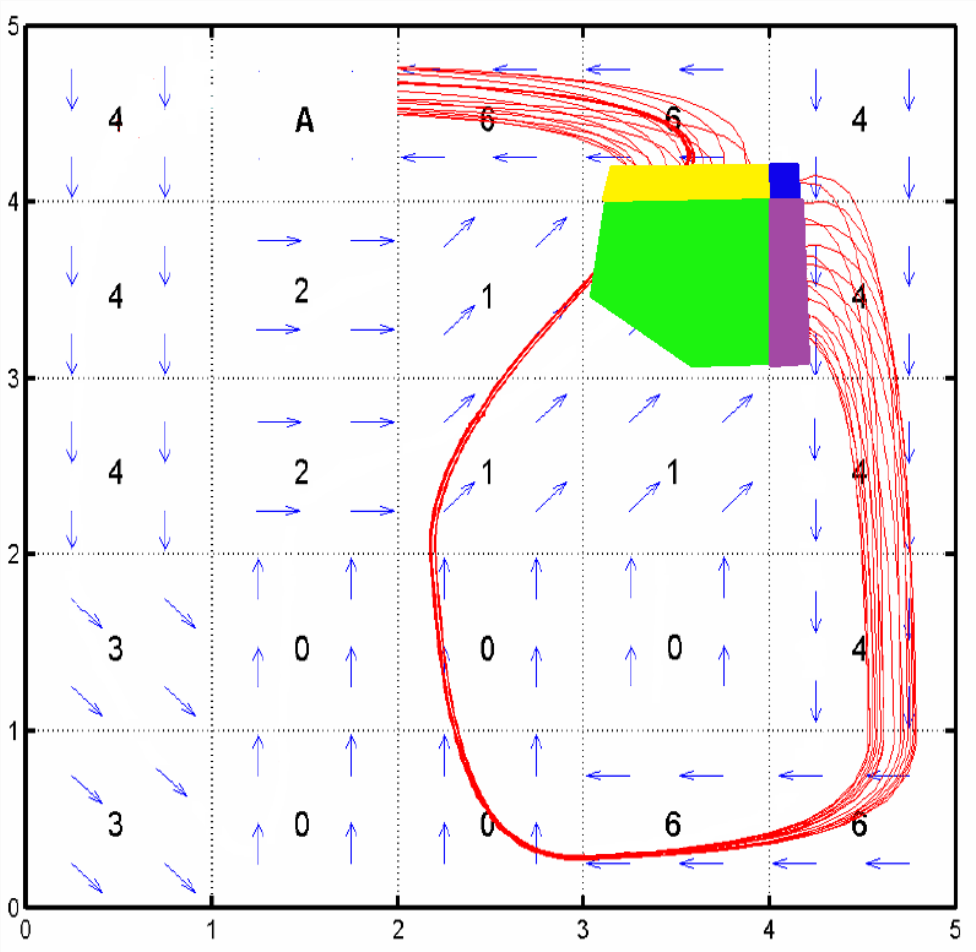
NAV Example



NAV Example



NAV Example



Falsification for Hybrid Systems (1)

- **Goal:** Find errors as fast as possible
- **Problem:** Hybrid MC algorithms not scalable
- **Approach:** Heuristics to guide symbolic search (up to 700 times performance improvement)
- **Generic:** Heuristics are computed automatically based on abstractions
- **Question:** Appropriate abstractions for this purpose?

Falsification for Hybrid Systems (2)

- **Current abstraction application: verification**
- **Novel abstraction application:**
  - **falsification**
  - **more precise abstractions – better search behavior**
  - **algorithm stays sound for every abstraction**
- **Scope: Related to AI planning (search not for a bad state, but for a good state)**

Outline

- **Box based distance approach**
  - **Focuses on continuous dynamics**
- **Pattern-database approach**
  - **Focuses on both discrete and continuous behavior**

Box-based distance approach

- **Goal: First consider paths leading to bad states which will probably require less resources to be computed**
- **Observation: Continuous post computation is the most time consuming part in the reachability analysis of hybrid systems**
- **Approximation: Minimize accumulated dwell time (i.e., passed time) in the case of hybrid systems**

Accumulated dwell time

- **Define cost(s) as a minimal sum of dwell times ranging over the error traces that start in s**
- **Problem: Exact computation of cost(s) is computationally infeasible**
- **Solution: Find a function h(s) which approximates cost(s) and still posesses enough precision to provide clever guidance**

Order-Preserving

- **A cost measure h is order-preserving with respect to cost if cost(s) < cost(s') implies h(s) < h(s')**
- **Observation: Order-preserving cost measures allow perfect prioritization**

Trajectory-Based Distance Measure

$dist_E(s)$:= length of a shortest trajectory from s to an error state.

Restricted Hybrid Systems

Hybrid system is called restricted if

- **all differential equations in H are of the form $\dot{x}_i(t) = \pm c_i$**

for every continous variable $x_i \in Var$ and a constant $c_i \in N$,

- **all updates in H are identity relations.**

Proposition: $dist_E(s)$ is order-preserving for restricted hybrid systems.

Euclidean distance measure (1)

- **Problem:** $dist_E(s)$ **cannot still be easily computed**
- **Solution: Instead of computing the exact length of trajectories between two points x and x′, use Euclidian distance measure** $dist_{eq}(x, x')$

Euclidean distance measure (2)

Observation: Euclidean distance $dist_{eq}(x, x')$ is not order-preserving for restricted systems.

Proposition: For restricted systems H with $\dot{x}_i(t) = c_i$, i.e. for restricted systems where all locations have the same continuous behavior, $dist_E^{eq}(x, x')$ is order-preserving.

Euclidean distance measure (3)

- **Coarse approximation of trajectory based measure**
- **Accurate when system dynamics only depends on the continuous state, e.g., when complex dynamics is approximated with a simpler one through state space partitioning:**
  - **phase portrait approximations (Henzinger et al. ’96)**
  - **approximation techniques employed by PHAVer (Frehse ’05)**
  - **hybridization techniques (Asarin et al. ’07)**
- **There exists a class of systems where it is even order-preserving**
- **Suggestion: Use Euclidean distance as a heuristic for general classes of hybrid systems**

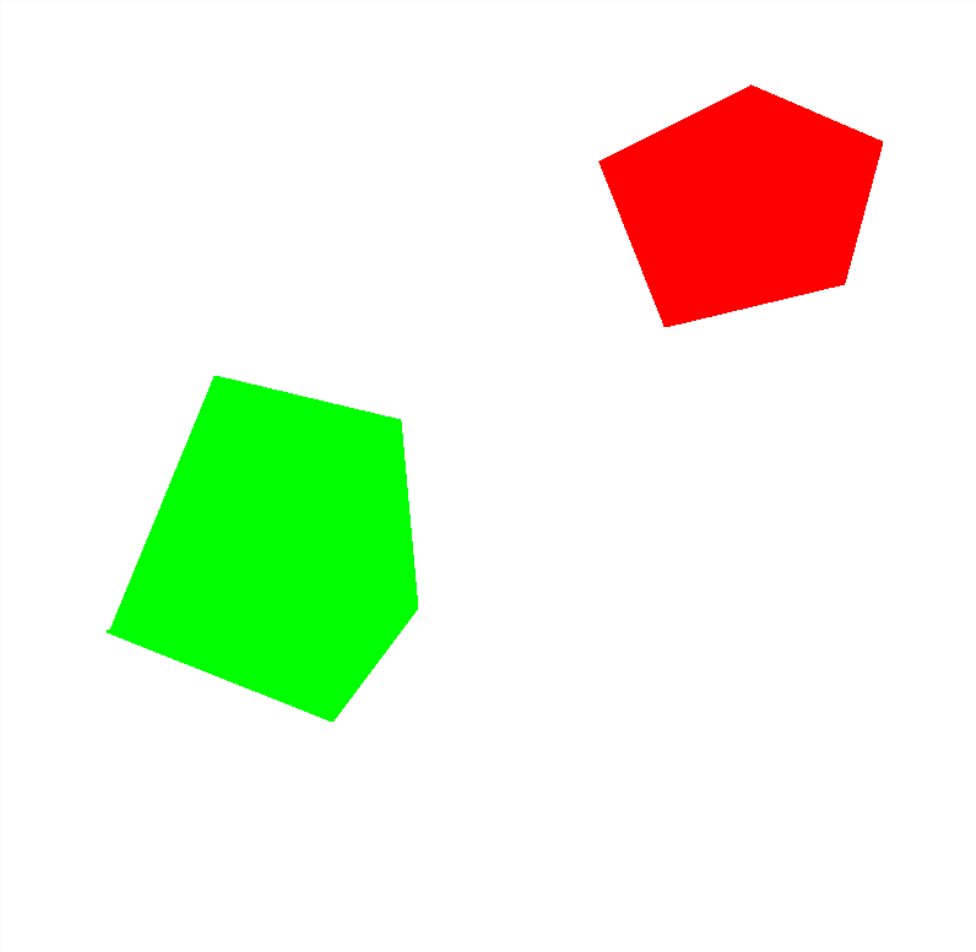
Box-based distance measure (1)

Function $h^{eq}(s)$ is called box-based distance measure if for every $s = (\ell, R)$ it returns the length of the shortest segment connecting the centers of the smallest bounding boxes of region R and some bad region.

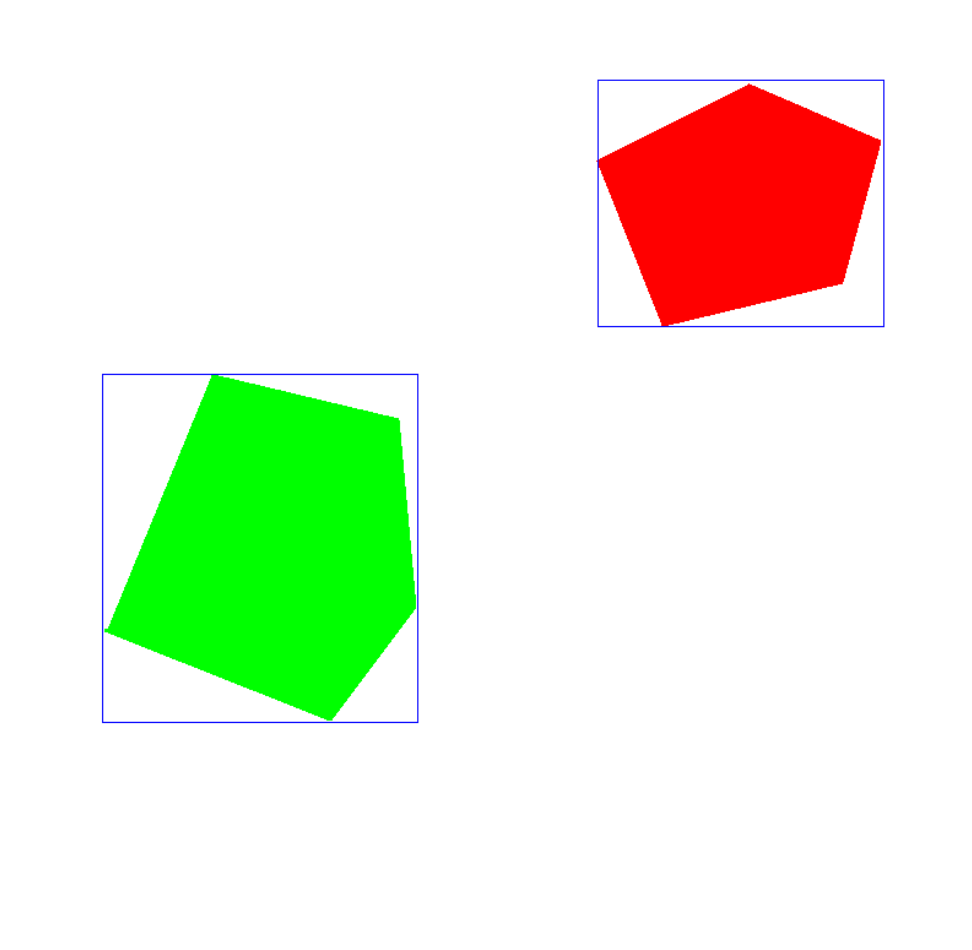
Formally,

$$h^{eq}(s) := min_{s_e=(\ell_e,R_e)} dist_{eq}(Center(\mathrm{B}(R)), Center(\mathrm{B}(R_e)))$$

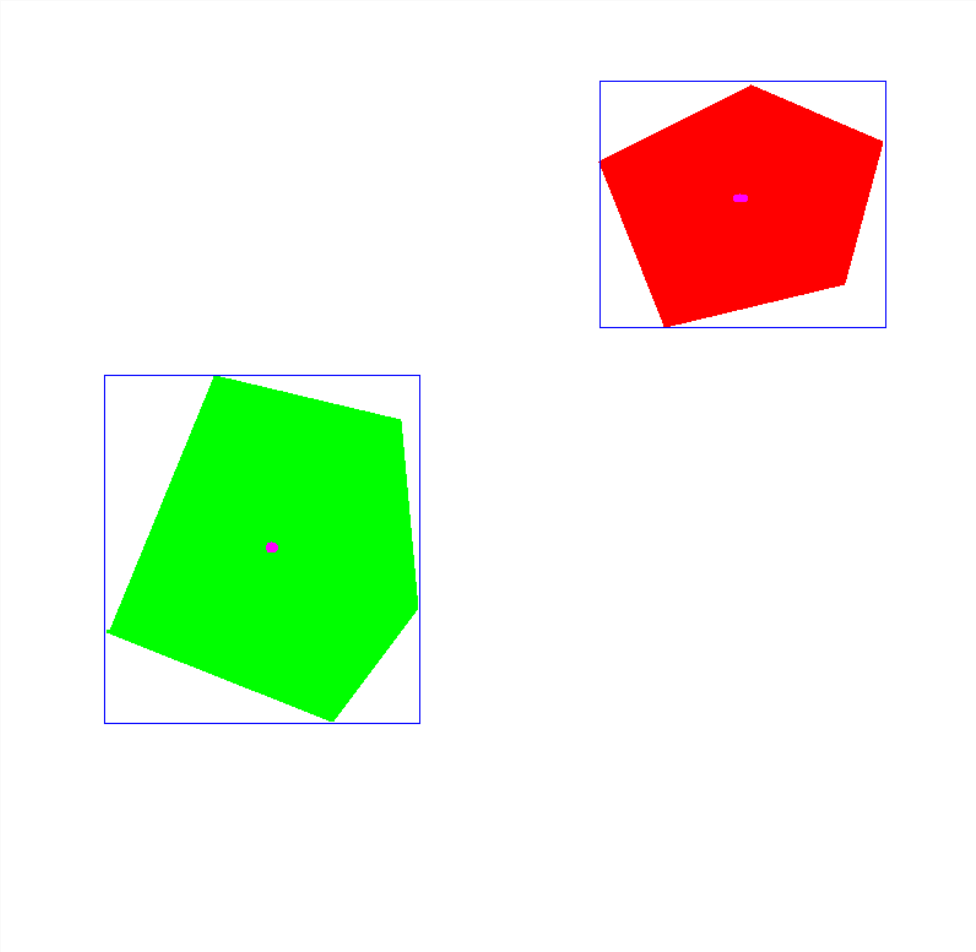
Box-based distance measure (2)



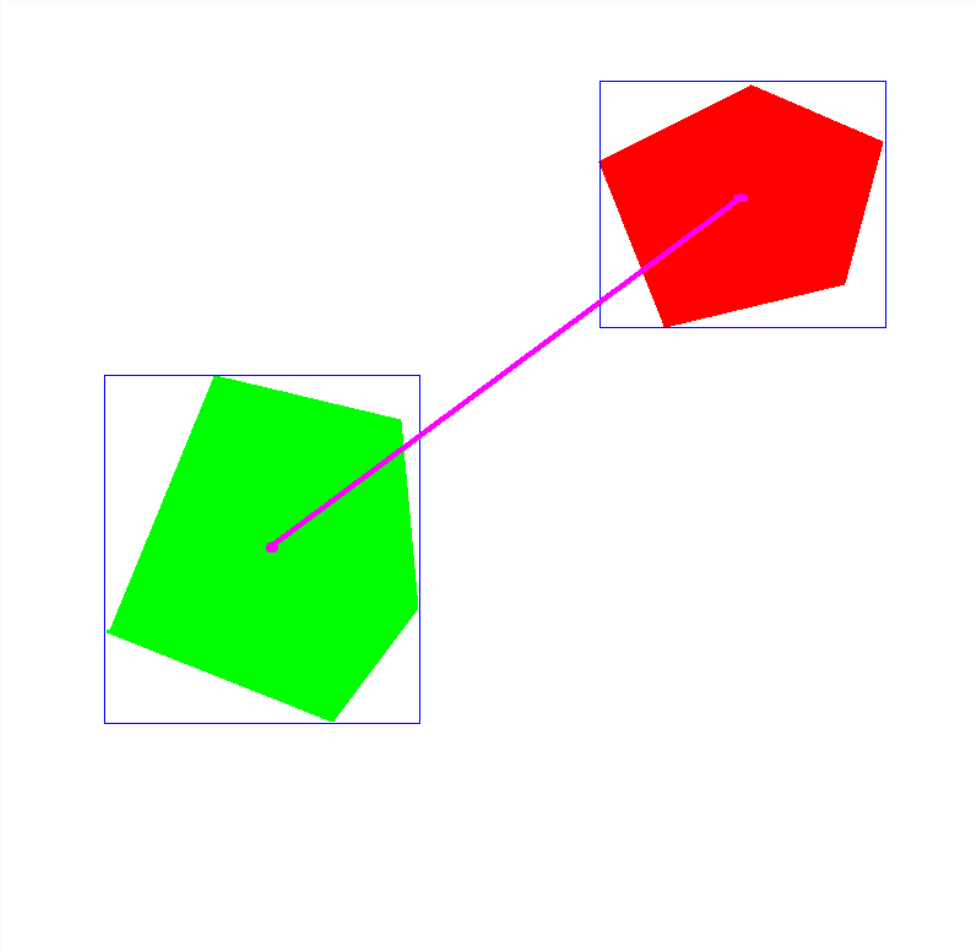
Box-based distance measure (3)



Box-based distance measure (4)



Box-based distance measure (5)



Experiments

- **Our techniques are implemented in SpaceEx model checker**
- **Models: Satellites on the orbit and navigation benchmark**
- **High degree of non-determinism and large branching factor**

Satellite Benchmark

Inst.	#loc	Uninformed DFS			Box heuristic		
		#it	length	time	#it	length	time
1	36	116	32	27.1	75	10	**13.4**
2	36	464	24	**101.3**	473	13	116.9
3	64	718	87	31.5	278	87	**11.0**
4	100	111	107	38.1	44	15	**21.1**
5	100	109	104	262.9	45	15	**178.6**
6	159	2170	∞	78.9	1352	∞	**49.9**
7	324	323	102	**105.6**	1289	106	457.7
8	557	1637	42	45.8	936	42	**26.3**
9	574	7113	41	223.6	561	10	**17.5**
10	575	9092	4	284.8	387	5	**12.3**
11	576	5693	3769	816.6	257	13	**36.5**
12	576	32966	13	7059.5	826	13	**118.9**
13	576	n/a	n/a	OOM	579	52	**579.7**
14	1293	13691	∞	436.1	7719	∞	**249.6**
15	1293	n/a	n/a	OOM	1806	142	**1869.7**

Satellite Benchmark

Inst.	#loc	Uninformed DFS			Box heuristic		
		#it	length	time	#it	length	time
1	36	116	32	27.1	75	10	**13.4**
2	36	464	24	**101.3**	473	13	116.9
3	64	718	87	31.5	278	87	**11.0**
4	100	111	107	38.1	44	15	**21.1**
5	100	109	104	262.9	45	15	**178.6**
6	159	2170	∞	78.9	1352	∞	**49.9**
7	324	323	102	**105.6**	1289	106	457.7
8	557	1637	42	45.8	936	42	**26.3**
9	574	7113	41	223.6	561	10	**17.5**
10	575	9092	4	284.8	387	5	**12.3**
11	576	5693	3769	816.6	257	13	**36.5**
12	576	32966	13	7059.5	826	13	**118.9**
13	576	n/a	n/a	OOM	579	52	**579.7**
14	1293	13691	∞	436.1	7719	∞	**249.6**
15	1293	n/a	n/a	OOM	1806	142	**1869.7**

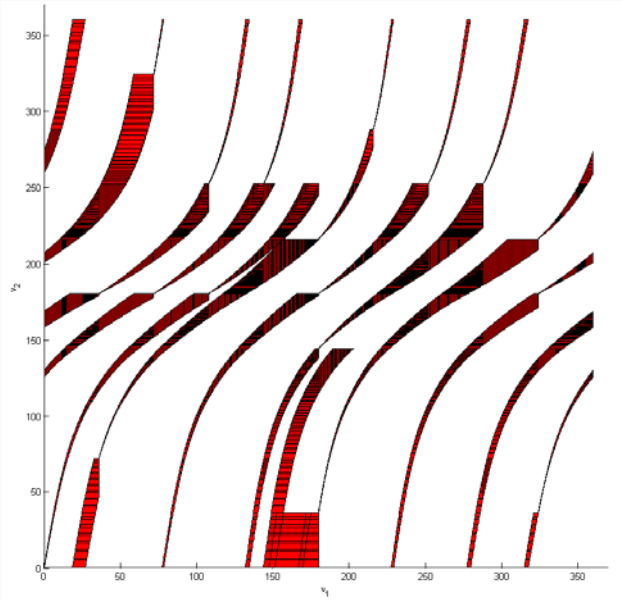
Satellite Benchmark

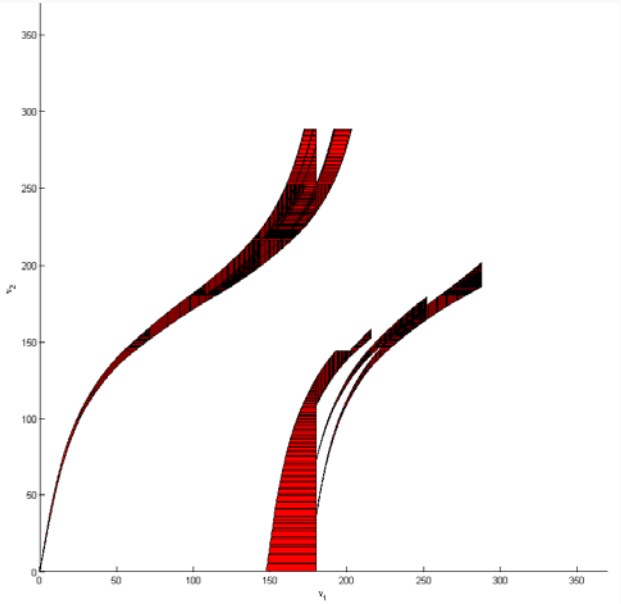
Inst.	#loc	Uninformed DFS			Box heuristic		
		#it	length	time	#it	length	time
1	36	116	32	27.1	75	10	**13.4**
2	36	464	24	**101.3**	473	13	116.9
3	64	718	87	31.5	278	87	**11.0**
4	100	111	107	38.1	44	15	**21.1**
5	100	109	104	262.9	45	15	**178.6**
6	159	2170	∞	78.9	1352	∞	**49.9**
7	324	323	102	**105.6**	1289	106	457.7
8	557	1637	42	45.8	936	42	**26.3**
9	574	7113	41	223.6	561	10	**17.5**
10	575	9092	4	284.8	387	5	**12.3**
11	576	5693	3769	816.6	257	13	**36.5**
12	576	32966	13	7059.5	826	13	**118.9**
13	576	n/a	n/a	OOM	579	52	**579.7**
14	1293	13691	∞	436.1	7719	∞	**249.6**
15	1293	n/a	n/a	OOM	1806	142	**1869.7**

Satellite Benchmark

Inst.	#loc	Uninformed DFS			Box heuristic		
		#it	length	time	#it	length	time
1	36	116	32	27.1	75	10	**13.4**
2	36	464	24	**101.3**	473	13	116.9
3	64	718	87	31.5	278	87	**11.0**
4	100	111	107	38.1	44	15	**21.1**
5	100	109	104	262.9	45	15	**178.6**
6	159	2170	∞	78.9	1352	∞	**49.9**
7	324	323	102	**105.6**	1289	106	457.7
8	557	1637	42	45.8	936	42	**26.3**
9	574	7113	41	223.6	561	10	**17.5**
10	575	9092	4	284.8	387	5	**12.3**
11	576	5693	3769	816.6	257	13	**36.5**
12	576	32966	13	7059.5	826	13	**118.9**
13	576	n/a	n/a	OOM	579	52	**579.7**
14	1293	13691	∞	436.1	7719	∞	**249.6**
15	1293	n/a	n/a	OOM	1806	142	**1869.7**

Satellite Benchmark





Uninformed DFS

Box-heuristic

Navigation Benchmark

Inst.	#loc	Uninformed DFS			Box heuristic		
		#it	length	time	#it	length	time
1	400	122	15	145.8	62	15	**70.5**
2	400	183	33	186.9	86	33	**120.4**
3	625	75	33	70.7	34	33	**36.6**
4	625	268	158	261.9	231	158	**209.6**
5	625	85	79	118.8	26	25	**37.8**
6	625	96	53	110.8	101	53	**104.9**
7	625	227	34	198.9	105	34	**96.9**
8	625	178	25	266.1	86	25	**137.3**
9	625	297	17	356,0	102	17	**131.9**
10	625	440	30	534,0	136	30	**201.8**
11	900	234	72	269.3	129	21	**149.1**
12	900	317	43	339.1	174	61	**198.3**
13	900	367	37	421.9	148	37	**190.4**
14	900	411	32	434.6	278	32	**297.9**
15	900	379	44	445.9	107	44	**137.8**

Outline

- Box based distance approach
  - Focuses on continuous dynamics
- **Pattern-database approach**
  - **Focuses on both discrete and continuous dynamics**

PDB approach

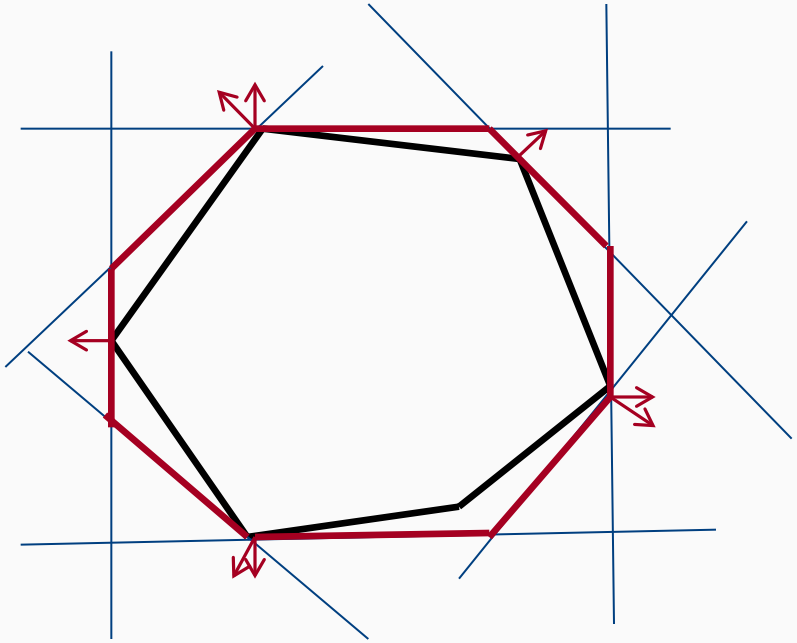
- **Goal:** Develop heuristic which
  - **Efficiently:** take discrete structure into account
  - **Utilize:** pattern database (PDB) approach
- **Precomputation:** Explore abstract state space
  - **Reachable state:** Compute its distance to the bad state
- **Analysis:** Explore concrete state space
  - **Use:** Abstract distance to select successors

Abstraction

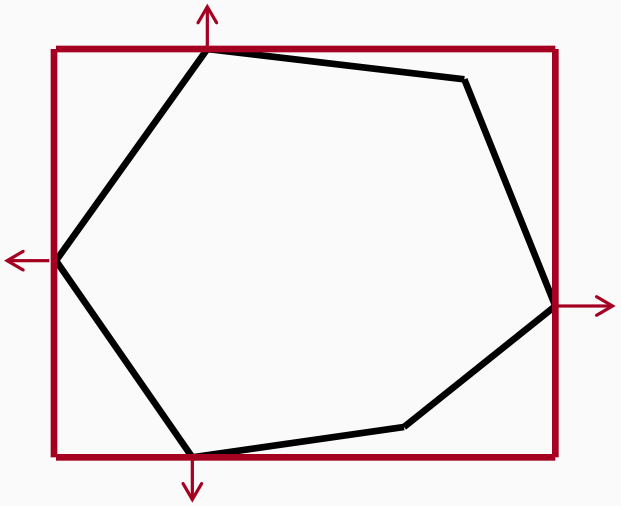
- **Utilize** the internal representation of polyhedra
  - **Based on:** Support functions implemented in SpaceEx
- **Precision** of polyhedra representation depends
  - **Direction set:** Direction and No of polyhedral faces
  - **Sampling time:** Time increment of continuous part

Abstraction: Direction Sets

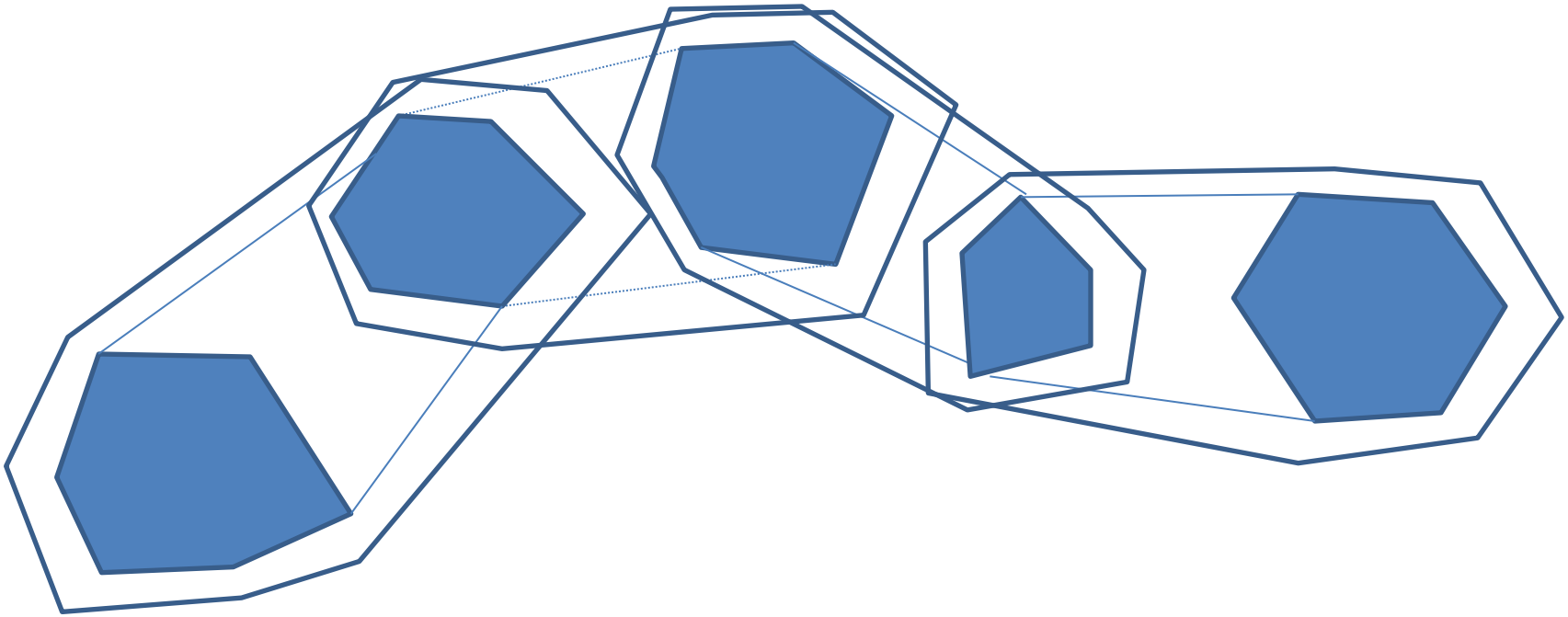
Octagonal directions (45 degrees)



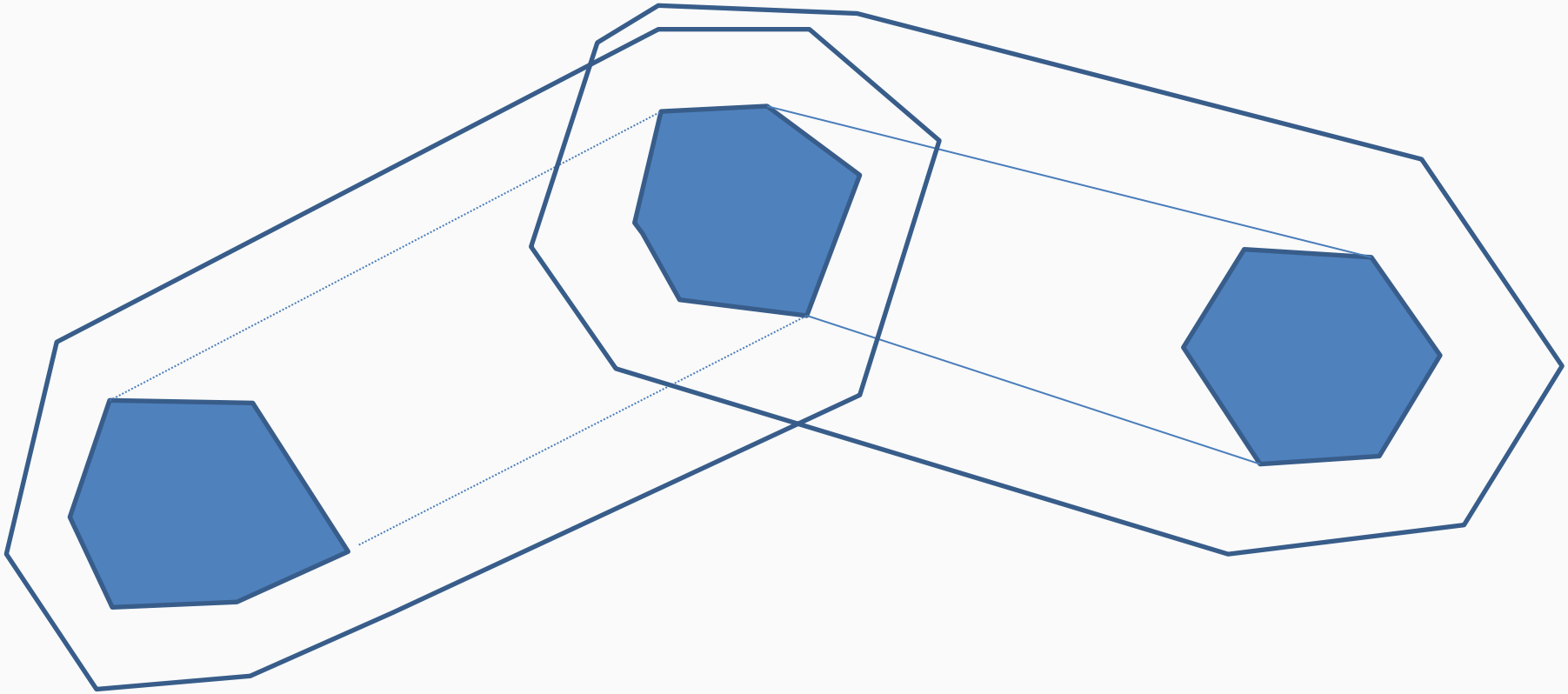
Box directions (90 degrees)



Abstraction: Sampling Time



Abstraction: Larger Sampling Time



Abstraction: Time-Directions

Thus by considering:

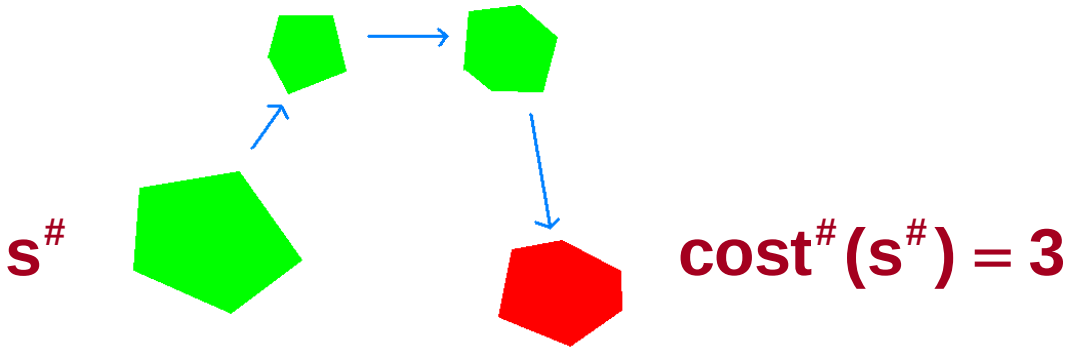
- **Smaller direction sets**
- **Larger sampling time**

we end up with coarser representation

Abstract Cost function

Given abstract symbolic state $s^{\#}$

the abstract cost function $cost^{\#}(s^{\#})$ is equal to the minimal number of discrete jumps to reach an abstract error state from $s^{\#}$



Concrete cost function

- Concrete cost function $cost^P(s) = cost^\#(s^\#)$
  - $s^\#$ is a corresponding abstract state to s
  - $cost^\#$ is an abstract cost funtion
- Abstract state $s^\#$ is called corresponding to s if
  - $s.discrete = s^\#.discrete$ same discrete part
  - $s.cont \subseteq s^\#.cont$ inclusion among cont parts
  - $cost^\#(s^\#)$ minimal among AS satisfying above

Partial Pattern Data Base (PDB)

- **Downside of complete PDB:**
  - **Precomputation might become quite expensive**
- **Solution is to consider partial PDB:**
  - **Explore only a fraction of the abstract region space (AS)**
  - **Focusing on AS likely to suffice for the concrete search**

Partial PDB

- **PDB which contains only**
  - **Abstract state/cost value pairs for abstract states**
  - **That are part of some trajectory of shortest length**
  - **From an initial state to an abstract error state**

$$\text{cost}^{PP}(s) = \begin{cases} \text{cost}^{\#}(s^{\#}), & \text{if there is a corresponding } s^{\#} \text{ to } s \\ \text{Infinity}, & \text{otherwise} \end{cases}$$

Partial PDB

- Utilize BFS and stop as soon as
  - All paths of minimal length to
  - An abstract bad state are explored
- Contains only abstract states
  - Explored on some shortest trajectory
- Equivalent to complete PDB behavior if
  - For every considered concrete state
  - A corresp abstract state in partial PDB can be found

Experiments

- **Our techniques are implemented in SpaceEx model checker**
- **Models: Satellites on the orbit and navigation benchmark**
- **High degree of non-determinism and large branching factor**

Satellite Benchmark

Inst.	#loc	Uninformed DFS			Box heuristic			PDB		
		#it	length	time	#it	length	time	#it	length	time
1	36	116	32	27.1	75	10	13.4	16	10	**10.3** (7.4)
2	36	464	24	101.3	473	13	116.9	30	13	**16.3** (12.2)
3	64	718	87	31.5	278	87	**11.0**	263	121	20.4 (9.5)
4	100	111	107	38.1	44	15	21.1	23	14	**14.8** (6.0)
5	100	109	104	262.9	45	15	178.6	23	14	**62.9** (5.9)
6	159	2170	∞	78.9	1352	∞	49.9	0	∞	**15.6** (15.6)
7	324	323	102	105.6	1289	106	457.7	25	24	**32.1** (8.8)
8	557	1637	42	45.8	936	42	**26.3**	156	42	44.1 (39.7)
9	574	7113	41	223.6	561	10	17.5	14	10	**6.6** (6.2)
10	575	9092	4	284.8	387	5	12.3	15	4	**2.4** (2.0)
11	576	5693	3769	816.6	257	13	36.5	15	13	**9.9** (5.9)
12	576	32966	13	7059.5	826	13	118.9	15	13	**10.0** (5.8)
13	576	n/a	n/a	OOM	579	52	579.7	58	52	**163.2** (82.0)
14	1293	13691	∞	436.1	7719	∞	249.6	0	∞	**135.5** (135.5)
15	1293	n/a	n/a	OOM	1806	142	1869.7	206	139	**617.4** (434.7)

Satellite Benchmark

Inst.	#loc	Uninformed DFS			Box heuristic			PDB		
		#it	length	time	#it	length	time	#it	length	time
1	36	116	32	27.1	75	10	13.4	16	10	**10.3** (7.4)
2	36	464	24	101.3	473	13	116.9	30	13	**16.3** (12.2)
3	64	718	87	31.5	278	87	**11.0**	263	121	20.4 (9.5)
4	100	111	107	38.1	44	15	21.1	23	14	**14.8** (6.0)
5	100	109	104	262.9	45	15	178.6	23	14	**62.9** (5.9)
6	159	2170	∞	78.9	1352	∞	49.9	0	∞	**15.6** (15.6)
7	324	323	102	105.6	1289	106	457.7	25	24	**32.1** (8.8)
8	557	1637	42	45.8	936	42	**26.3**	156	42	44.1 (39.7)
9	574	7113	41	223.6	561	10	17.5	14	10	**6.6** (6.2)
10	575	9092	4	284.8	387	5	12.3	15	4	**2.4** (2.0)
11	576	5693	3769	816.6	257	13	36.5	15	13	**9.9** (5.9)
12	576	32966	13	7059.5	826	13	118.9	15	13	**10.0** (5.8)
13	576	n/a	n/a	OOM	579	52	579.7	58	52	**163.2** (82.0)
14	1293	13691	∞	436.1	7719	∞	249.6	0	∞	**135.5** (135.5)
15	1293	n/a	n/a	OOM	1806	142	1869.7	206	139	**617.4** (434.7)

Satellite Benchmark

Inst.	#loc	Uninformed DFS			Box heuristic			PDB		
		#it	length	time	#it	length	time	#it	length	time
1	36	116	32	27.1	75	10	13.4	16	10	**10.3** (7.4)
2	36	464	24	101.3	473	13	116.9	30	13	**16.3** (12.2)
3	64	718	87	31.5	278	87	**11.0**	263	121	20.4 (9.5)
4	100	111	107	38.1	44	15	21.1	23	14	**14.8** (6.0)
5	100	109	104	262.9	45	15	178.6	23	14	**62.9** (5.9)
6	159	2170	∞	78.9	1352	∞	49.9	0	∞	**15.6** (15.6)
7	324	323	102	105.6	1289	106	457.7	25	24	**32.1** (8.8)
8	557	1637	42	45.8	936	42	**26.3**	156	42	44.1 (39.7)
9	574	7113	41	223.6	561	10	17.5	14	10	**6.6** (6.2)
10	575	9092	4	284.8	387	5	12.3	15	4	**2.4** (2.0)
11	576	5693	3769	816.6	257	13	36.5	15	13	**9.9** (5.9)
12	576	32966	13	7059.5	826	13	118.9	15	13	**10.0** (5.8)
13	576	n/a	n/a	OOM	579	52	579.7	58	52	**163.2** (82.0)
14	1293	13691	∞	436.1	7719	∞	249.6	0	∞	**135.5** (135.5)
15	1293	n/a	n/a	OOM	1806	142	1869.7	206	139	**617.4** (434.7)

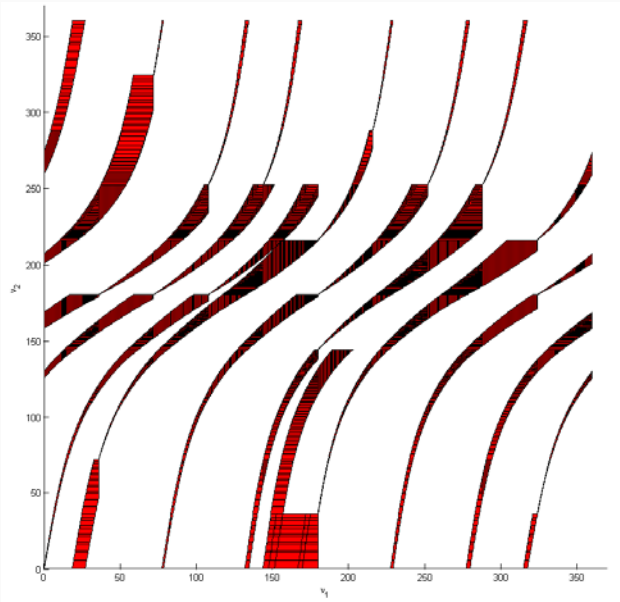
Satellite Benchmark

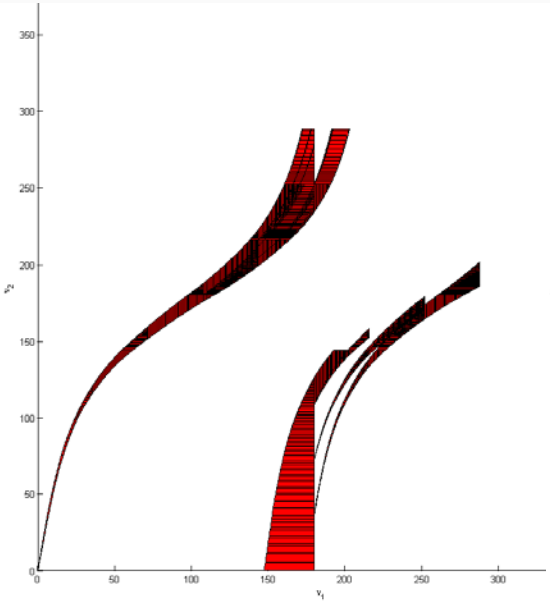
Inst.	#loc	Uninformed DFS			Box heuristic			PDB		
		#it	length	time	#it	length	time	#it	length	time
1	36	116	32	27.1	75	10	13.4	16	10	**10.3** (7.4)
2	36	464	24	101.3	473	13	116.9	30	13	**16.3** (12.2)
3	64	718	87	31.5	278	87	**11.0**	263	121	20.4 (9.5)
4	100	111	107	38.1	44	15	21.1	23	14	**14.8** (6.0)
5	100	109	104	262.9	45	15	178.6	23	14	**62.9** (5.9)
6	159	2170	∞	78.9	1352	∞	49.9	0	∞	**15.6** (15.6)
7	324	323	102	105.6	1289	106	457.7	25	24	**32.1** (8.8)
8	557	1637	42	45.8	936	42	**26.3**	156	42	44.1 (39.7)
9	574	7113	41	223.6	561	10	17.5	14	10	**6.6** (6.2)
10	575	9092	4	284.8	387	5	12.3	15	4	**2.4** (2.0)
11	576	5693	3769	816.6	257	13	36.5	15	13	**9.9** (5.9)
12	576	32966	13	7059.5	826	13	118.9	15	13	**10.0** (5.8)
13	576	n/a	n/a	OOM	579	52	579.7	58	52	**163.2** (82.0)
14	1293	13691	∞	436.1	7719	∞	249.6	0	∞	**135.5** (135.5)
15	1293	n/a	n/a	OOM	1806	142	1869.7	206	139	**617.4** (434.7)

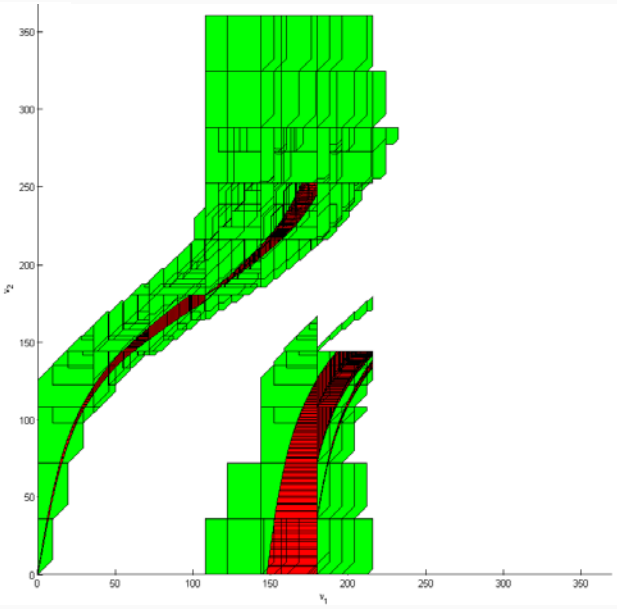
Satellite Benchmark

Inst.	#loc	Uninformed DFS			Box heuristic			PDB		
		#it	length	time	#it	length	time	#it	length	time
1	36	116	32	27.1	75	10	13.4	16	10	**10.3** (7.4)
2	36	464	24	101.3	473	13	116.9	30	13	**16.3** (12.2)
3	64	718	87	31.5	278	87	**11.0**	263	121	20.4 (9.5)
4	100	111	107	38.1	44	15	21.1	23	14	**14.8** (6.0)
5	100	109	104	262.9	45	15	178.6	23	14	**62.9** (5.9)
6	159	2170	∞	78.9	1352	∞	49.9	0	∞	**15.6** (15.6)
7	324	323	102	105.6	1289	106	457.7	25	24	**32.1** (8.8)
8	557	1637	42	45.8	936	42	**26.3**	156	42	44.1 (39.7)
9	574	7113	41	223.6	561	10	17.5	14	10	**6.6** (6.2)
10	575	9092	4	284.8	387	5	12.3	15	4	**2.4** (2.0)
11	576	5693	3769	816.6	257	13	36.5	15	13	**9.9** (5.9)
12	576	32966	13	7059.5	826	13	118.9	15	13	**10.0** (5.8)
13	576	n/a	n/a	OOM	579	52	579.7	58	52	**163.2** (82.0)
14	1293	13691	∞	436.1	7719	∞	249.6	0	∞	**135.5** (135.5)
15	1293	n/a	n/a	OOM	1806	142	1869.7	206	139	**617.4** (434.7)

Satellite Benchmark







Uninformed DFS **Box-heuristic** **PDB**

Navigation Benchmark

Inst.	#loc	Uninformed DFS			Box heuristic			PDB		
		#it	length	time	#it	length	time	#it	length	time
1	400	122	15	145.8	62	15	70.5	16	15	**20.0** (1.9)
2	400	183	33	186.9	86	33	120.4	34	33	**53.9** (7.6)
3	625	75	33	70.7	34	33	**36.6**	34	33	44.7 (7.5)
4	625	268	158	261.9	231	158	209.6	159	158	**127.5** (10.5)
5	625	85	79	118.8	26	25	**37.8**	26	25	42.1 (3.7)
6	625	96	53	110.8	101	53	104.9	54	53	**76.3** (9.8)
7	625	227	34	198.9	105	34	96.9	35	34	**47.6** (9.4)
8	625	178	25	266.1	86	25	137.3	26	25	**43.5** (7.0)
9	625	297	17	356,0	102	17	131.9	18	17	**30.8** (7.6)
10	625	440	30	534,0	136	30	201.8	31	30	**60.9** (13.6)
11	900	234	72	269.3	129	21	149.1	22	21	**32.7** (8.1)
12	900	317	43	339.1	174	61	198.3	44	43	**62.8** (15.8)
13	900	367	37	421.9	148	37	190.4	38	37	**70.7** (20.1)
14	900	411	32	434.6	278	32	297.9	33	32	**57.7** (10.9)
15	900	379	44	445.9	107	44	137.8	45	44	**69.9** (9.0)

Conclusions

- **Done:** Novel heuristics for effective search guidance in concrete symbolic state space
- **Box-based heuristic:**
  - Light-weight on-the-fly heuristic estimation
  - Suited for systems with primarily continuous behavior
- **PDB heuristic:**
  - Involves pre-computation phase
  - Considers both discrete and continuous behavior
- **Future work:**
  - Combination of information through several heuristics
  - Exploration of complexity dimensions