

Classifying Data Races with Portend

Baris Kasikci, Cristian Zamfir, and George Candea

School of Computer & Communication Sciences



ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Data Races

Data Races

- Accesses to shared memory location

Data Races

- Accesses to shared memory location
 - *By multiple threads*

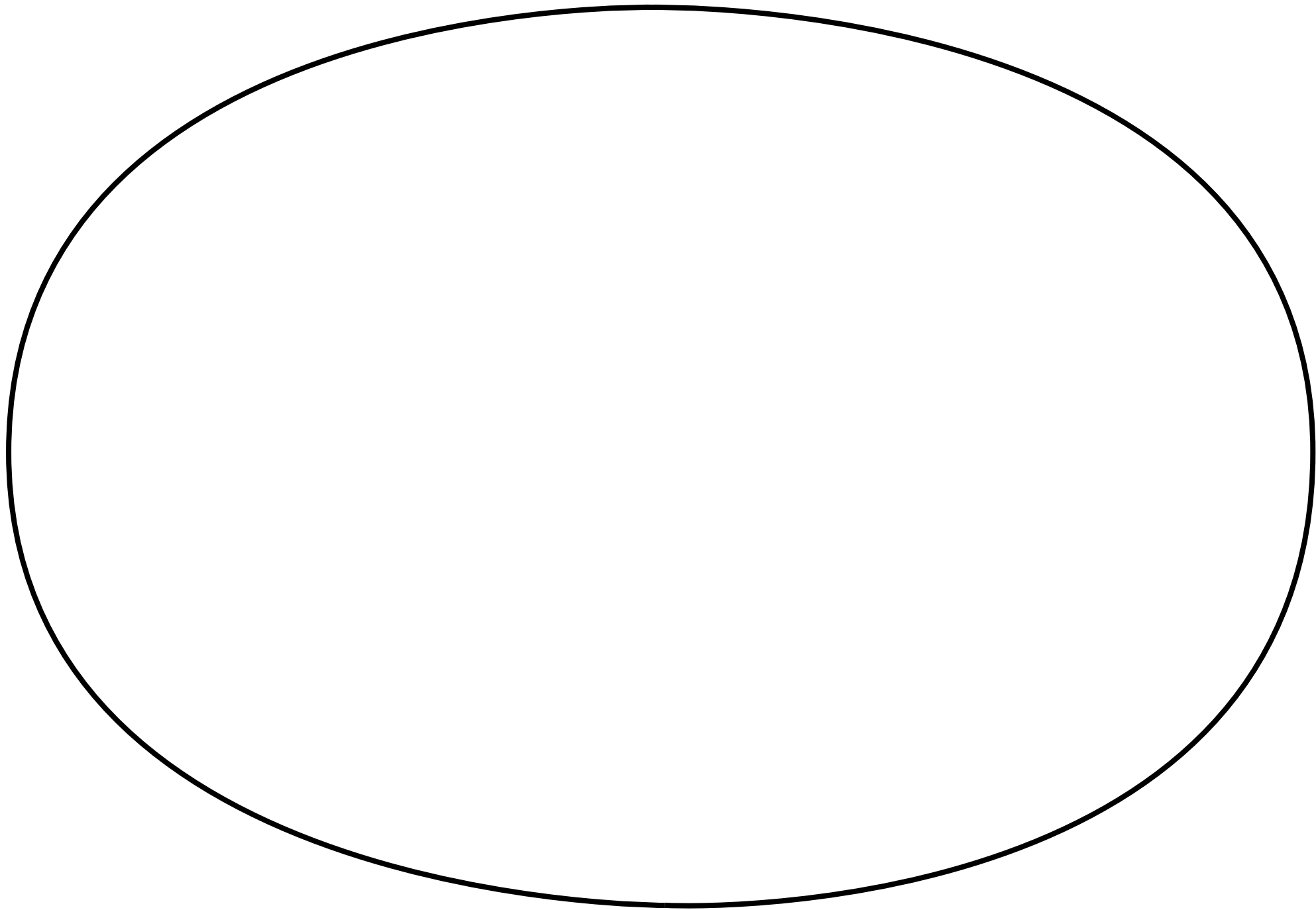
Data Races

- Accesses to shared memory location
 - *By multiple threads*
 - *At least one of the accesses is a write*

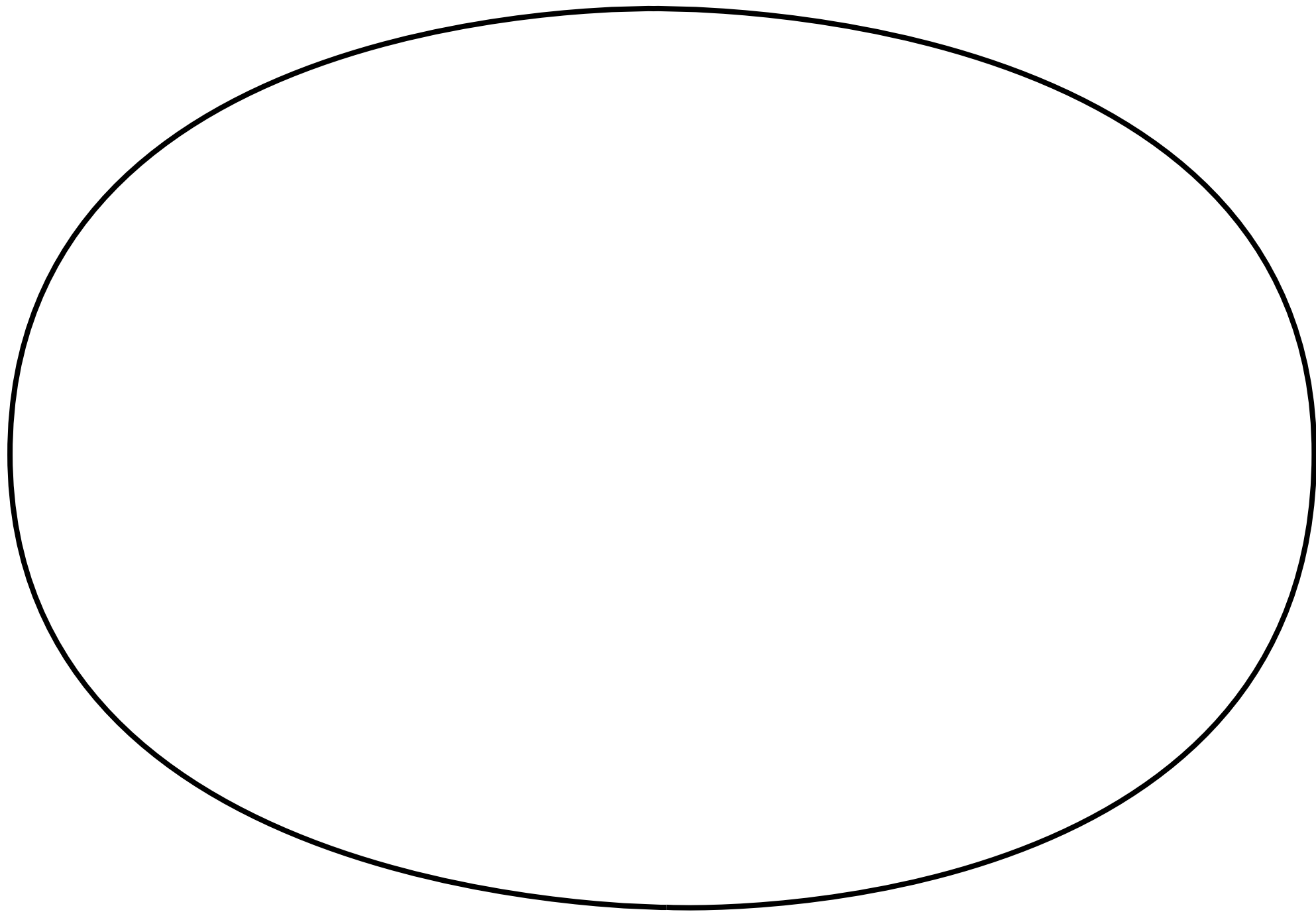
Data Races

- Accesses to shared memory location
 - *By multiple threads*
 - *At least one of the accesses is a write*
 - *The accesses can happen simultaneously*

Data Races



Data Races



Races are numerous in modern software

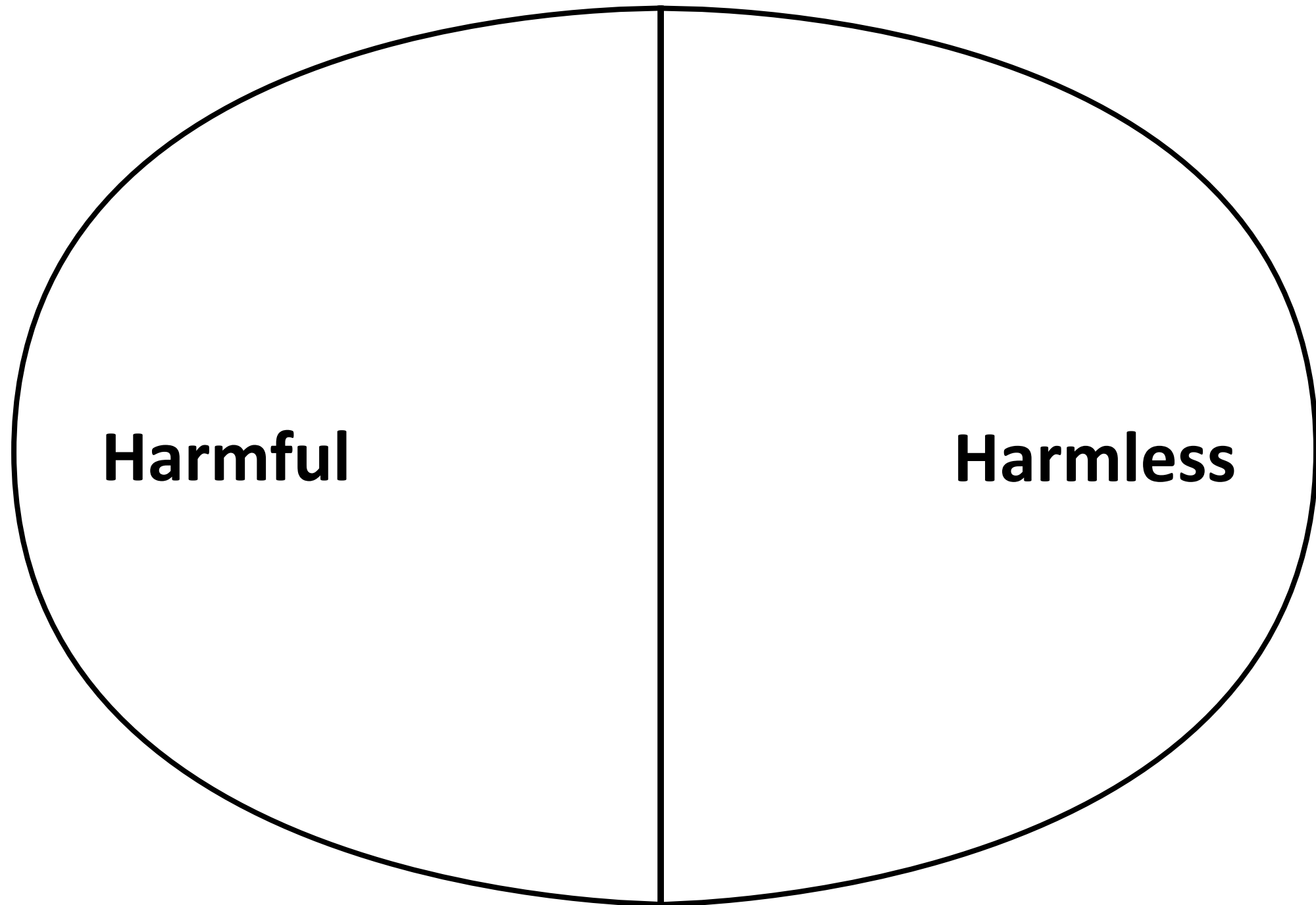
Data Races



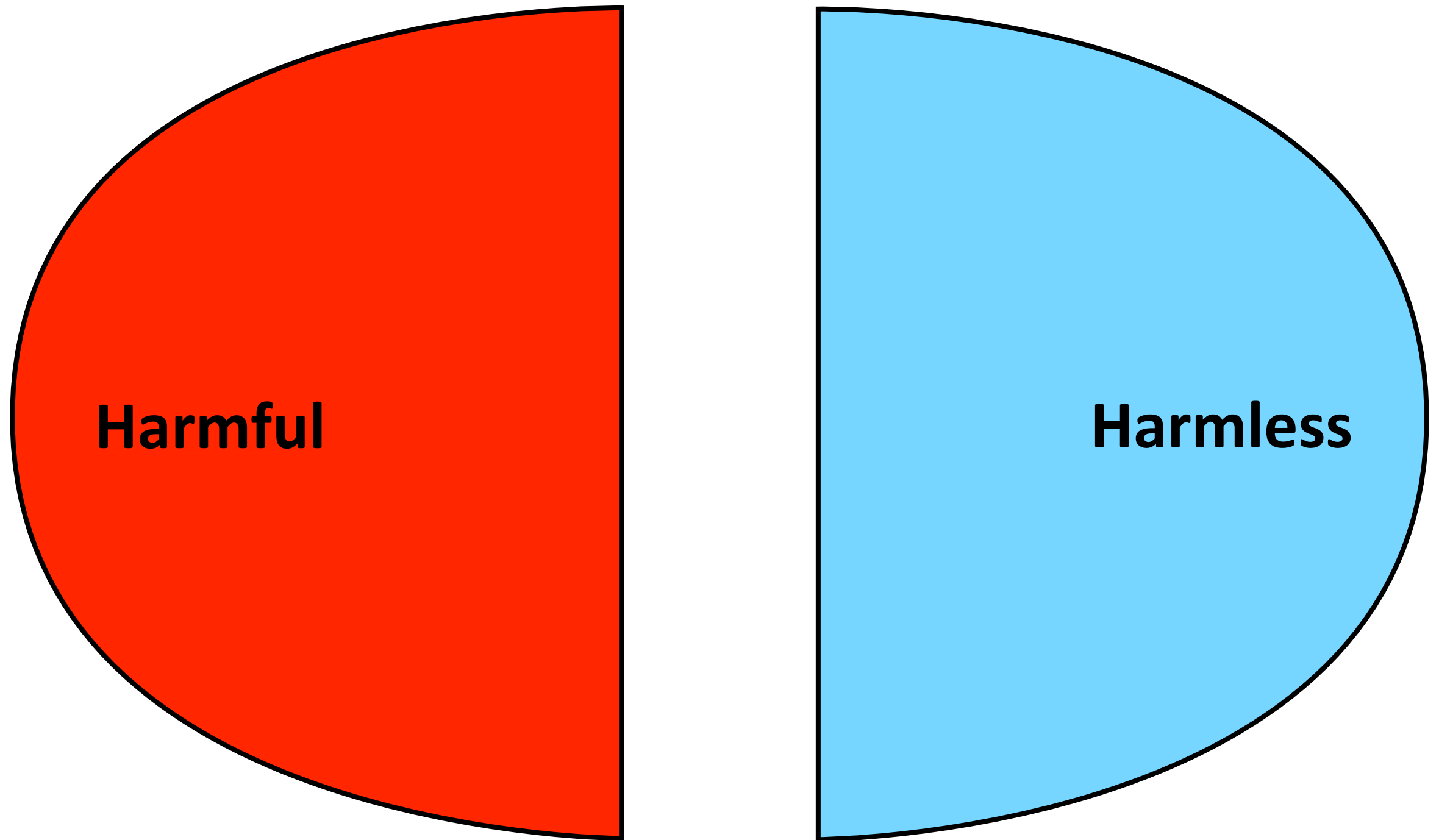
1000 Races

Races are numerous in modern software

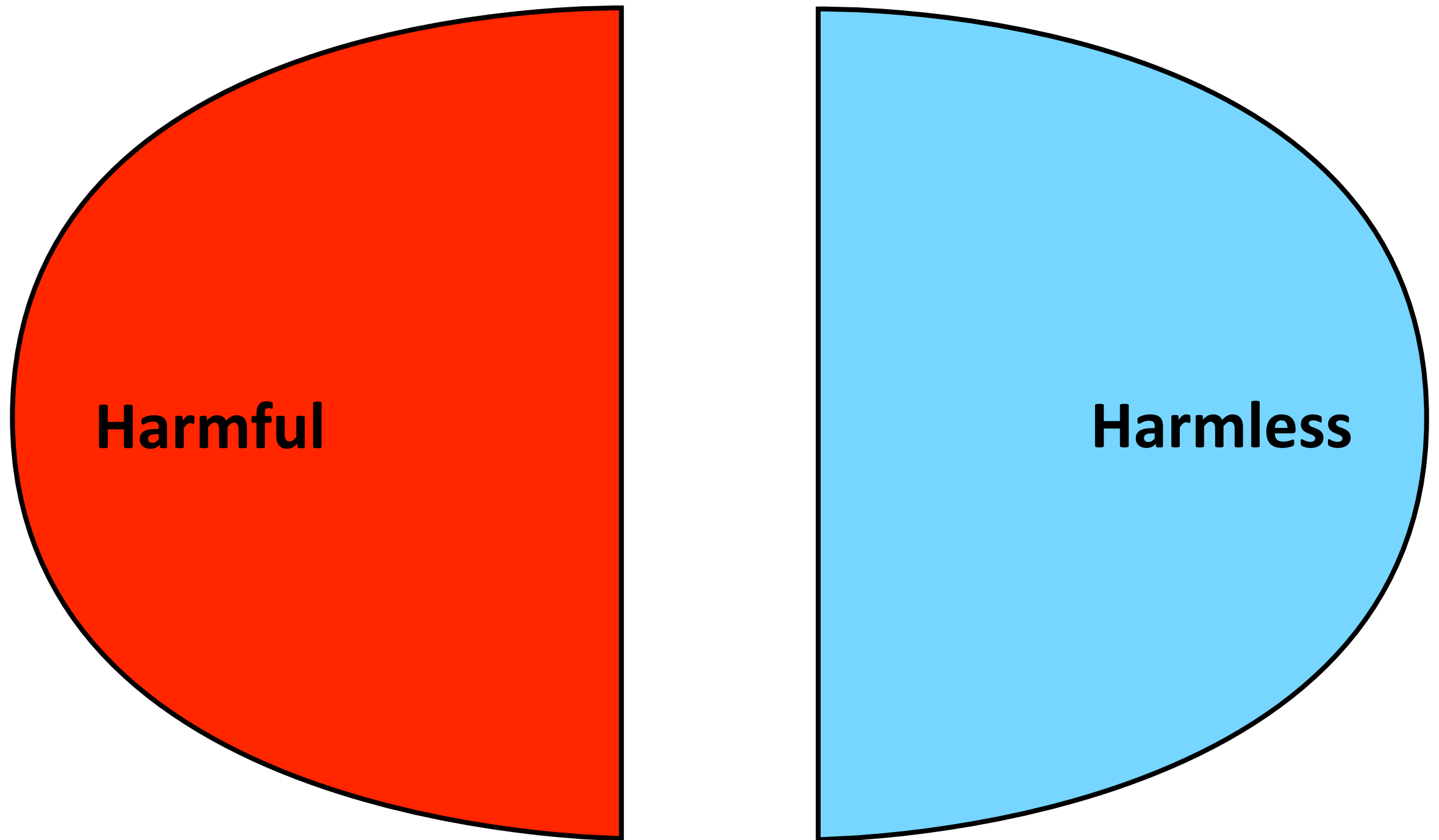
Data Races



Data Races

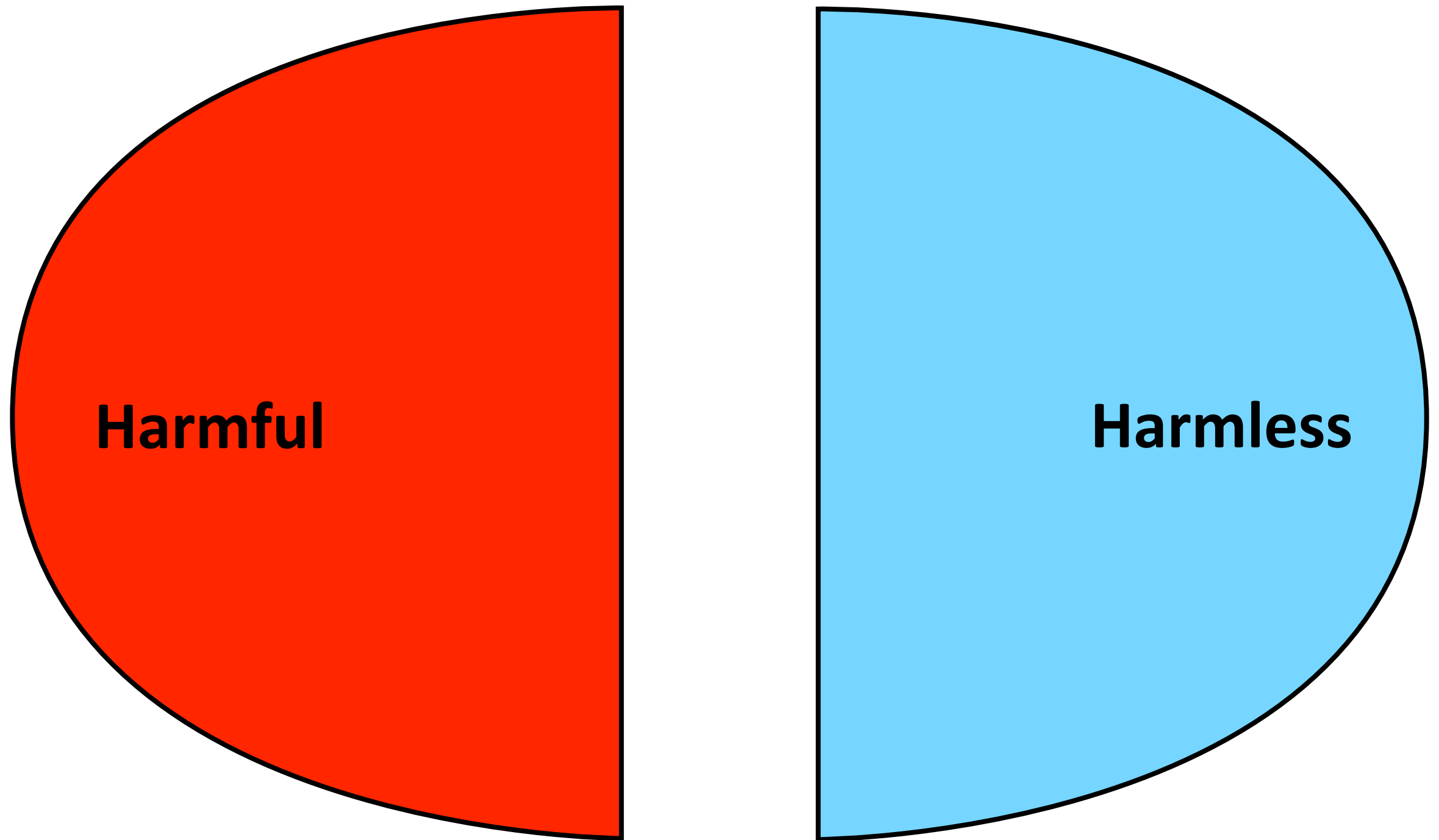


Data Races

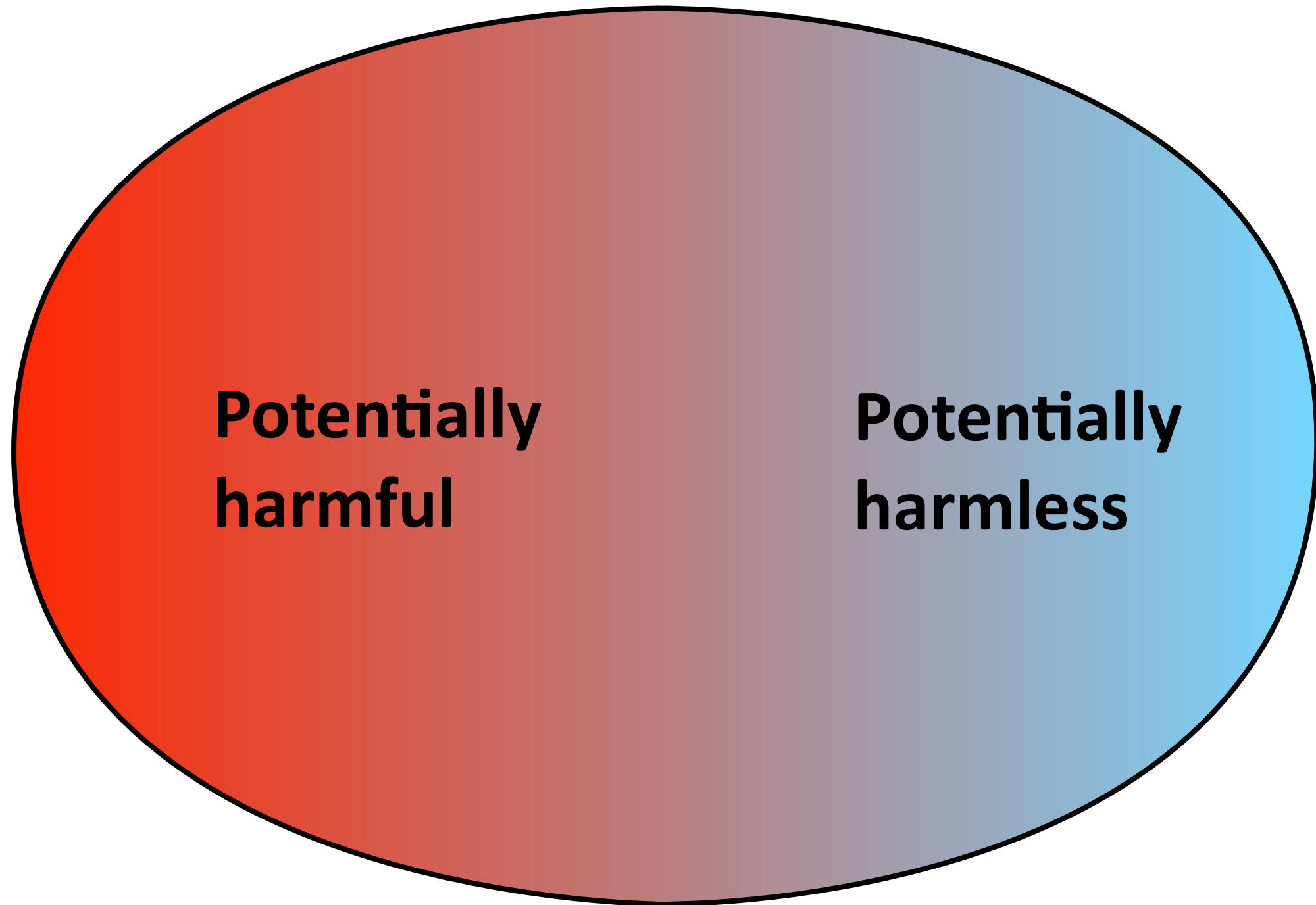


Fix harmful races first!

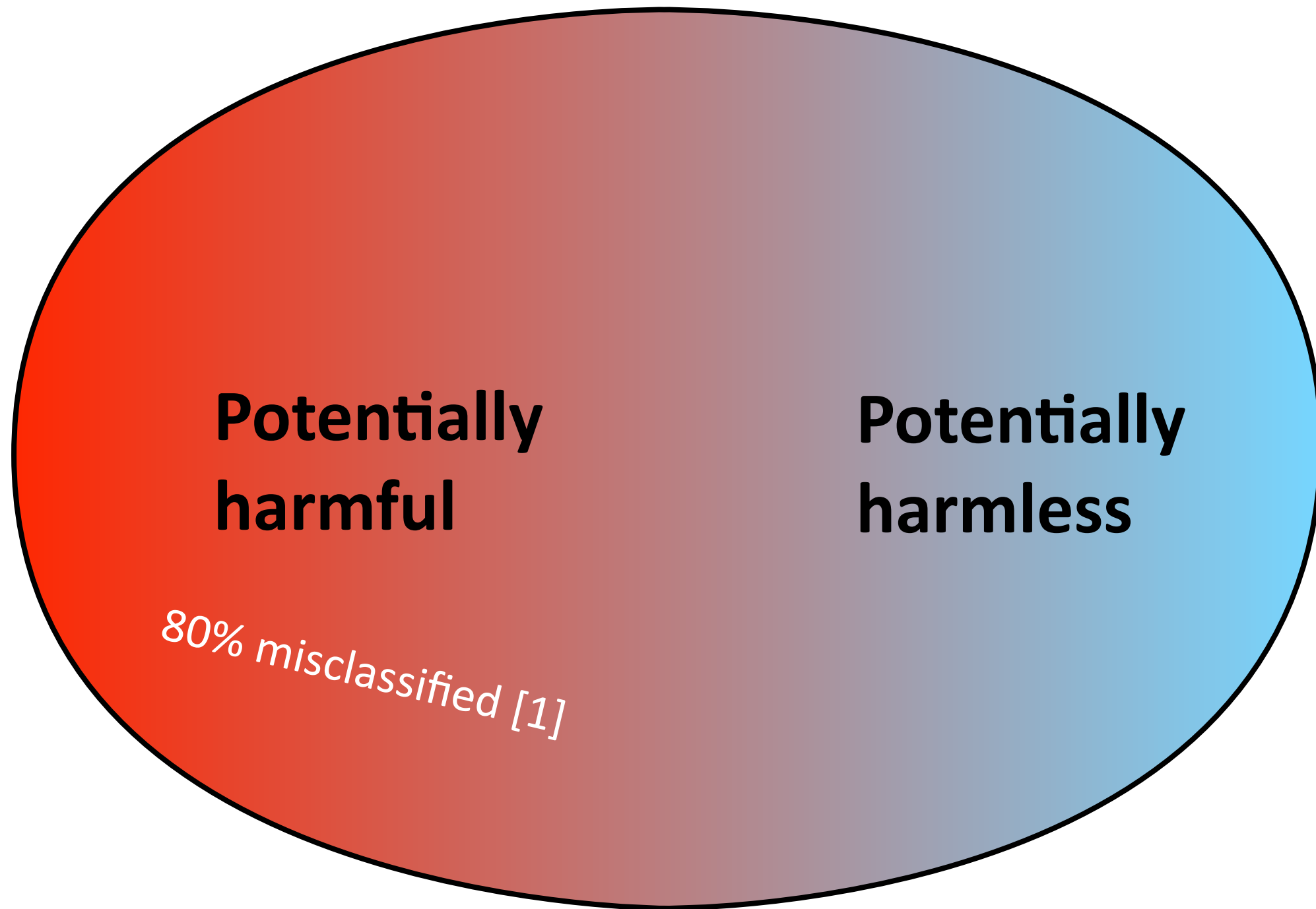
Data Races



Data Races

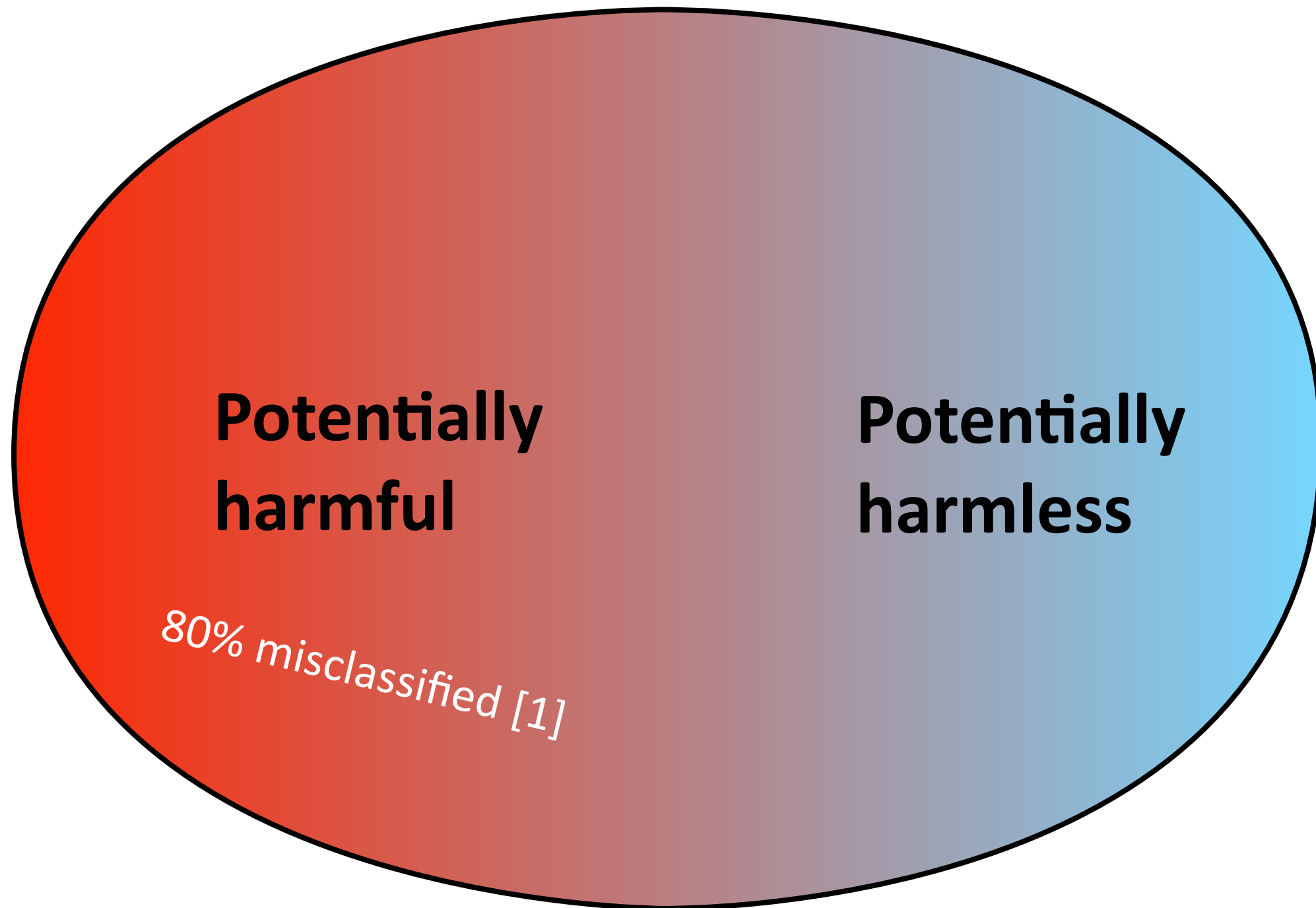


Data Races



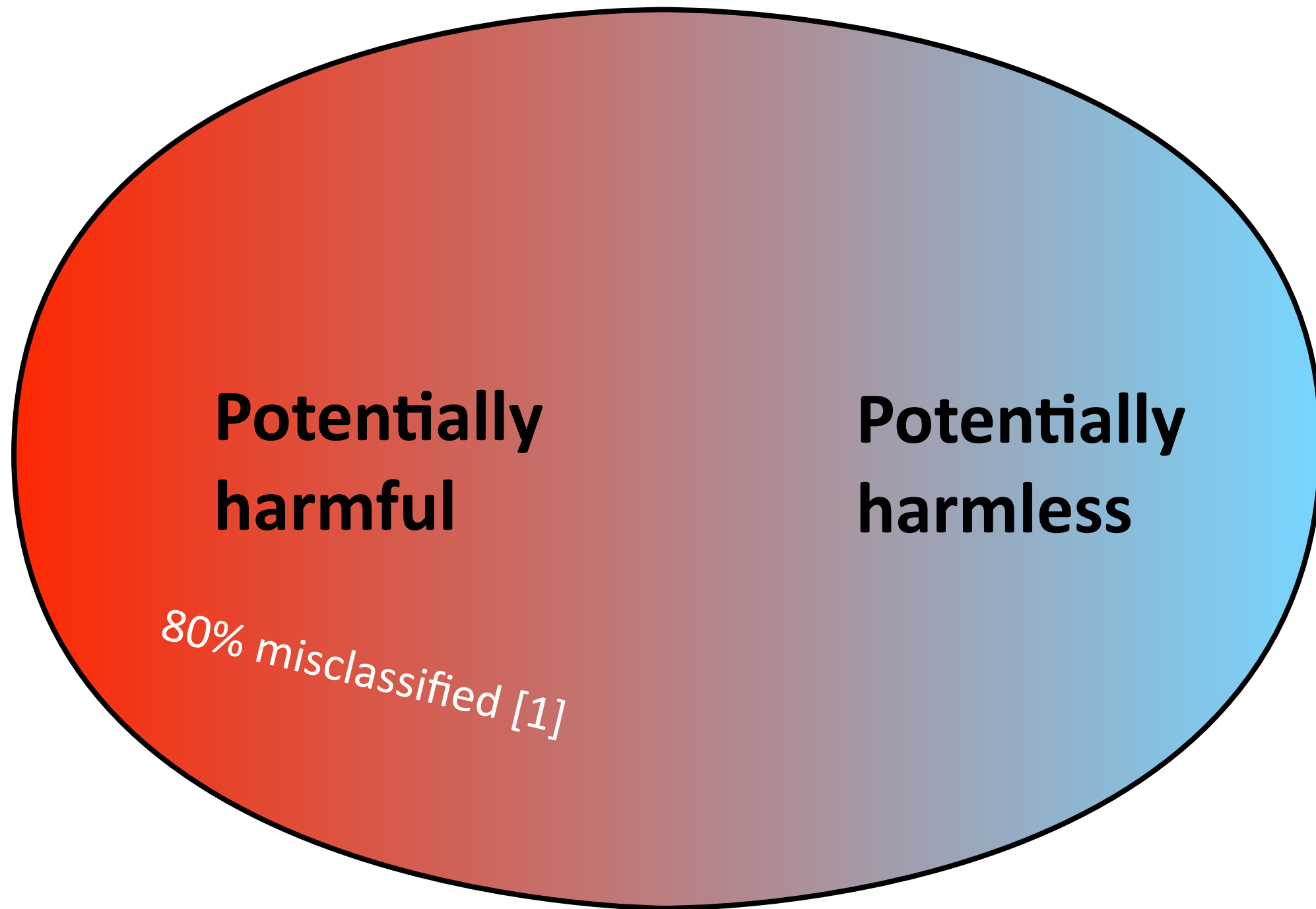
[1] S. Narayanasamy et. al., Automatically classifying benign and harmful data races using replay analysis. PLDI , 2007

Data Races



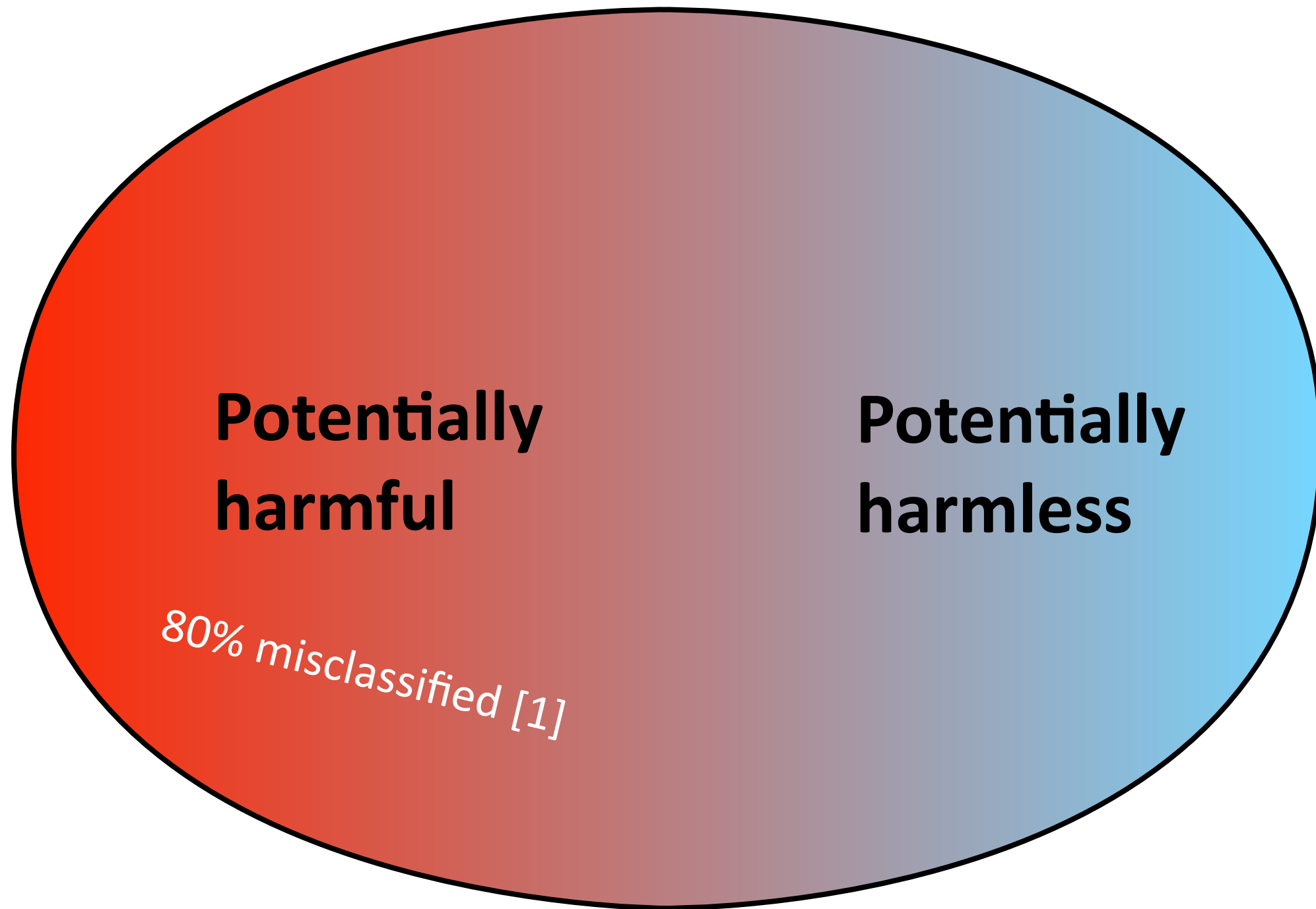
[2] P. Godefroid et al., Concurrency at Microsoft – An exploratory survey. CAV Workshop on Exploiting Concurrency Efficiently and Correctly, 2008

Data Races



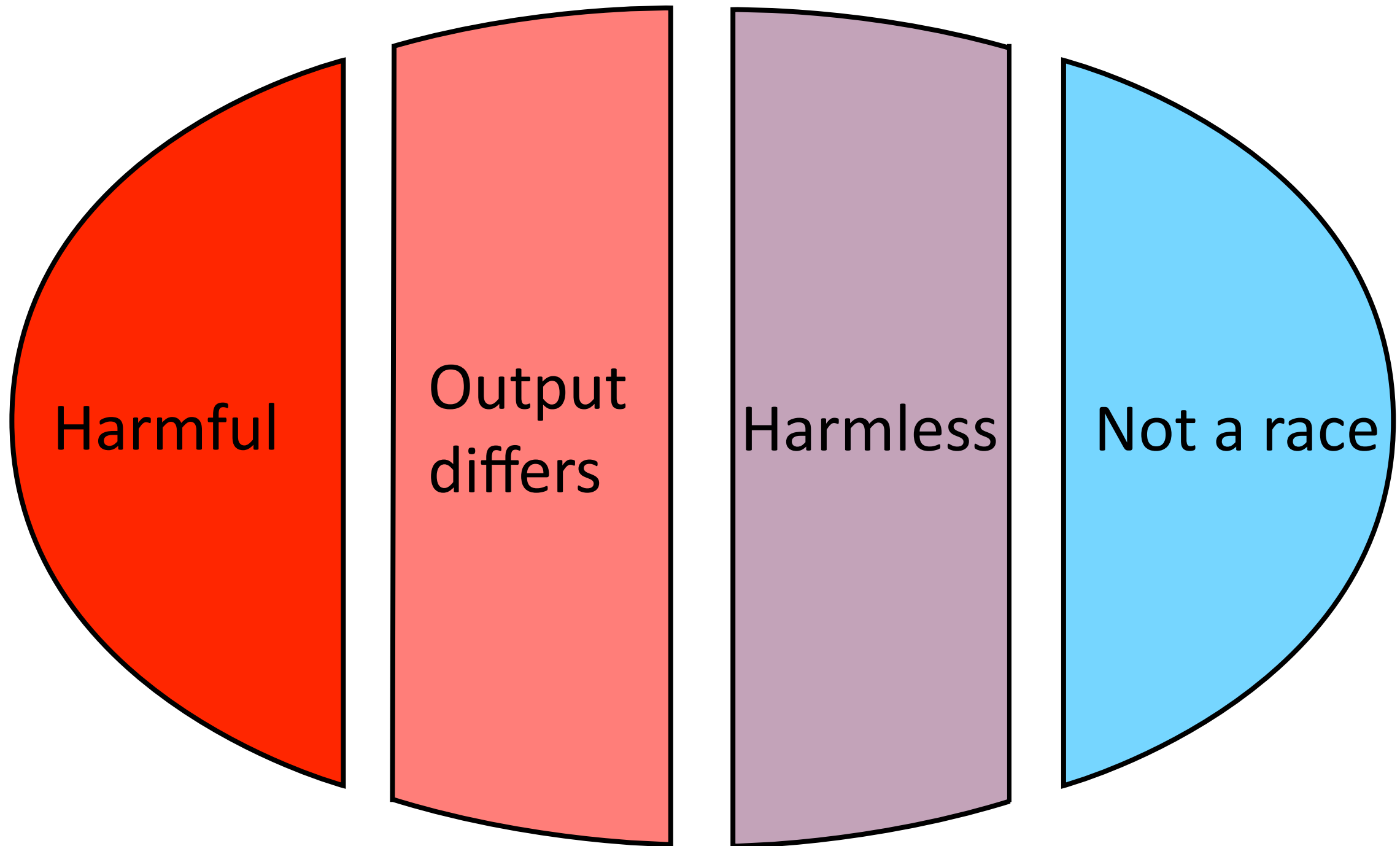
Vague taxonomy and low accuracy

Data Races

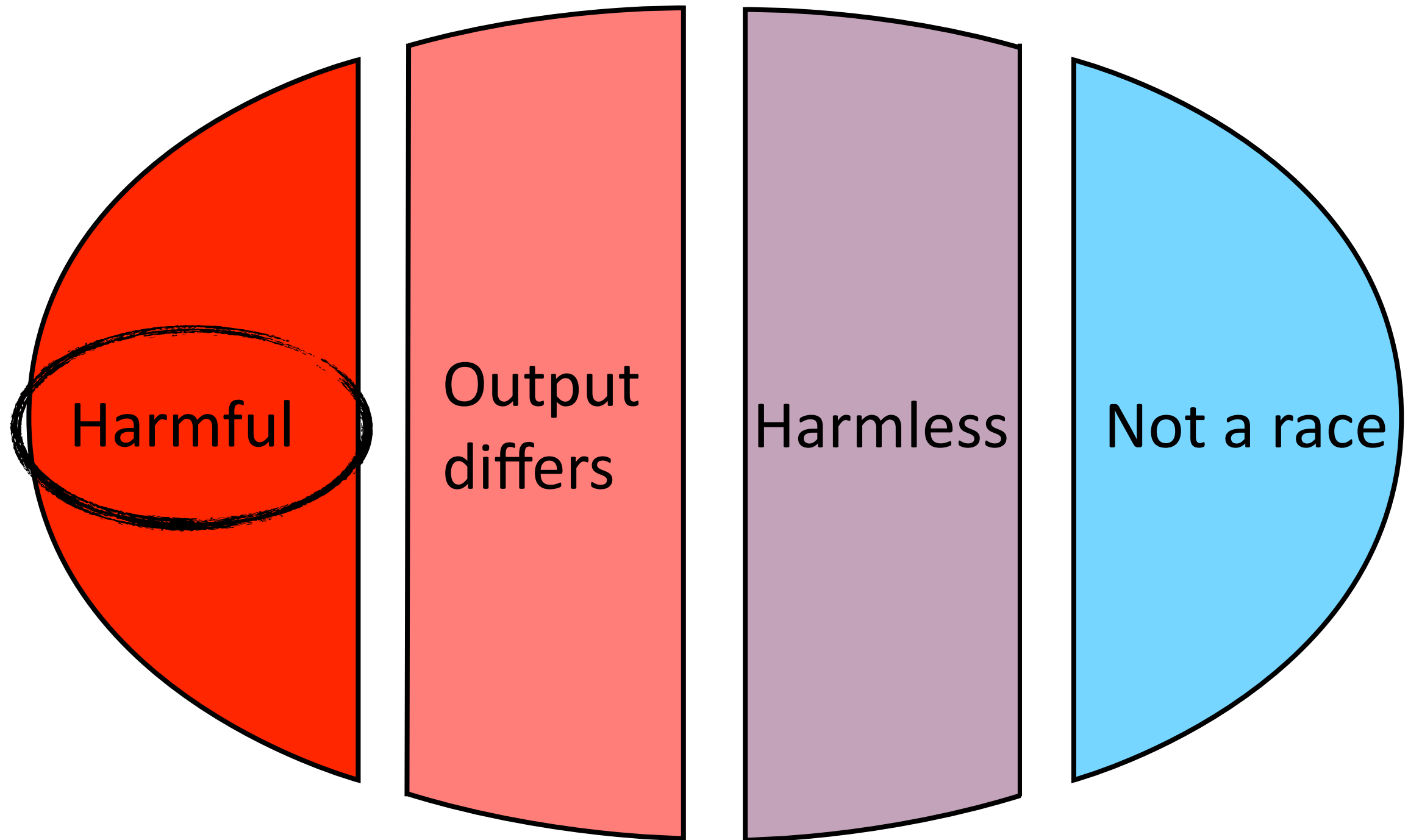


Vague taxonomy and low accuracy

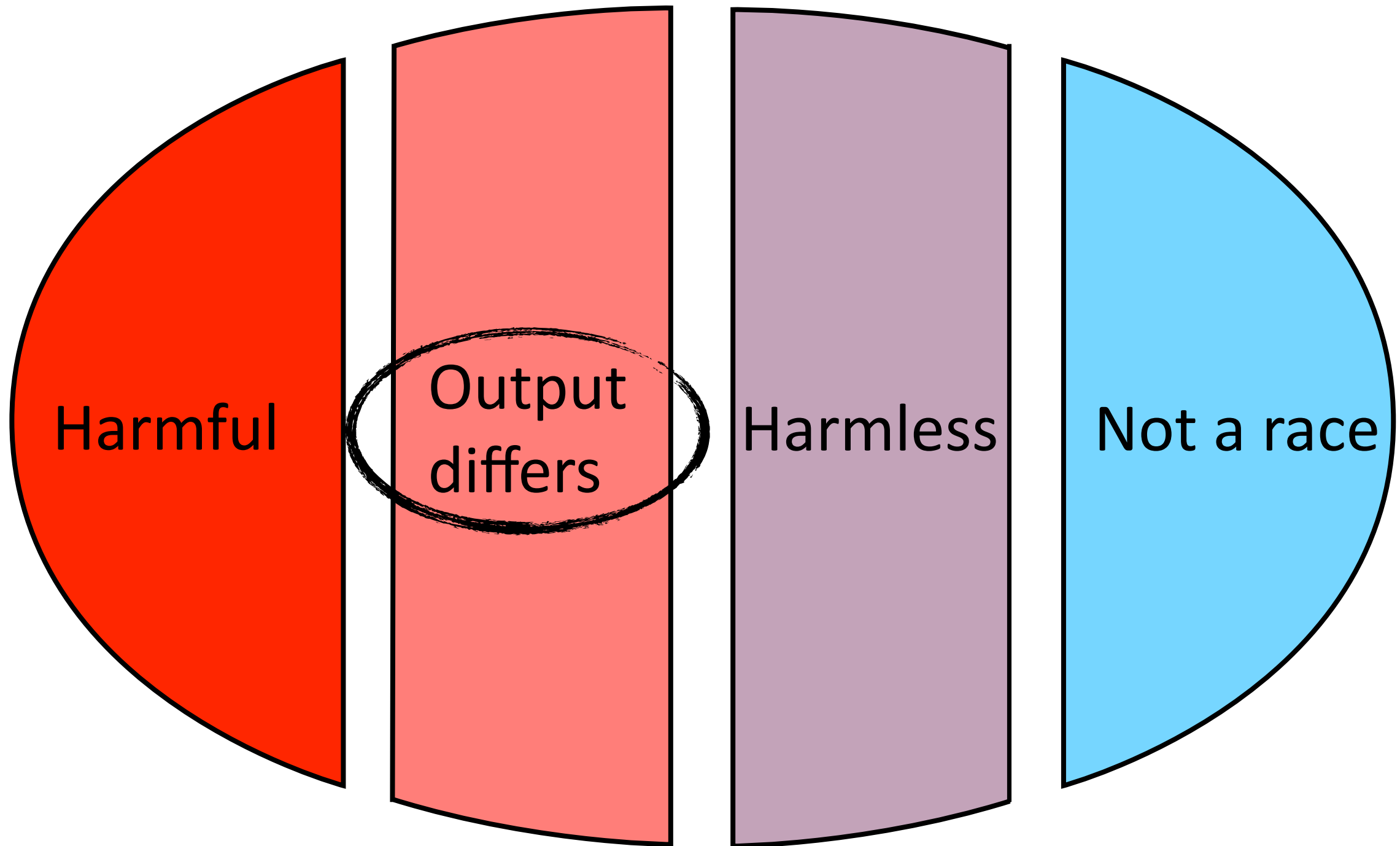
Data Races



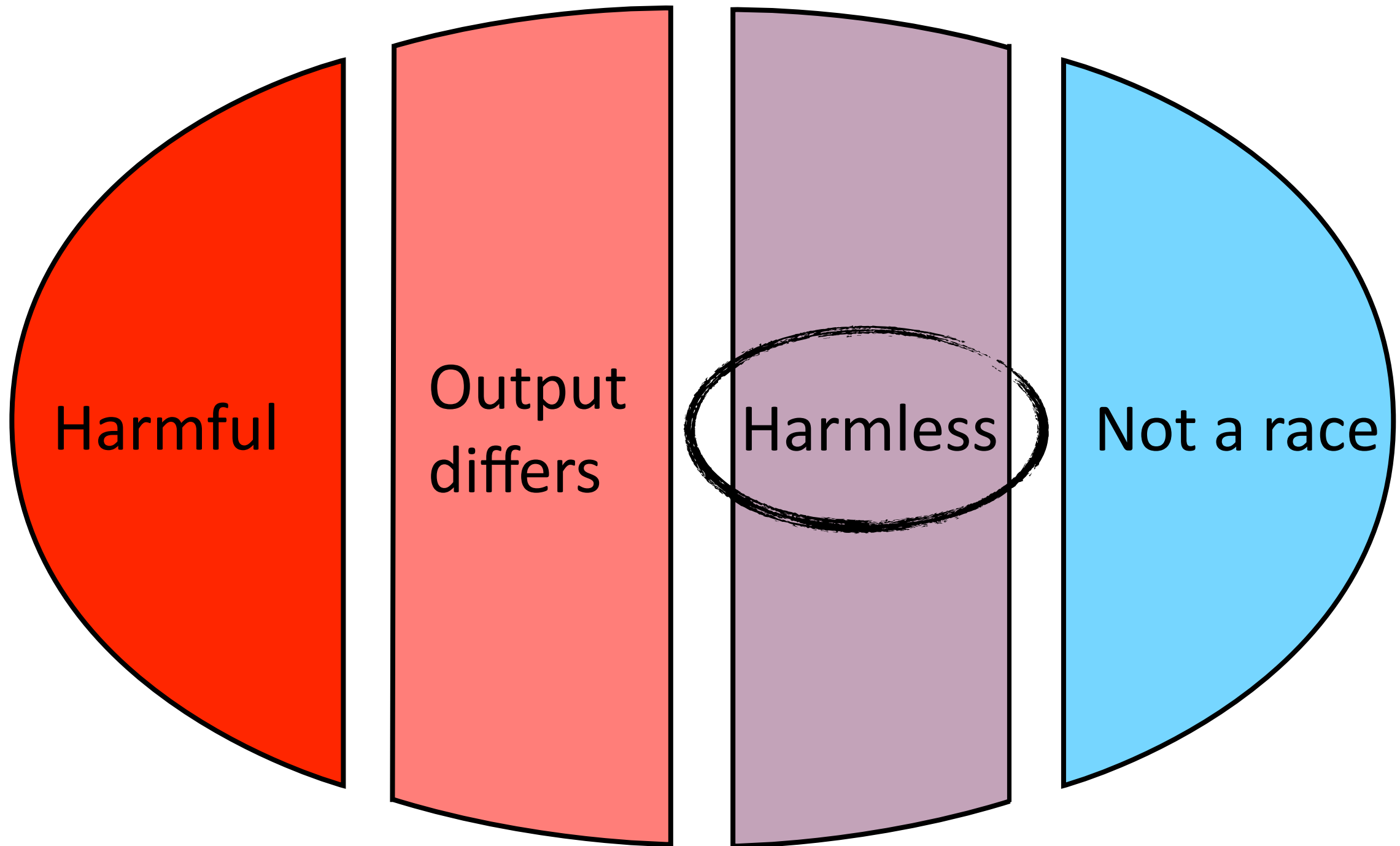
Data Races



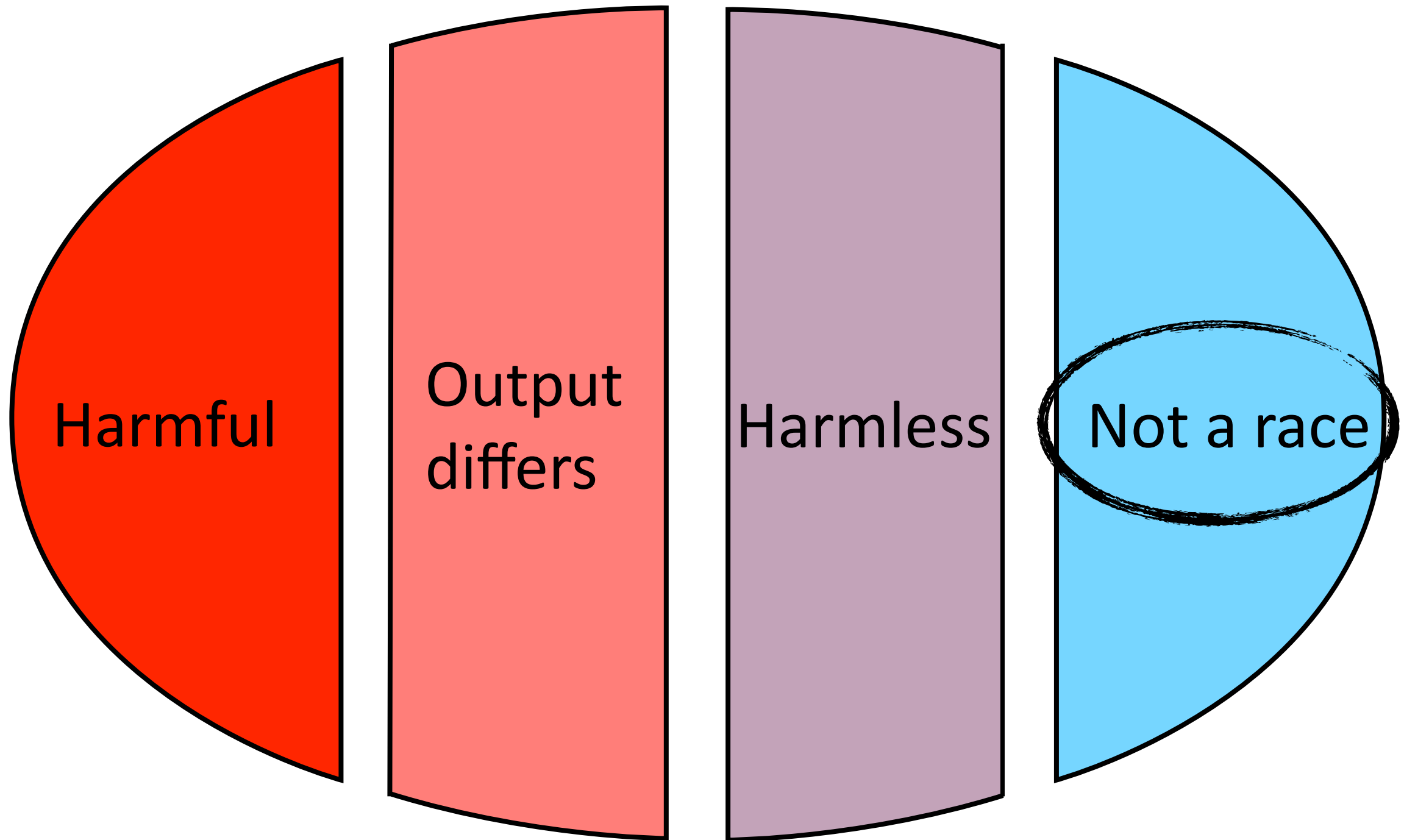
Data Races



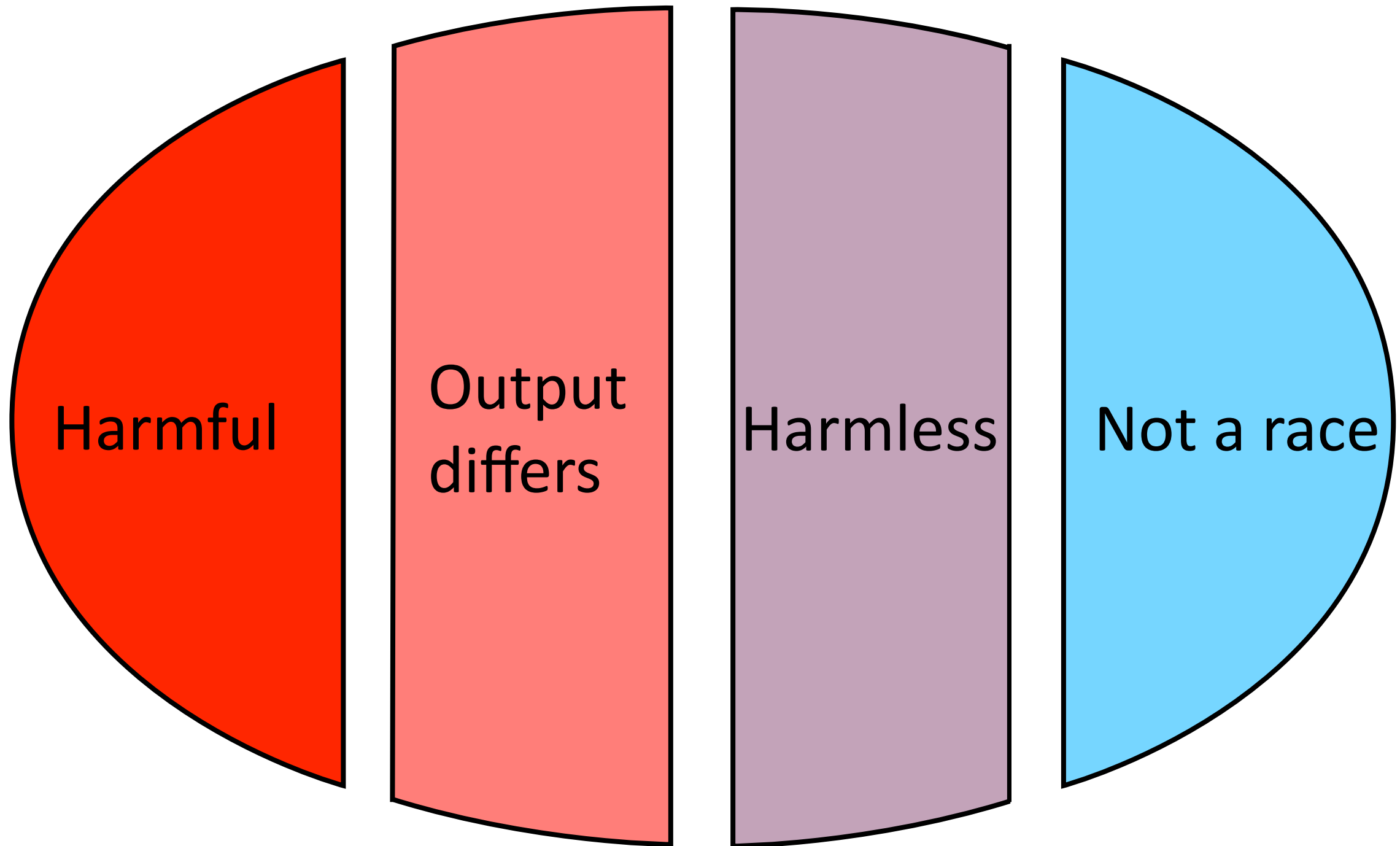
Data Races



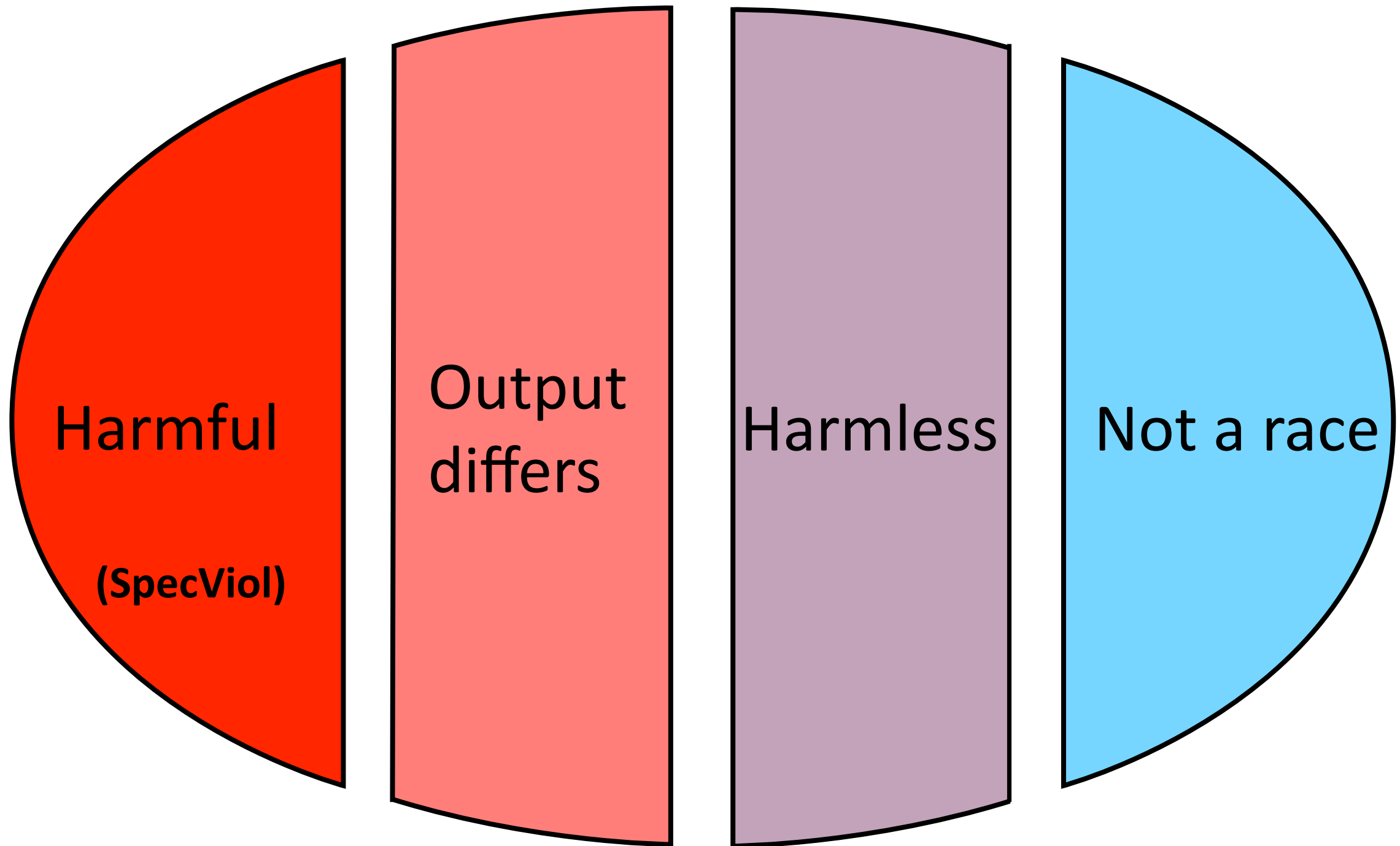
Data Races



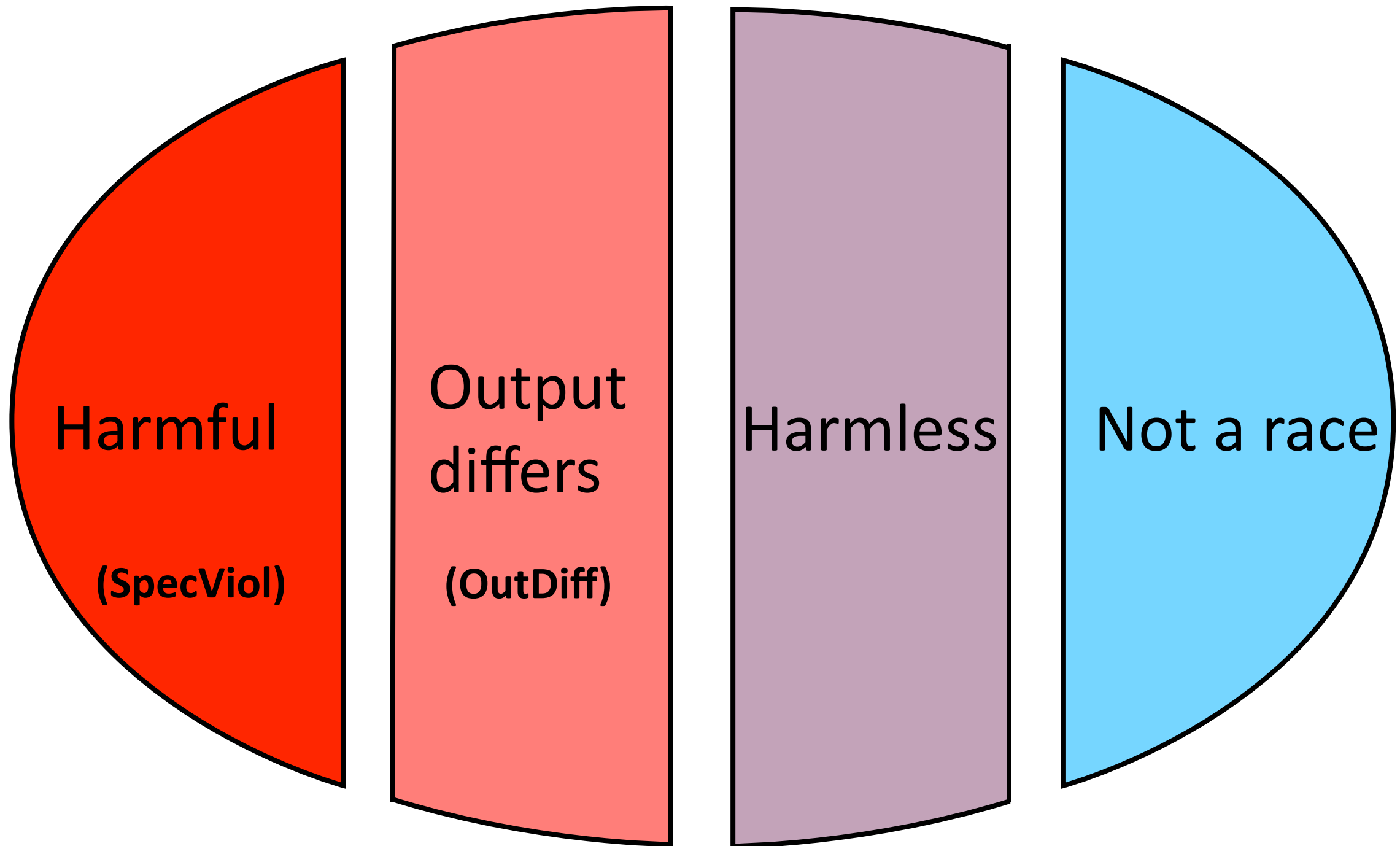
Data Races



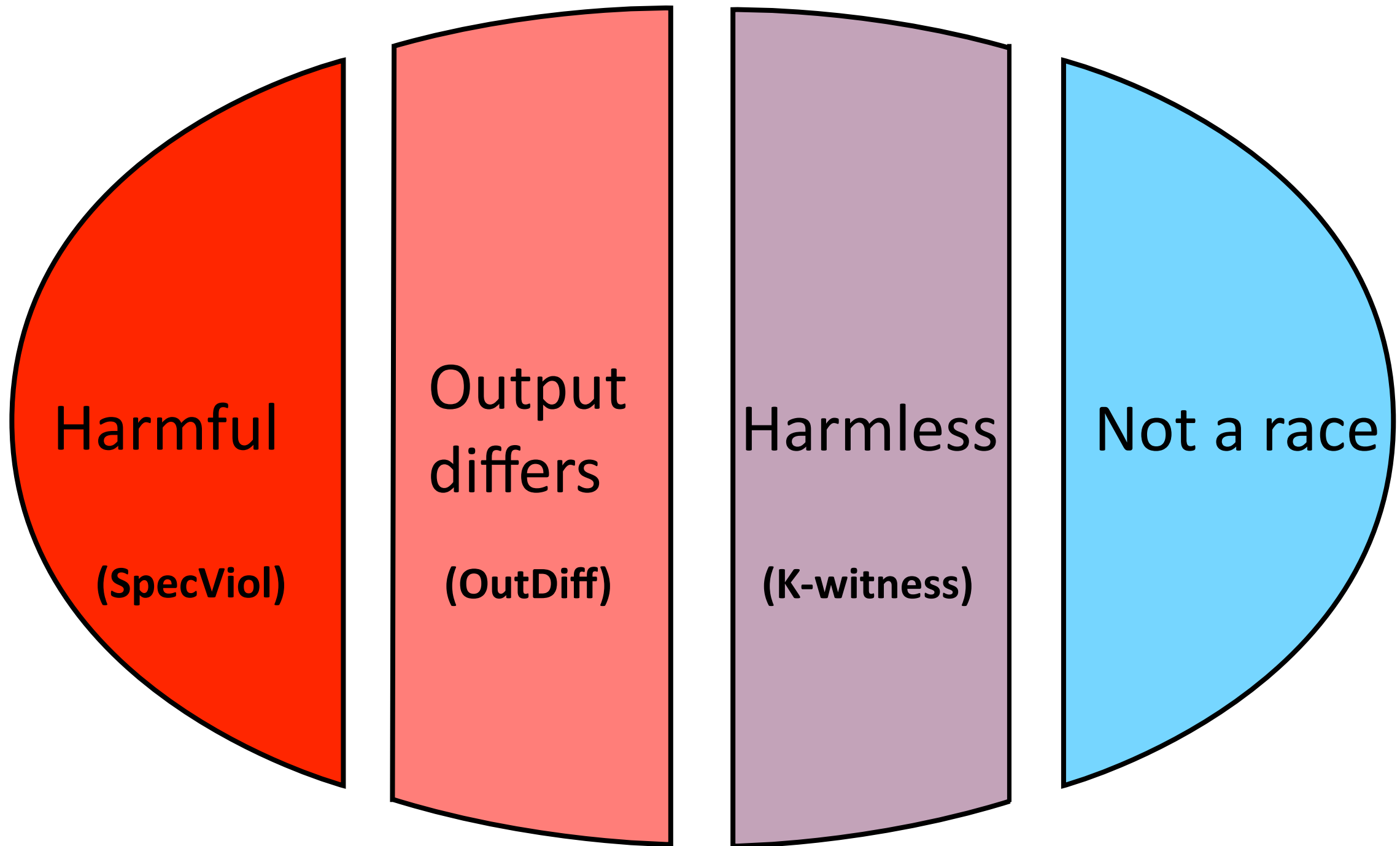
Data Races



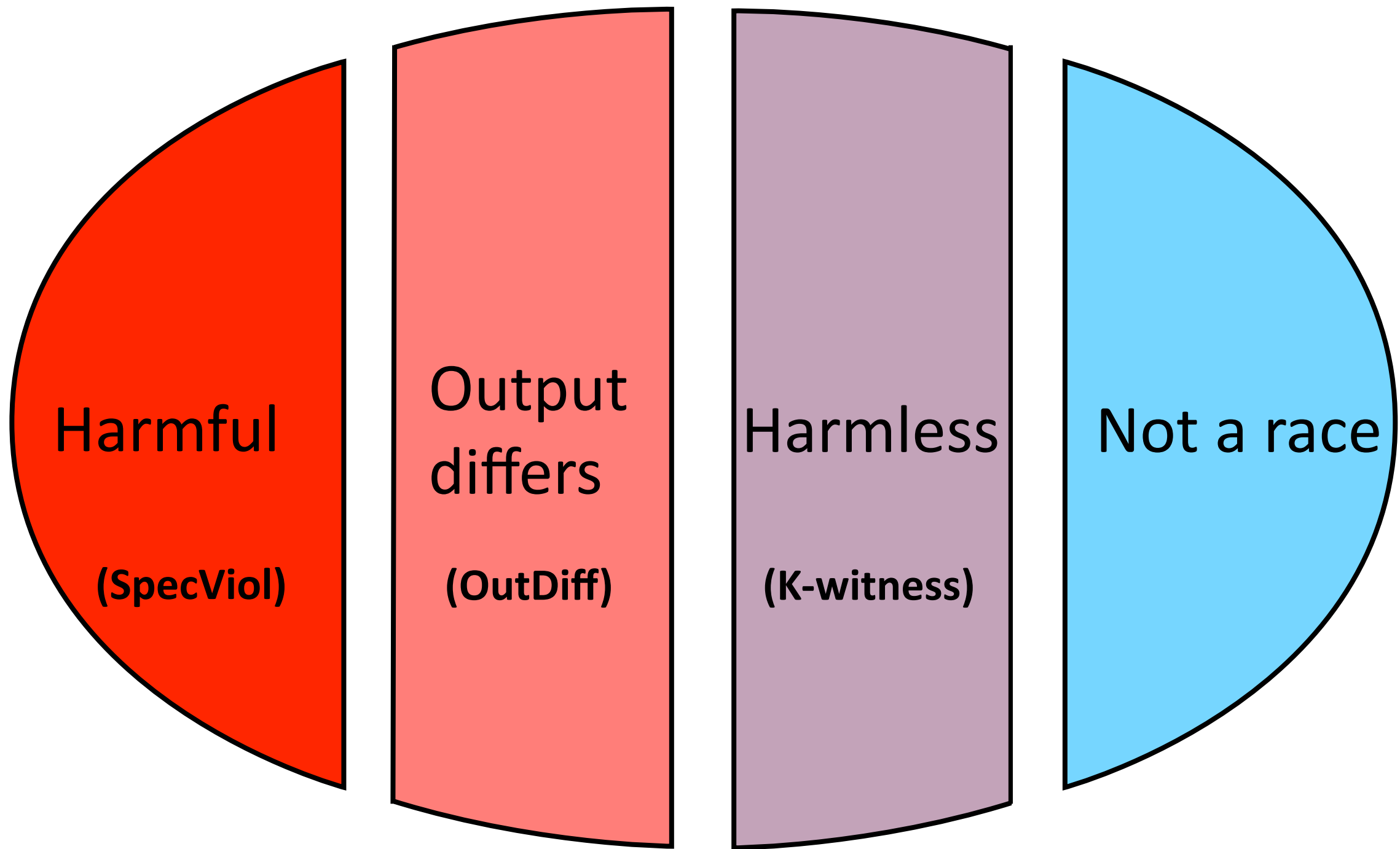
Data Races



Data Races

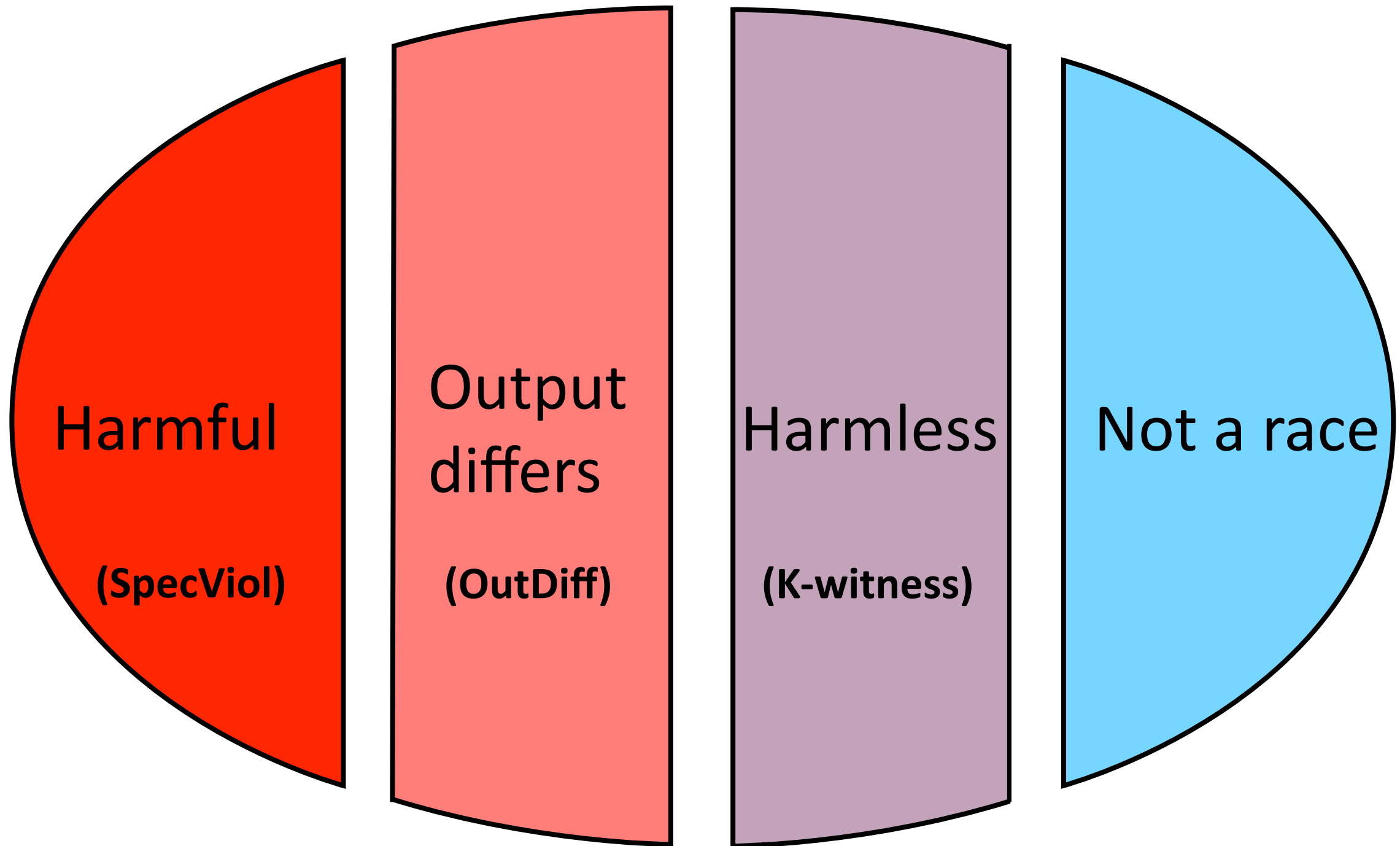


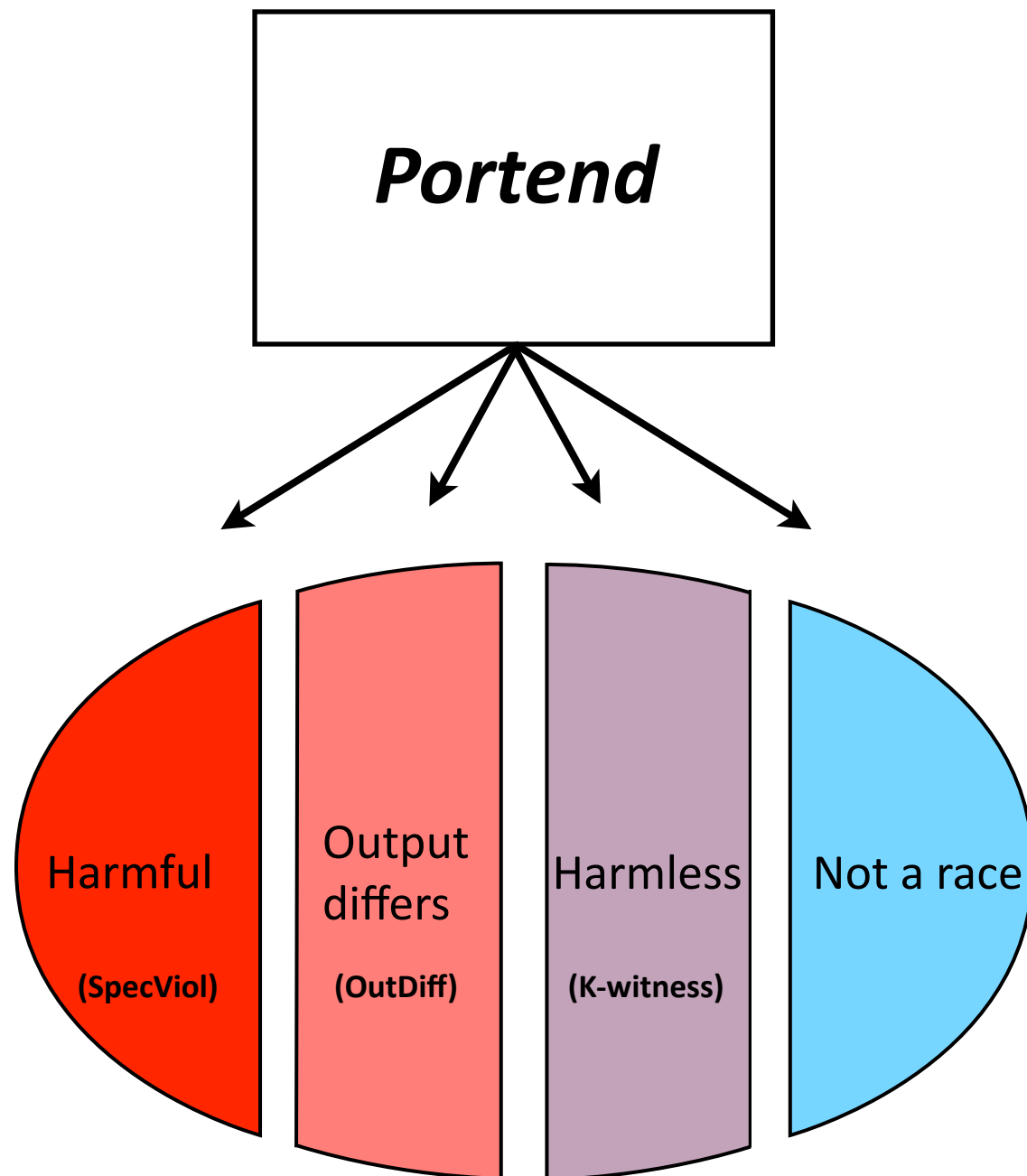
Data Races



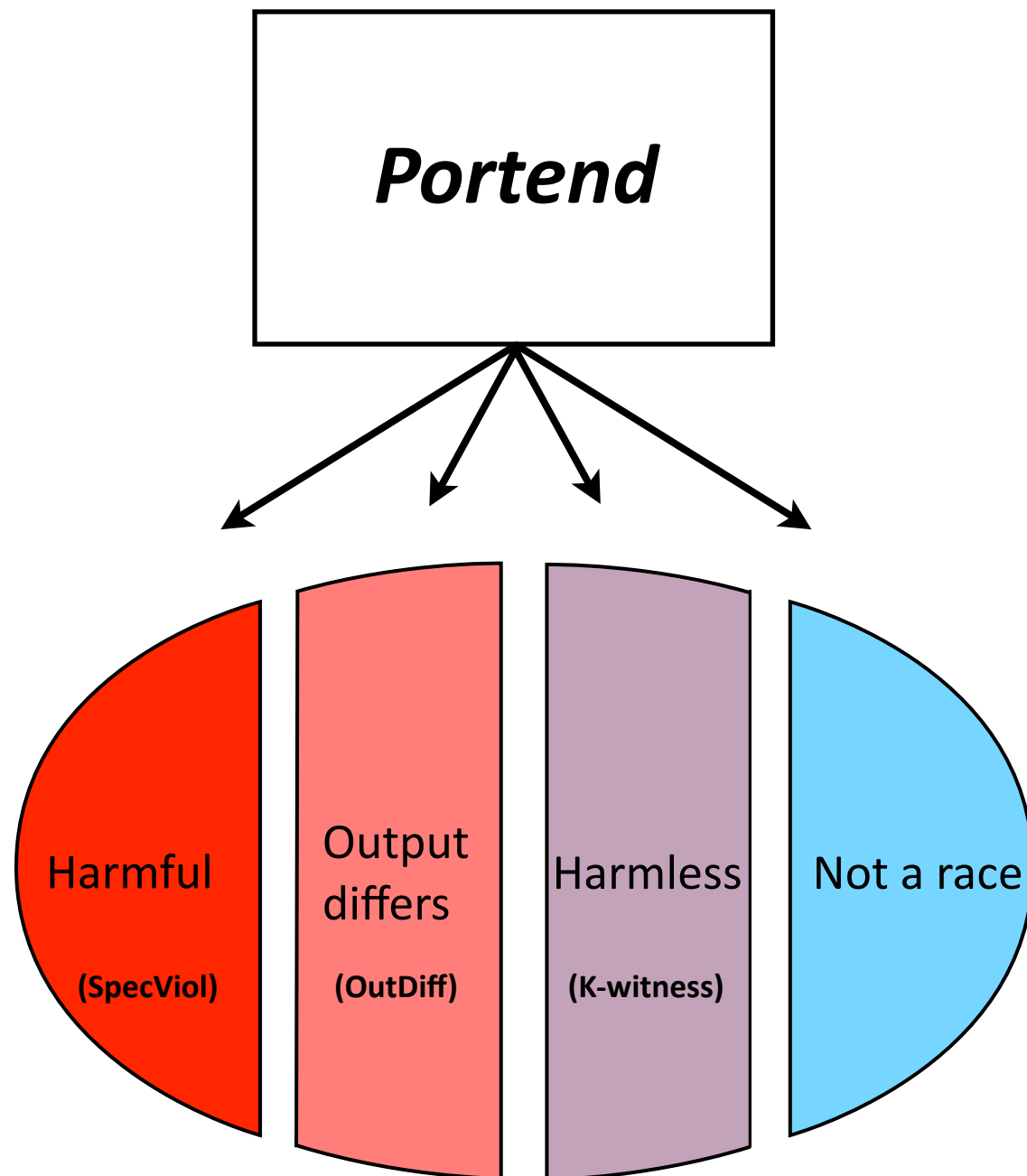
Developer can prioritize the inspection of races

Data Races

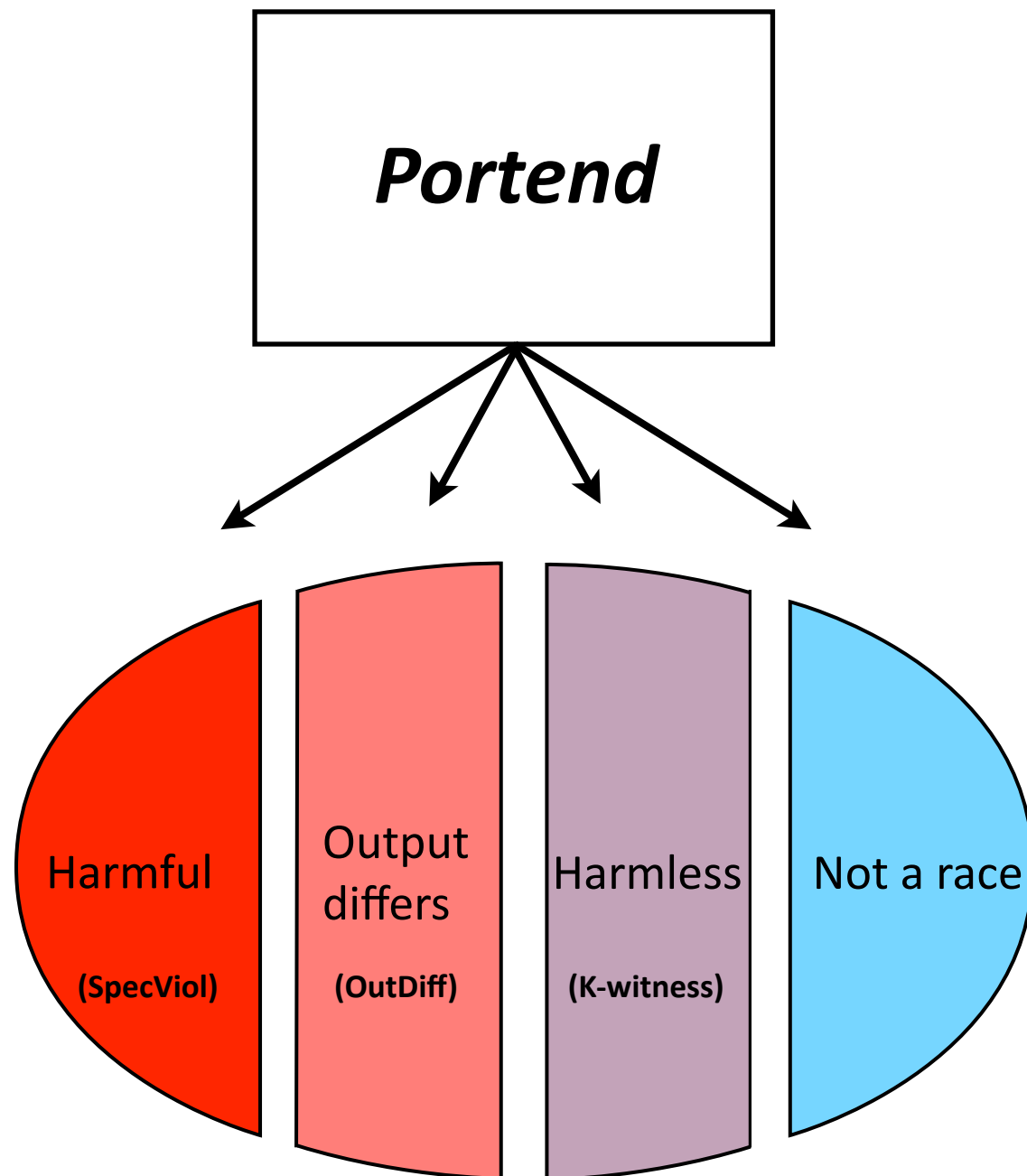




- Classified 93 real-world data races
- With 99% accuracy



- Classified 93 real-world data races
- With 99% accuracy
- In less than 5 minutes/race
- *Manual verified in 240 hours (1 person-month)*
- *Could have saved around 230 hours*



- Classified 93 real-world data races
- With 99% accuracy
- In less than 5 minutes/race
- *Manual verified in 240 hours (1 person-month)*
- *Could have saved around 230 hours*

More precise taxonomy and higher accuracy

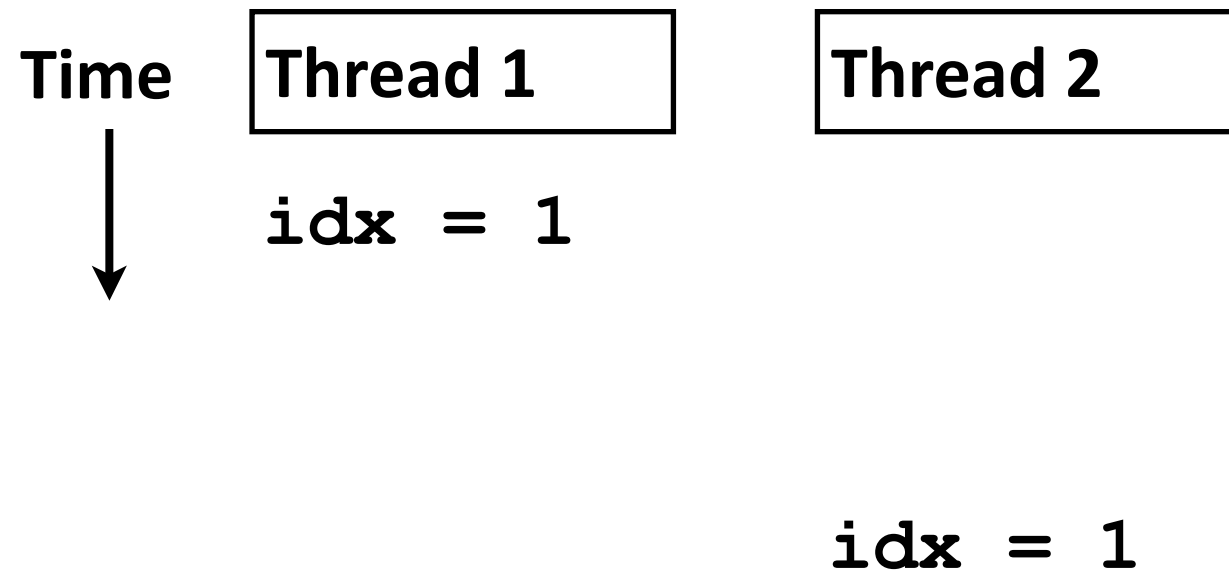
Contributions

- Finer grained, more precise taxonomy
- High precision data race classifier
 - *Multi-path multi-schedule data race analysis*
 - *Symbolic output comparison*

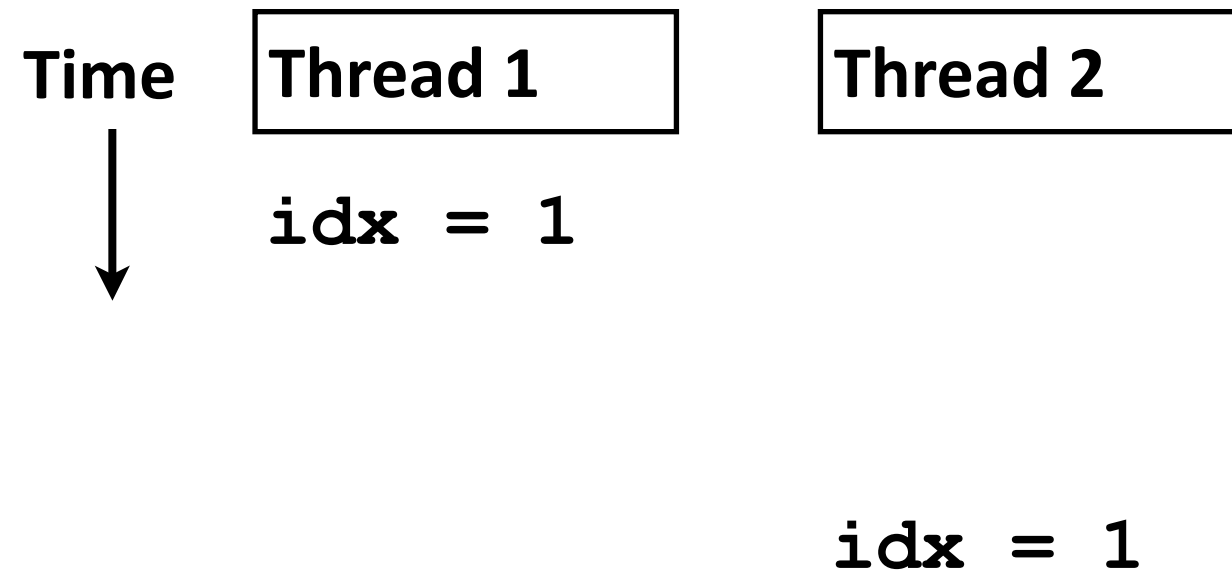
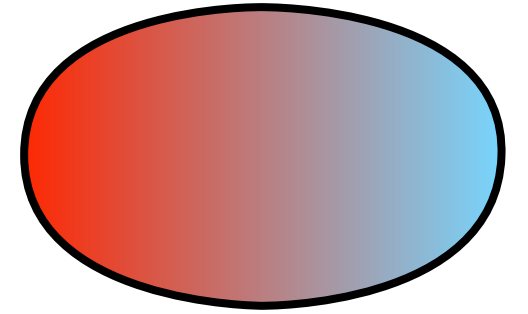
Contributions

- Finer grained, more precise taxonomy
- High precision data race classifier
 - *Multi-path multi-schedule data race analysis*
 - *Symbolic output comparison*

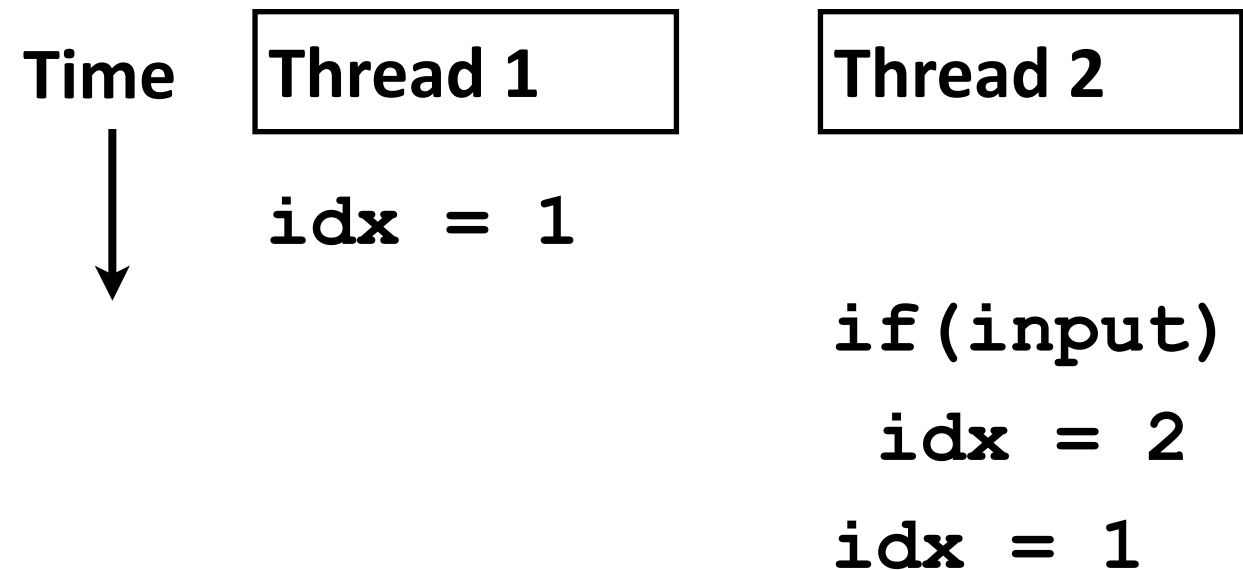
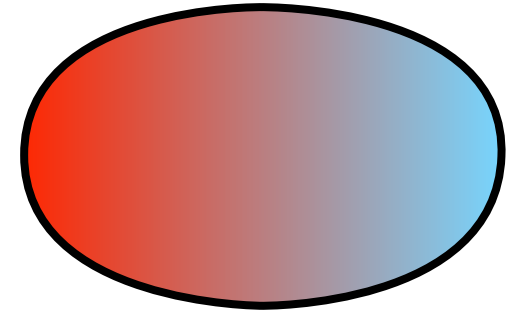
Single-path Analysis (prior work)



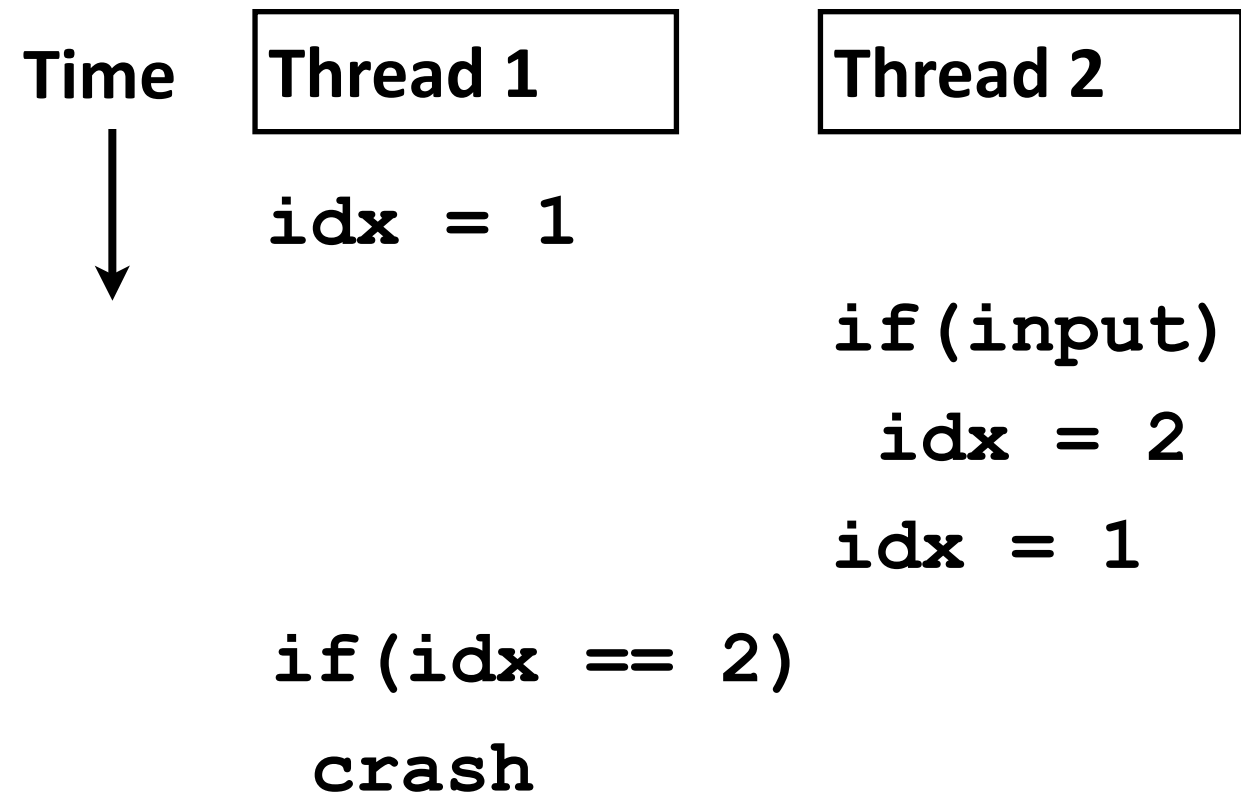
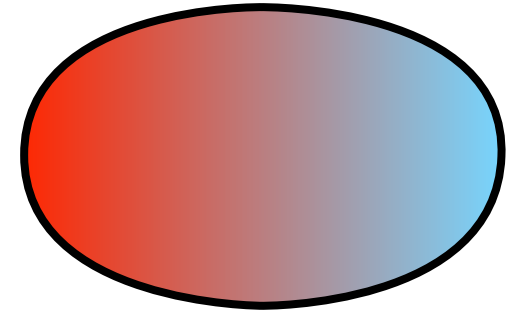
Single-path Analysis (prior work)



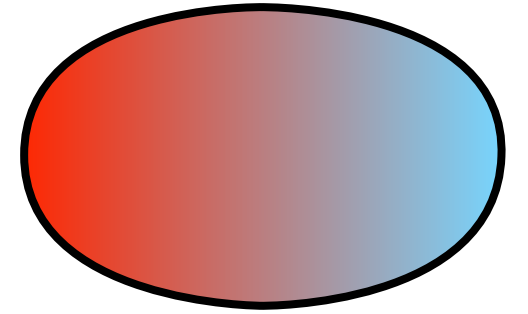
Single-path Analysis (prior work)



Single-path Analysis (prior work)



Single-path Analysis (prior work)



`input = false`

Time



Thread 1

`idx = 1`

Thread 2

`if(input)`

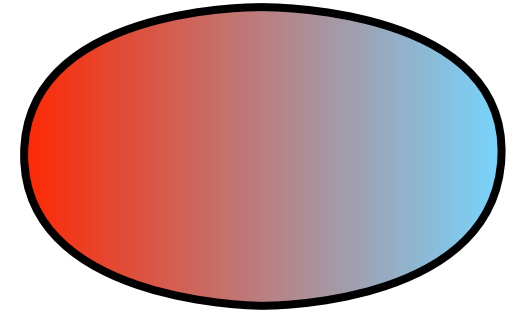
`idx = 2`

`idx = 1`

`if(idx == 2)`

`crash`

Single-path Analysis (prior work)



`input = false`

Time



Thread 1

`idx = 1`

Thread 2

`if(input)`

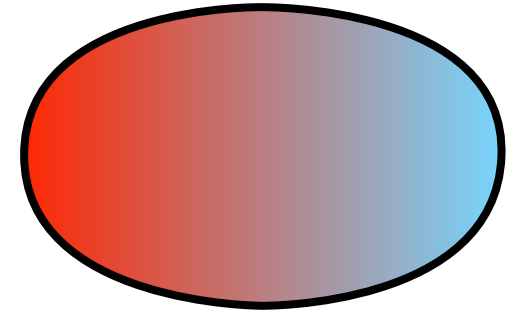
`idx = 2`

`idx = 1`

`if(idx == 2)`

`crash`

Single-path Analysis (prior work)



`input = false`

Time



Thread 1

`idx = 1`

Thread 2

`if(input)`

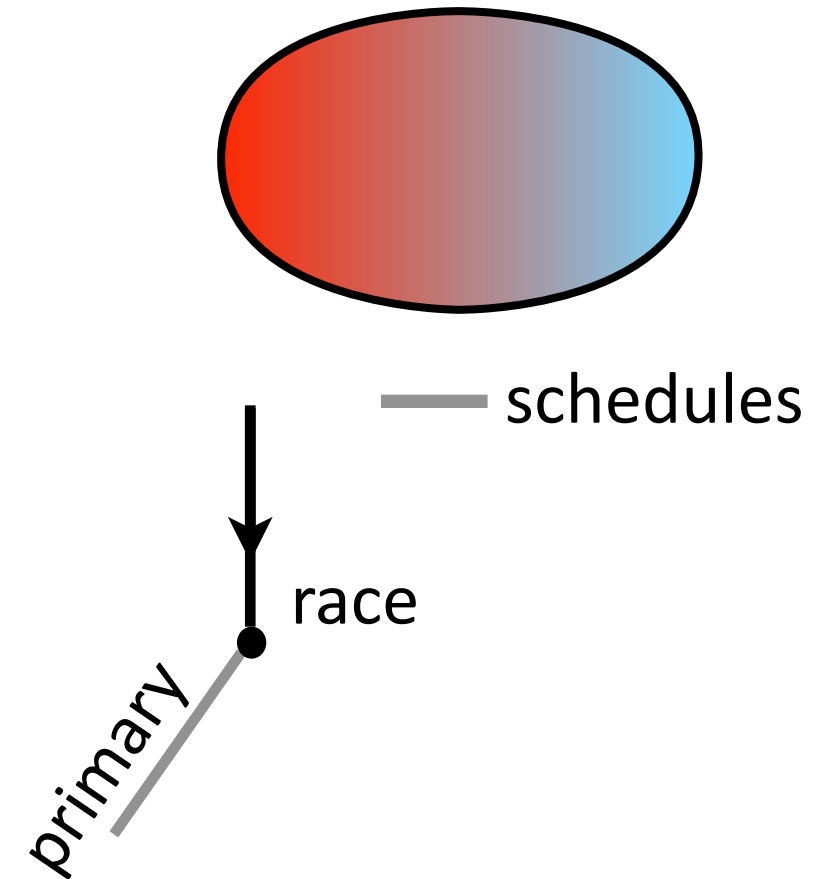
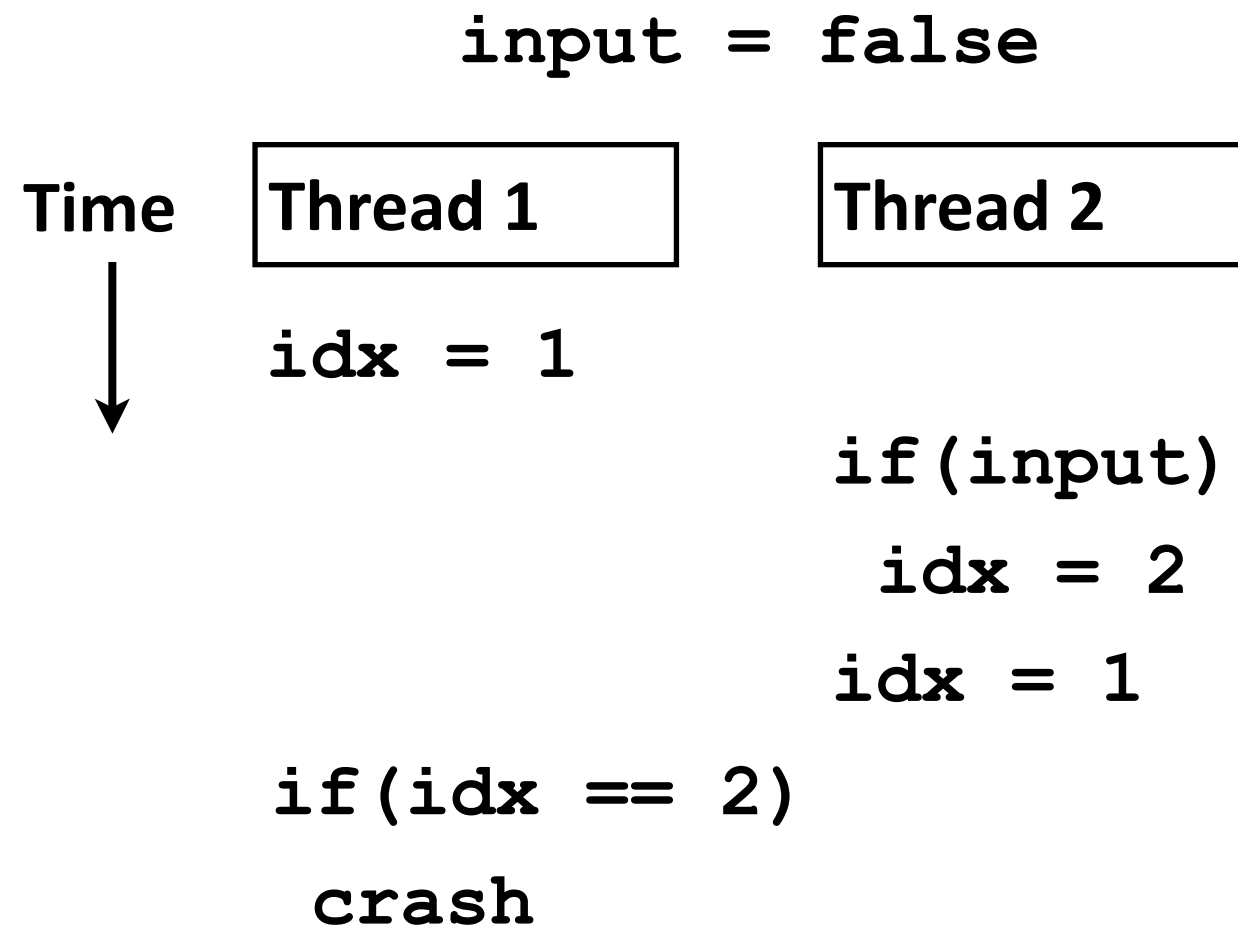
`idx = 2`

`idx = 1`

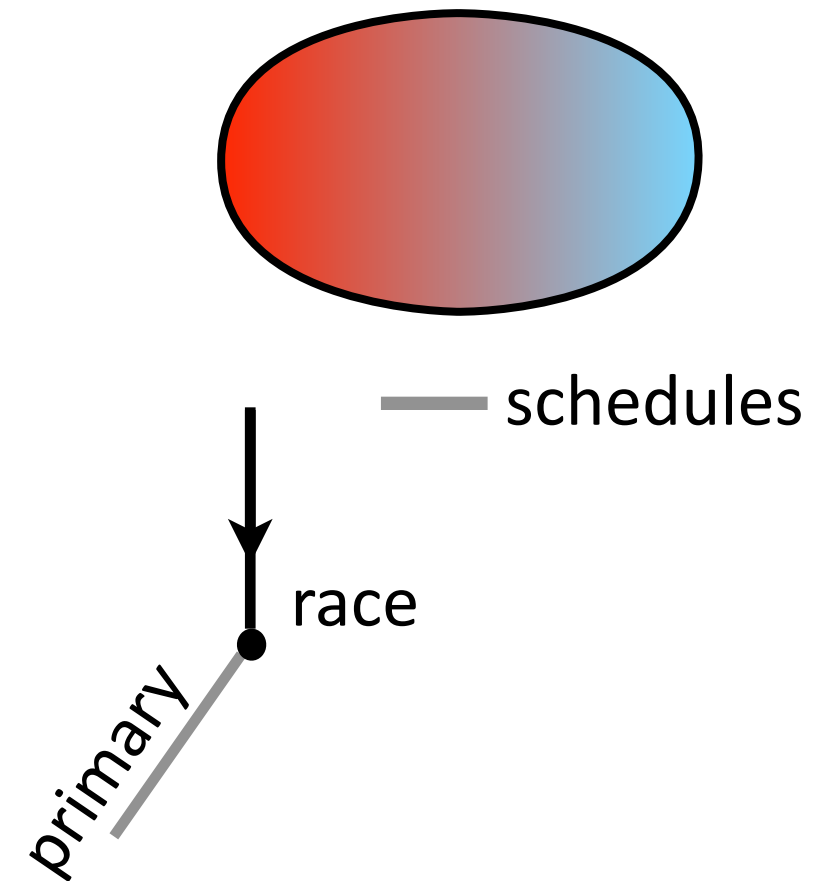
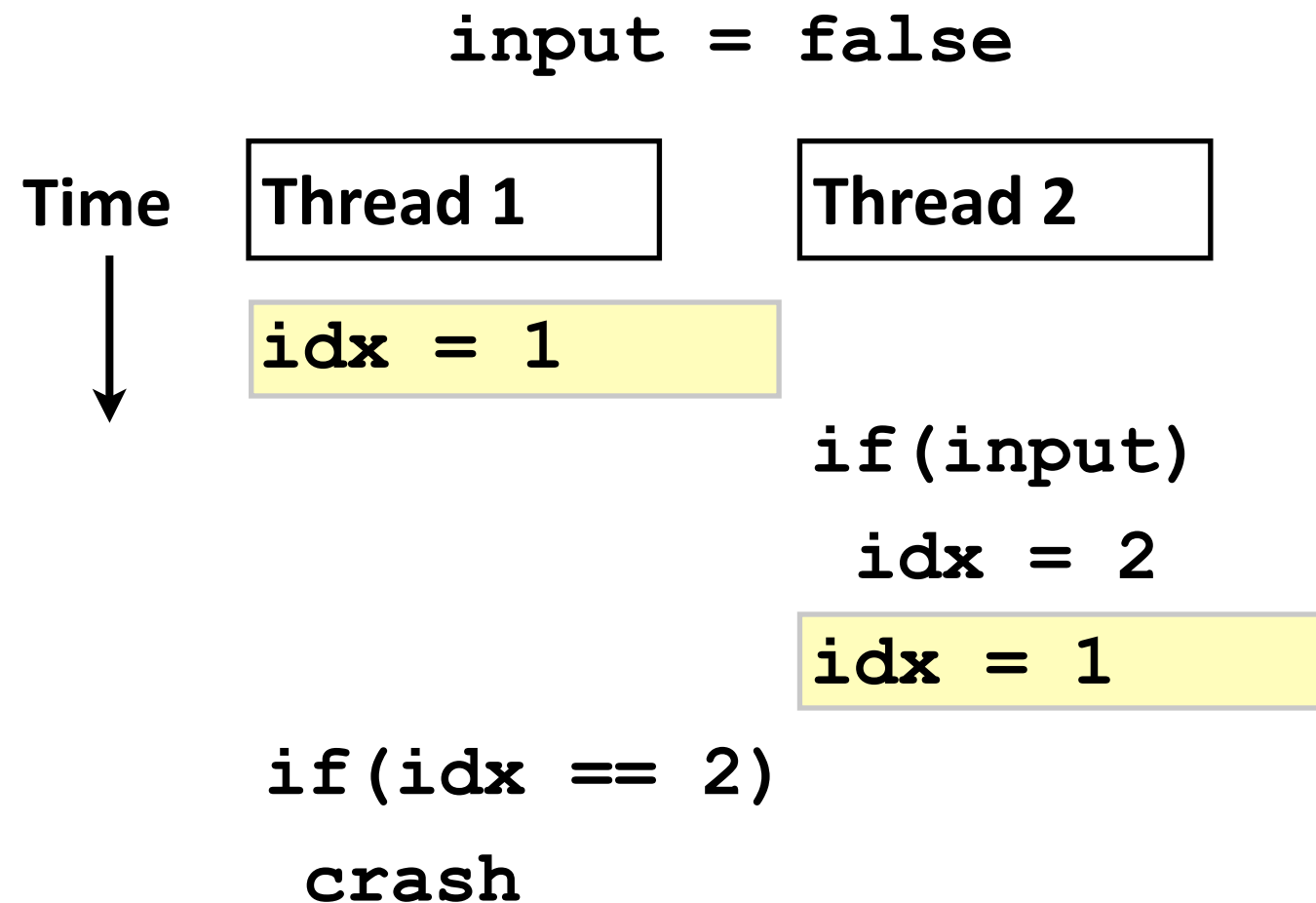
`if(idx == 2)`

`crash`

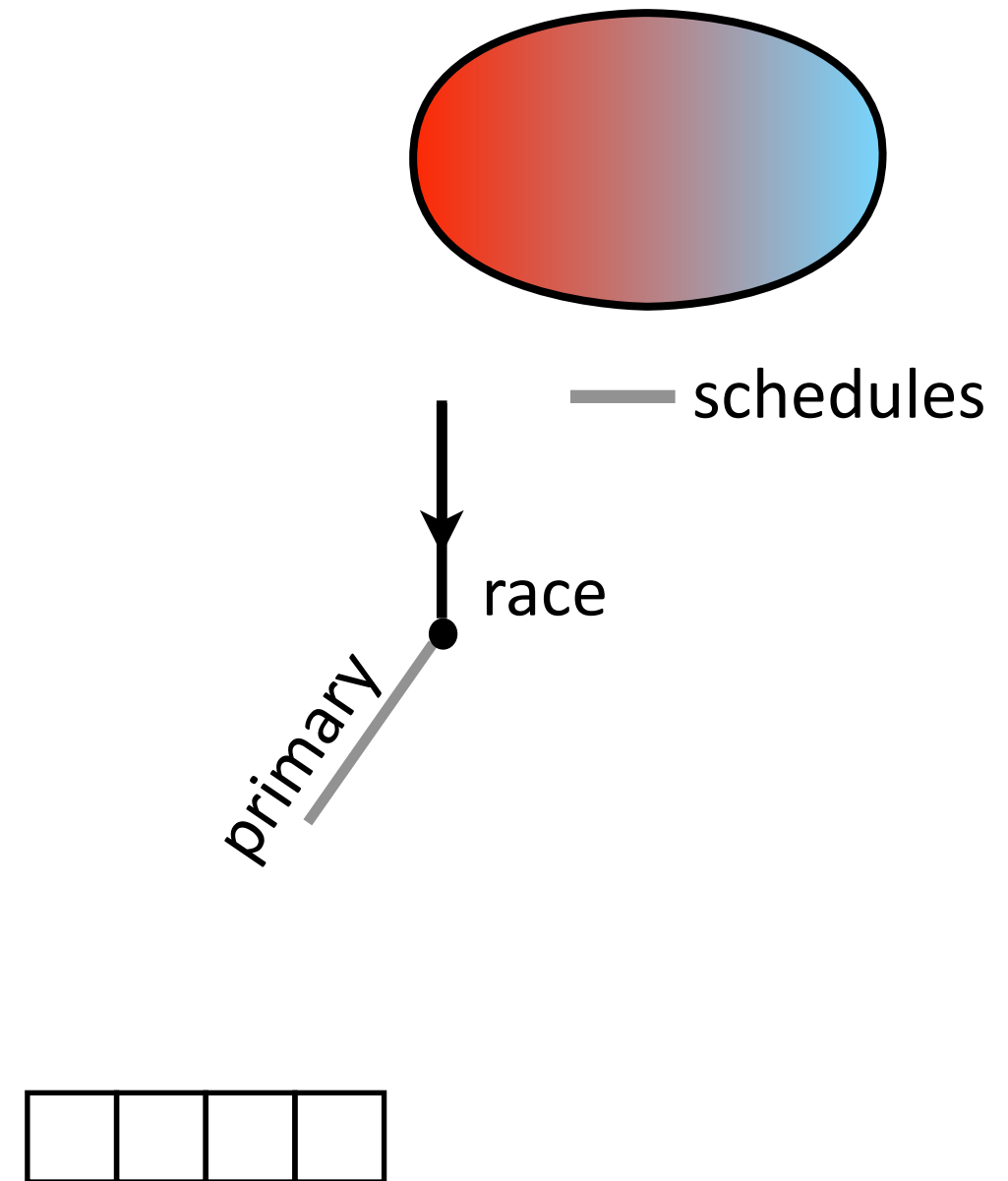
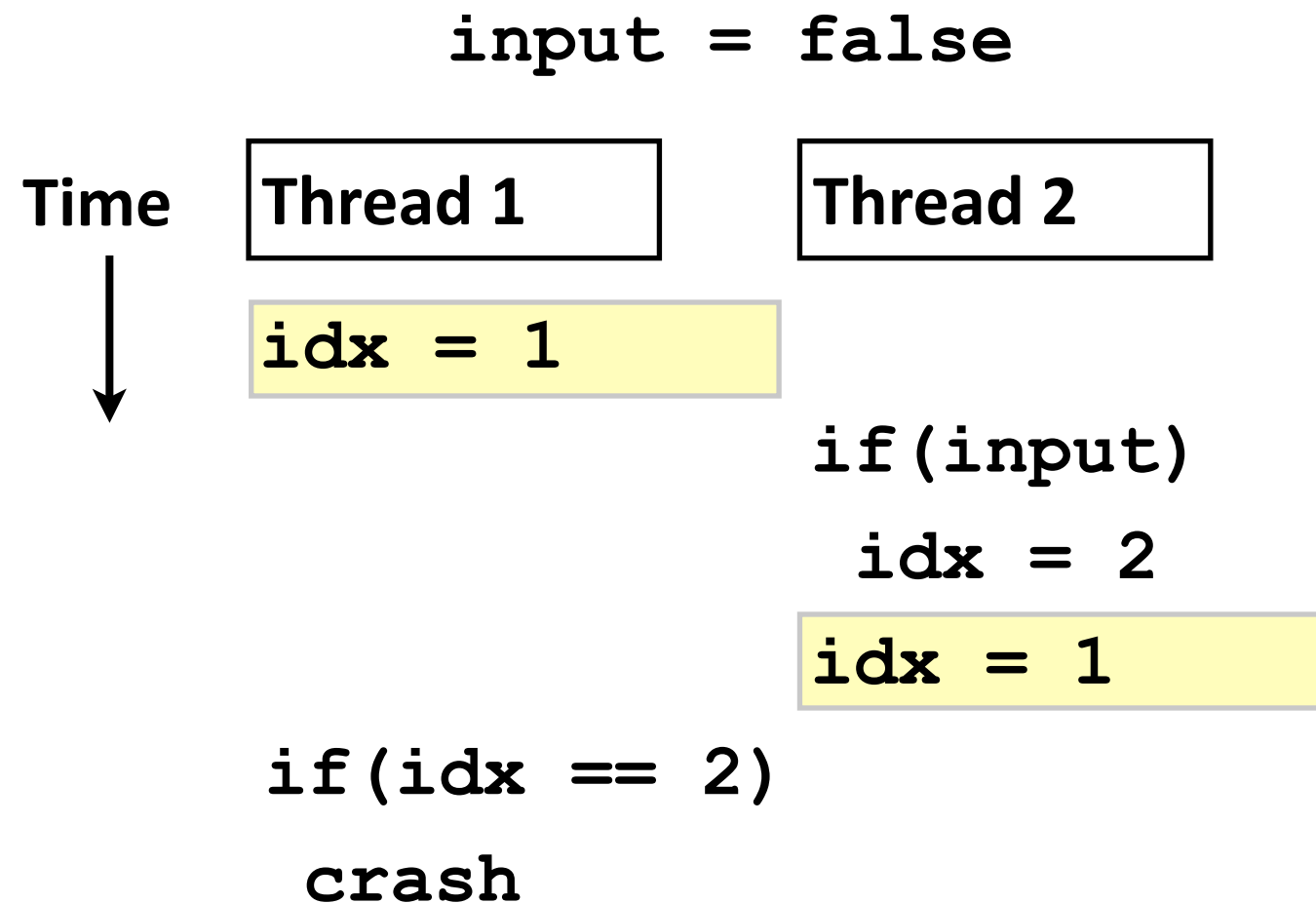
Single-path Analysis (prior work)



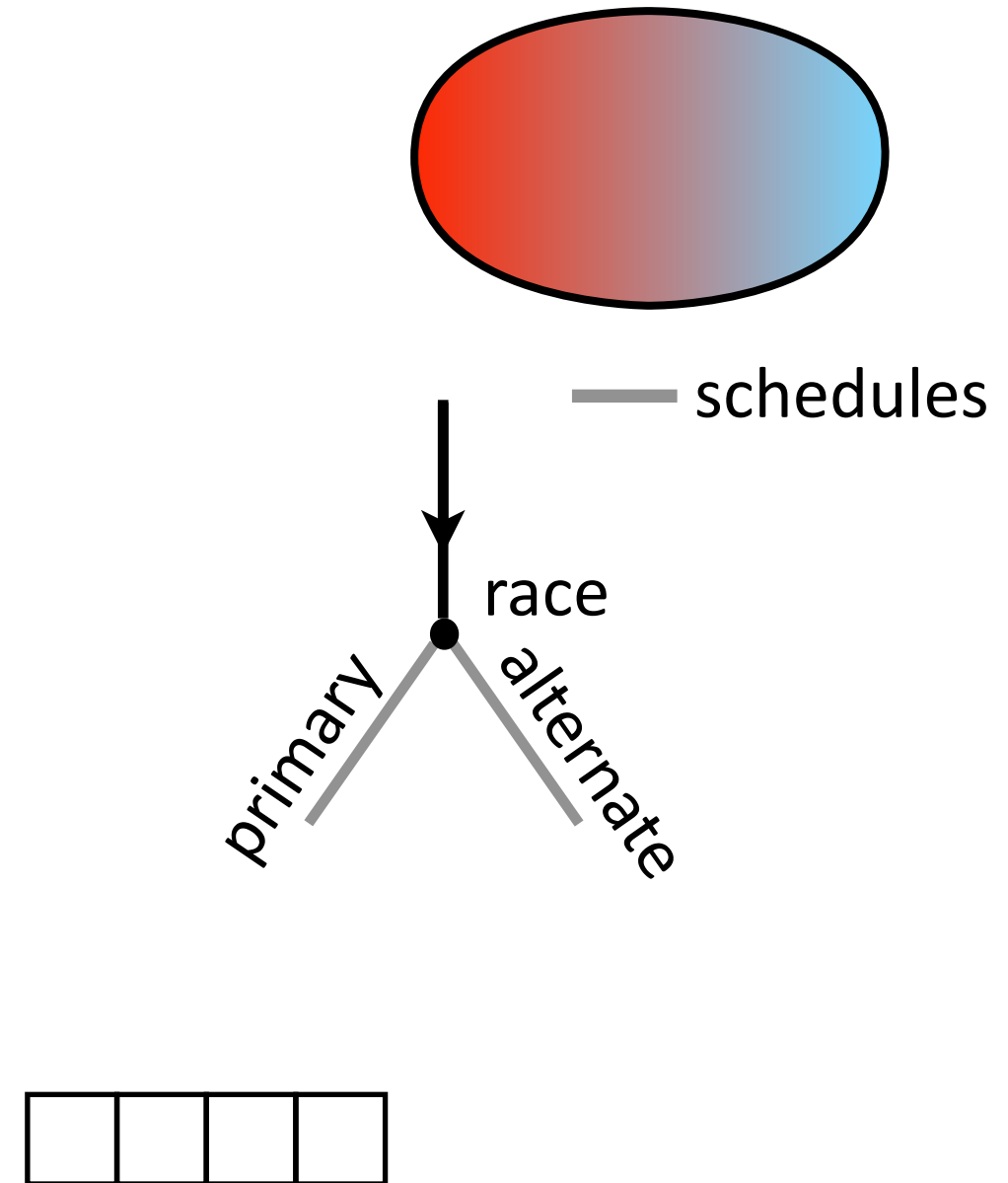
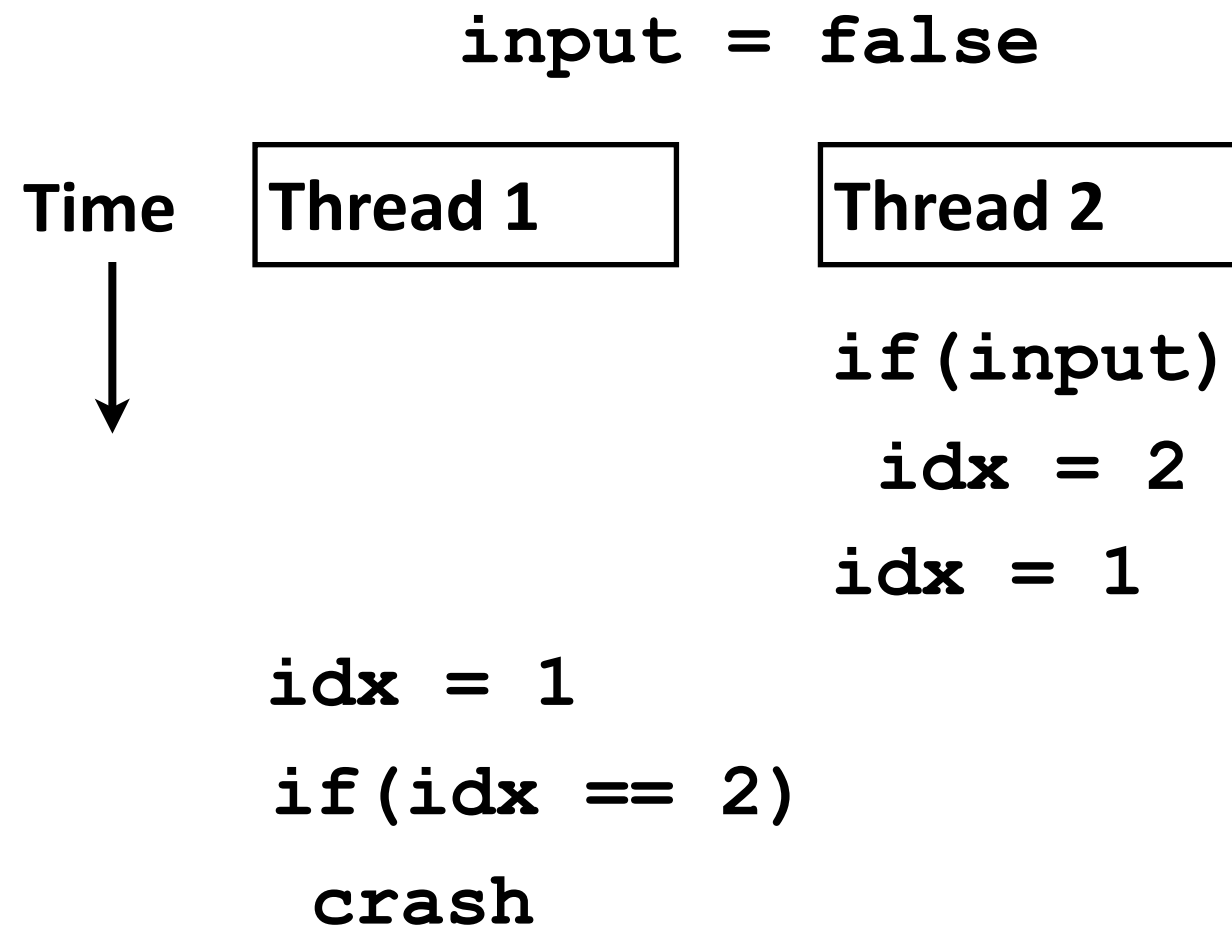
Single-path Analysis (prior work)



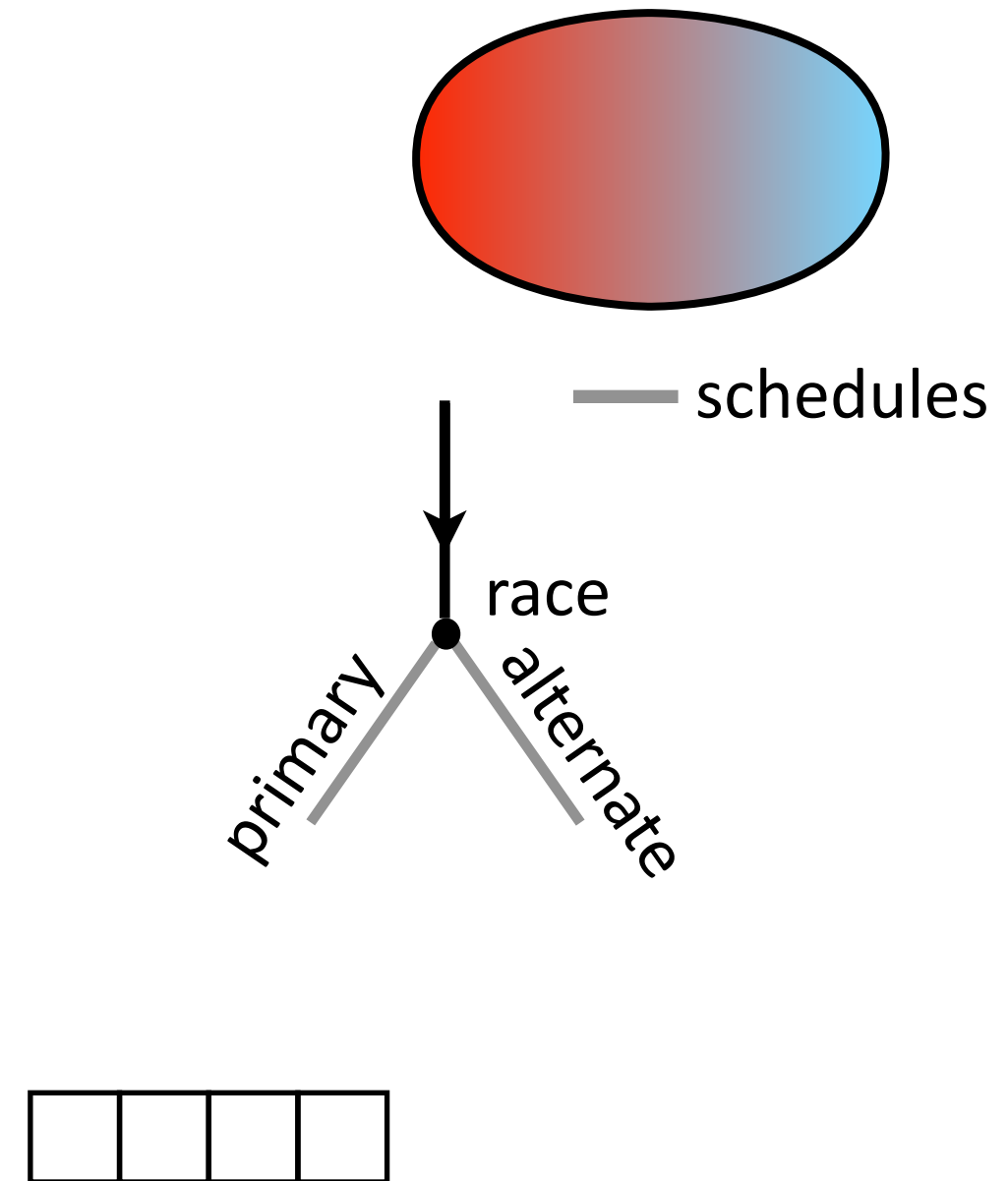
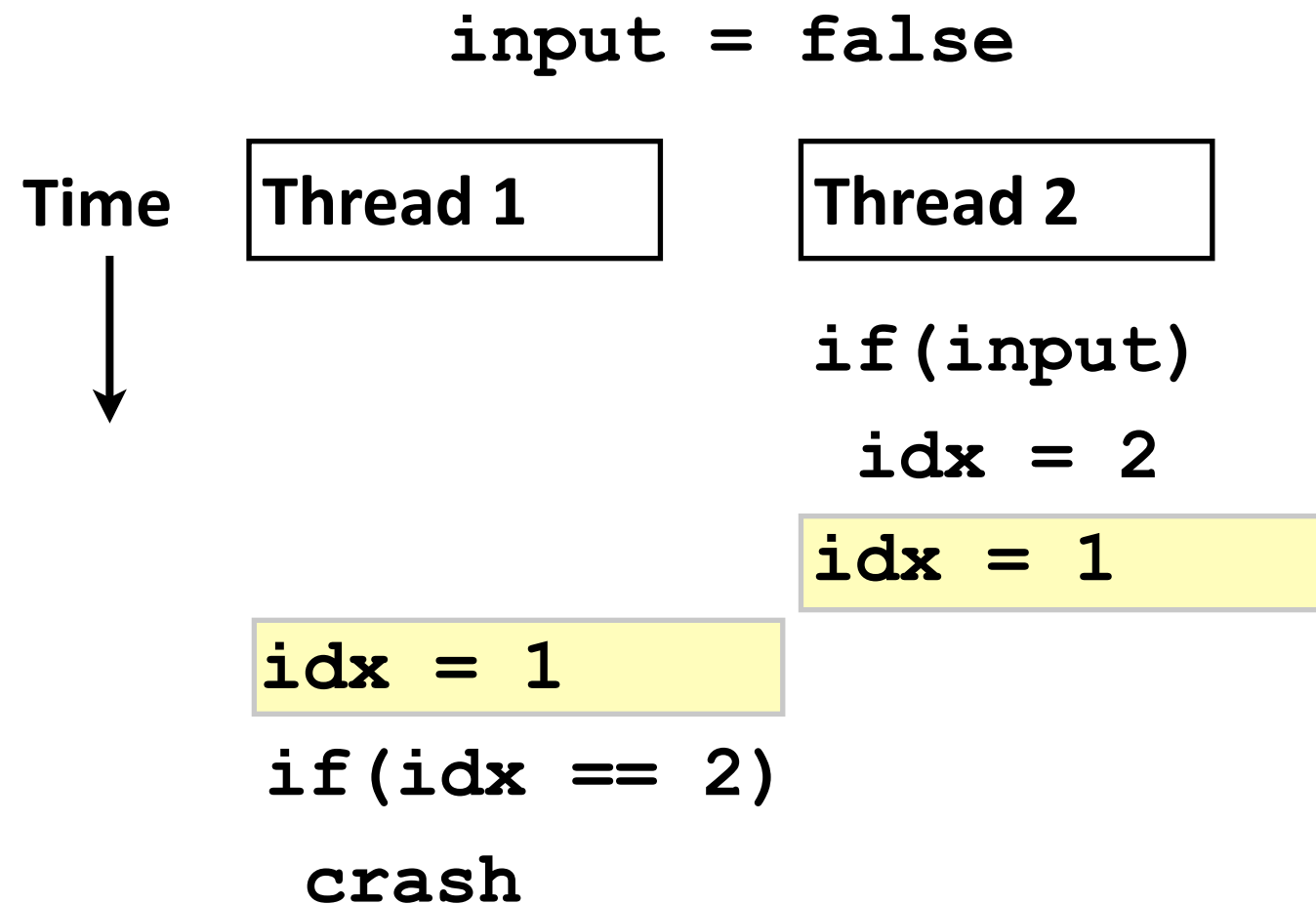
Single-path Analysis (prior work)



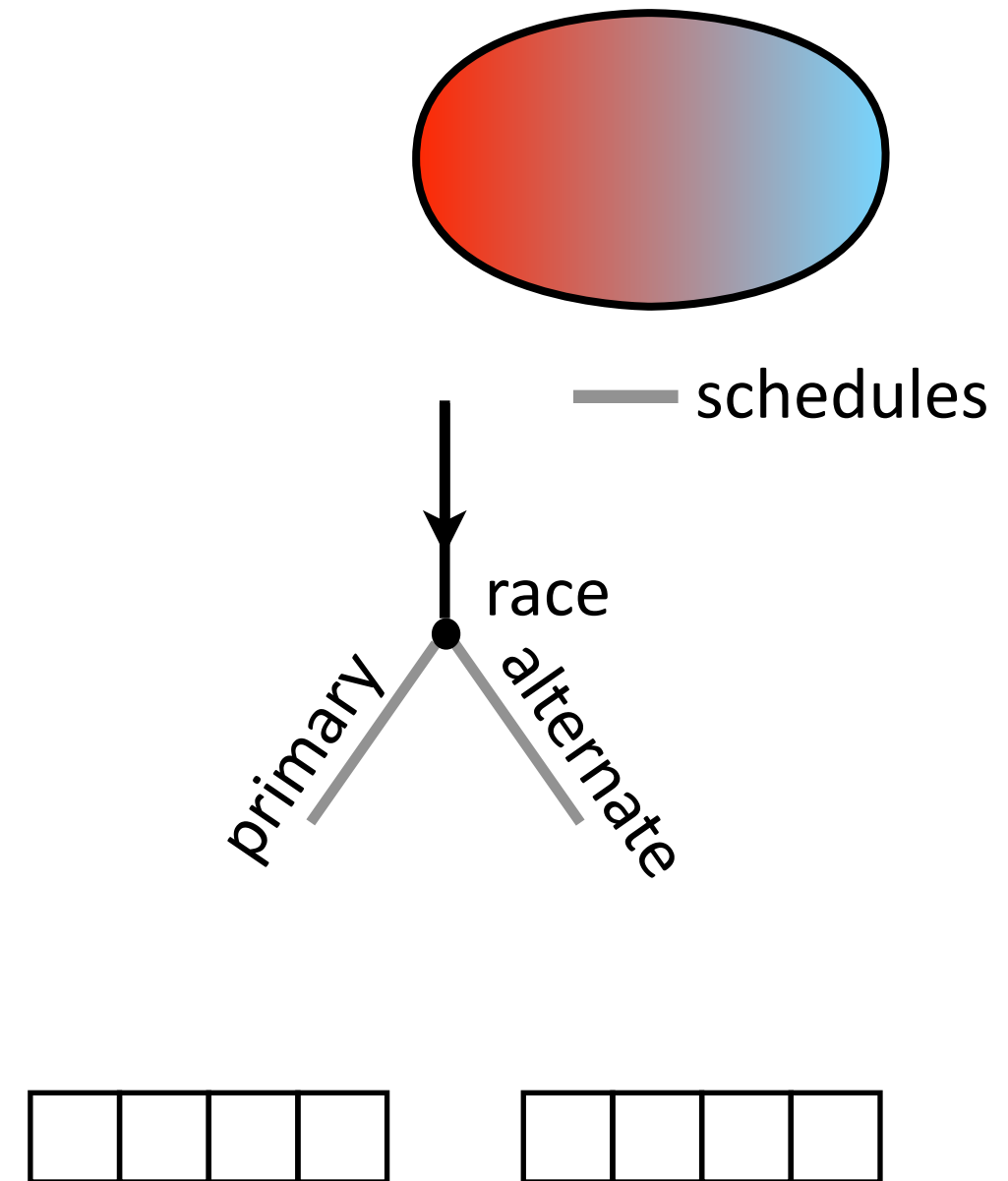
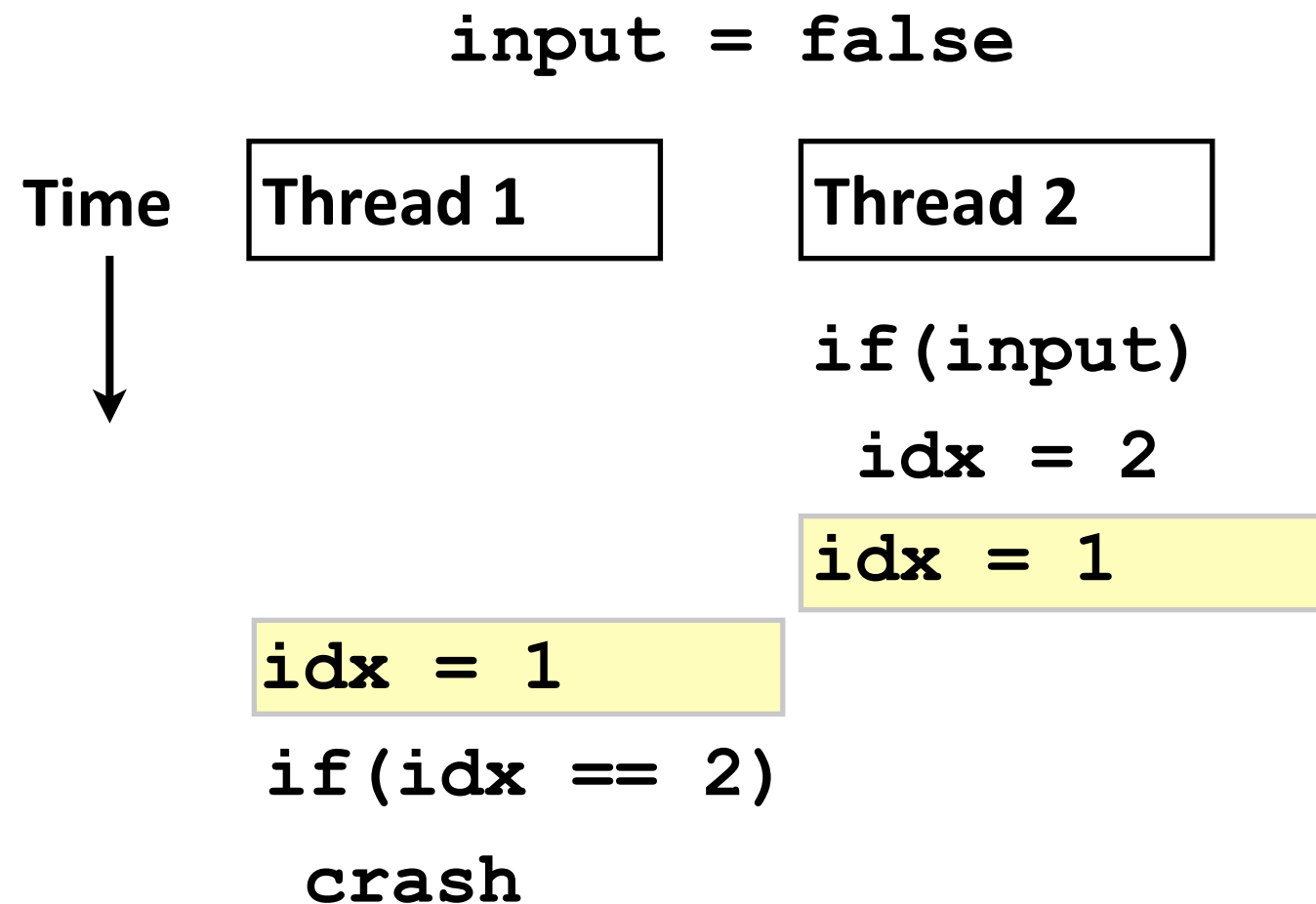
Single-path Analysis (prior work)



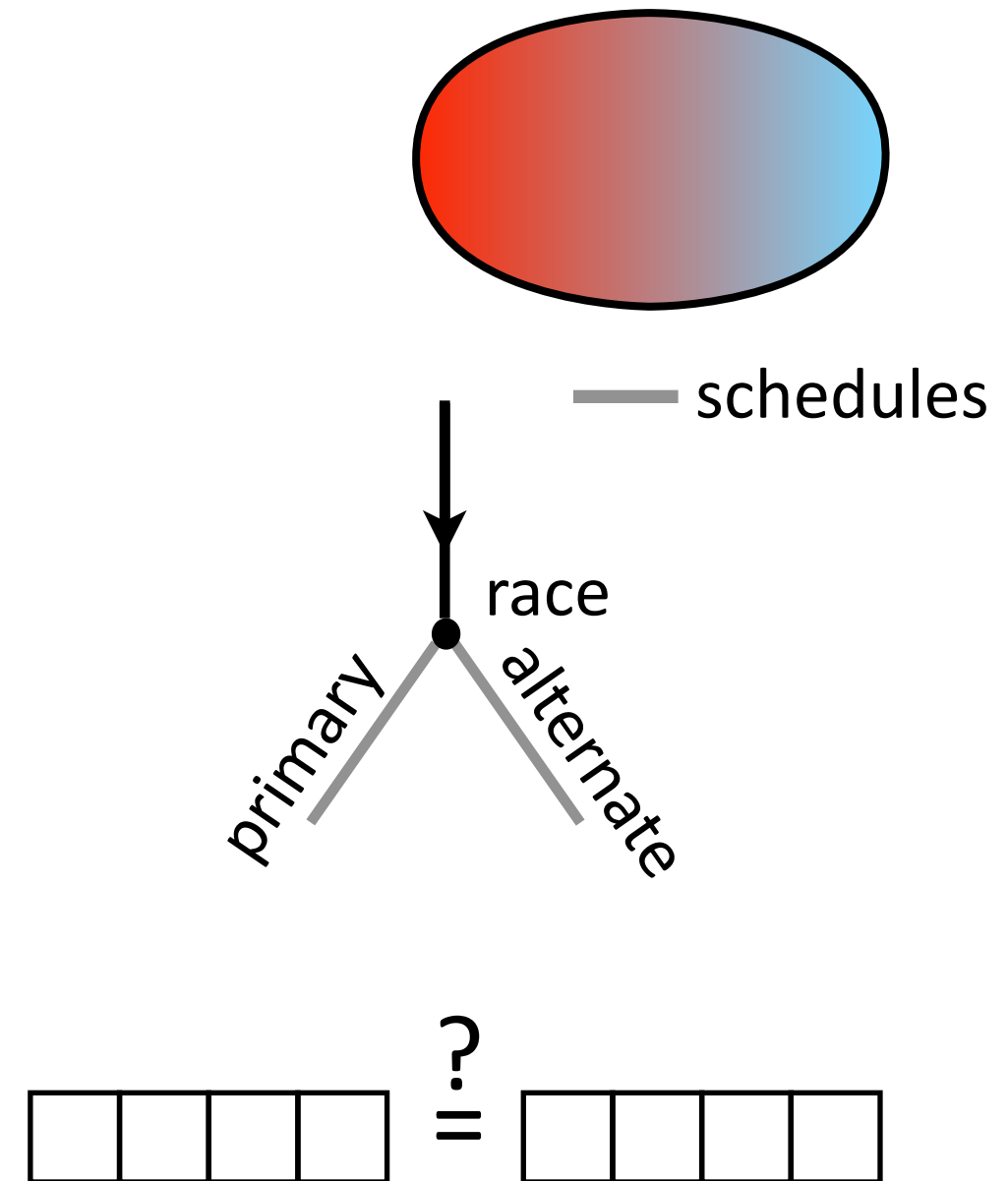
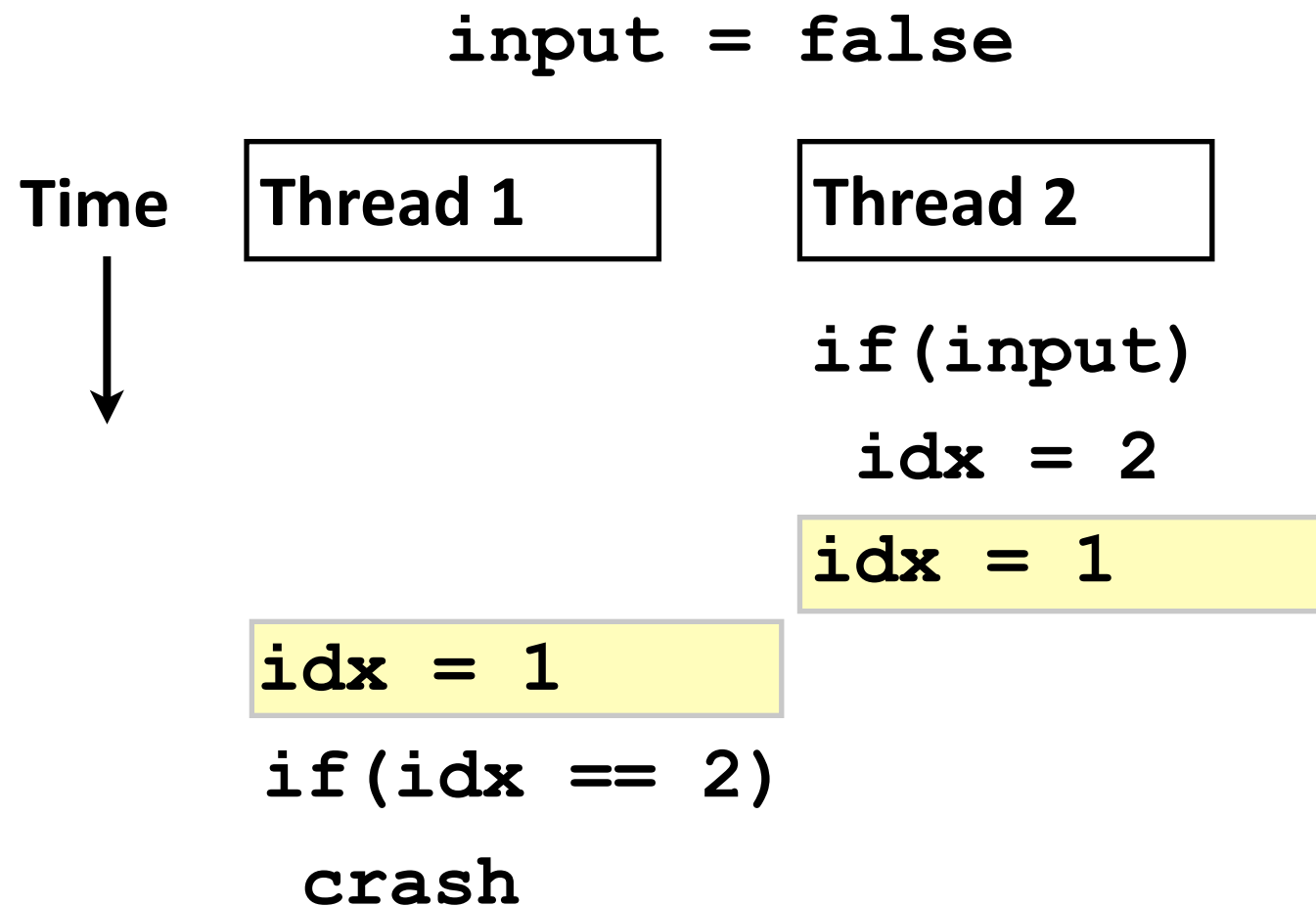
Single-path Analysis (prior work)



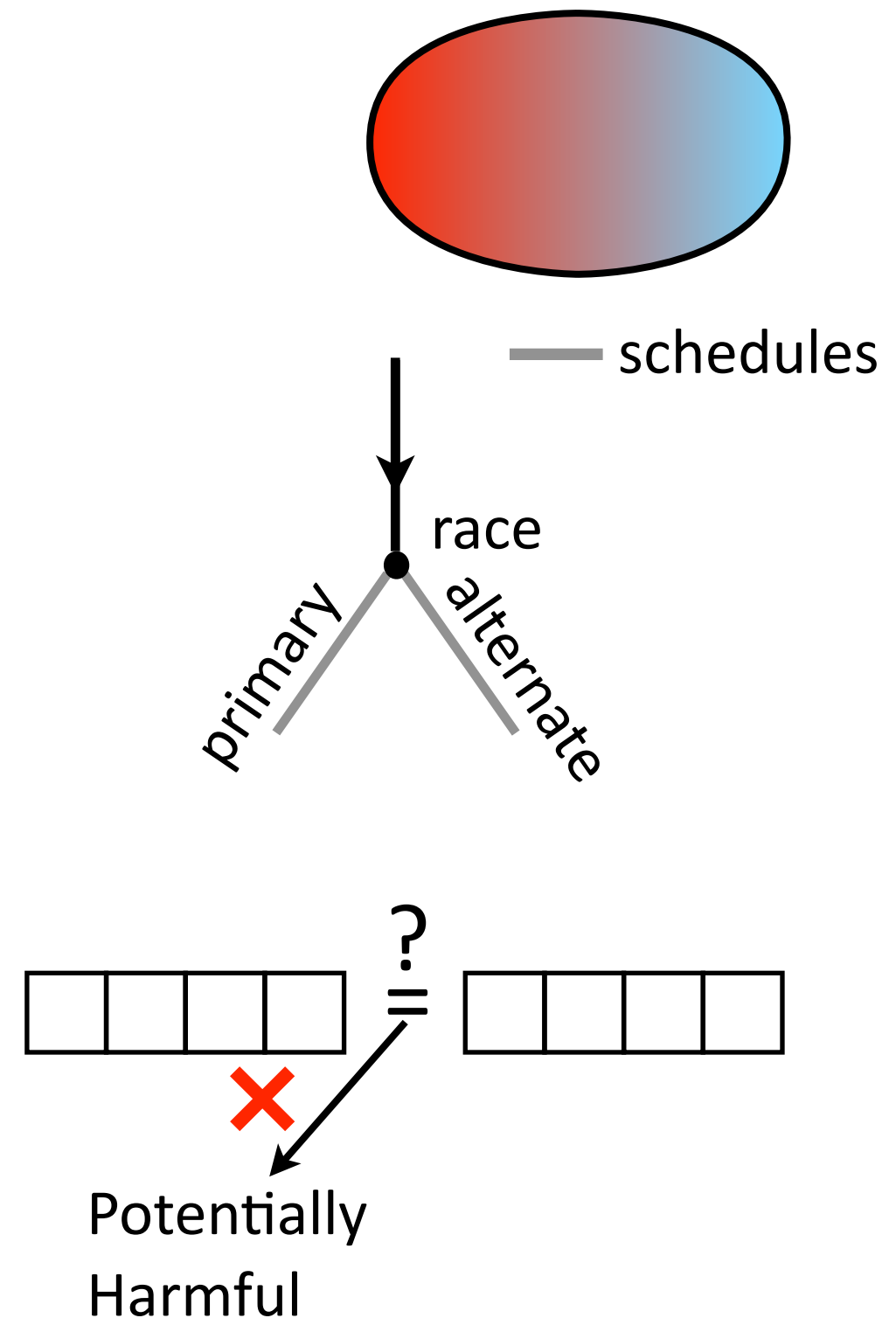
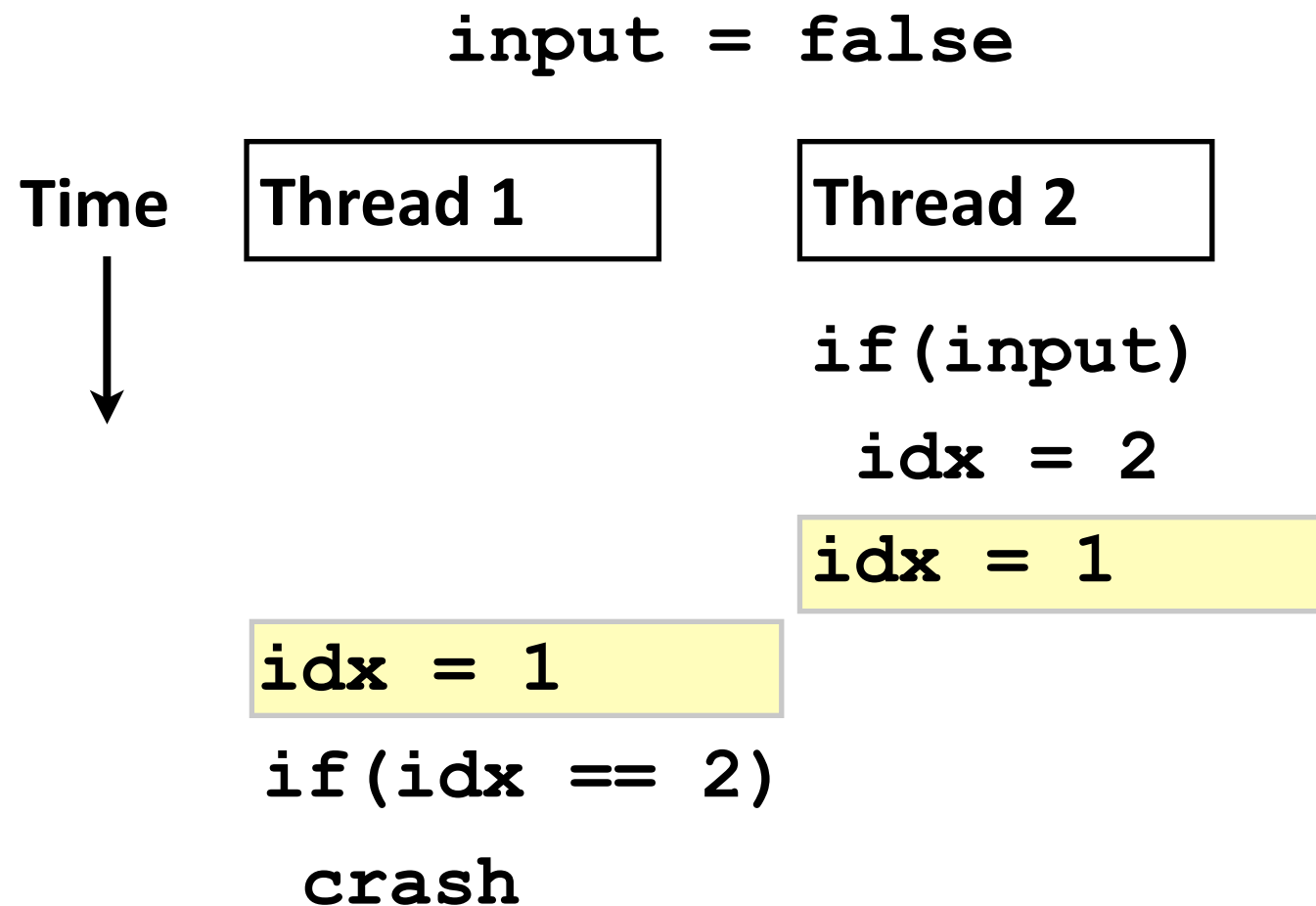
Single-path Analysis (prior work)



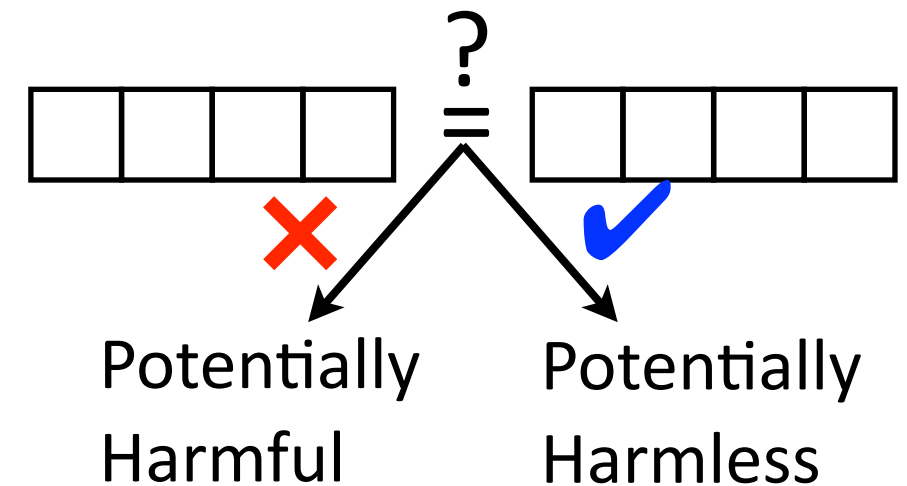
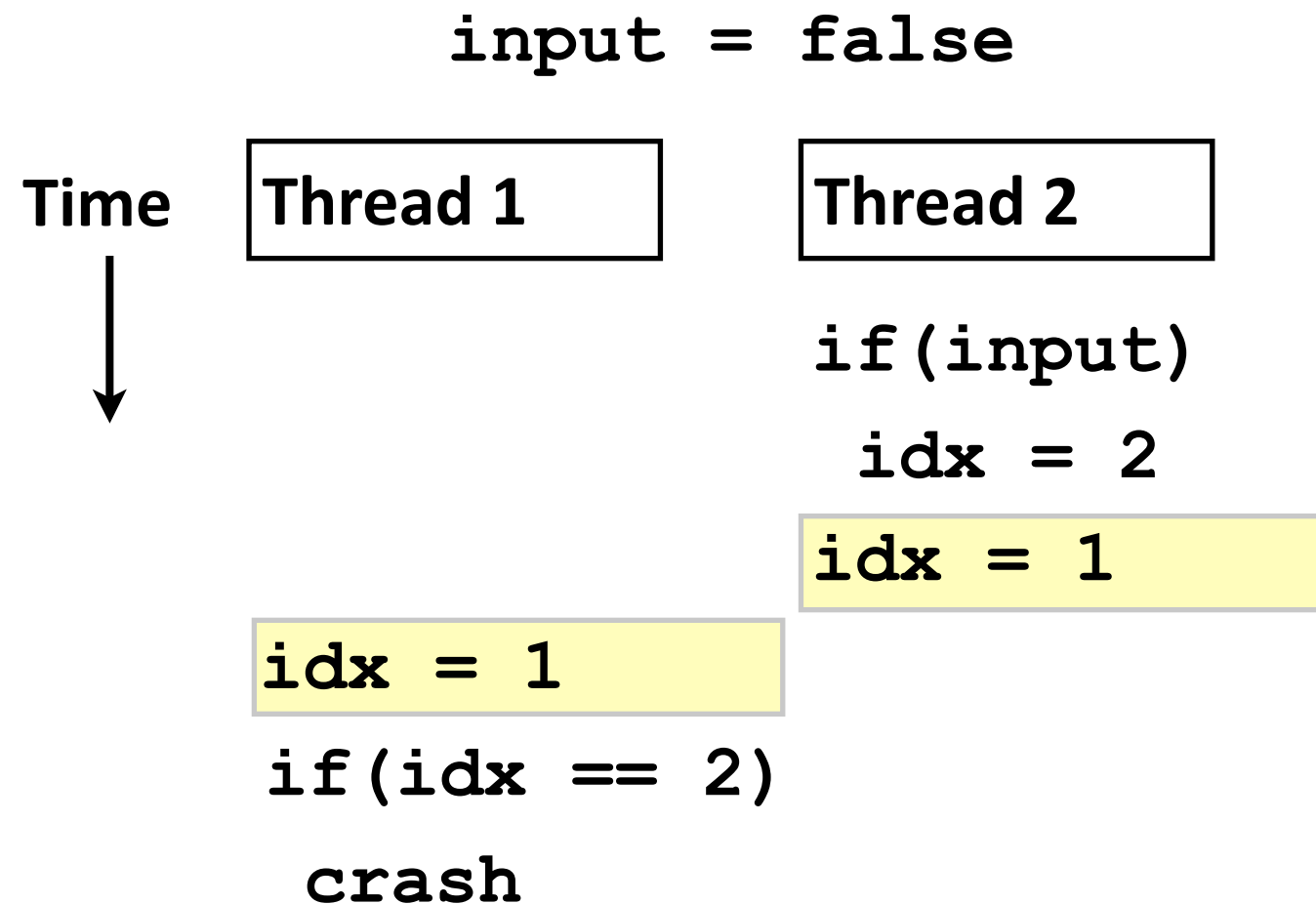
Single-path Analysis (prior work)



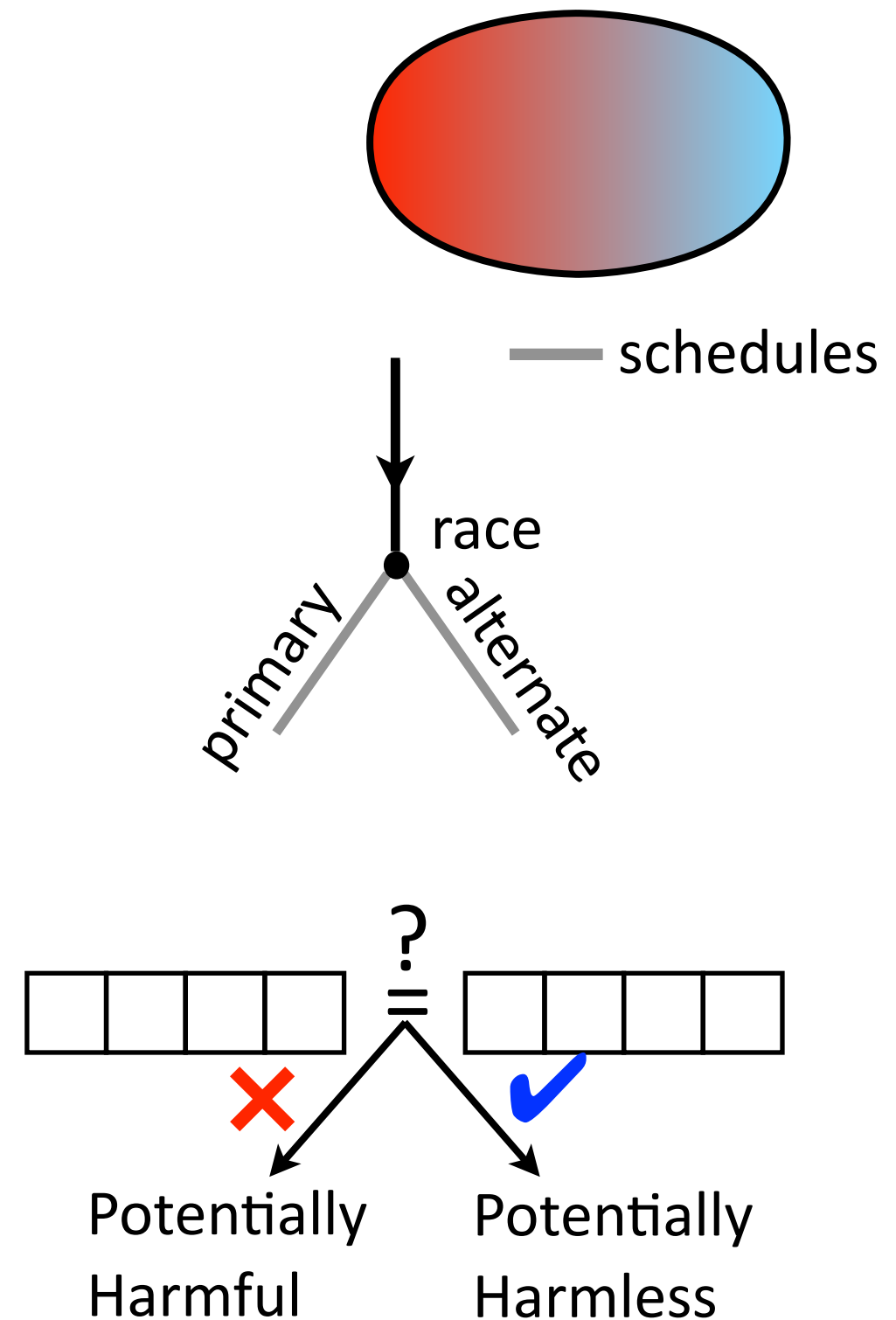
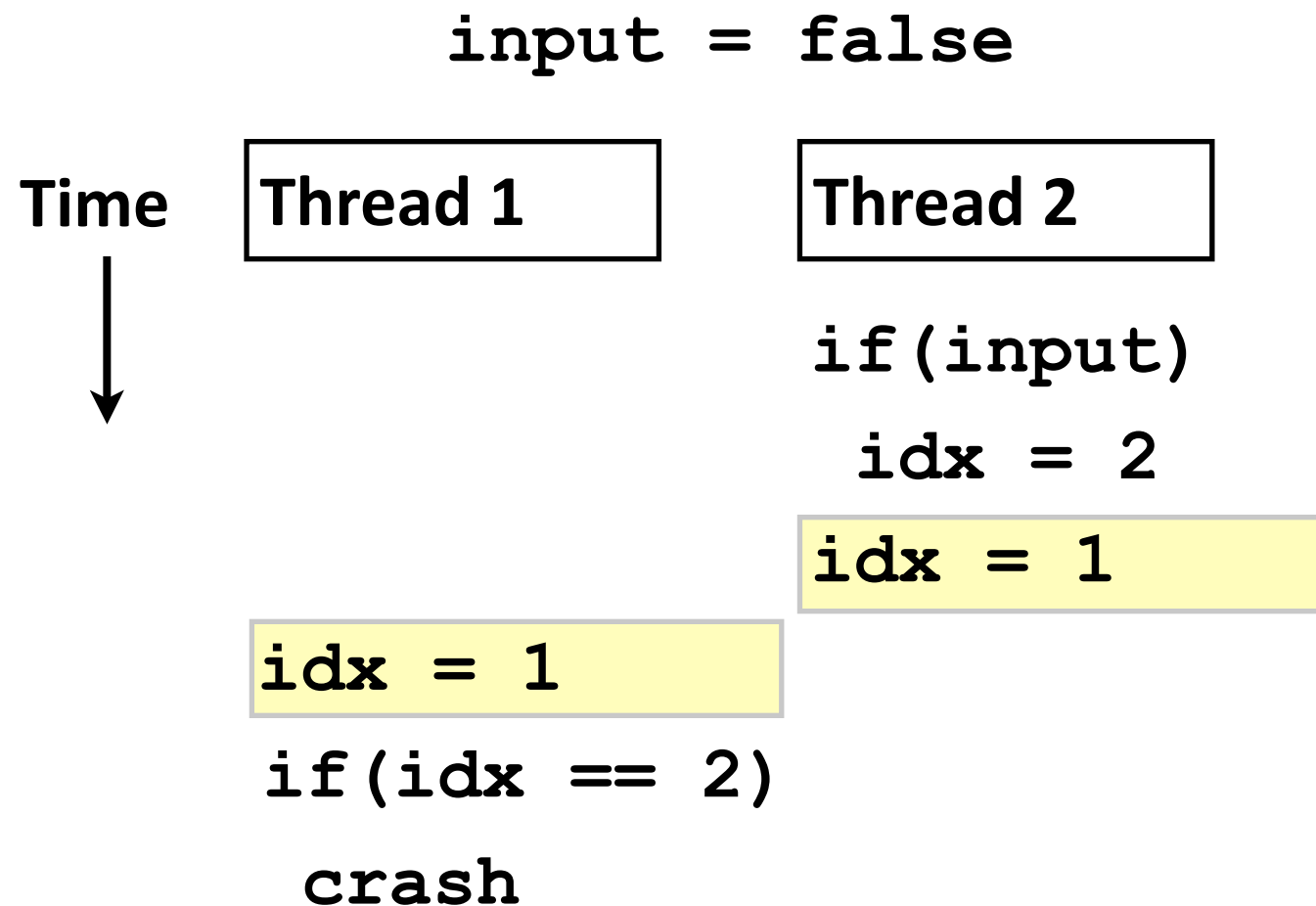
Single-path Analysis (prior work)



Single-path Analysis (prior work)

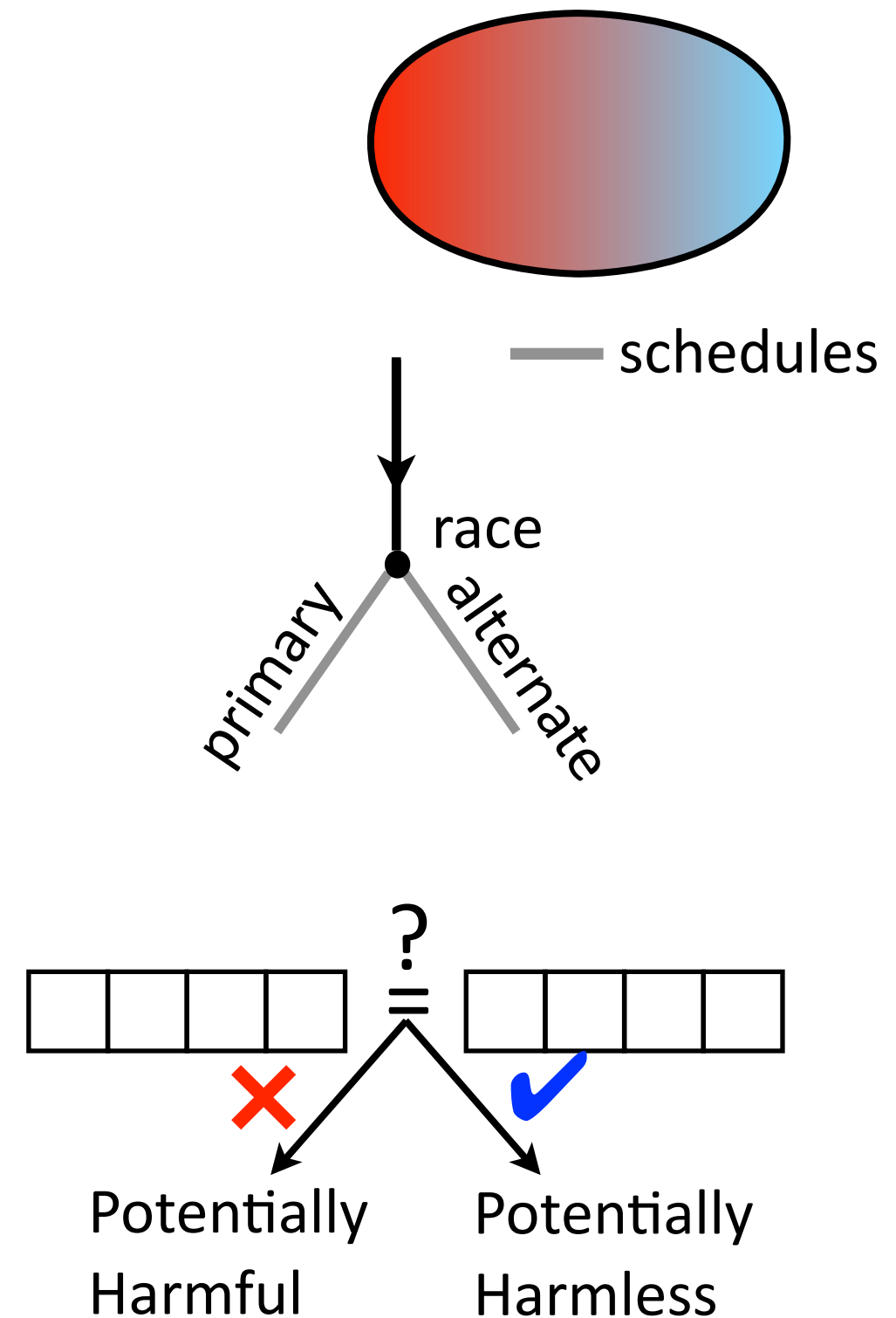
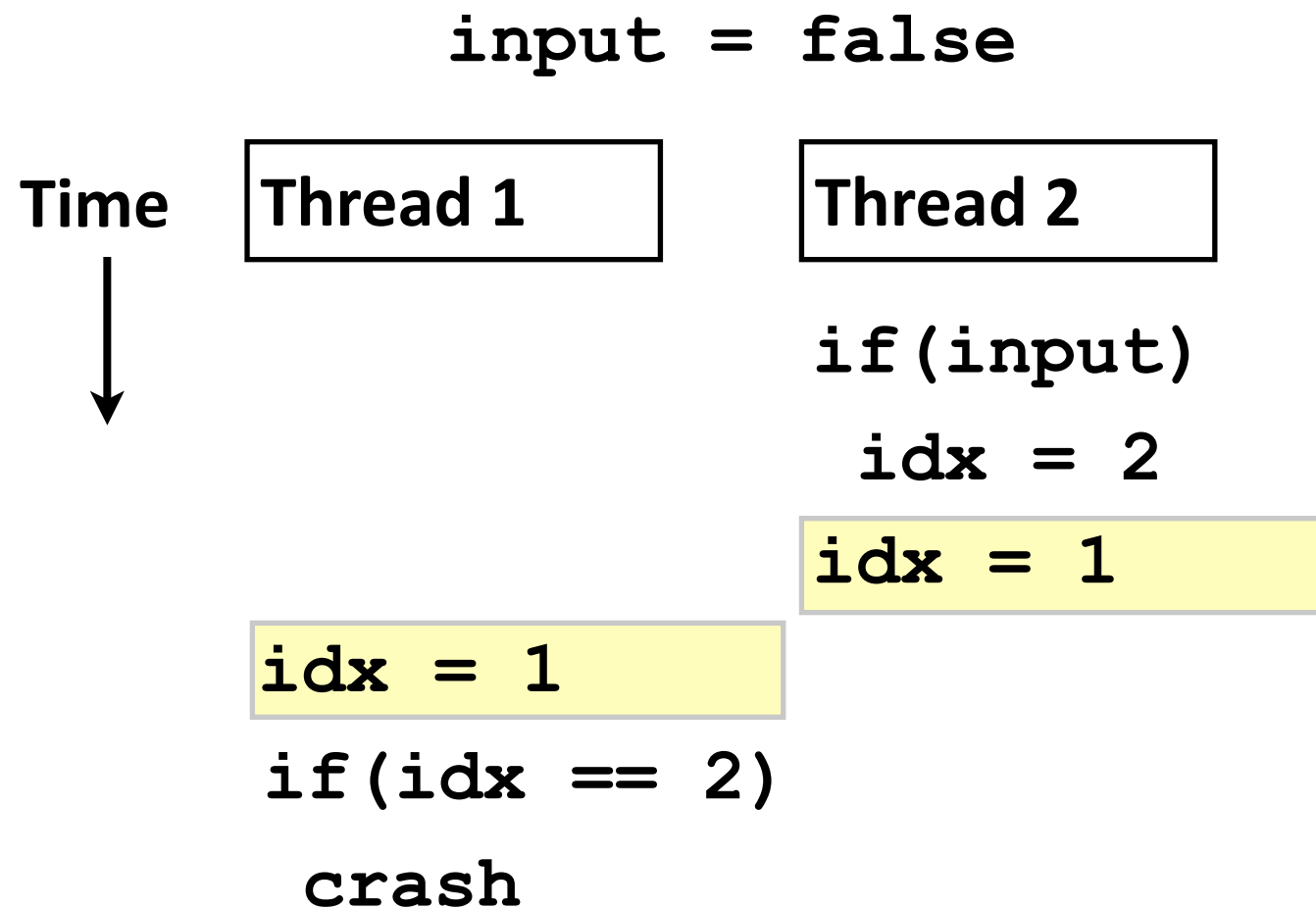


Single-path Analysis (prior work)



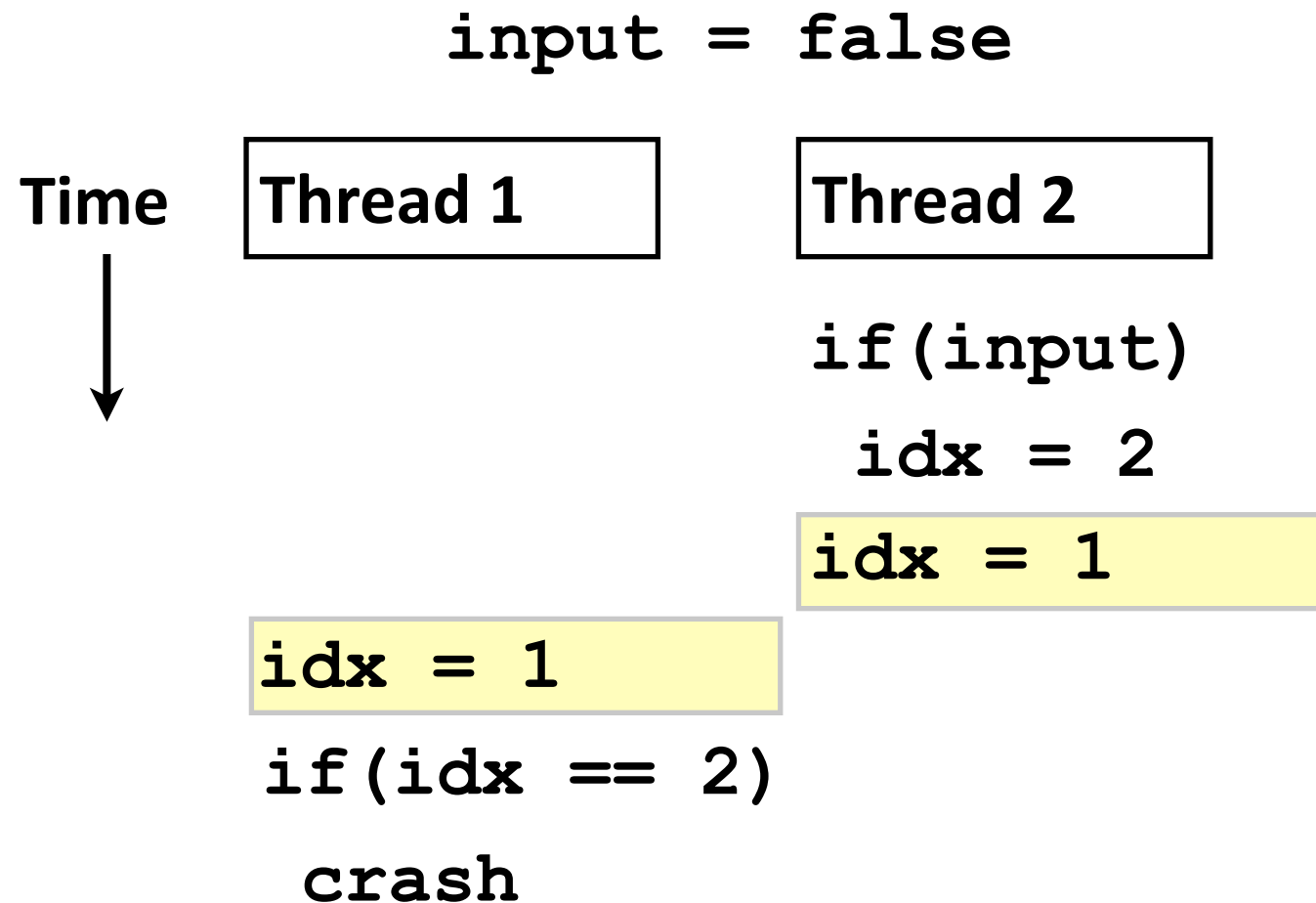
Analyze two schedules, compare memory and registers

Single-path Analysis (prior work)



Analyze two schedules, compare memory and registers

Single-path Analysis (prior work)



Analyze two schedules, compare memory and registers

`input = false`

Time



Thread 1

`idx = 1`

Thread 2

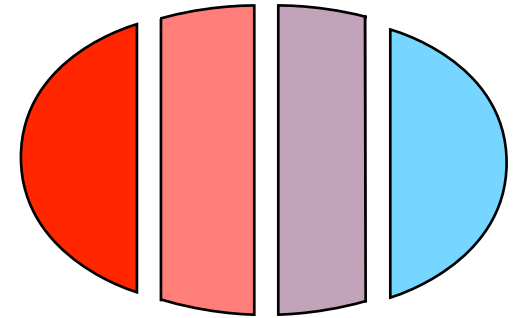
`if(input)`

`idx = 2`

`idx = 1`

`if(idx == 2)`

`crash`



`input = false`

Time



Thread 1

`idx = 1`

Thread 2

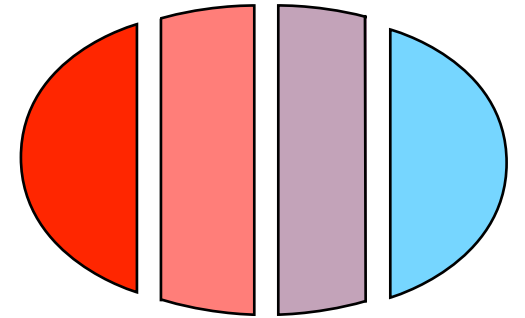
`if(input)`

`idx = 2`

`idx = 1`

`if(idx == 2)`

`crash`



`input = false`

Time



Thread 1

`idx = 1`

Thread 2

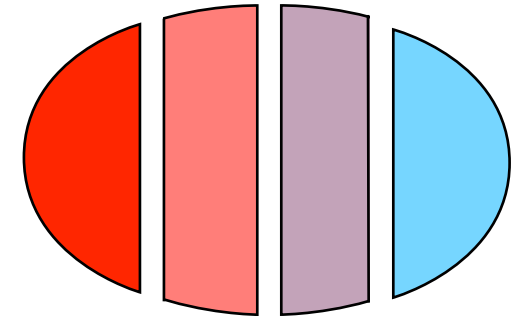
`if(input)`

`idx = 2`

`idx = 1`

`if(idx == 2)`

`crash`



`input = false`

Time



Thread 1

`idx = 1`

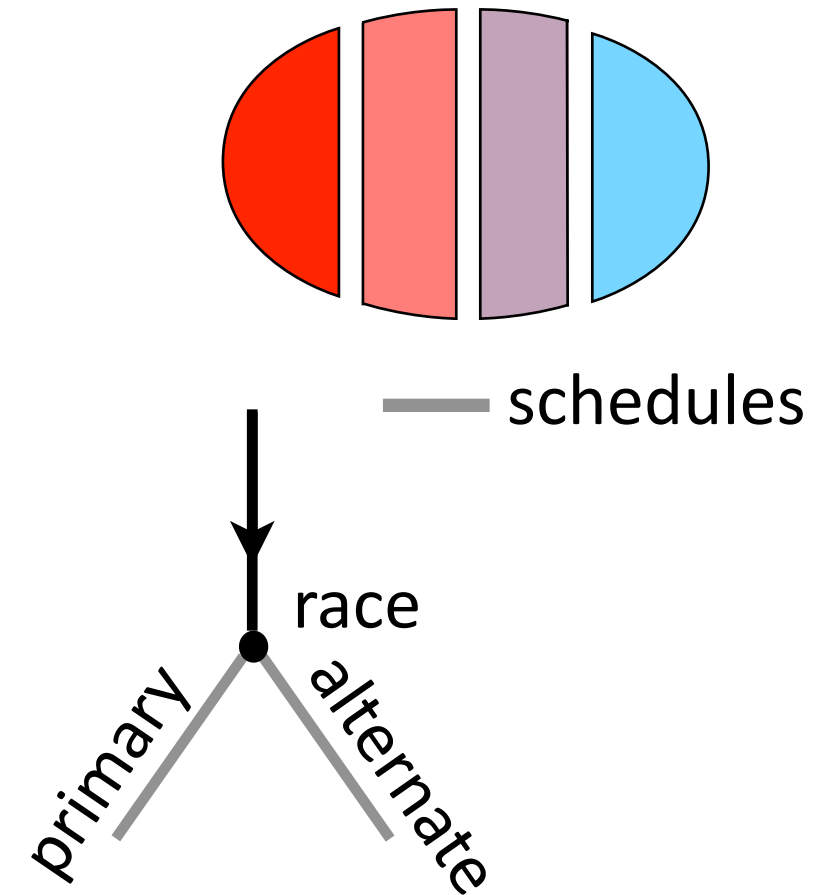
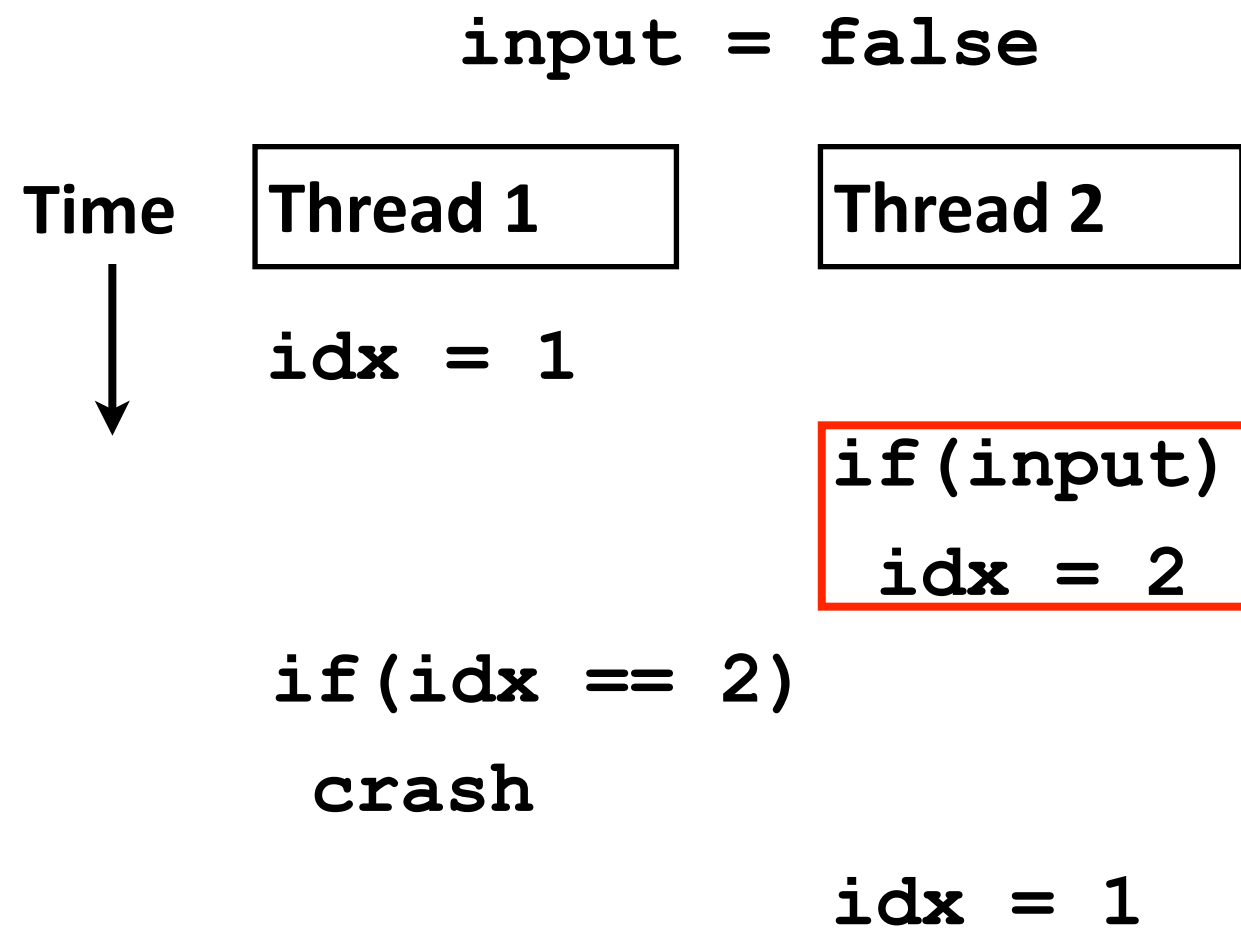
Thread 2

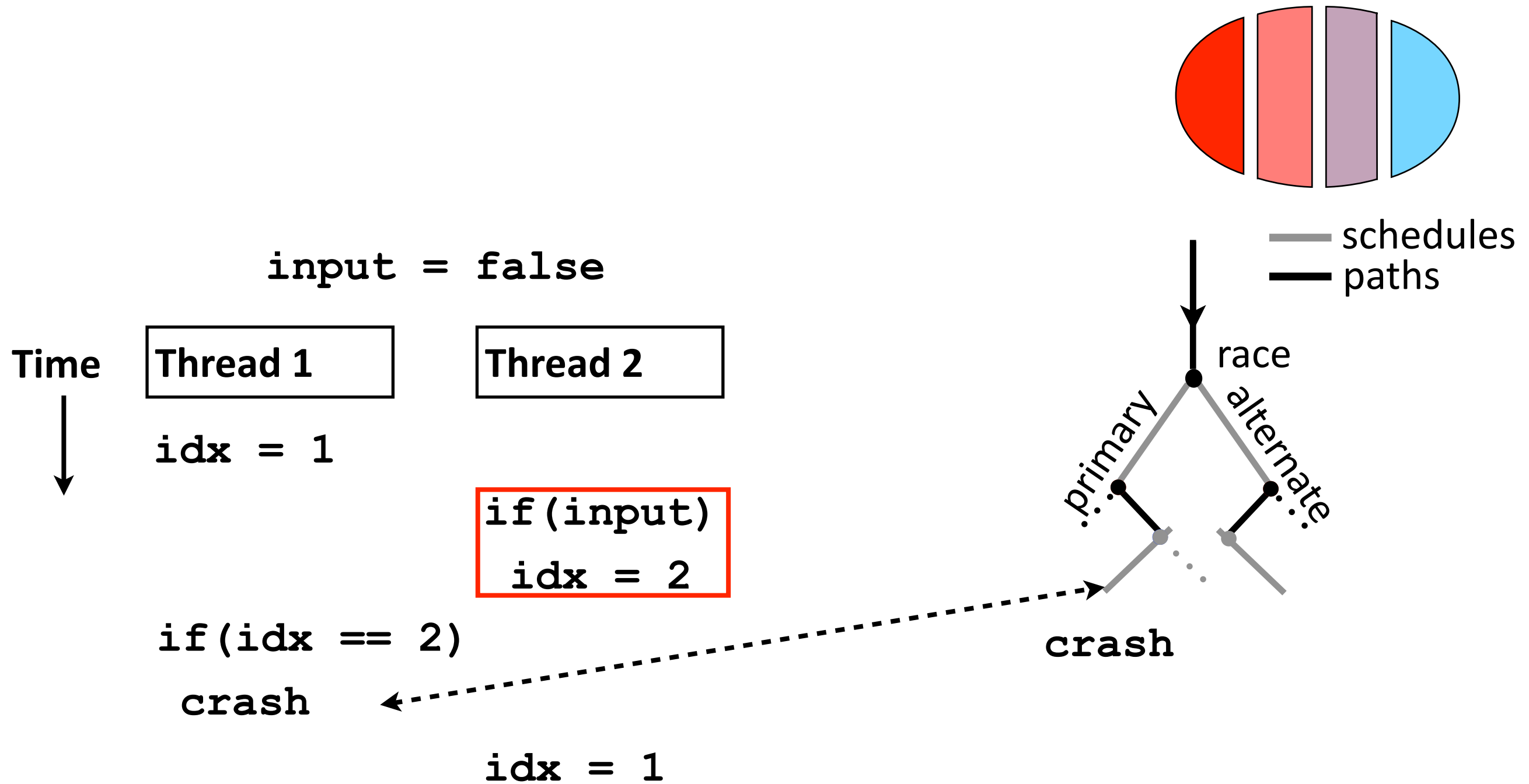
`if (input)`
`idx = 2`

`if (idx == 2)`

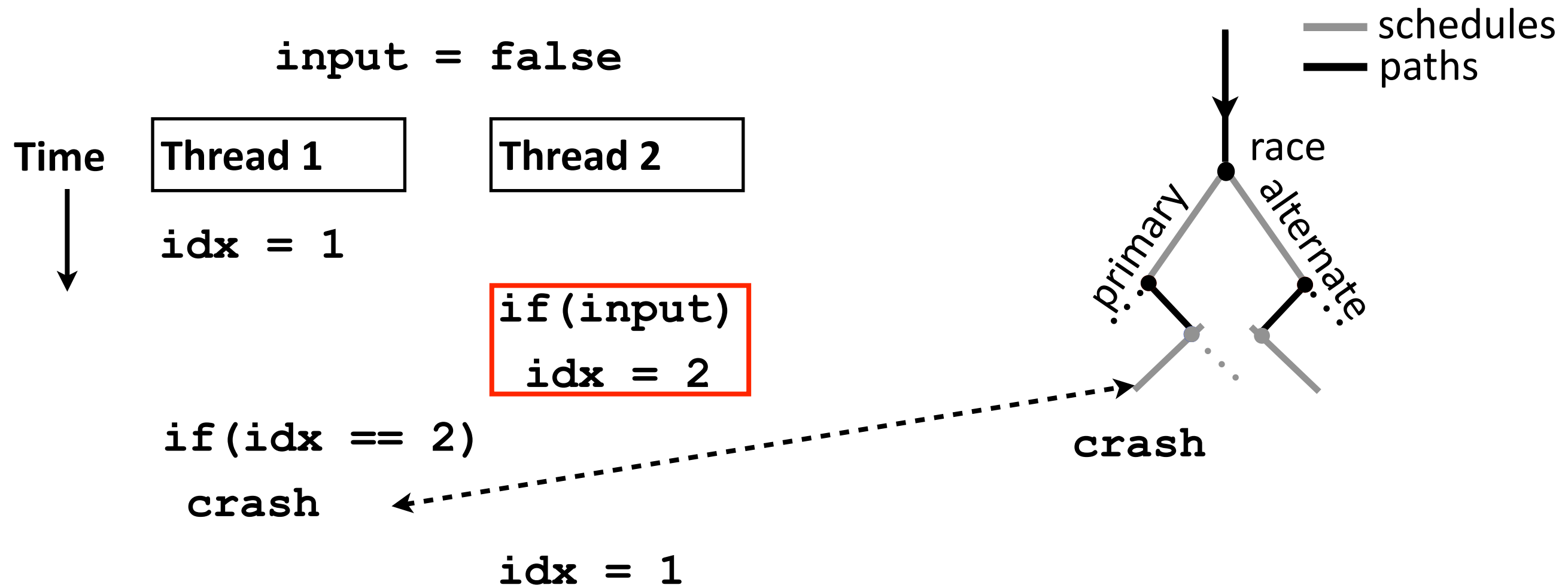
`crash`

`idx = 1`

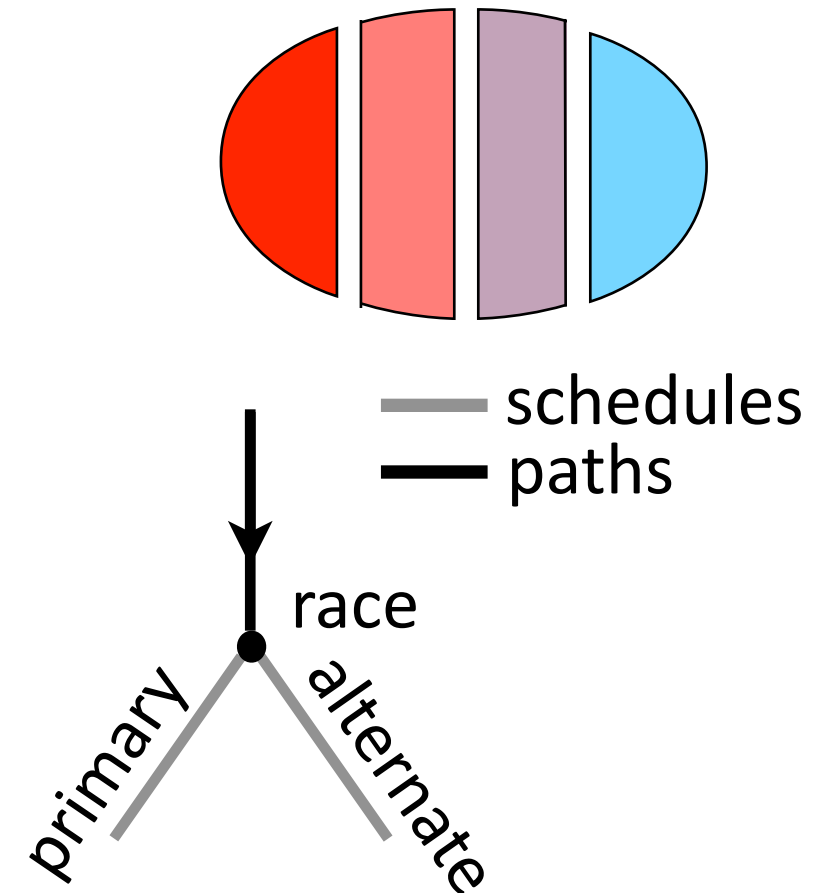
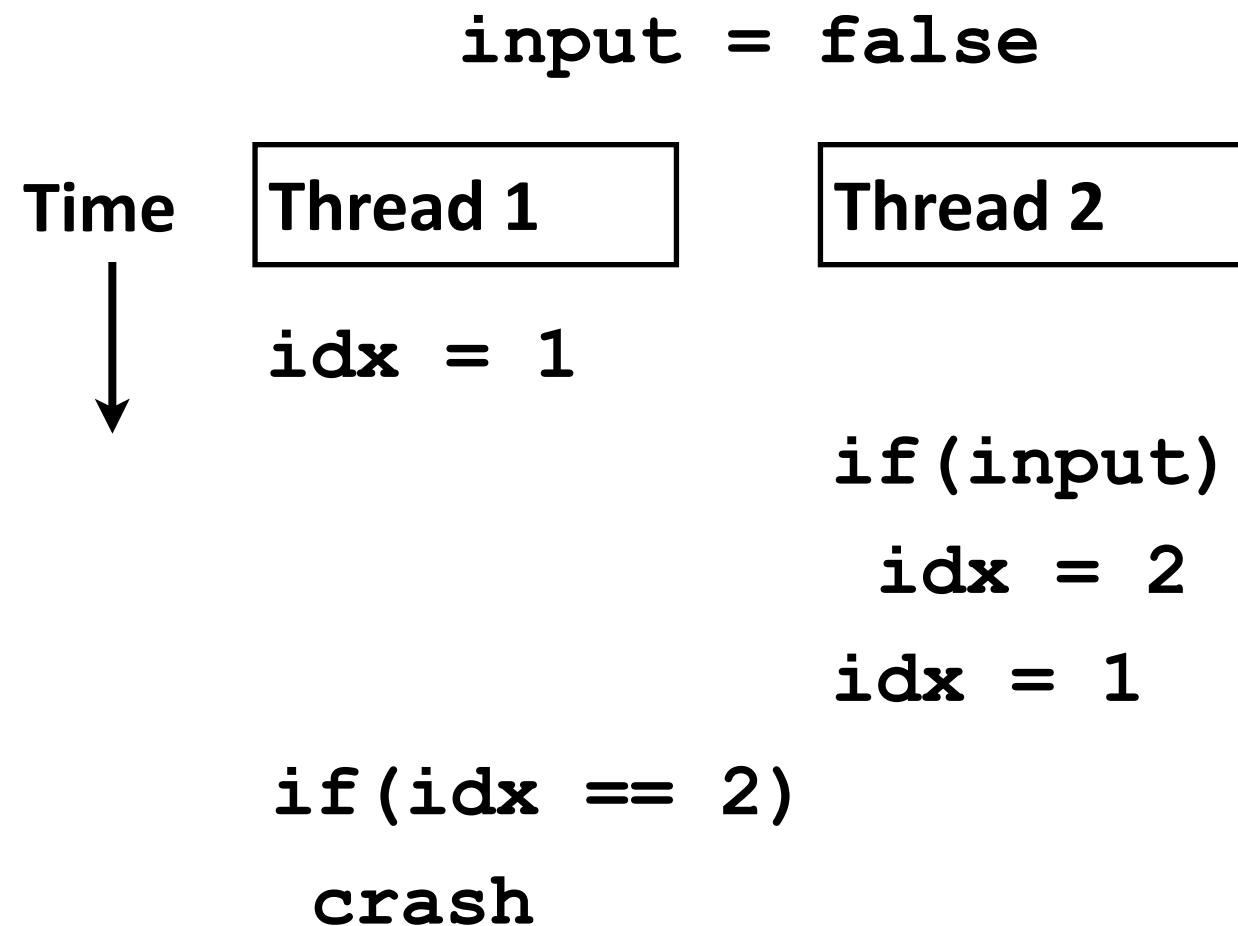




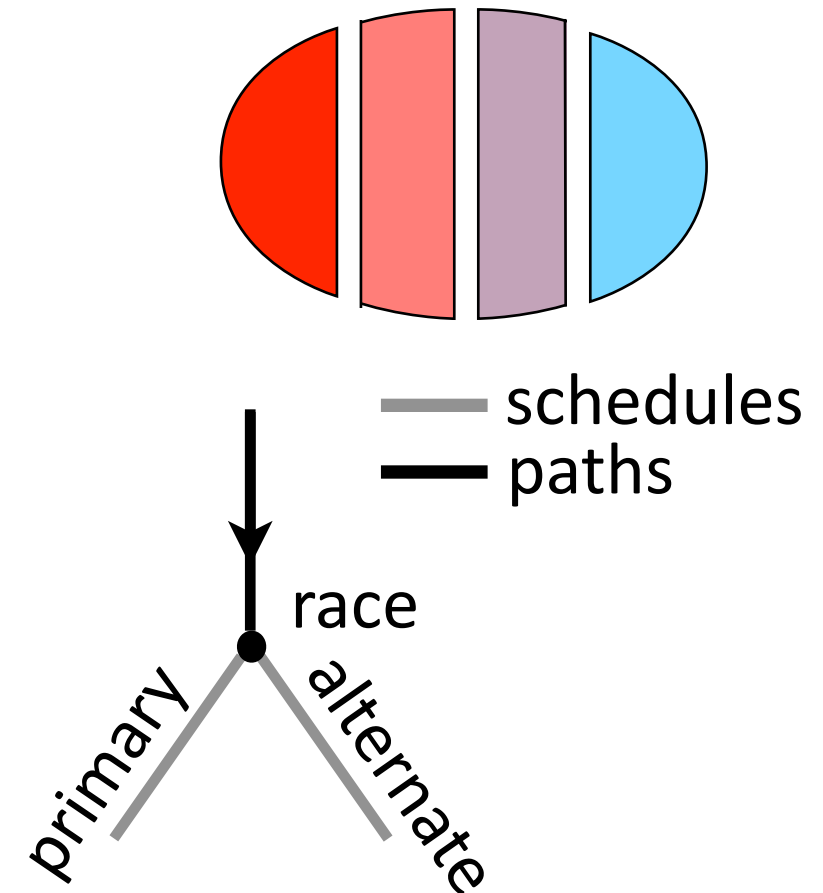
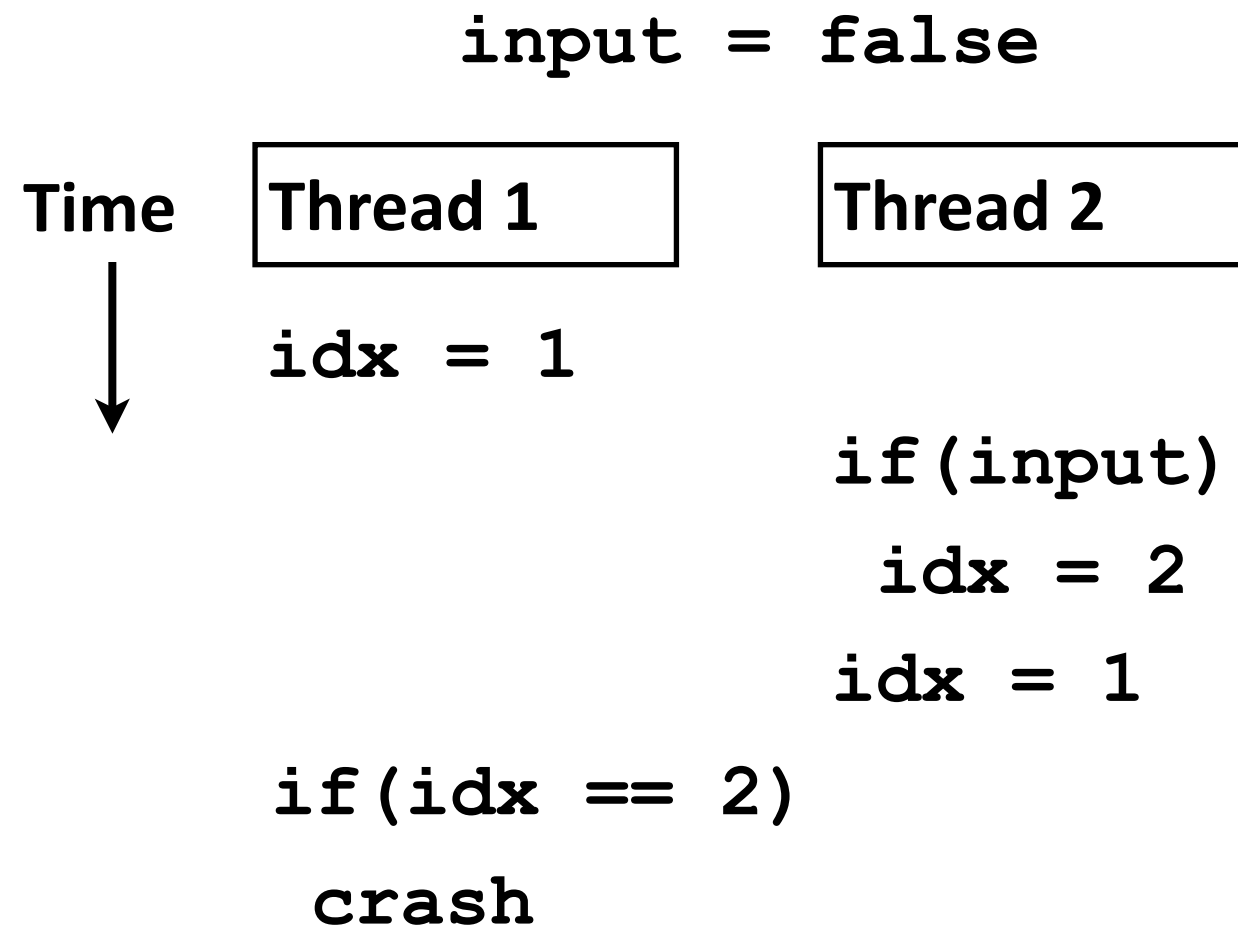
Multi-path Multi-schedule Analysis (our approach)



Multi-path Multi-schedule Analysis (our approach)

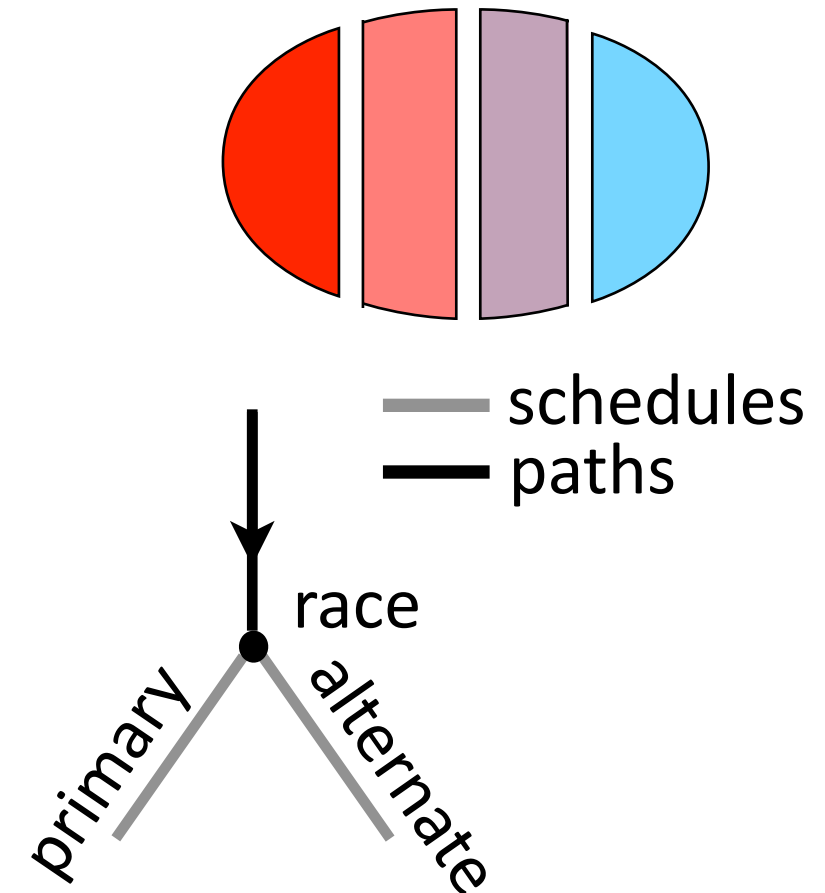
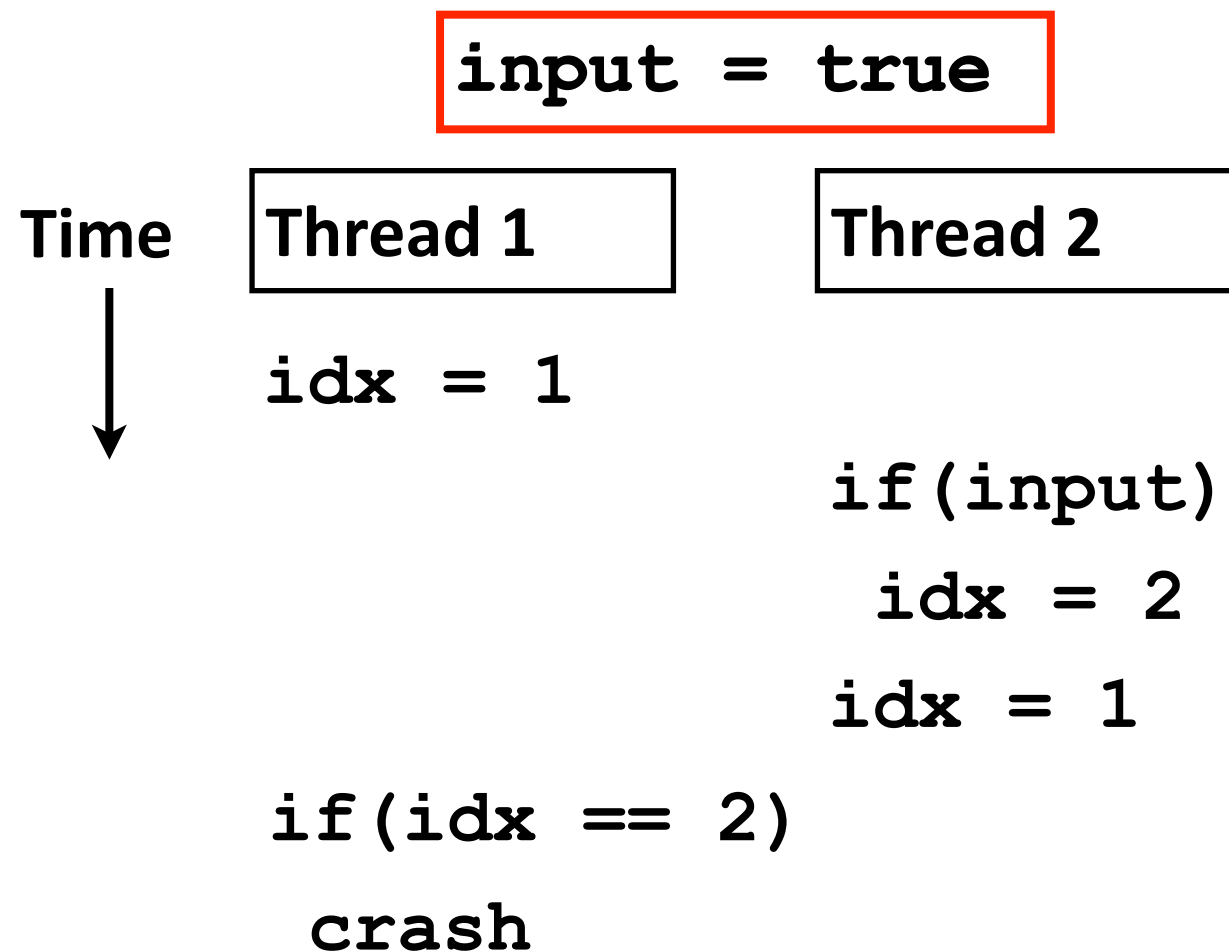


Multi-path Multi-schedule Analysis (our approach)



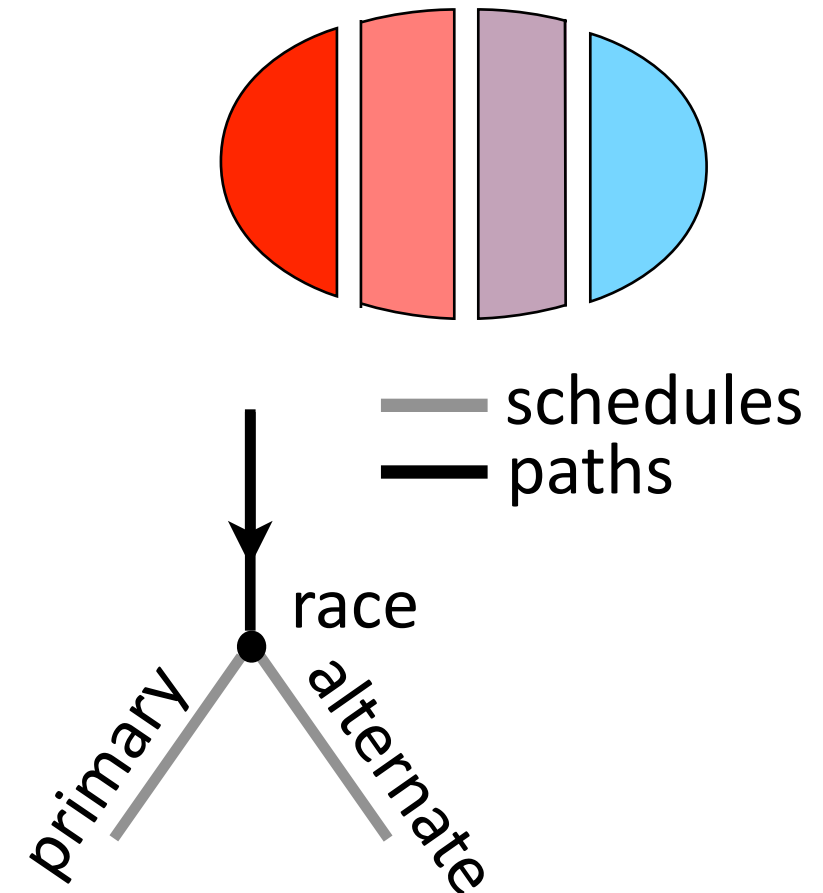
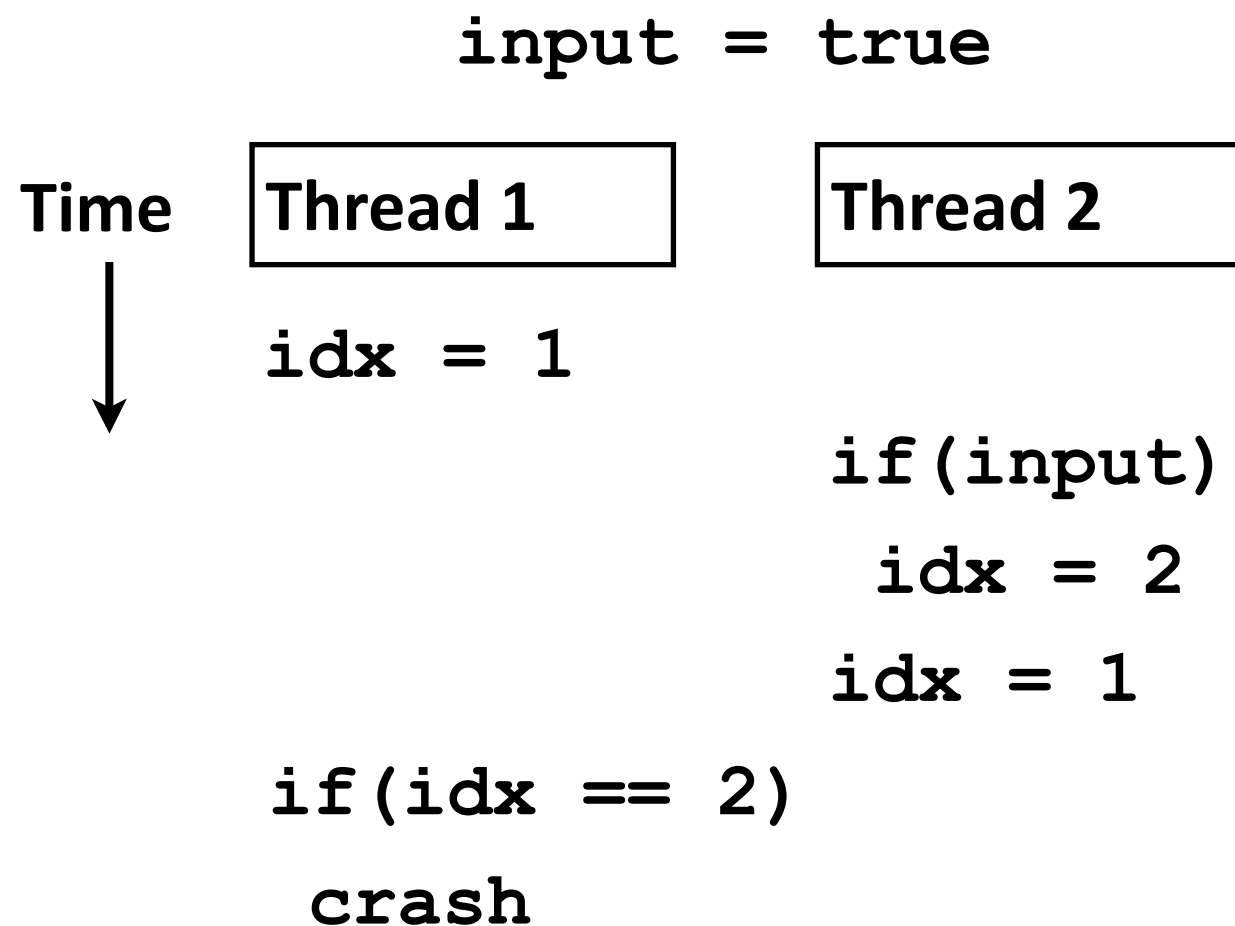
* Assume a sequentially consistent memory model

Multi-path Multi-schedule Analysis (our approach)



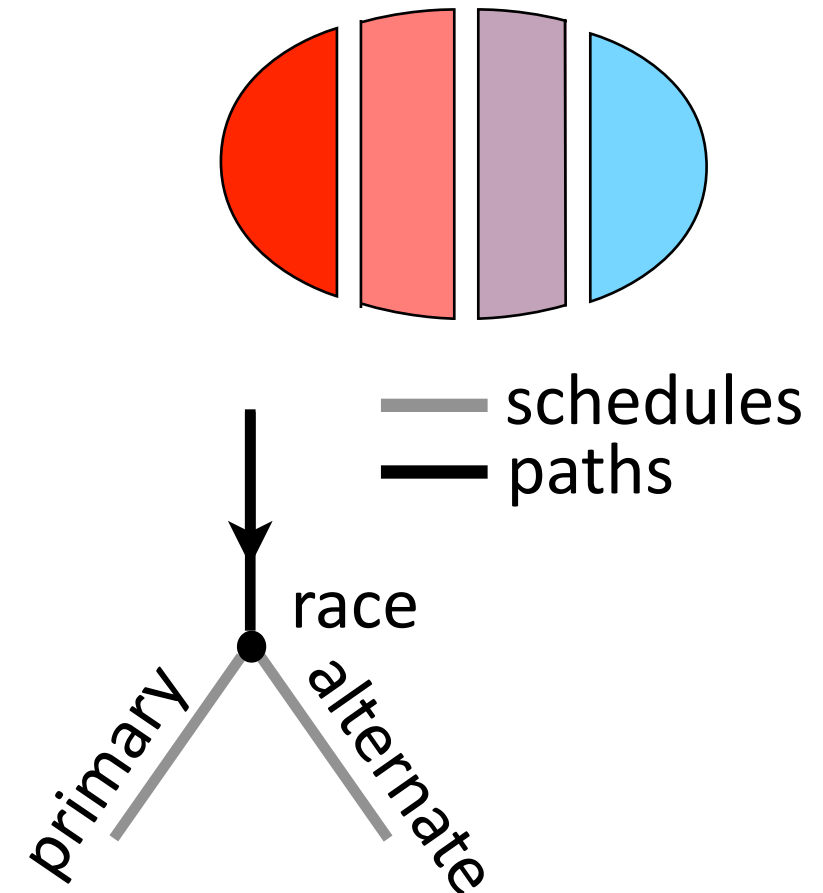
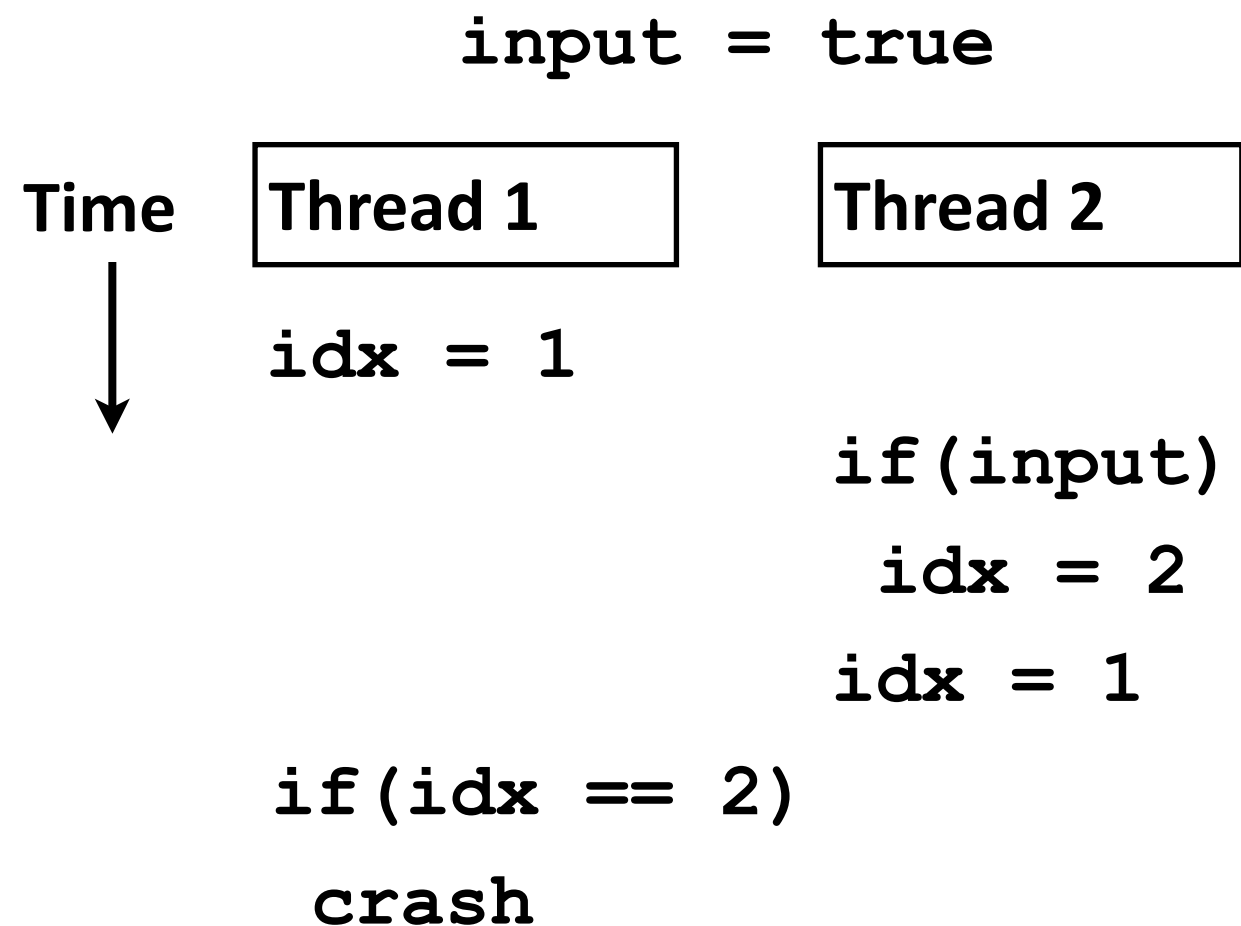
* Assume a sequentially consistent memory model

Multi-path Multi-schedule Analysis (our approach)



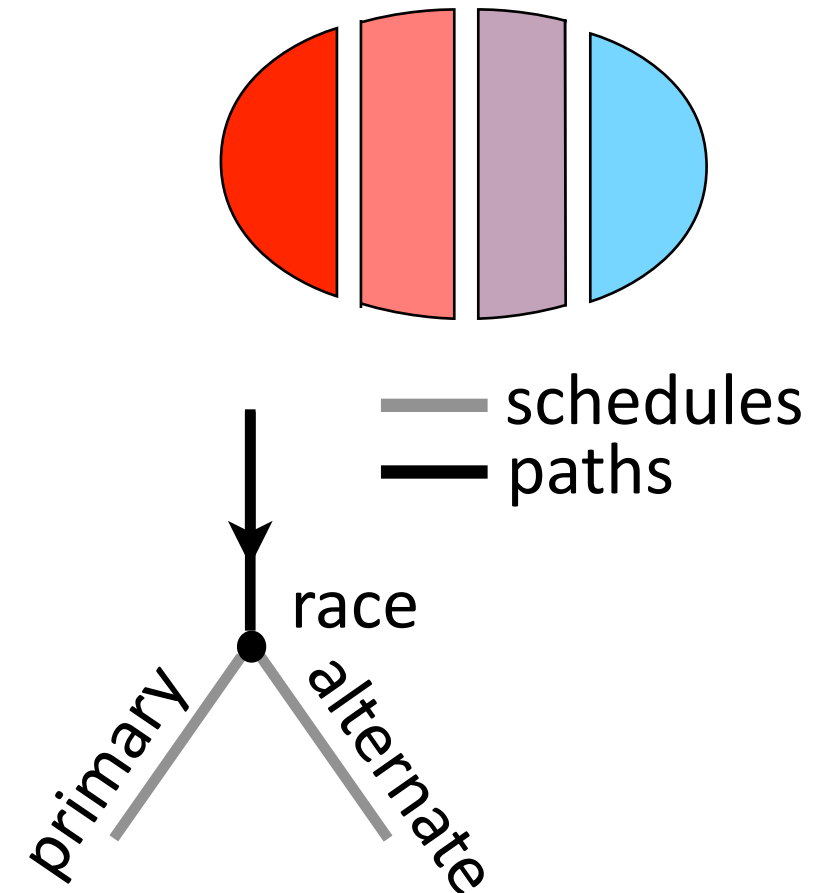
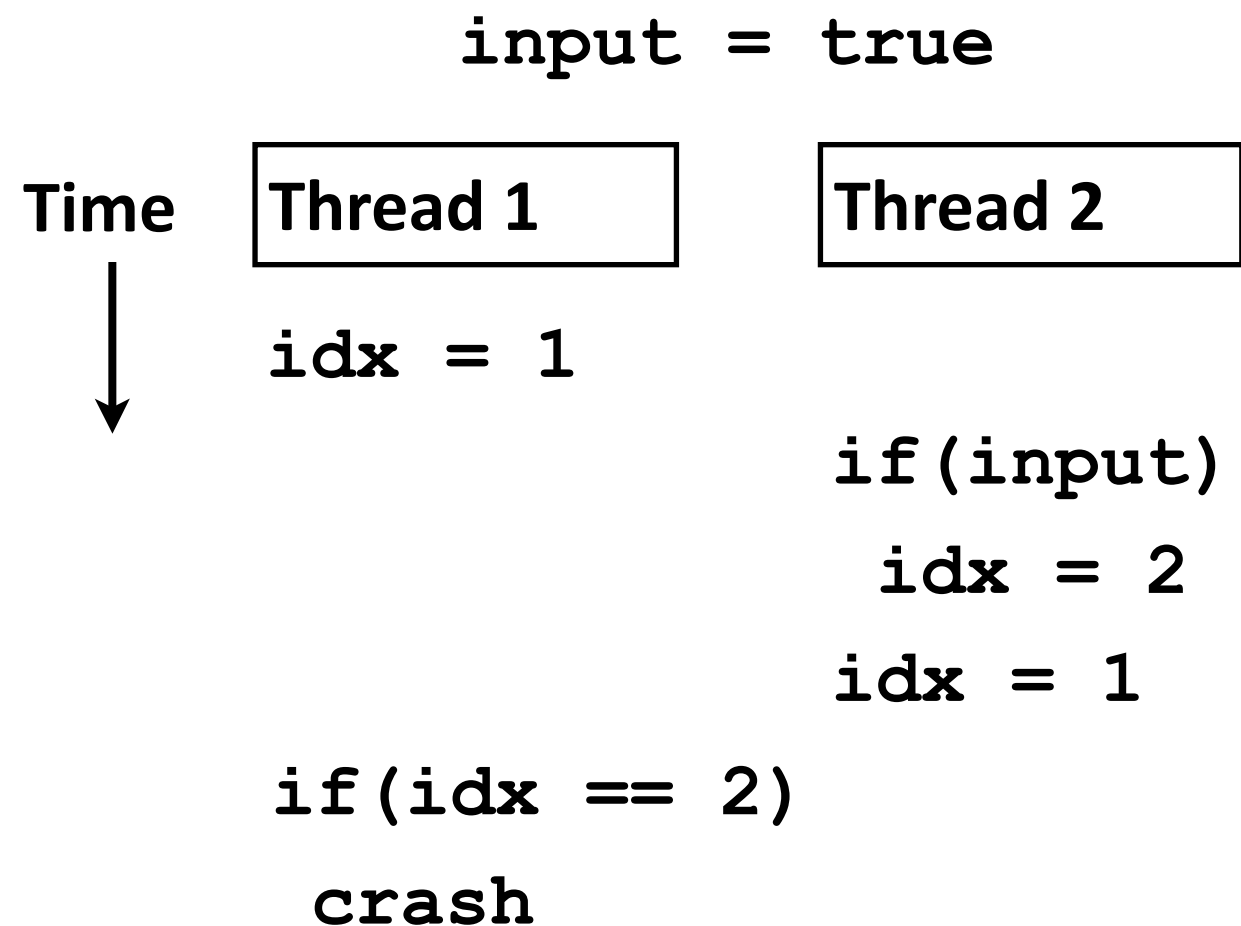
* Assume a sequentially consistent memory model

Multi-path Multi-schedule Analysis (our approach)



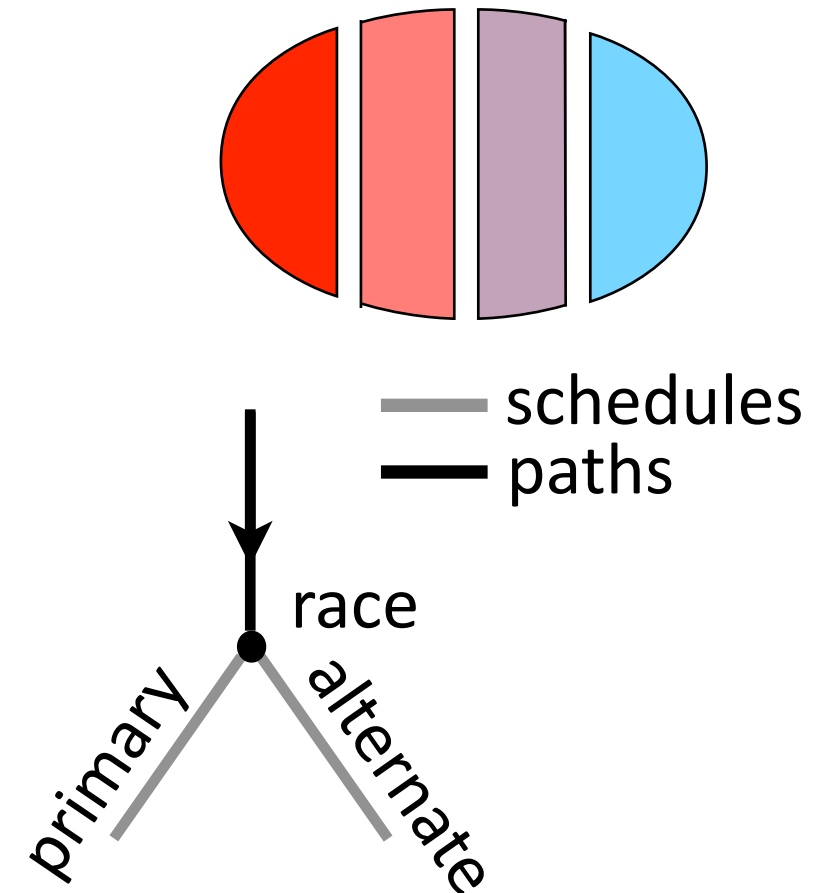
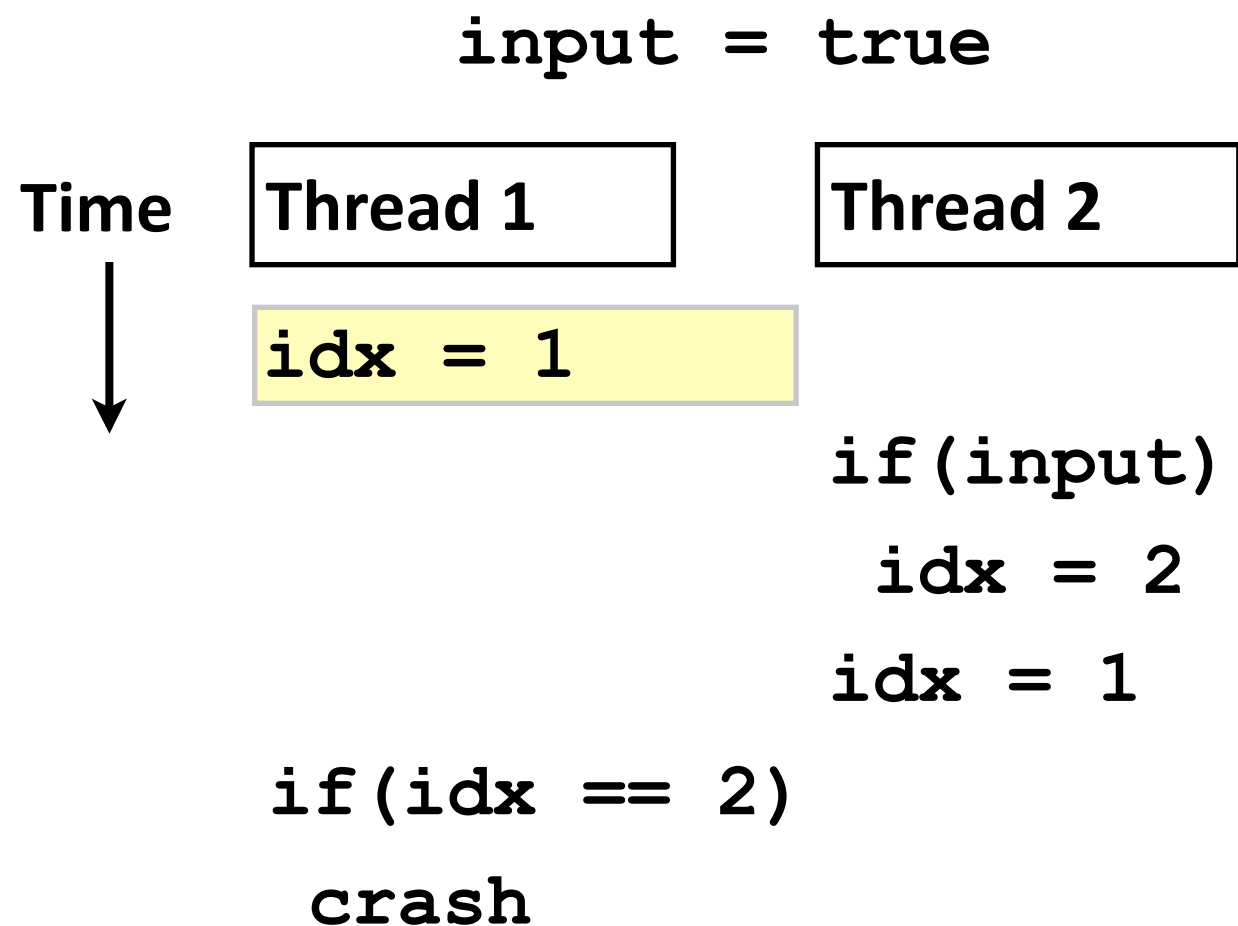
* Assume a sequentially consistent memory model

Multi-path Multi-schedule Analysis (our approach)



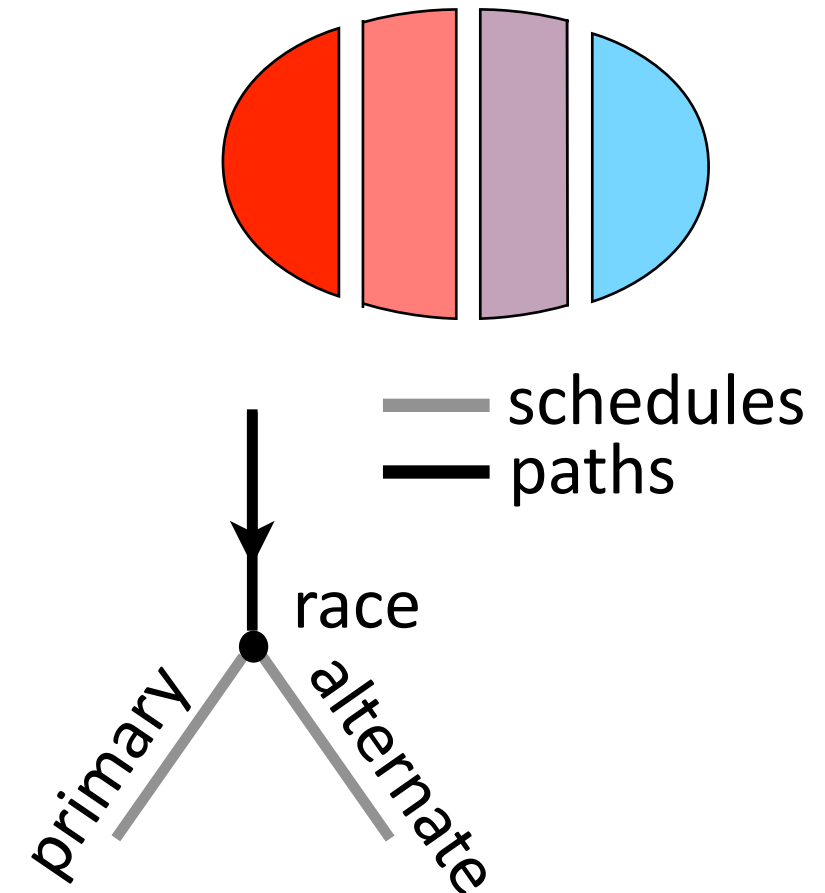
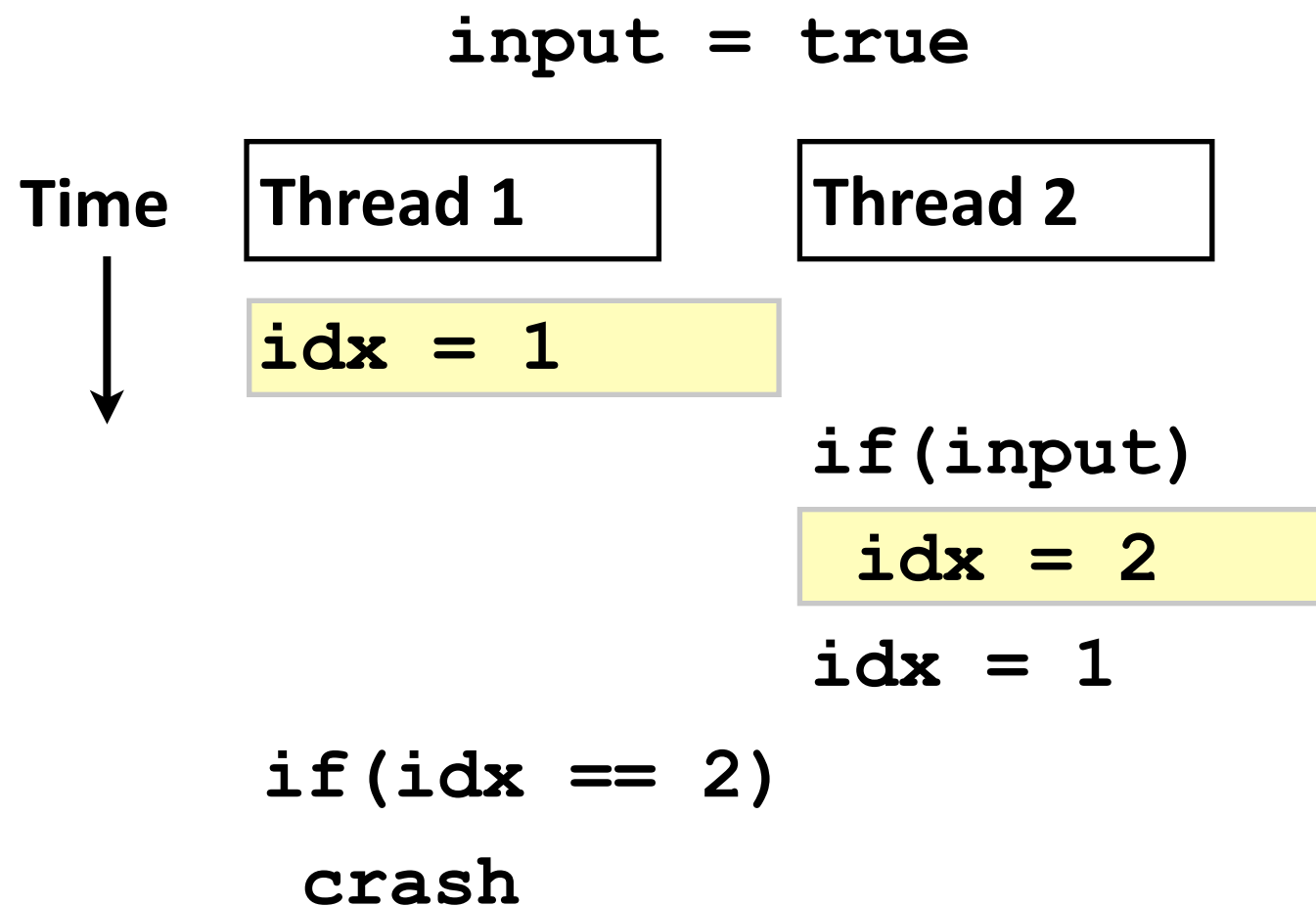
* Assume a sequentially consistent memory model

Multi-path Multi-schedule Analysis (our approach)



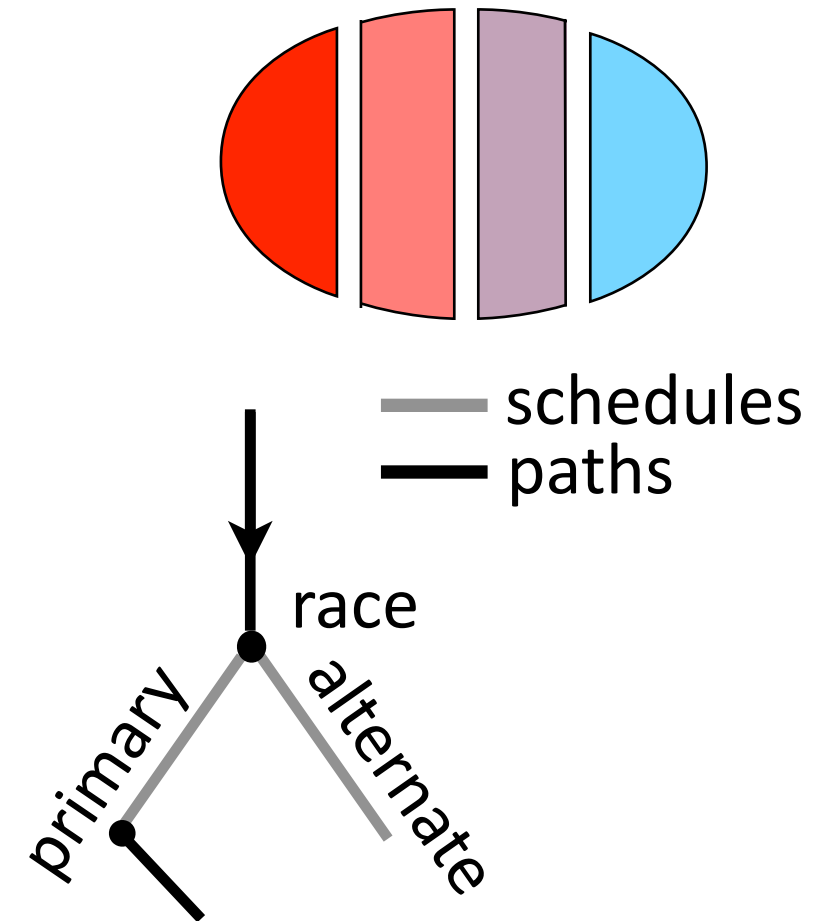
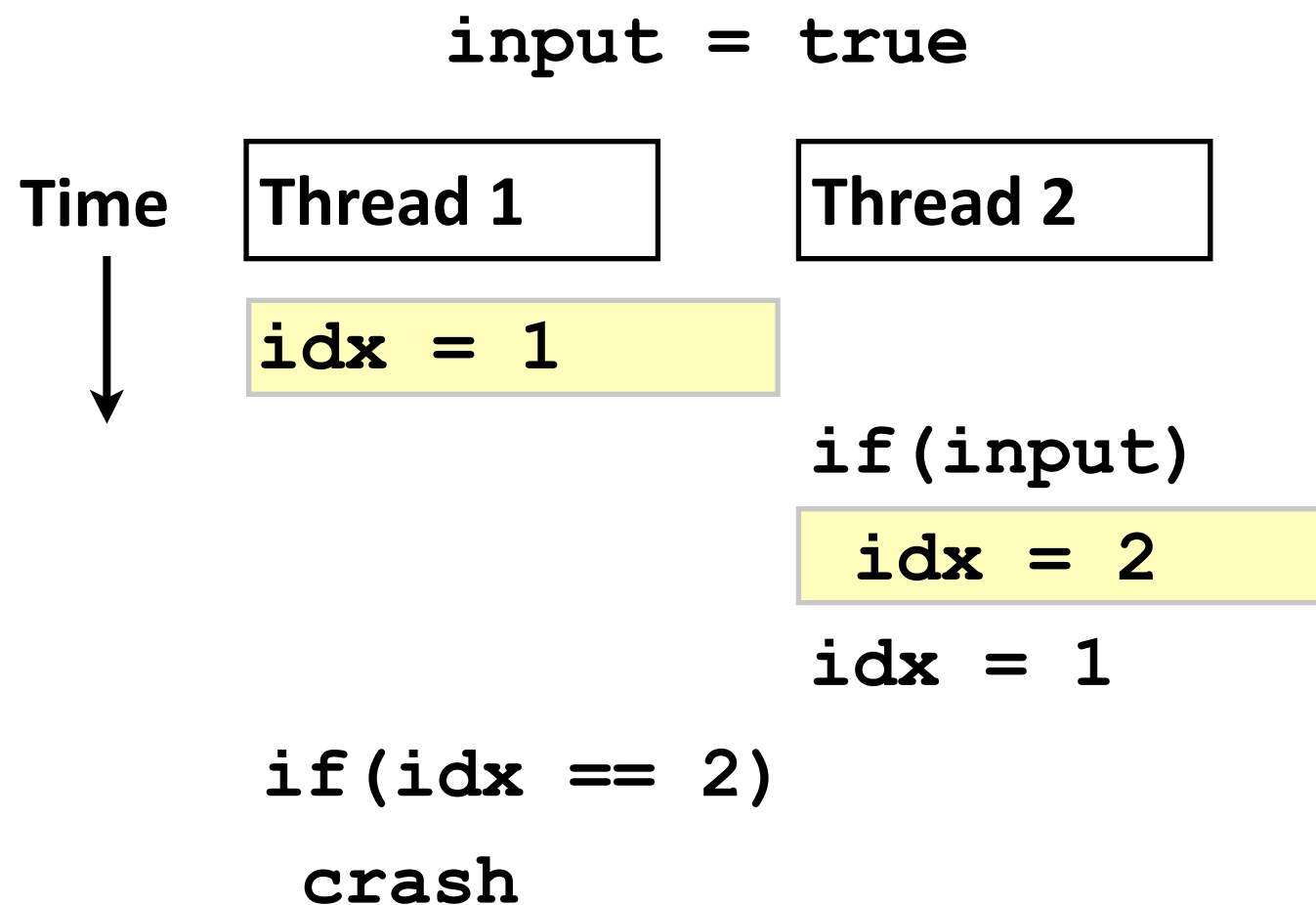
* Assume a sequentially consistent memory model

Multi-path Multi-schedule Analysis (our approach)



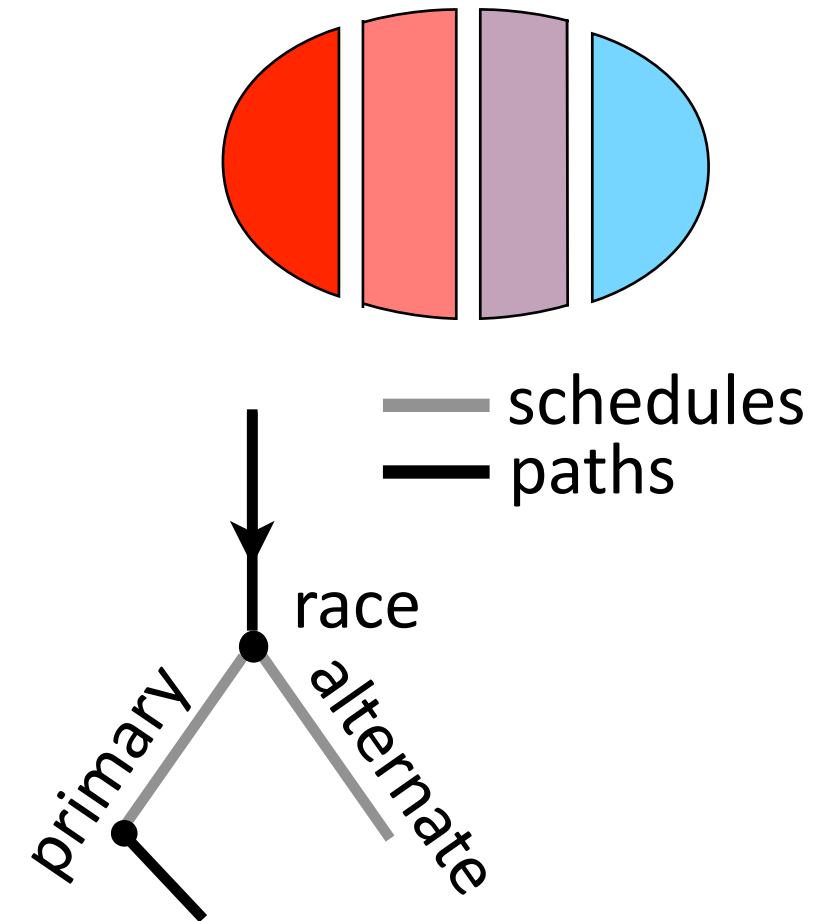
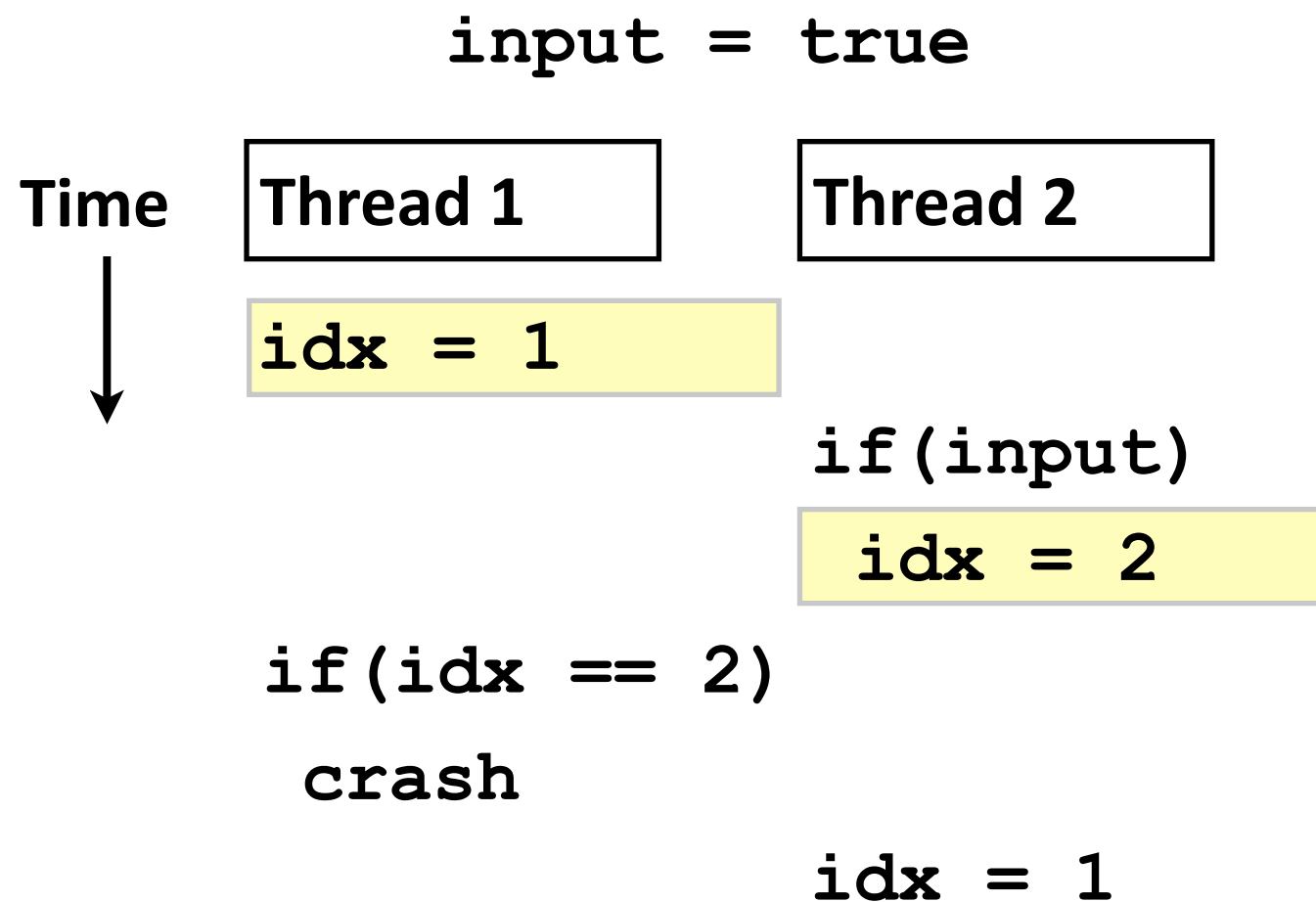
* Assume a sequentially consistent memory model

Multi-path Multi-schedule Analysis (our approach)



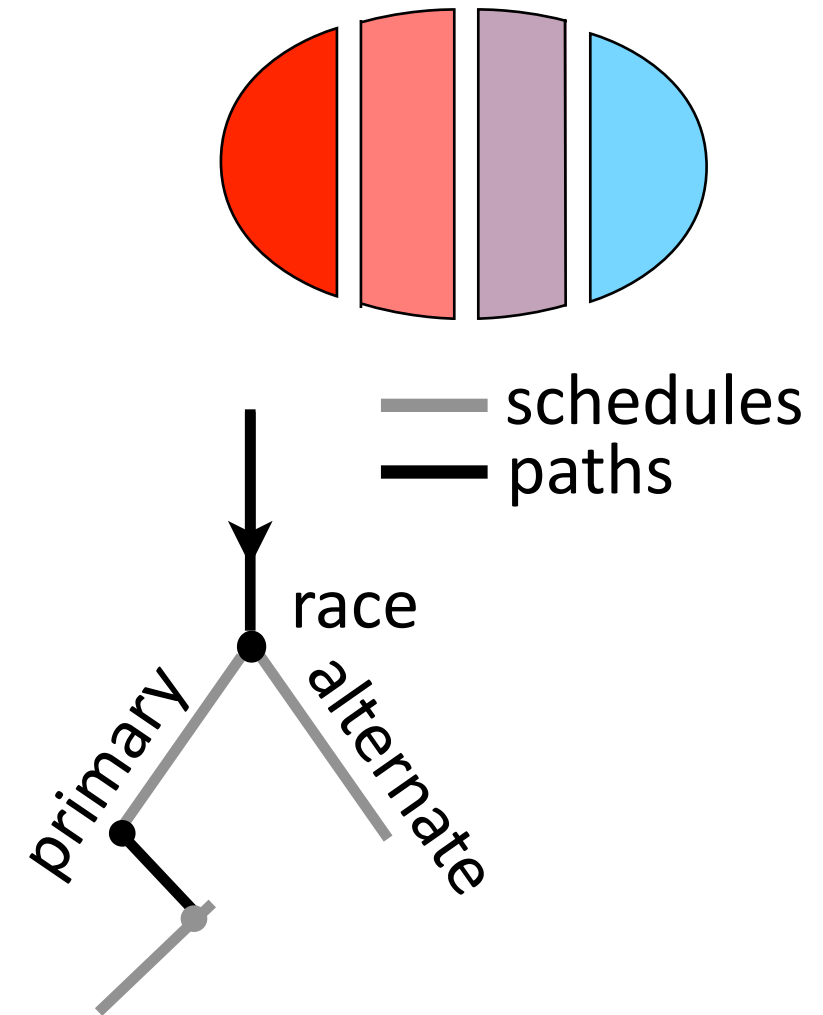
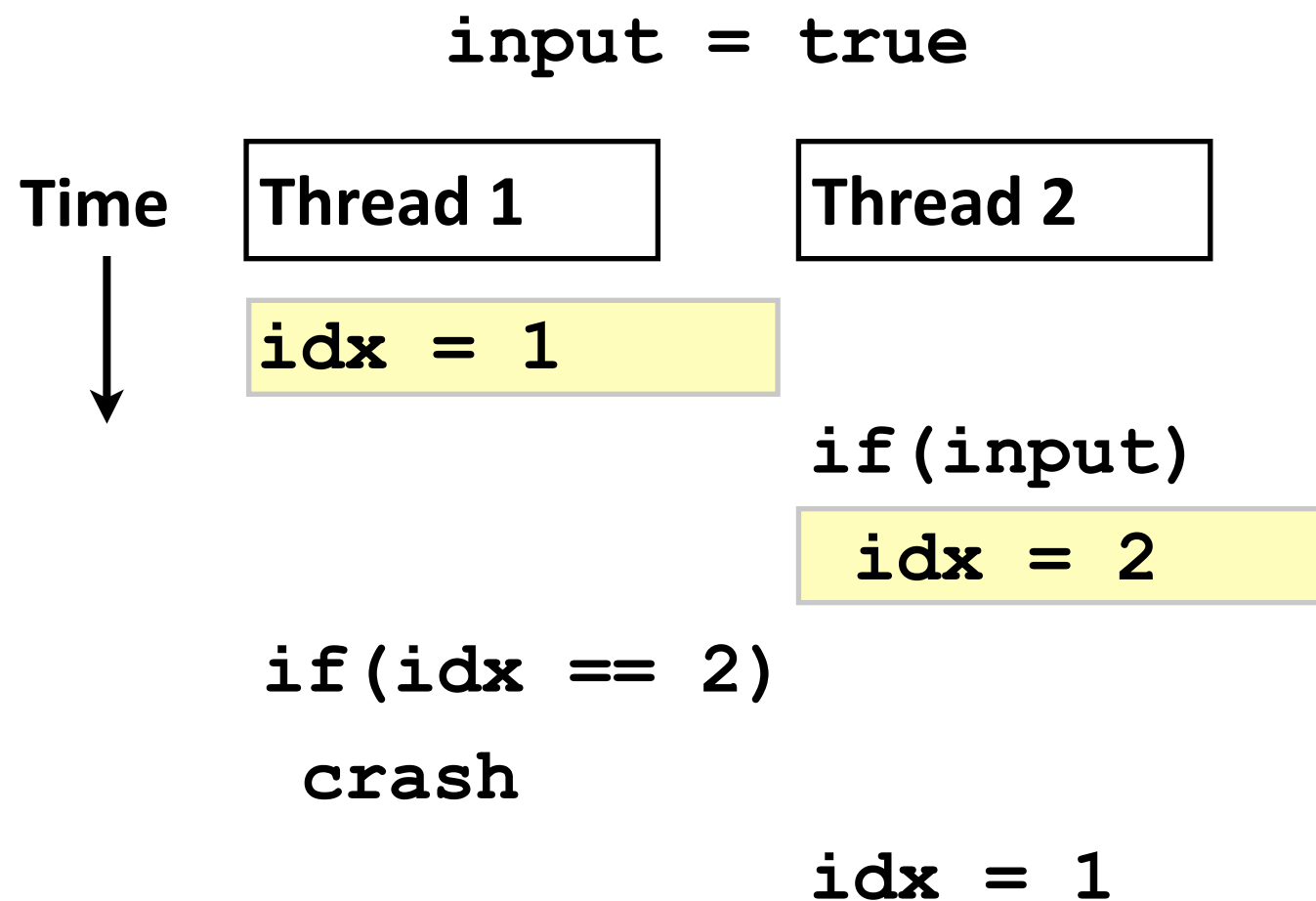
* Assume a sequentially consistent memory model

Multi-path Multi-schedule Analysis (our approach)



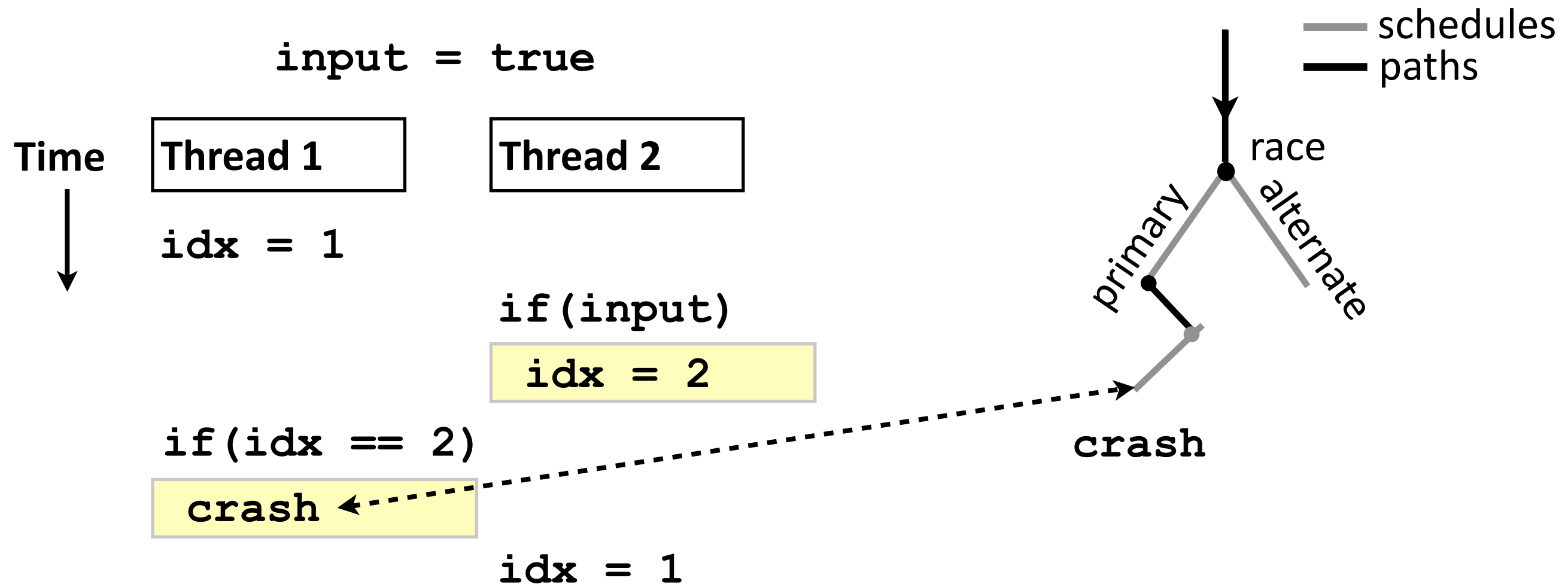
* Assume a sequentially consistent memory model

Multi-path Multi-schedule Analysis (our approach)



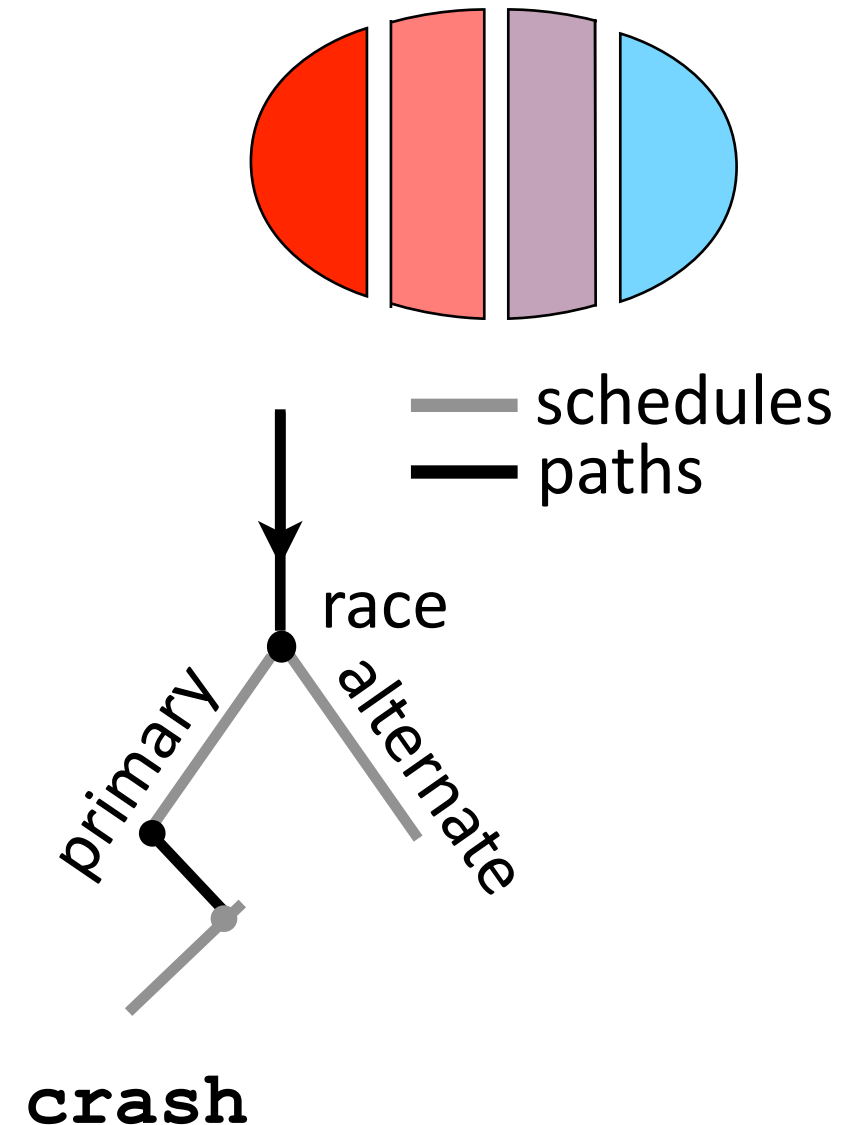
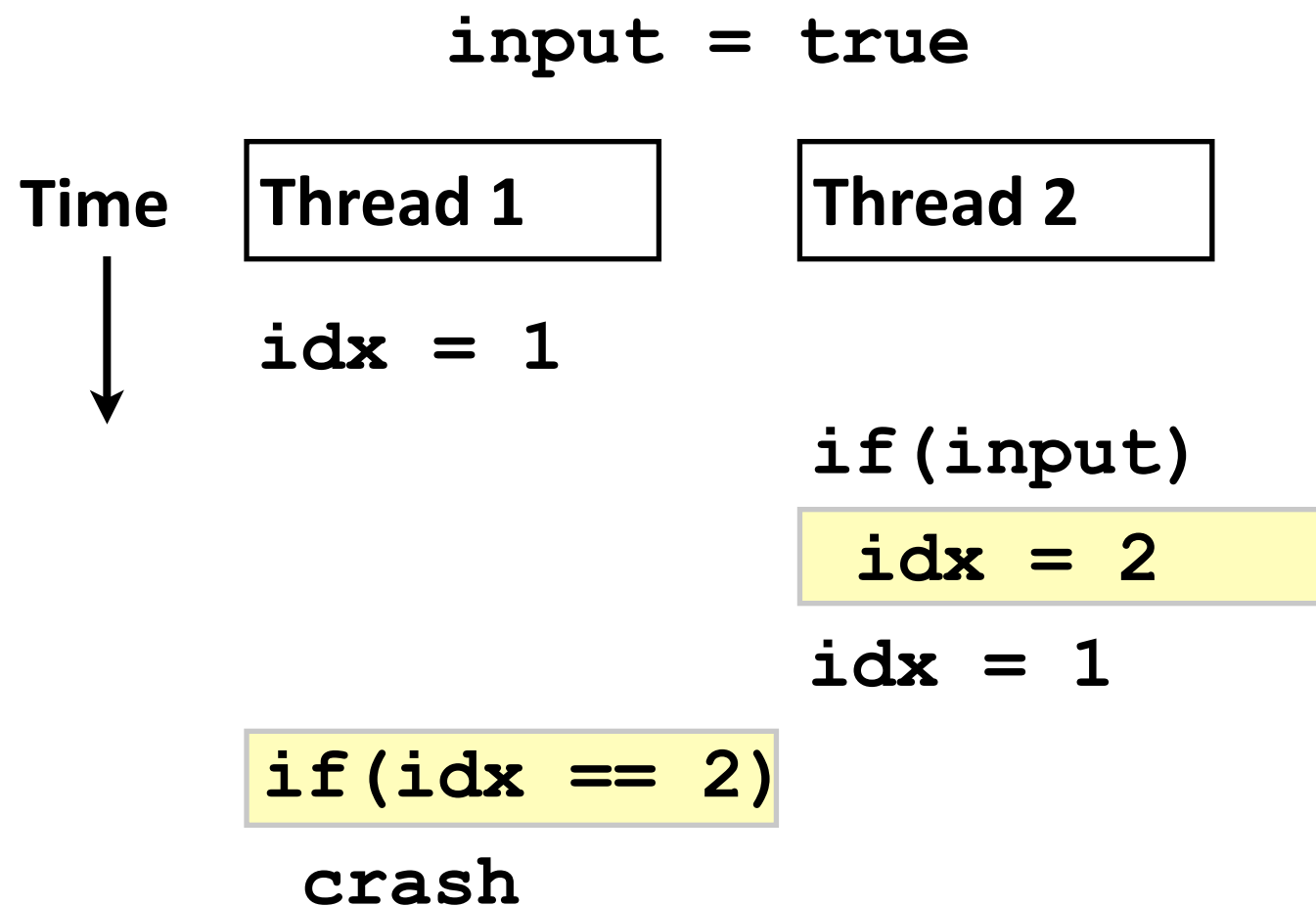
* Assume a sequentially consistent memory model

Multi-path Multi-schedule Analysis (our approach)



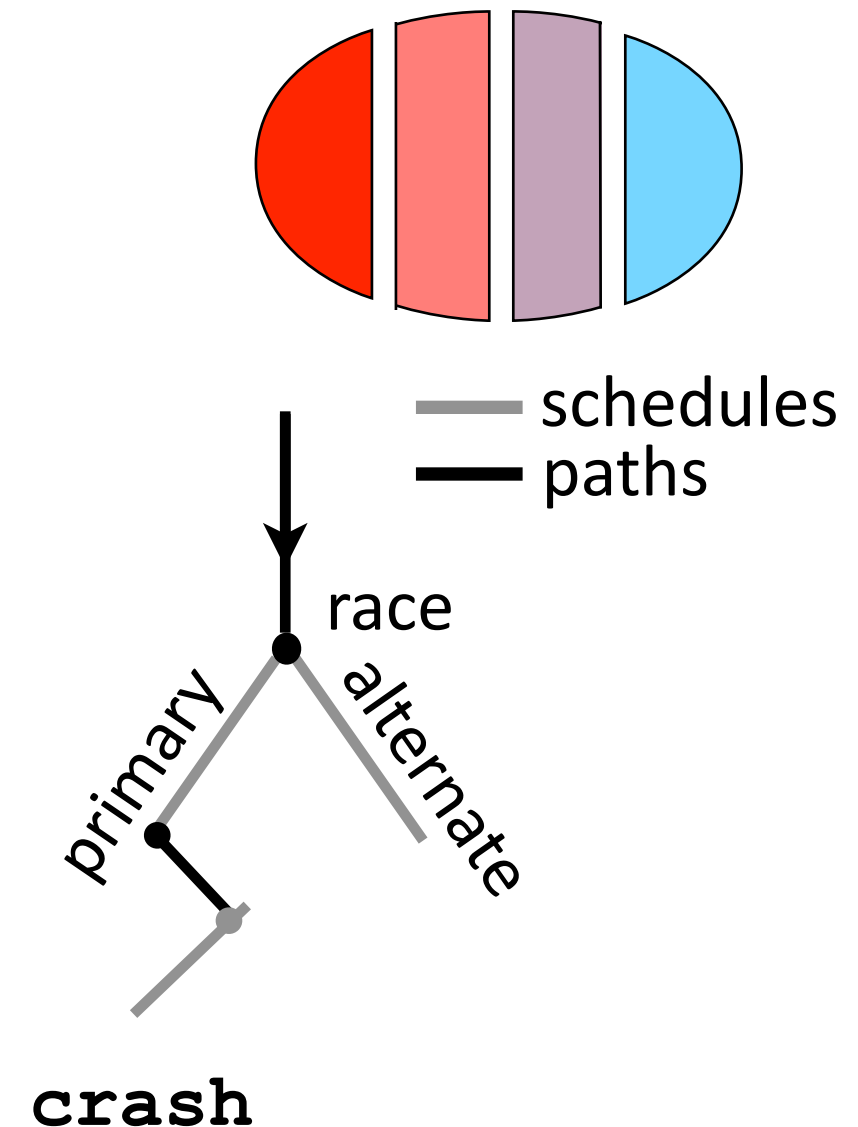
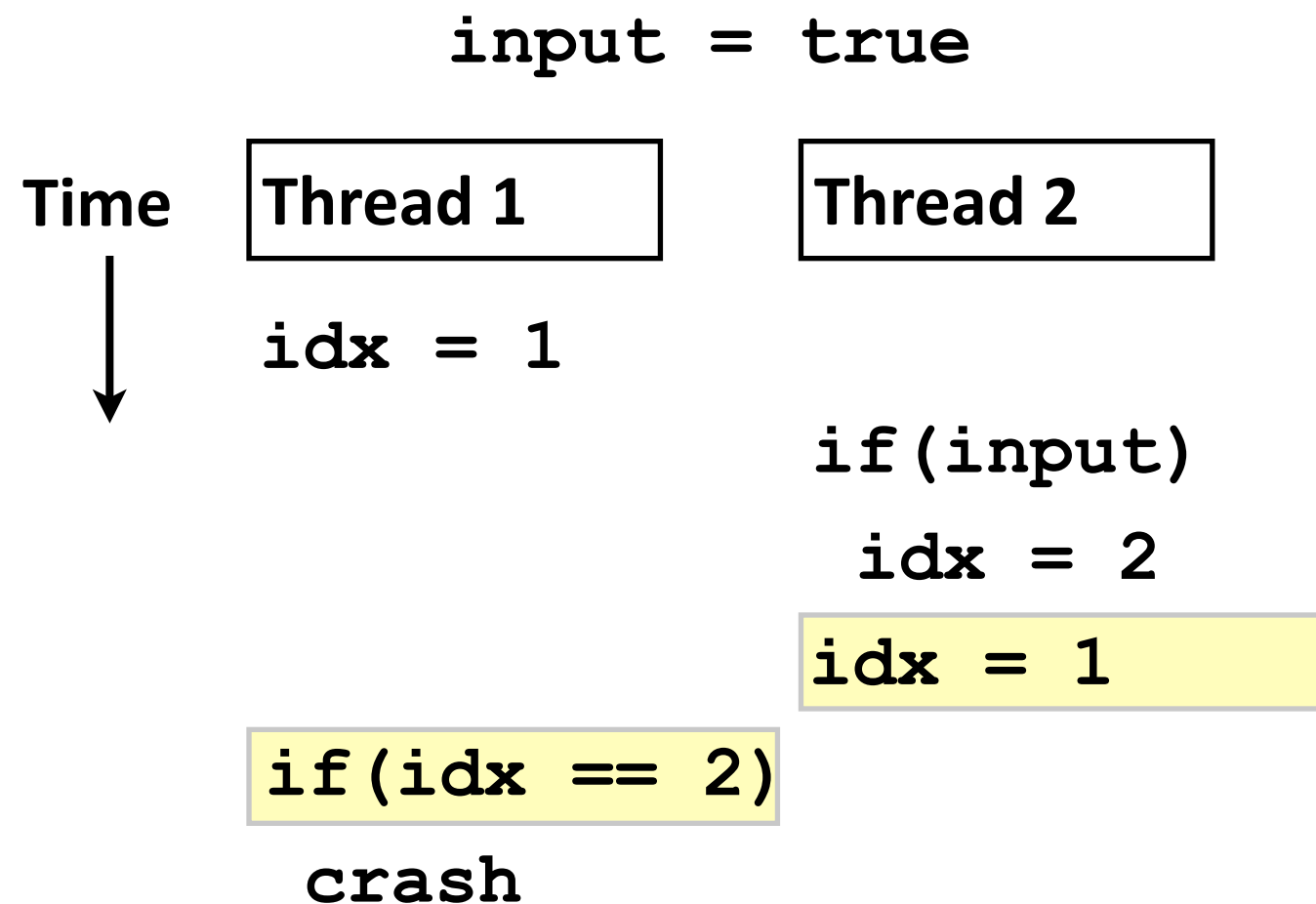
* Assume a sequentially consistent memory model

Multi-path Multi-schedule Analysis (our approach)



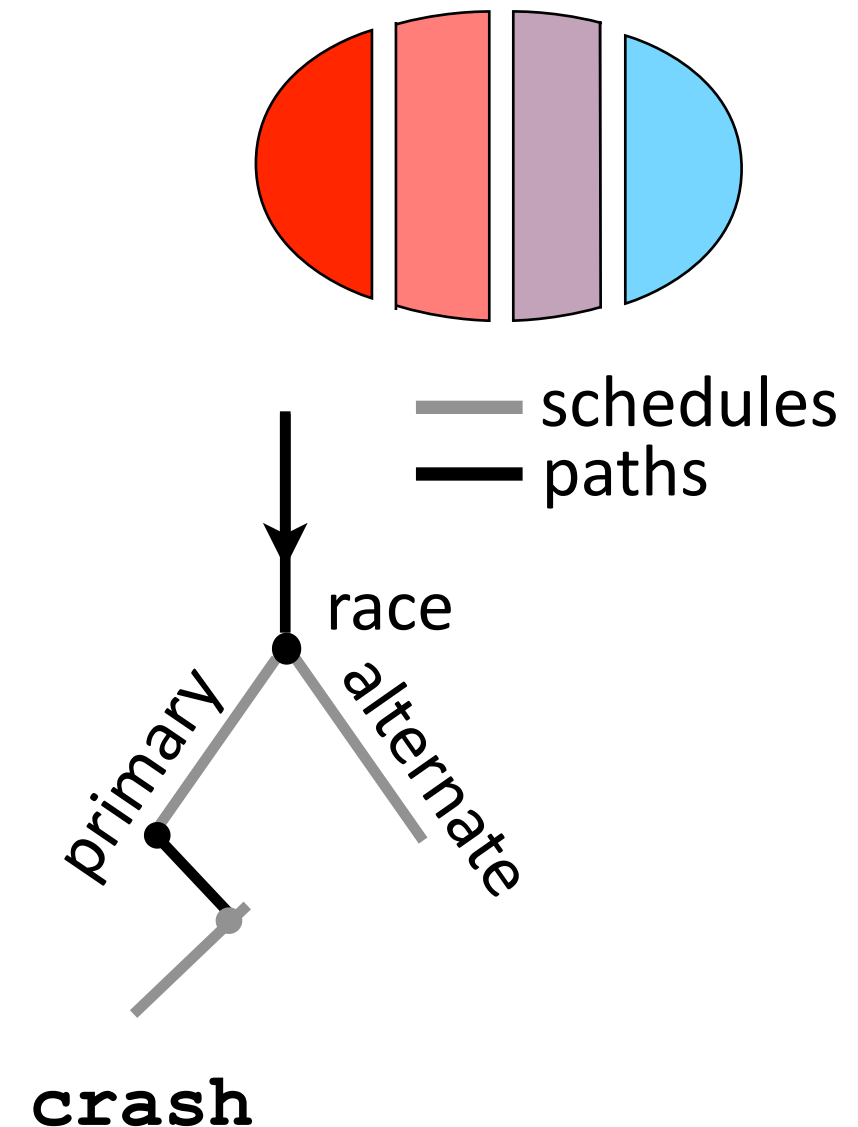
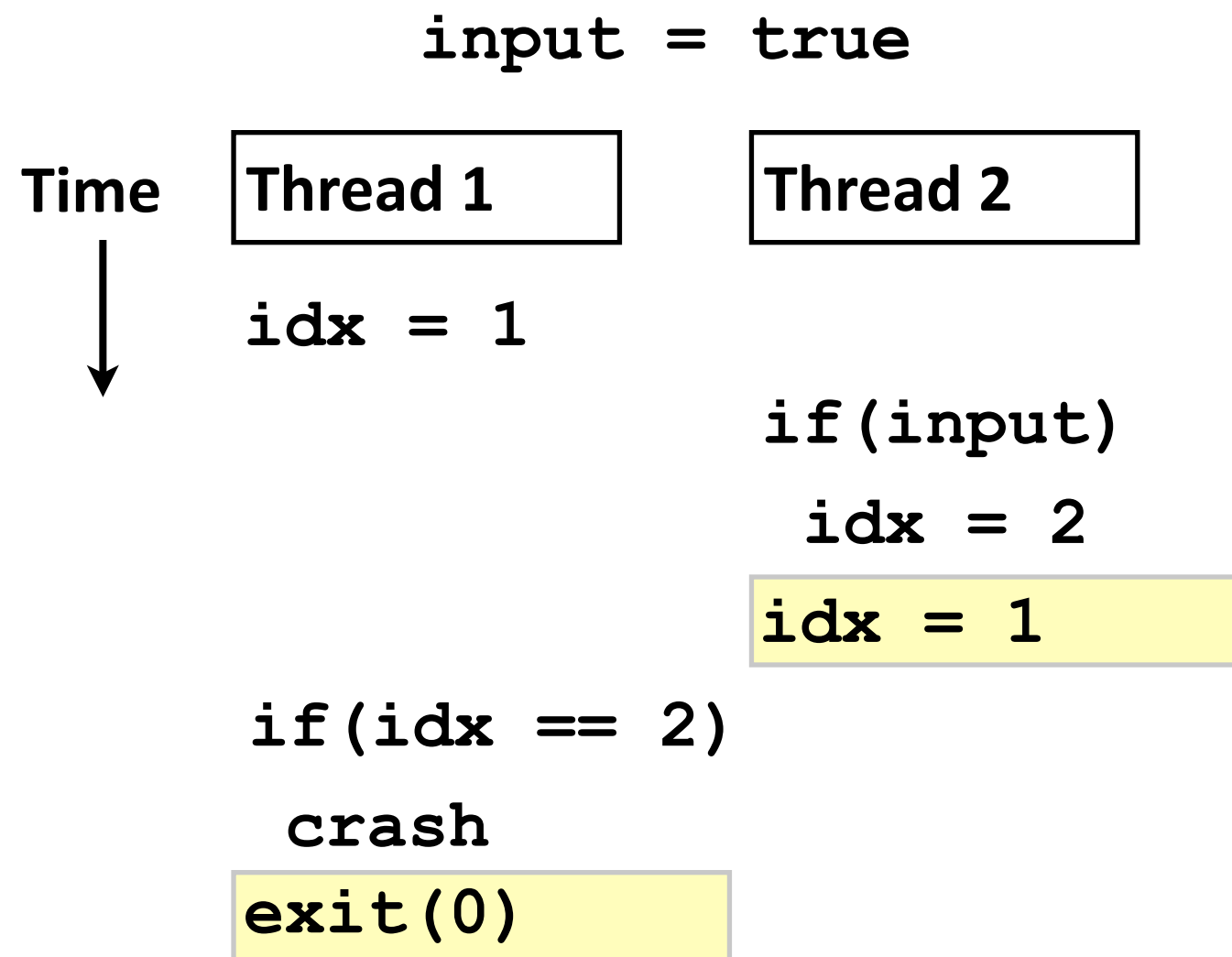
* Assume a sequentially consistent memory model

Multi-path Multi-schedule Analysis (our approach)

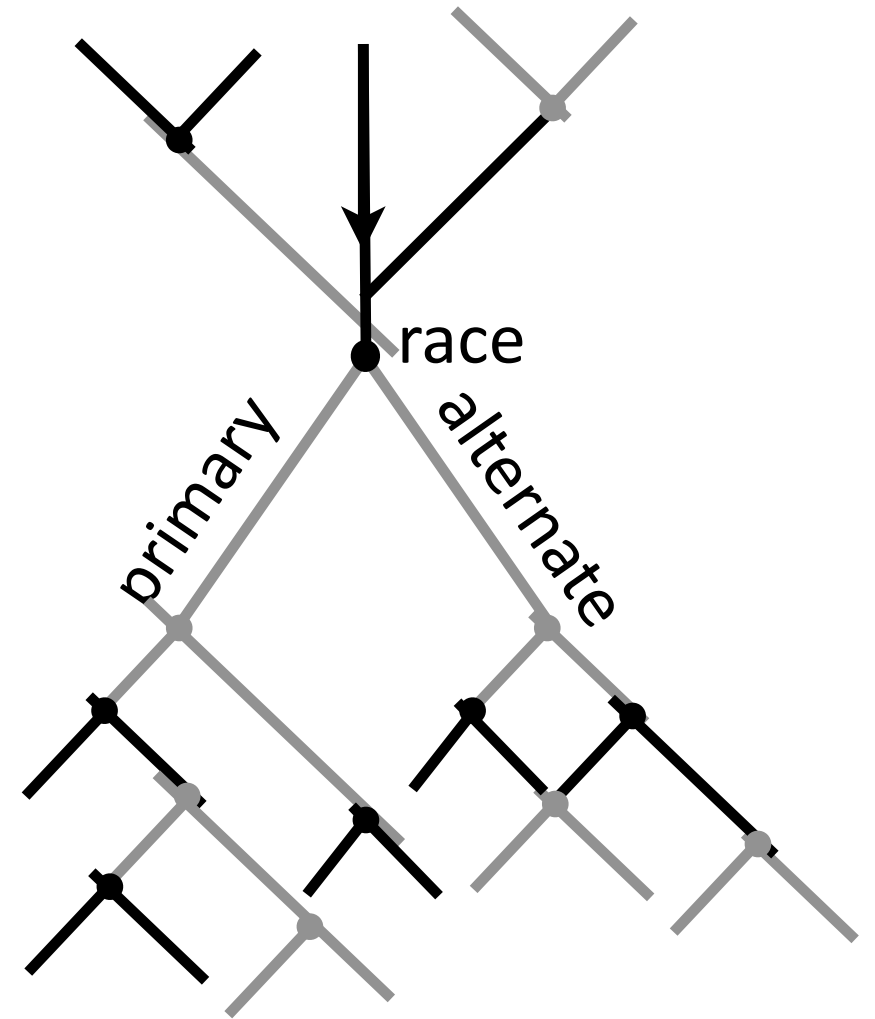
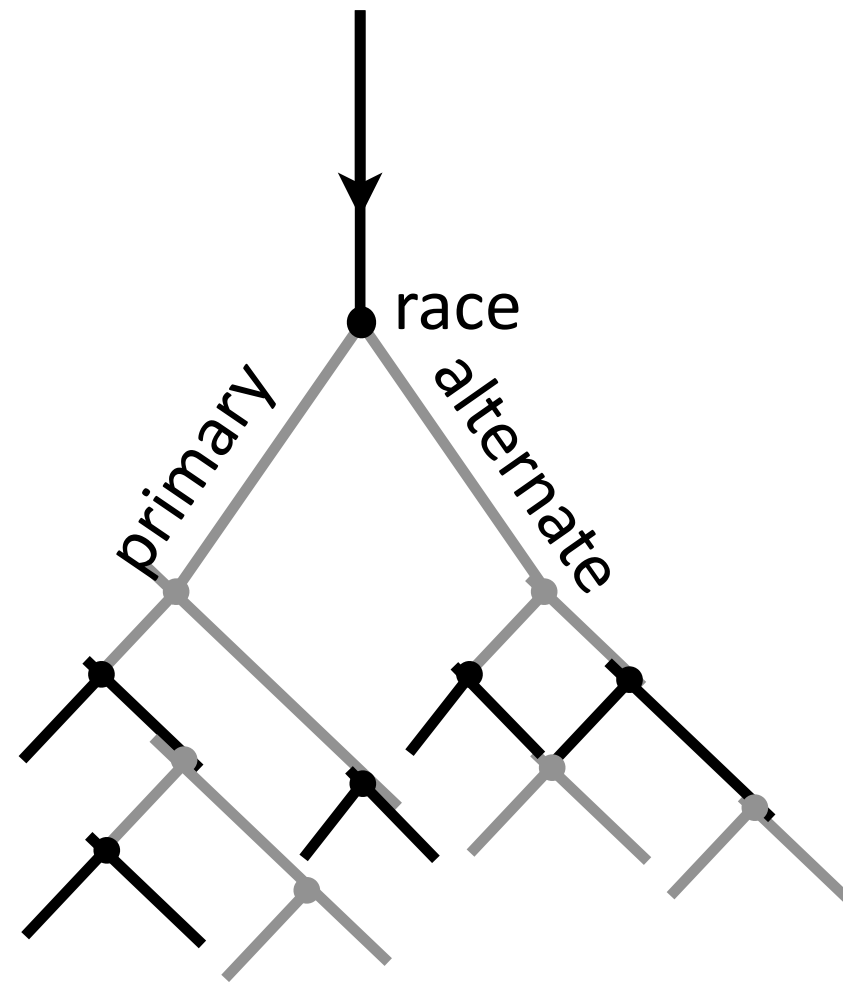
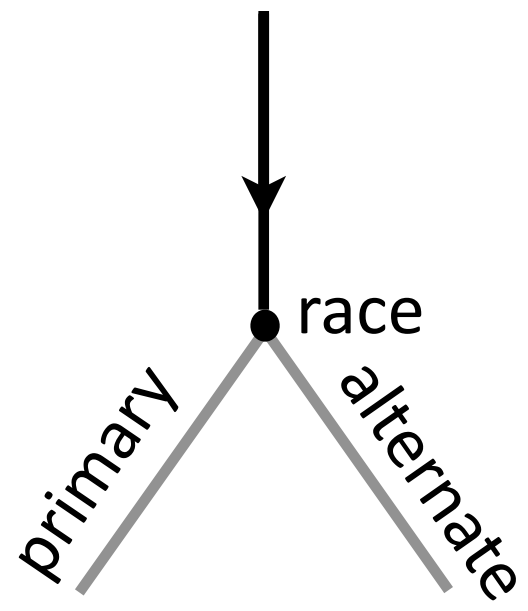


* Assume a sequentially consistent memory model

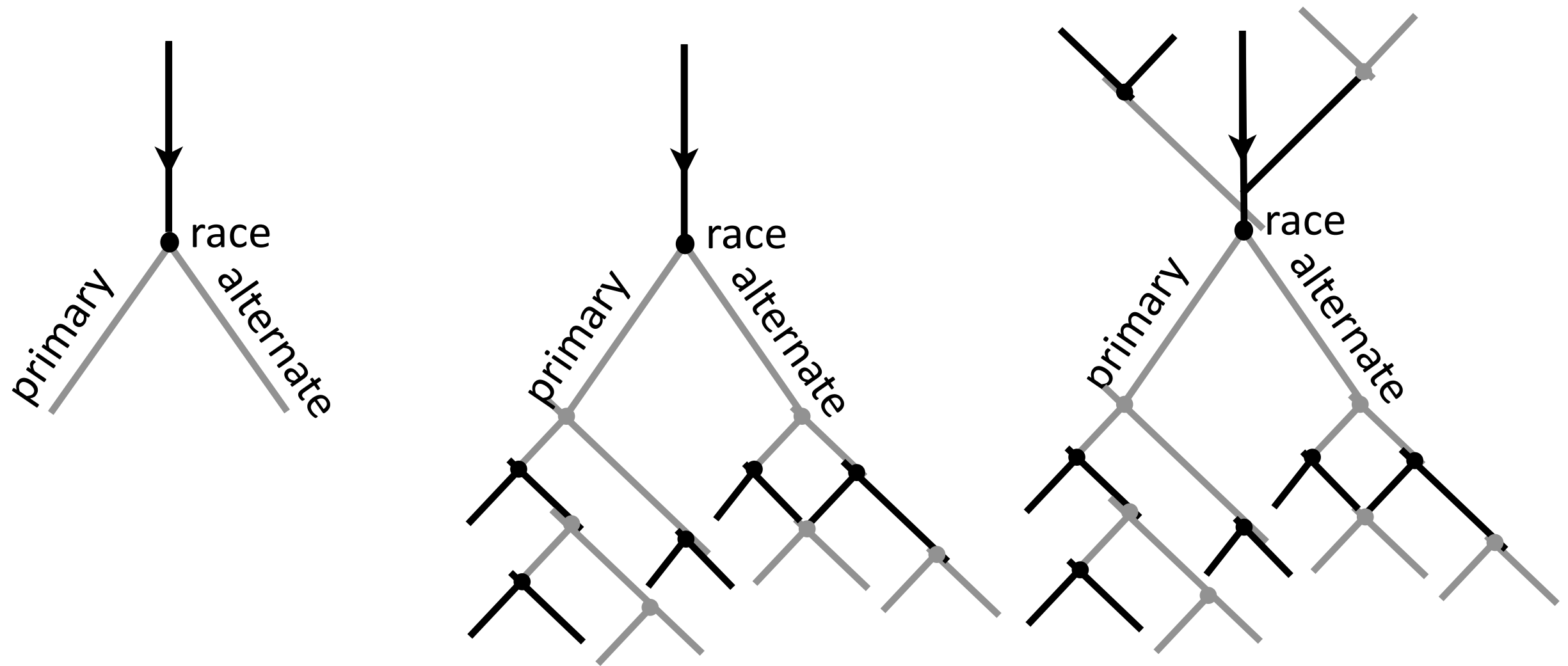
Multi-path Multi-schedule Analysis (our approach)



* Assume a sequentially consistent memory model

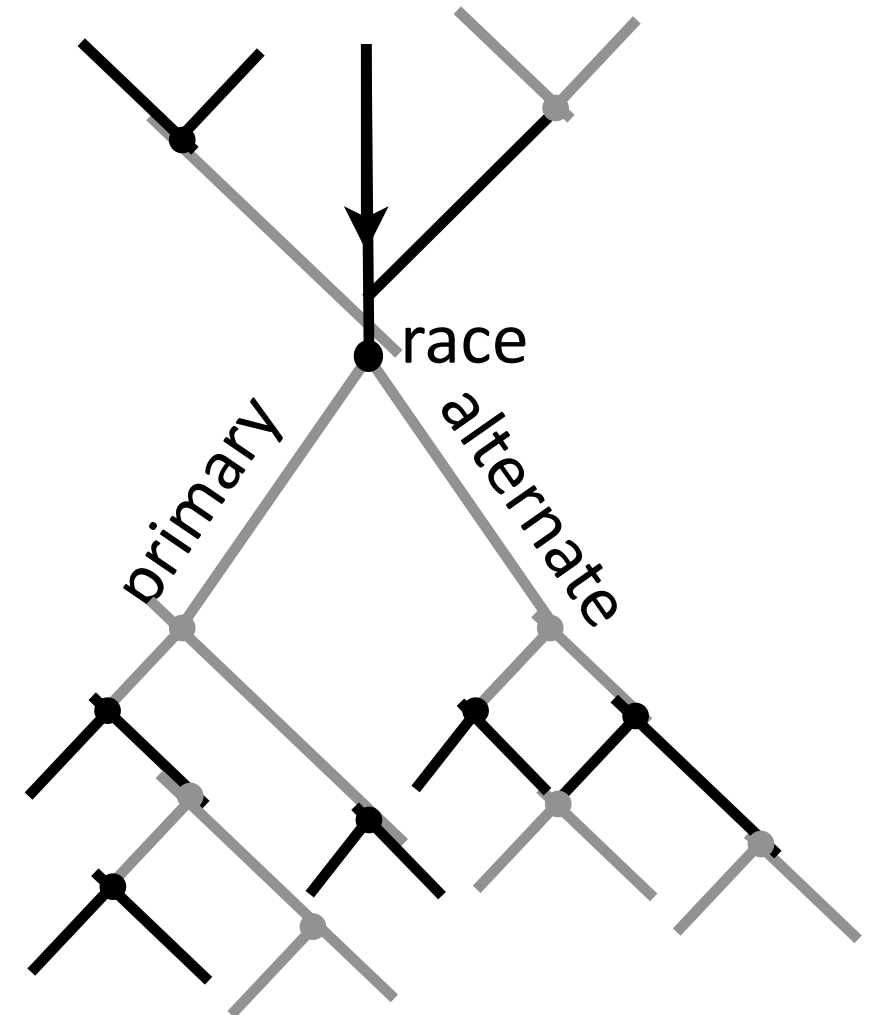
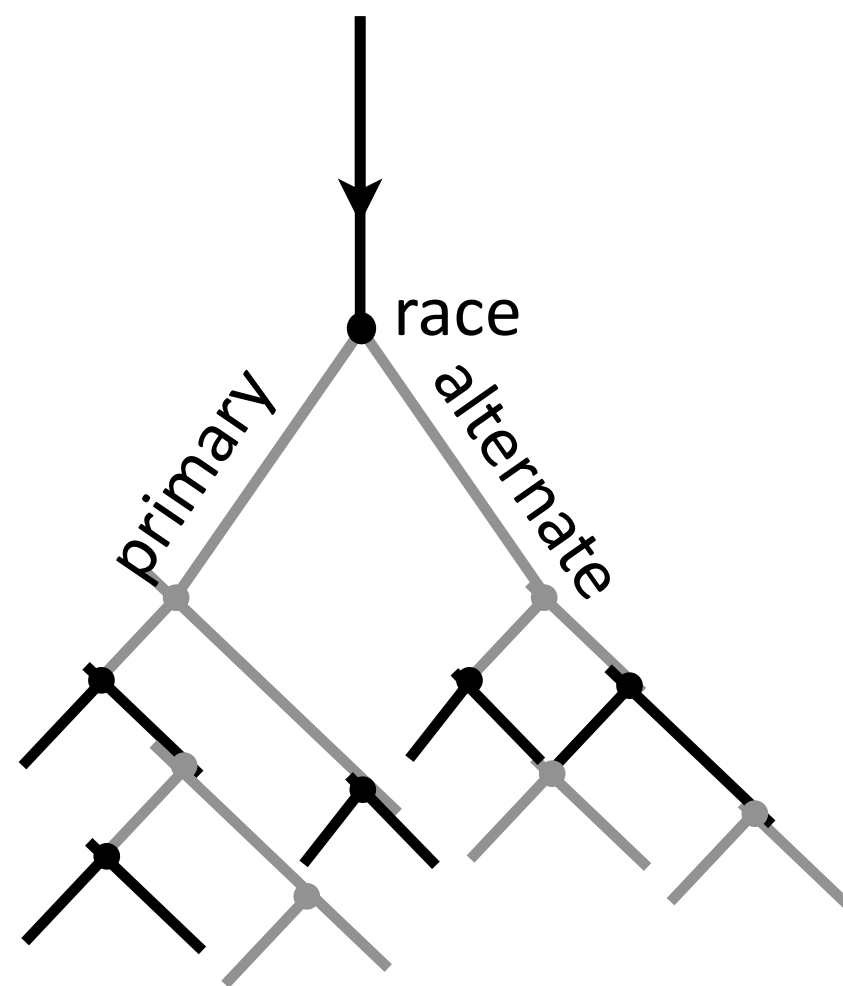
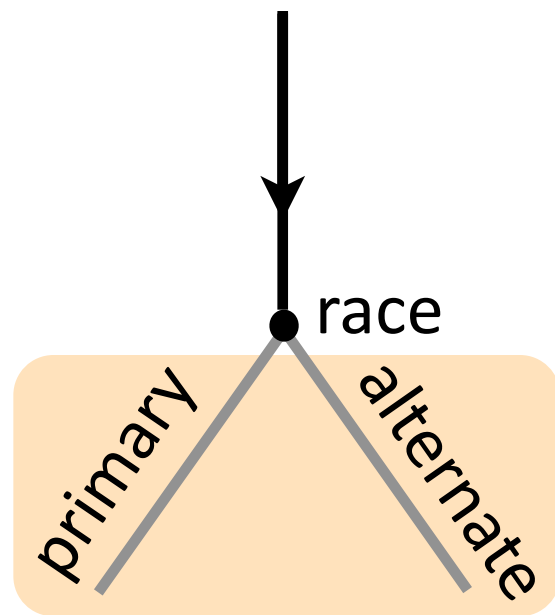


— schedules
 — paths



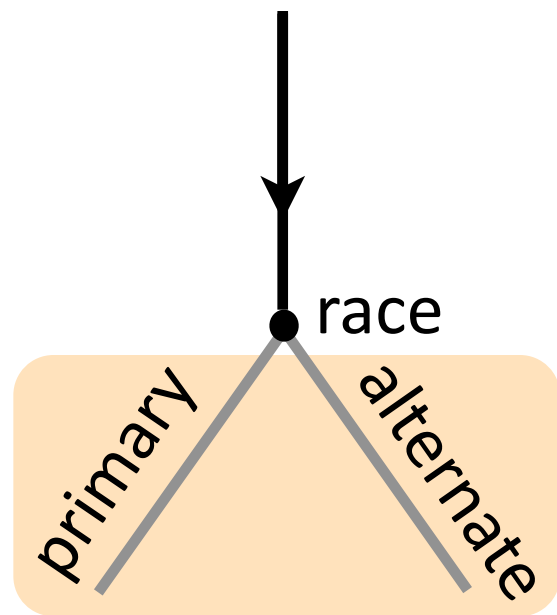
— schedules
— paths

Accuracy

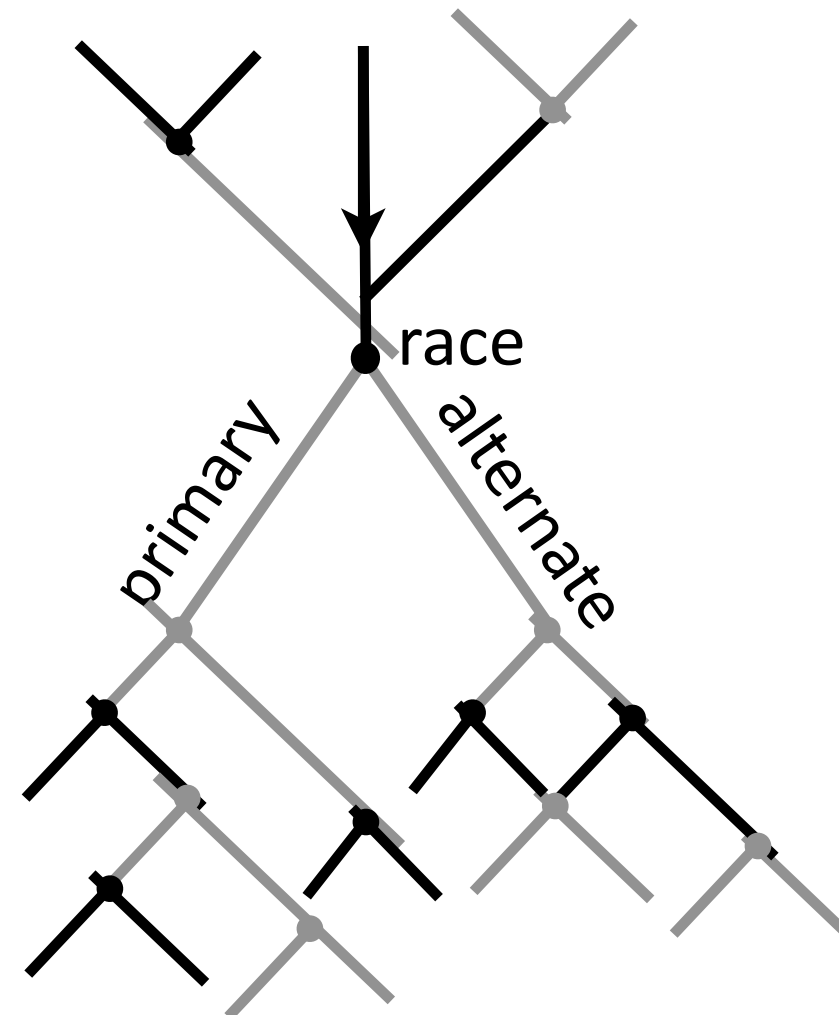
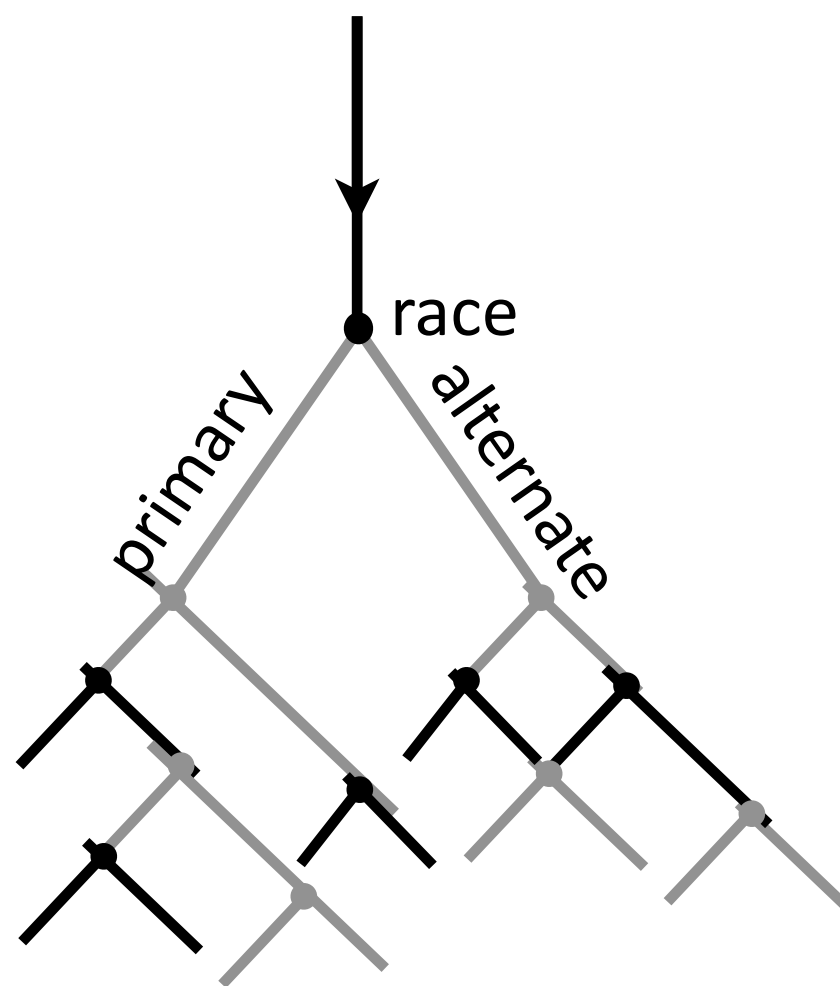


— schedules
— paths

Accuracy

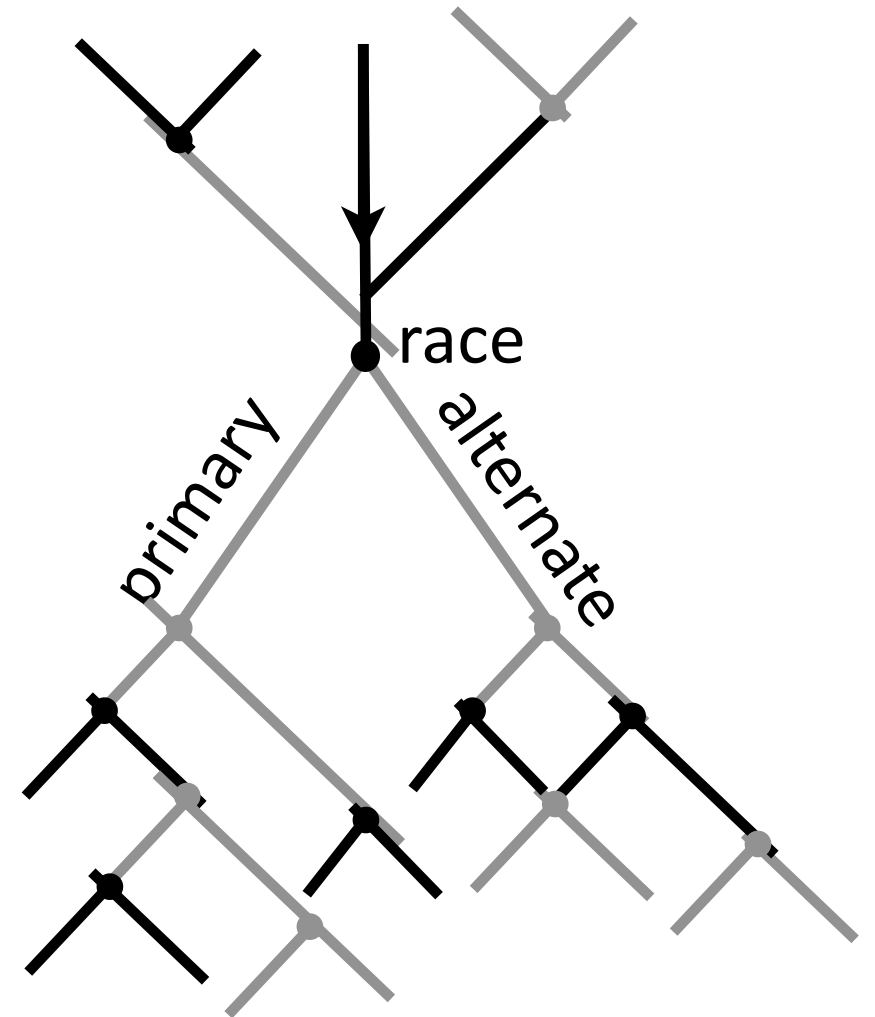
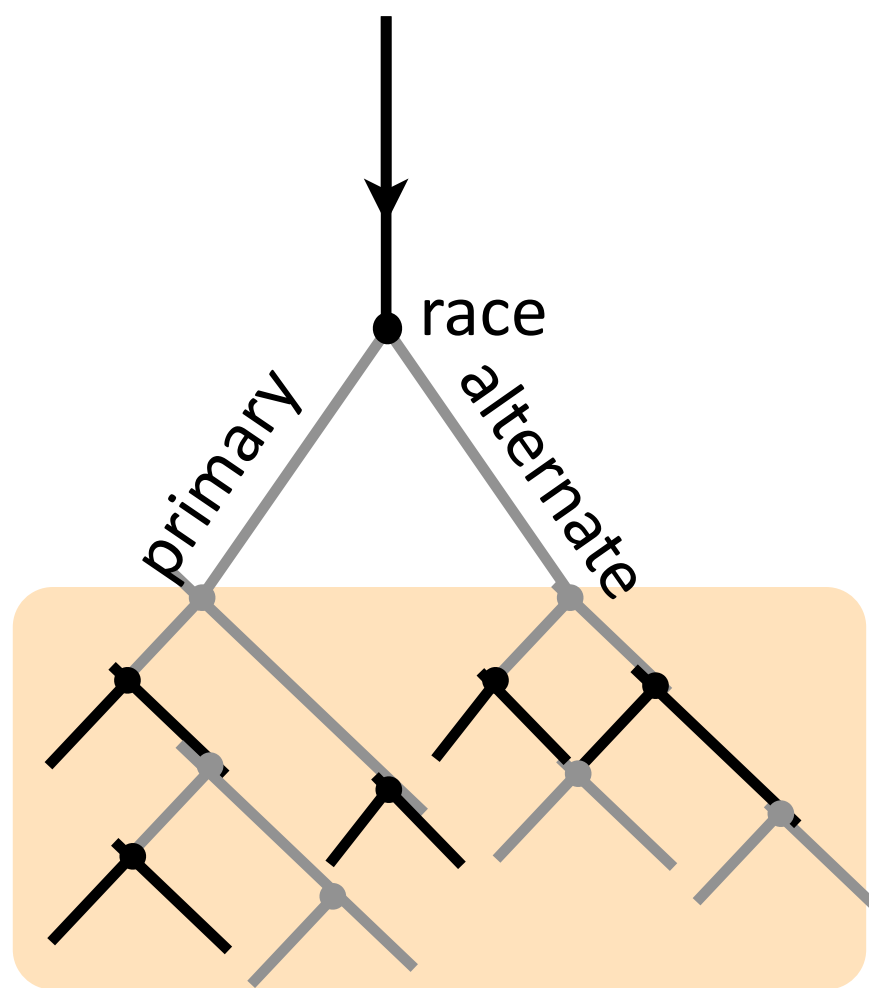
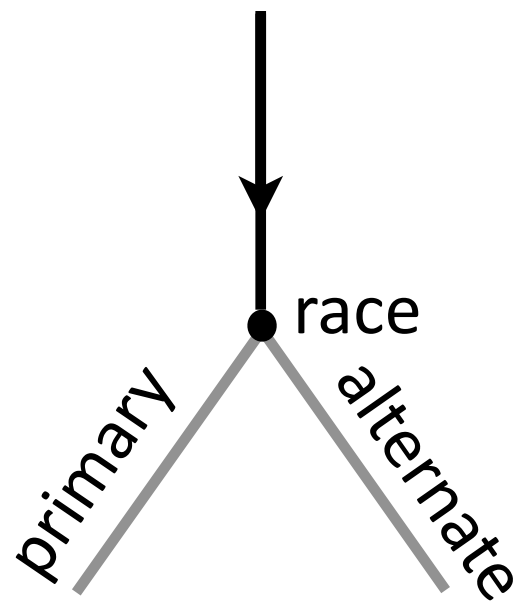


Check whether only a single order is possible



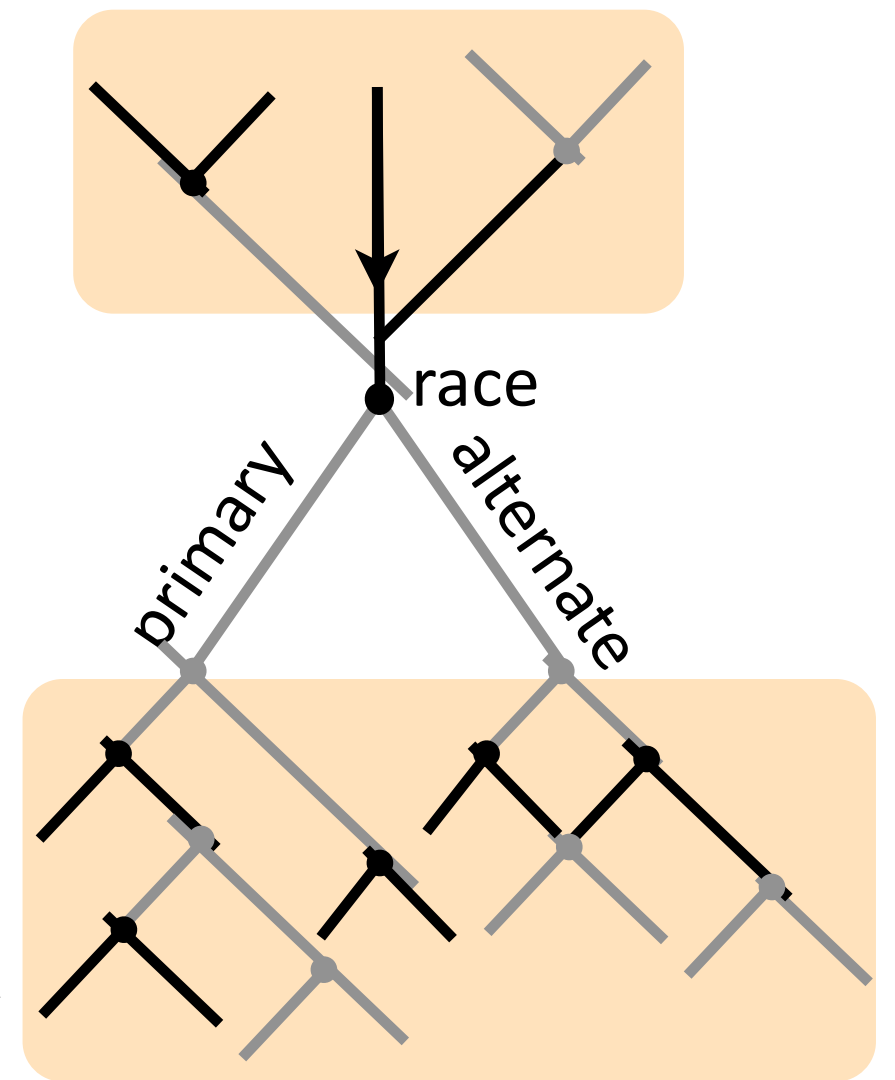
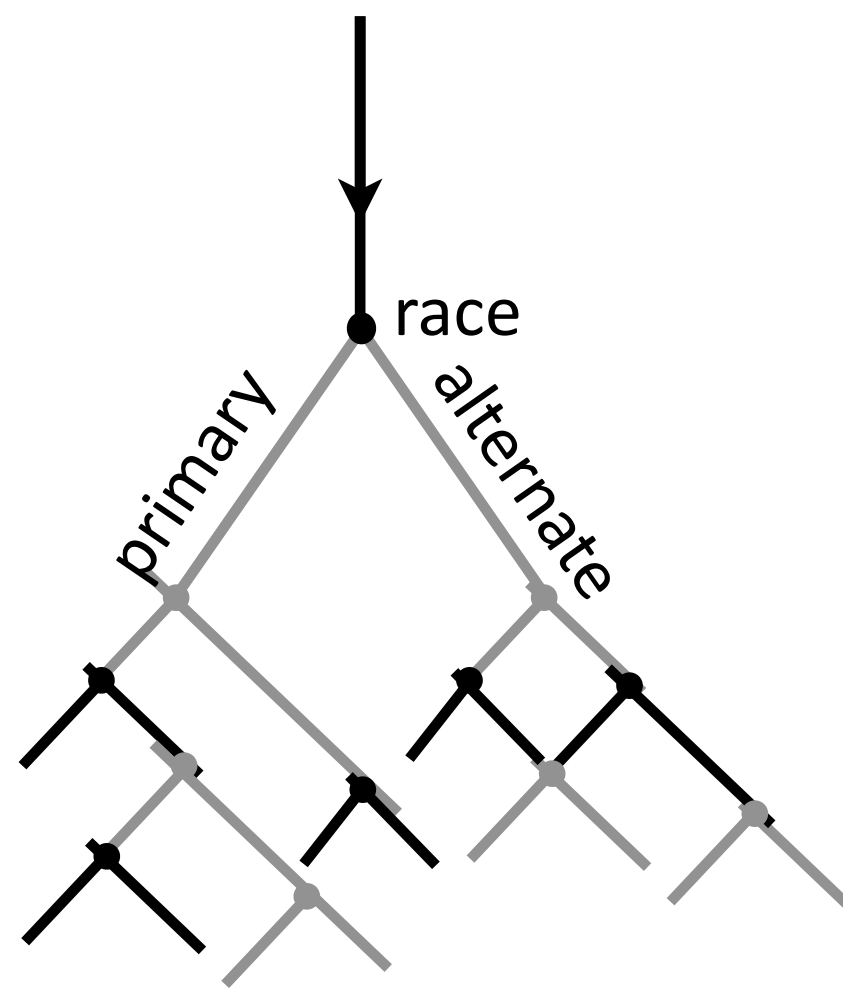
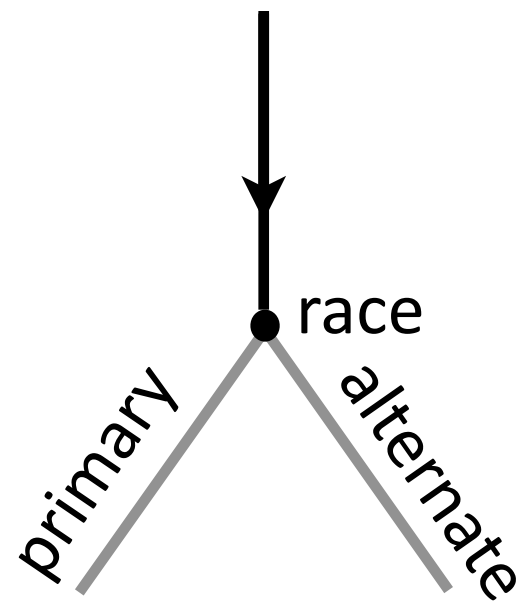
— schedules
— paths

Accuracy



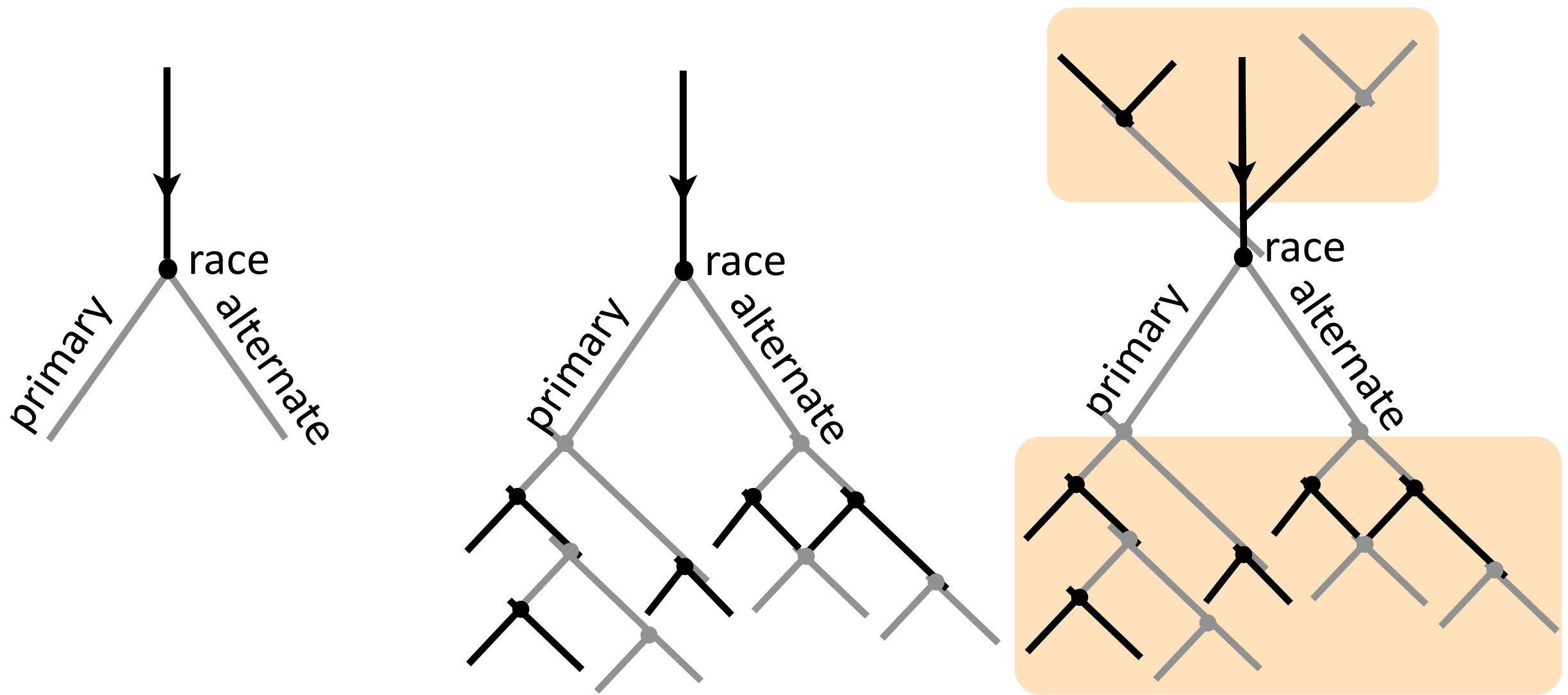
— schedules
— paths

Accuracy



— schedules
— paths

Accuracy



— schedules
— paths

Accuracy

Multi-path multi-schedule analysis
increases classification accuracy

Contributions

- Finer grained taxonomy
- High precision data race classifier
 - *Multi-path multi-schedule data race analysis*
 - *Symbolic output comparison*

Contributions

- Finer grained taxonomy
- High precision data race classifier
 - *Multi-path multi-schedule data race analysis*
 - *Symbolic output comparison* ***Portend***

Portend

Portend

Cloud9 on top of KLEE
Multithreaded symbolic execution engine

Portend

Record/replay & classification engine

Cloud9 on top of KLEE

Multithreaded symbolic execution engine

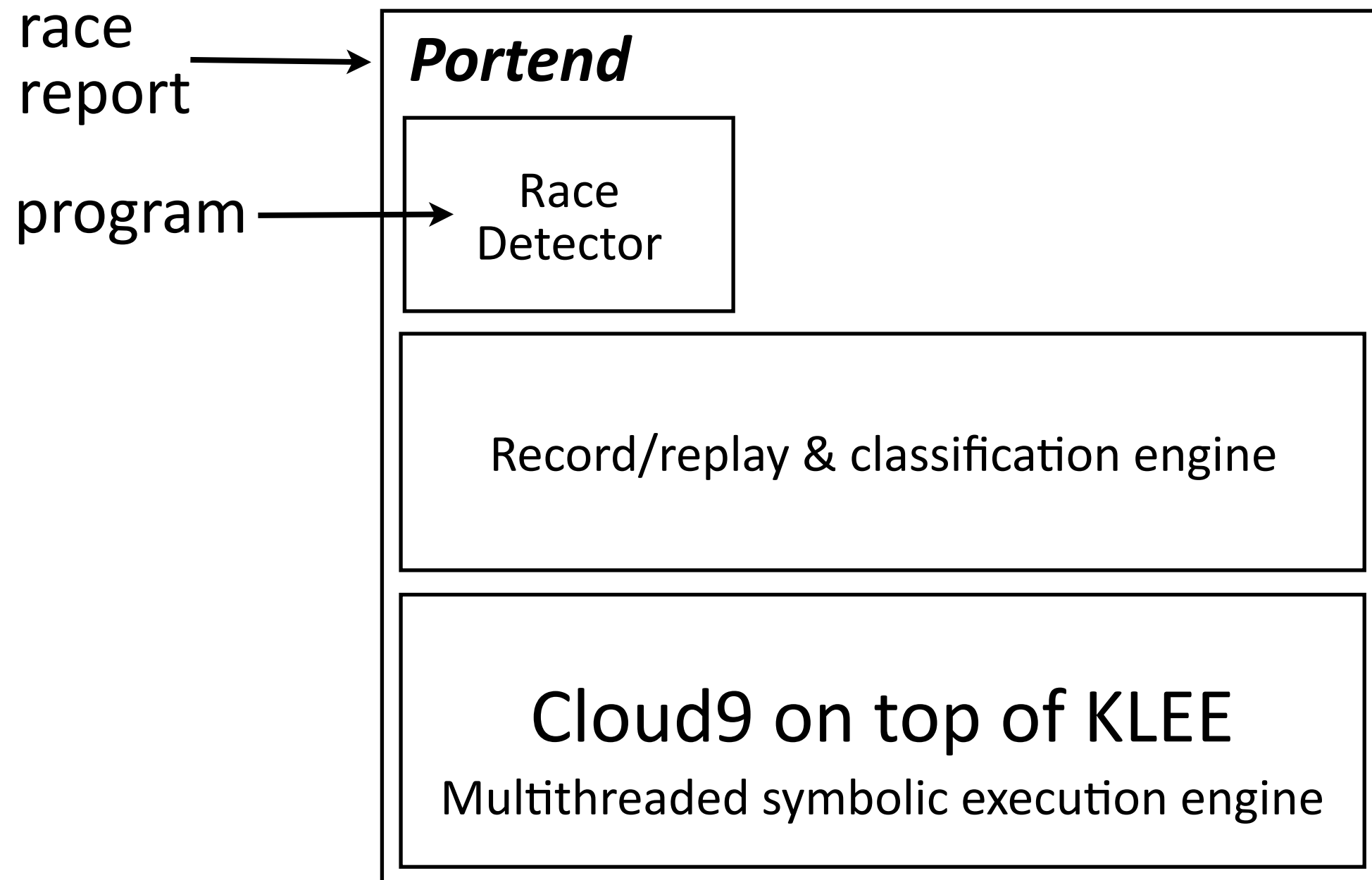
race
report

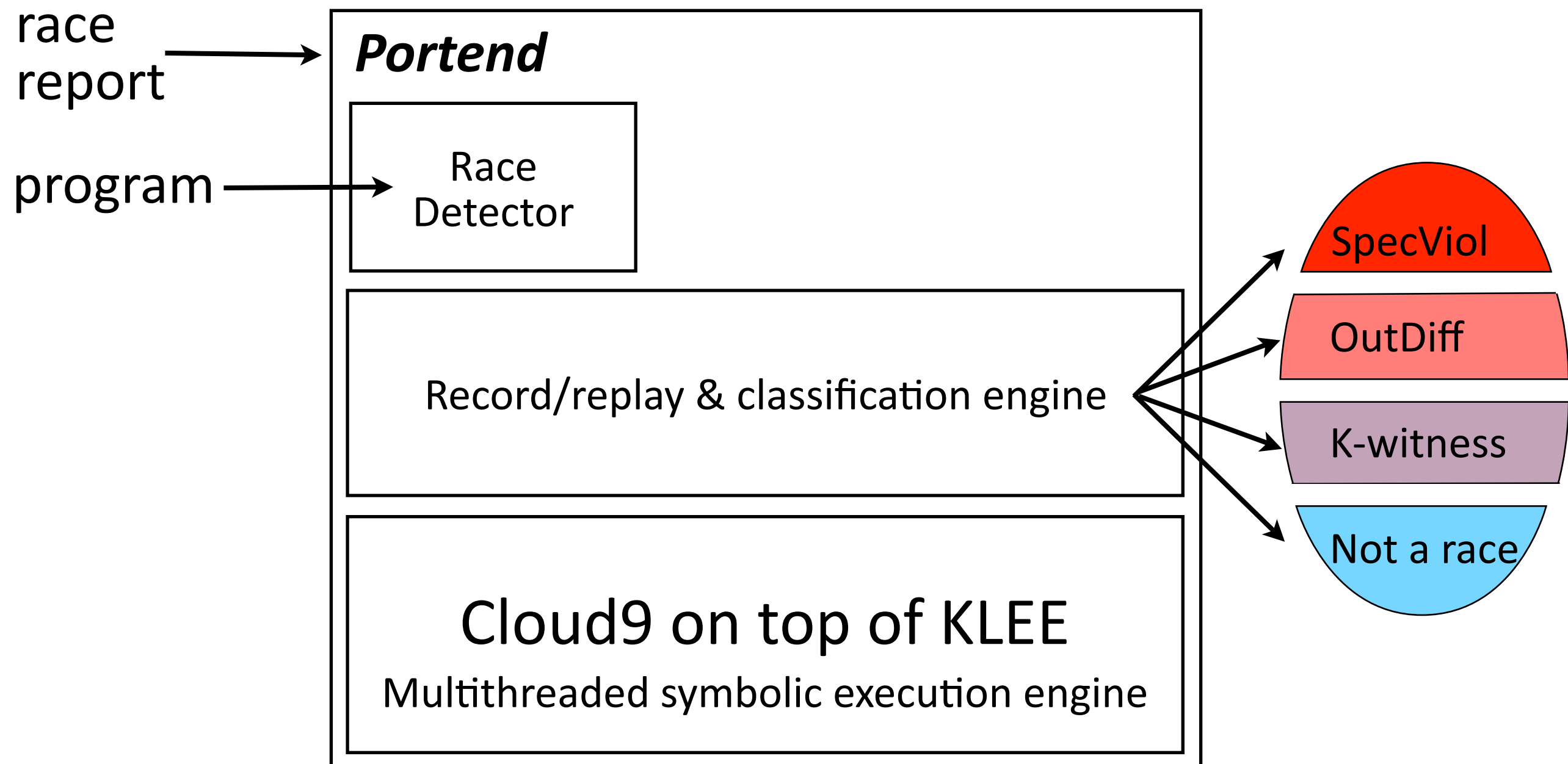


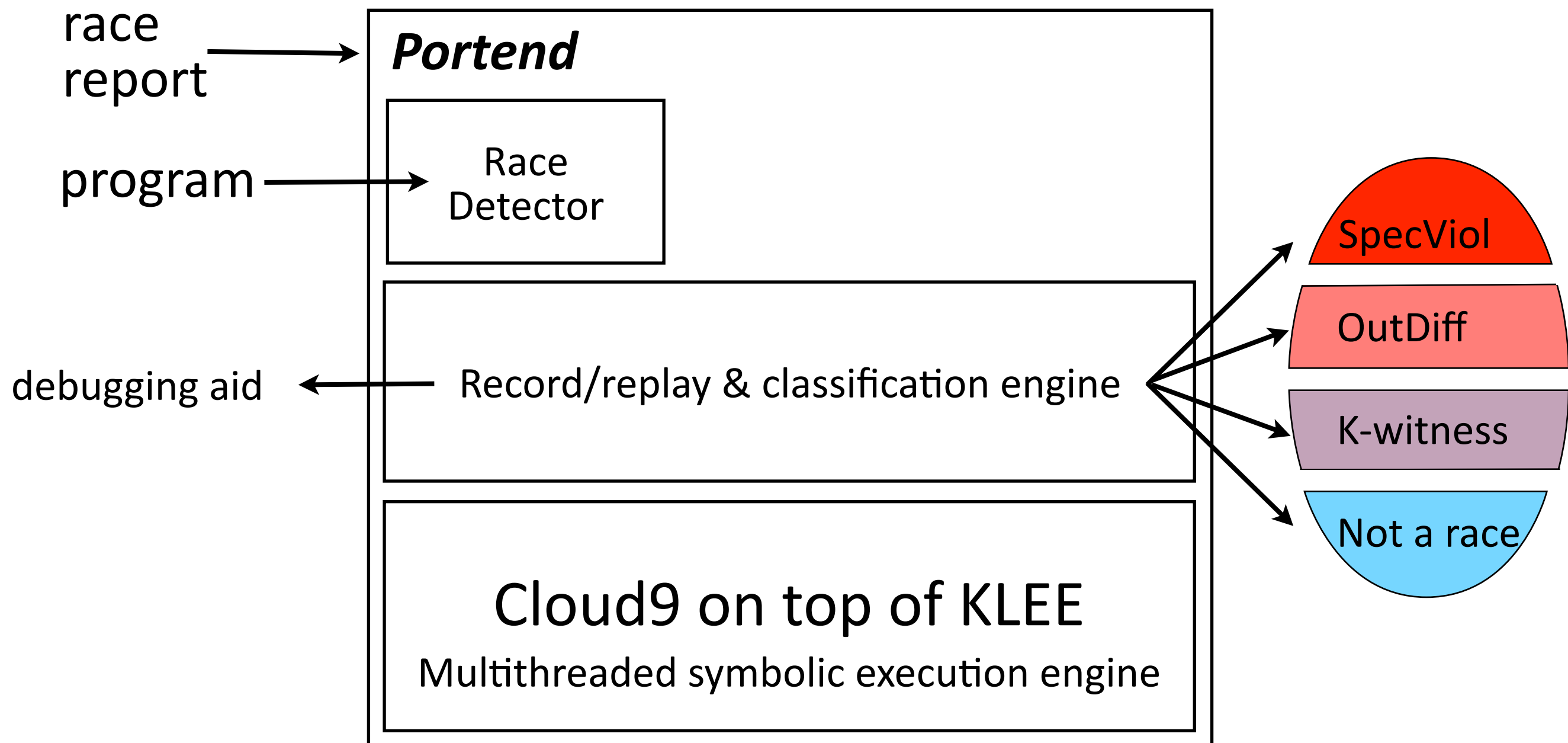
Portend

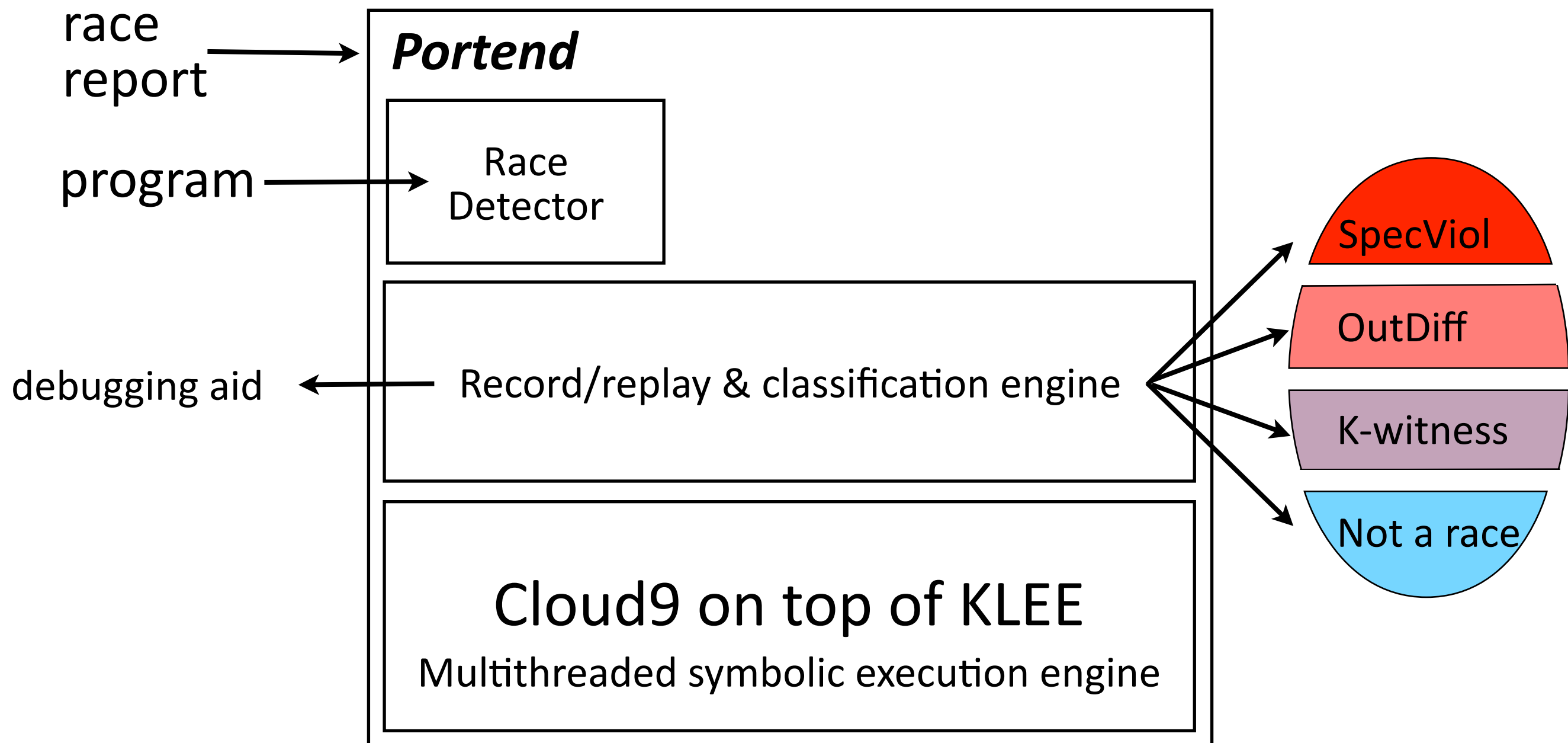
Record/replay & classification engine

Cloud9 on top of KLEE
Multithreaded symbolic execution engine

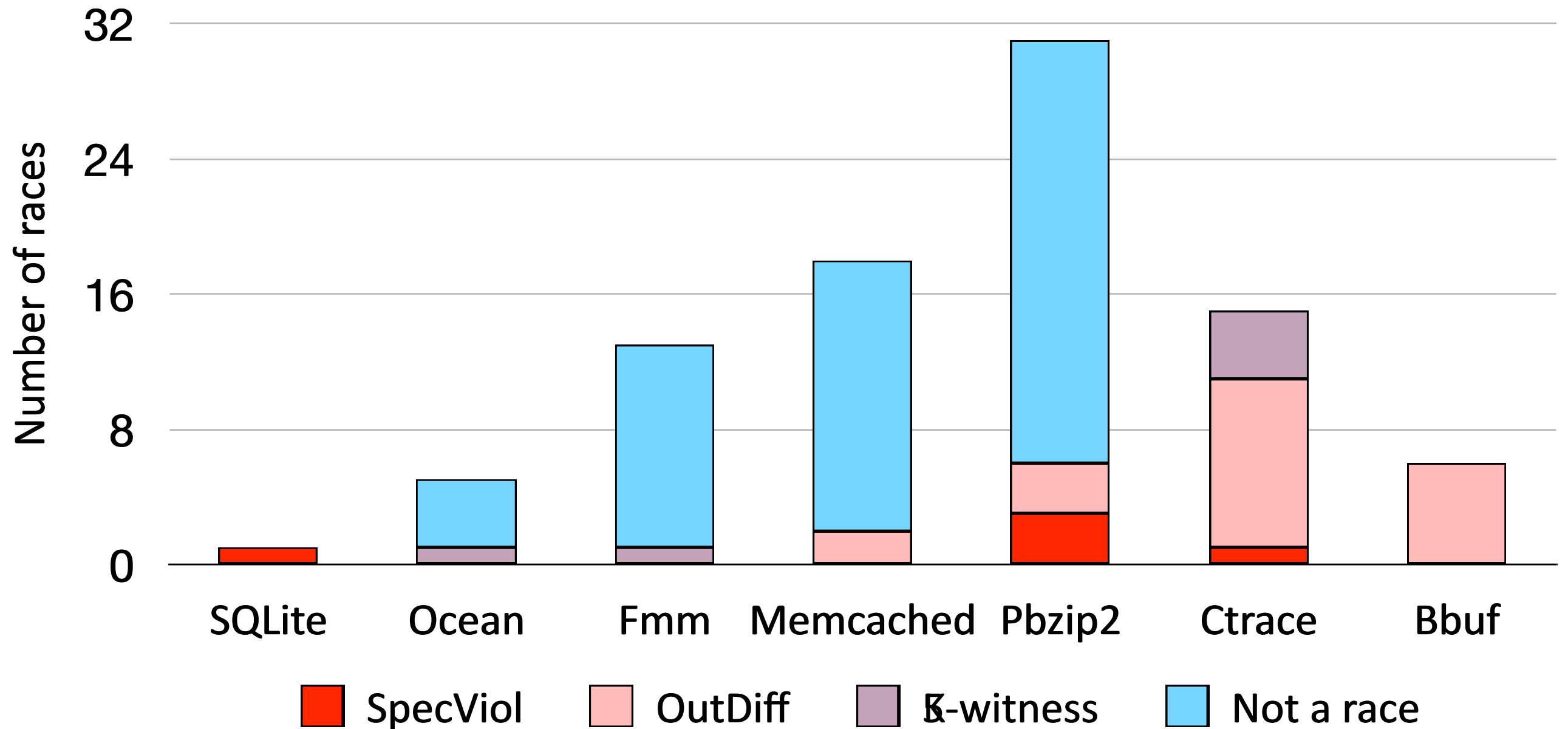




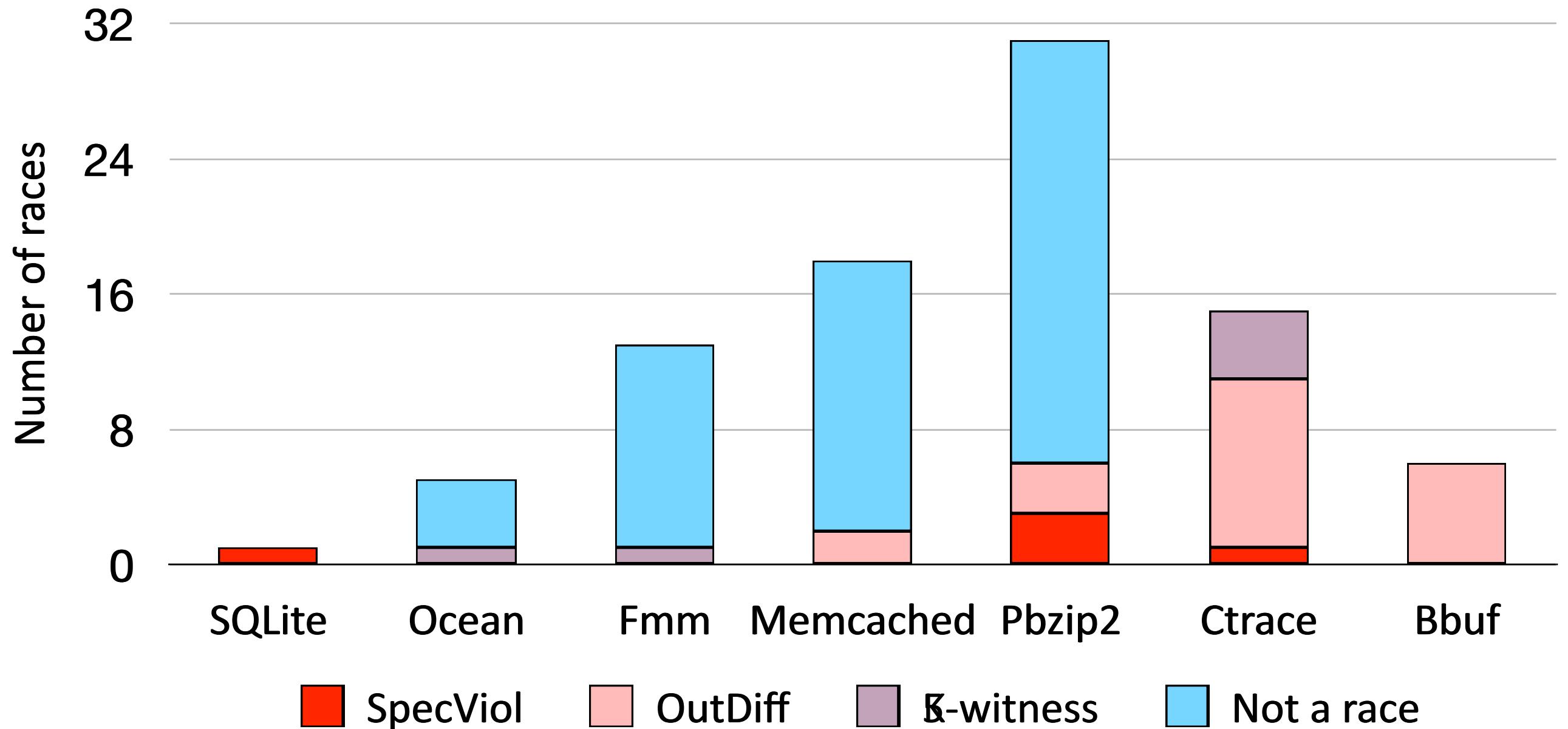




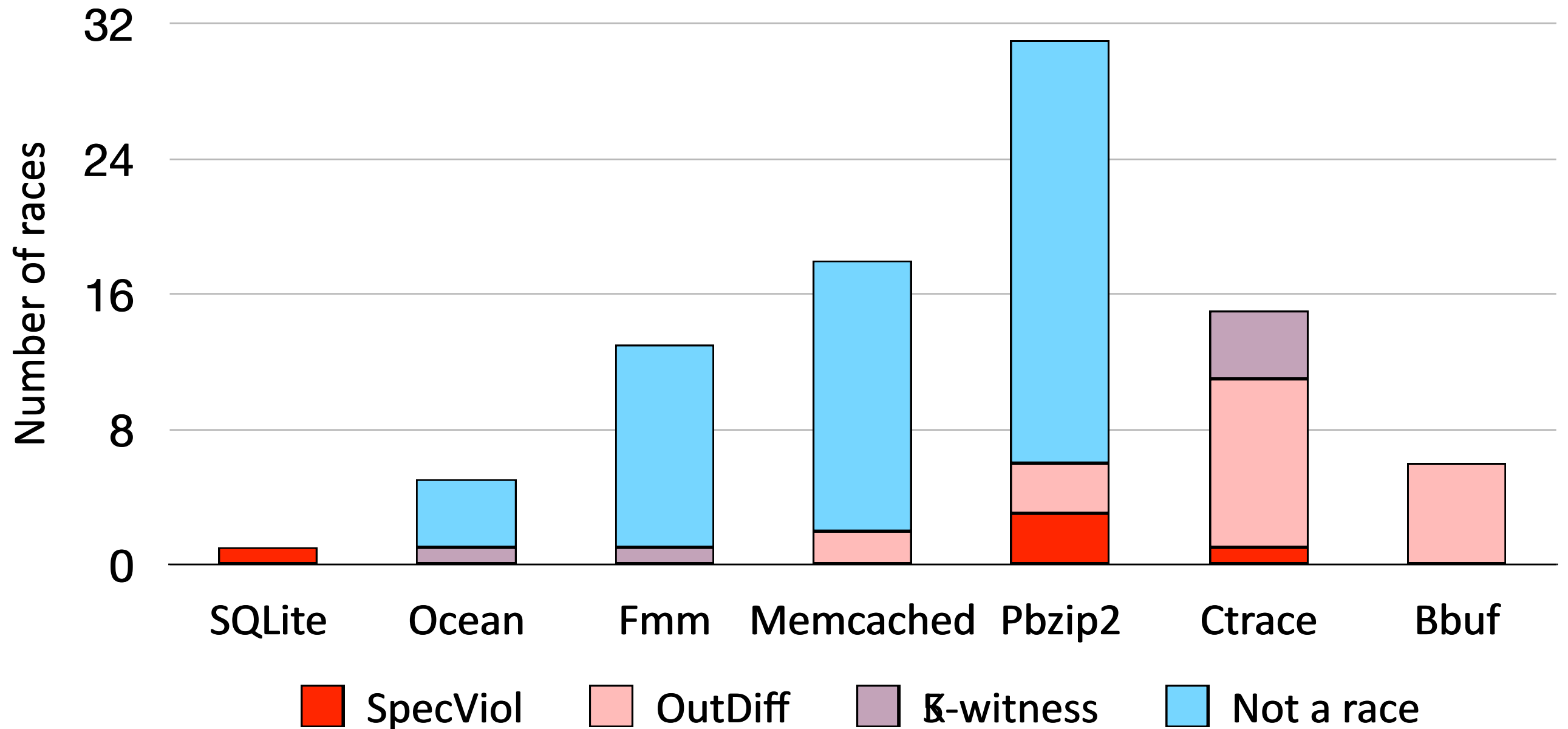
Classification Results



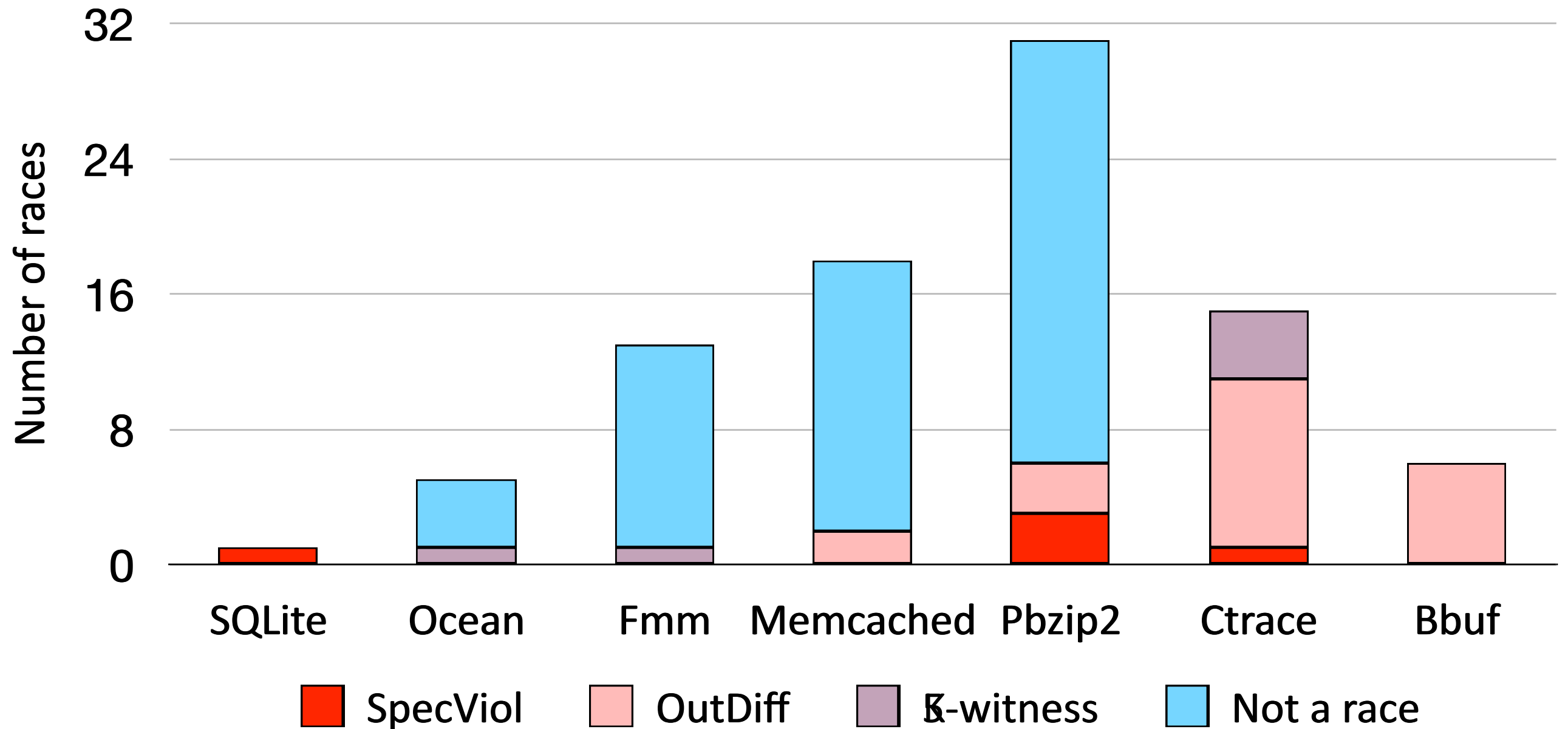
Classification Results



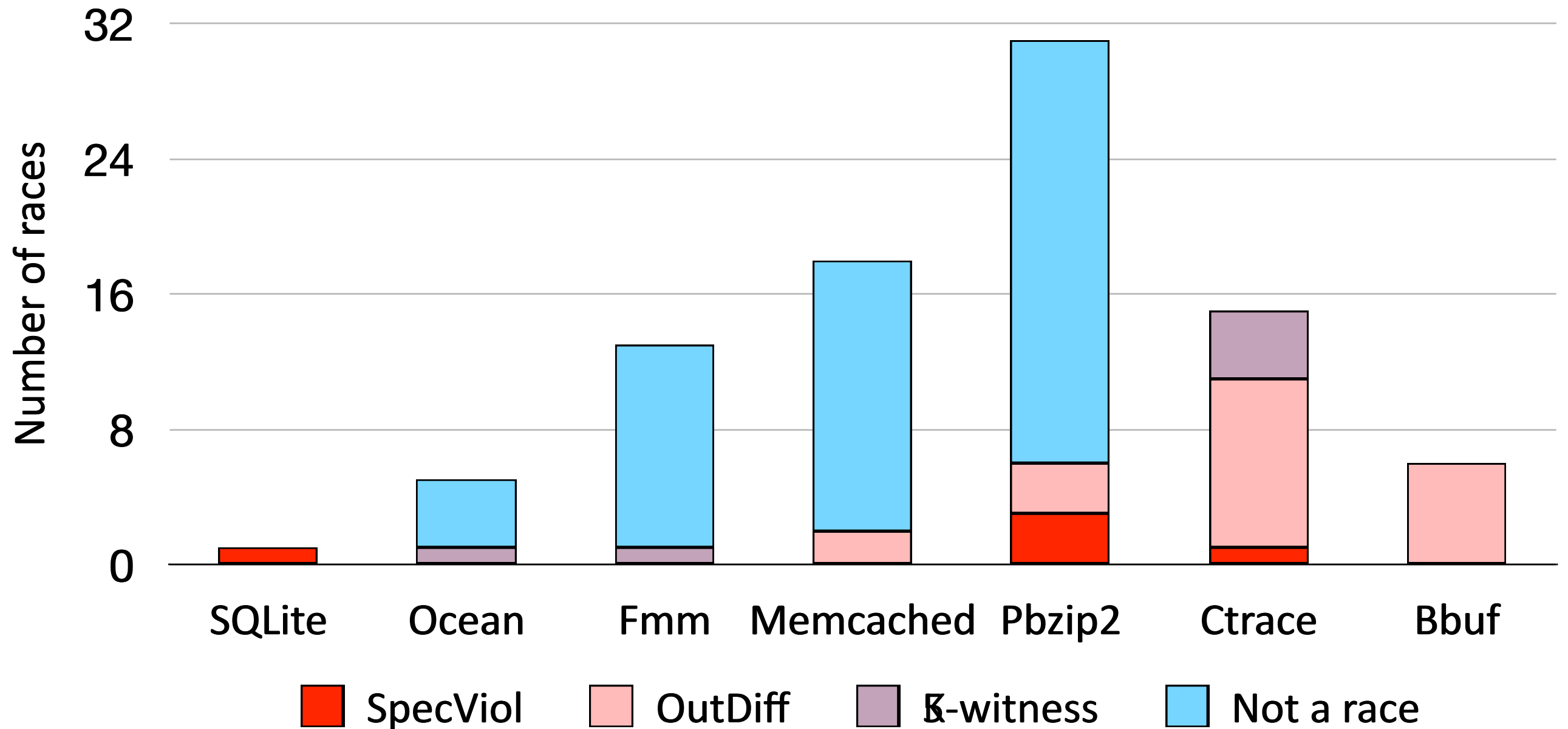
Classification Results



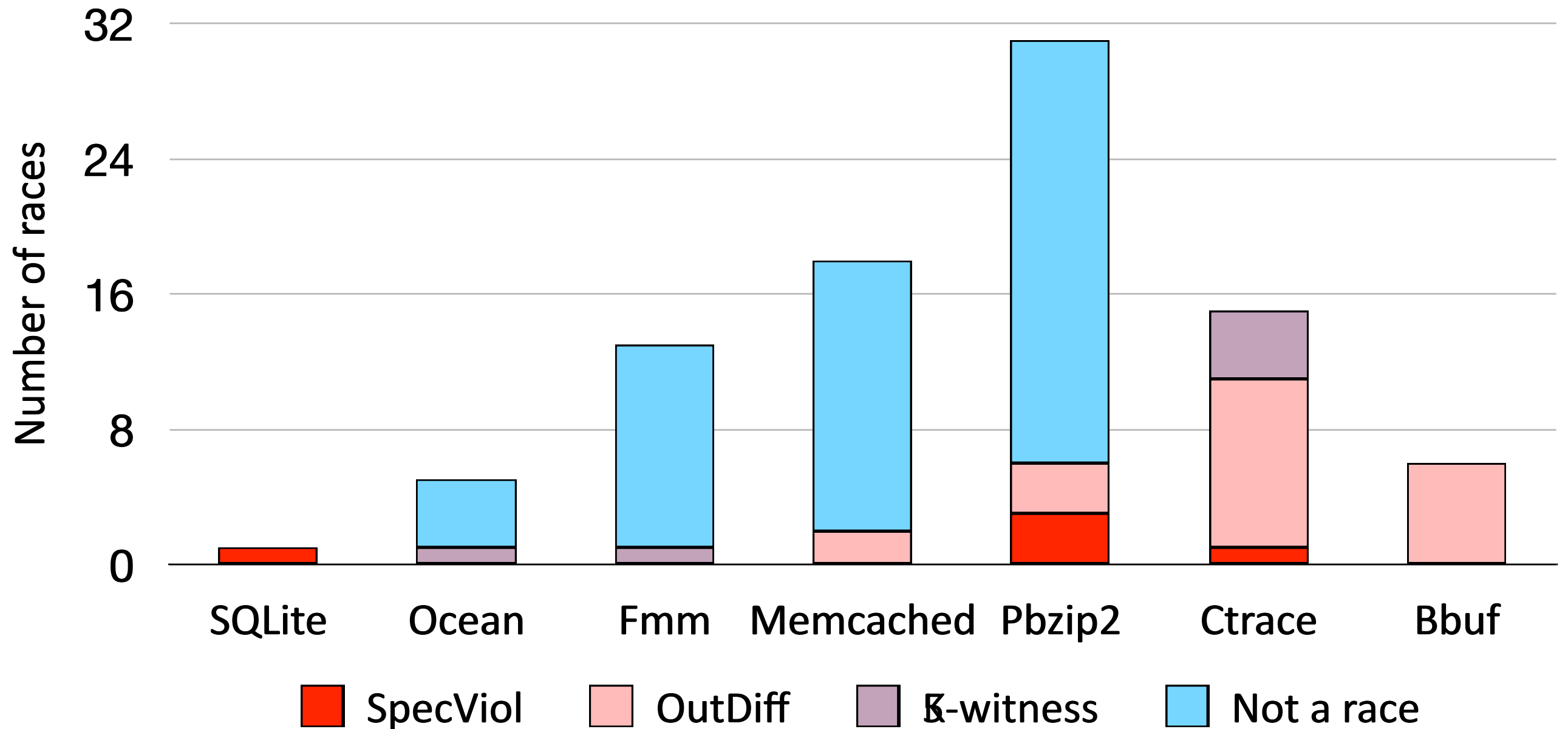
Classification Results



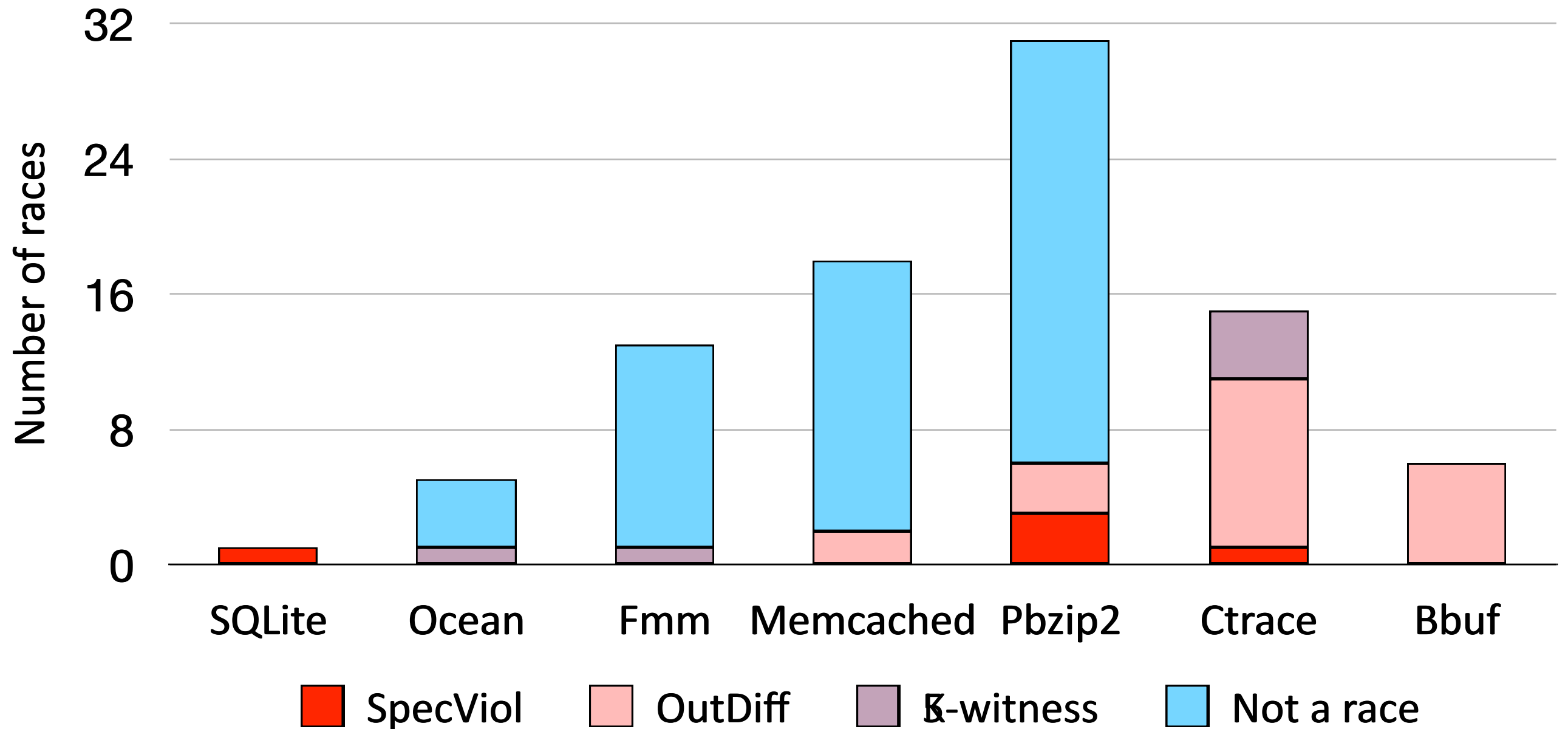
Classification Results



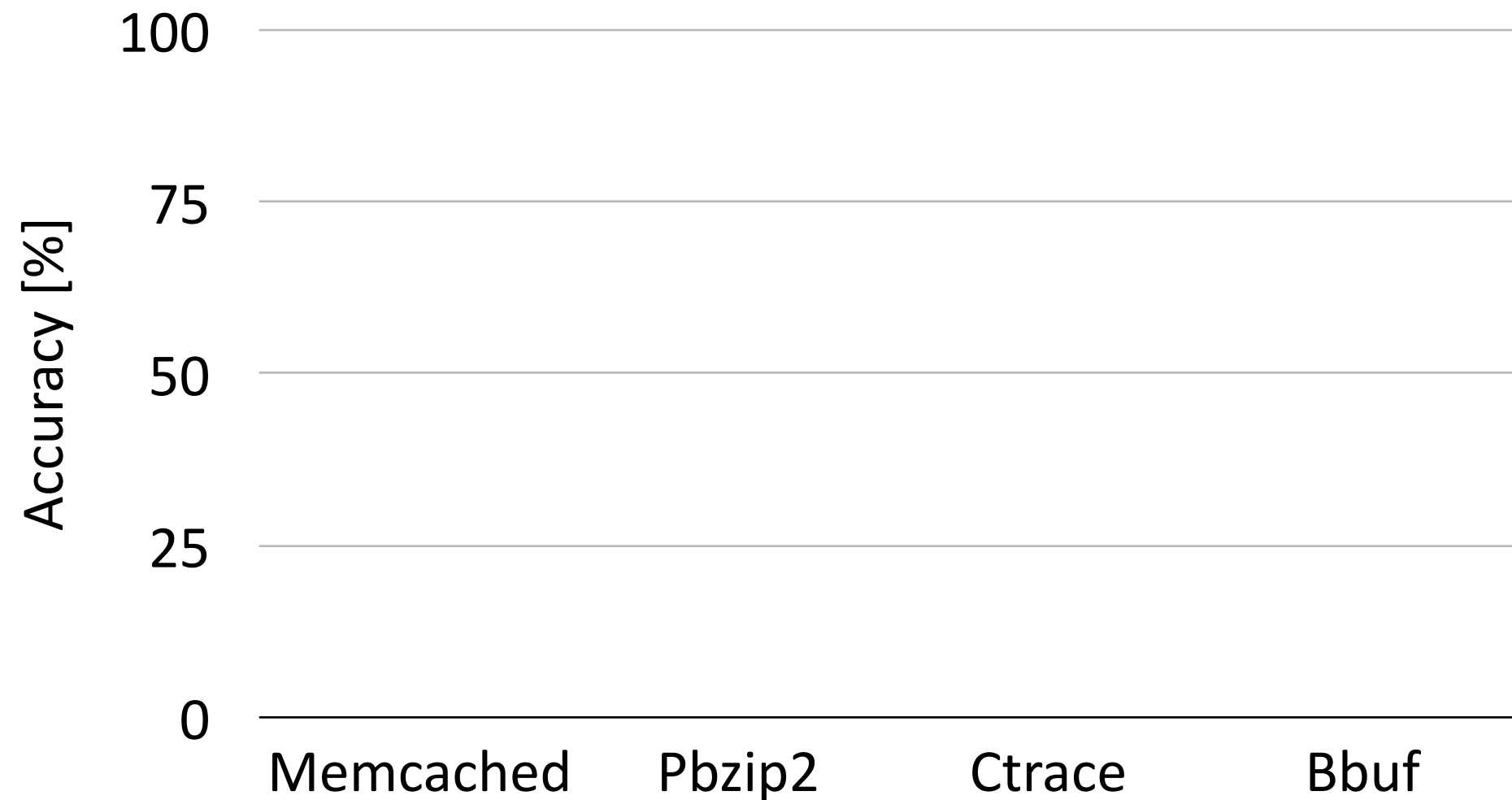
Classification Results



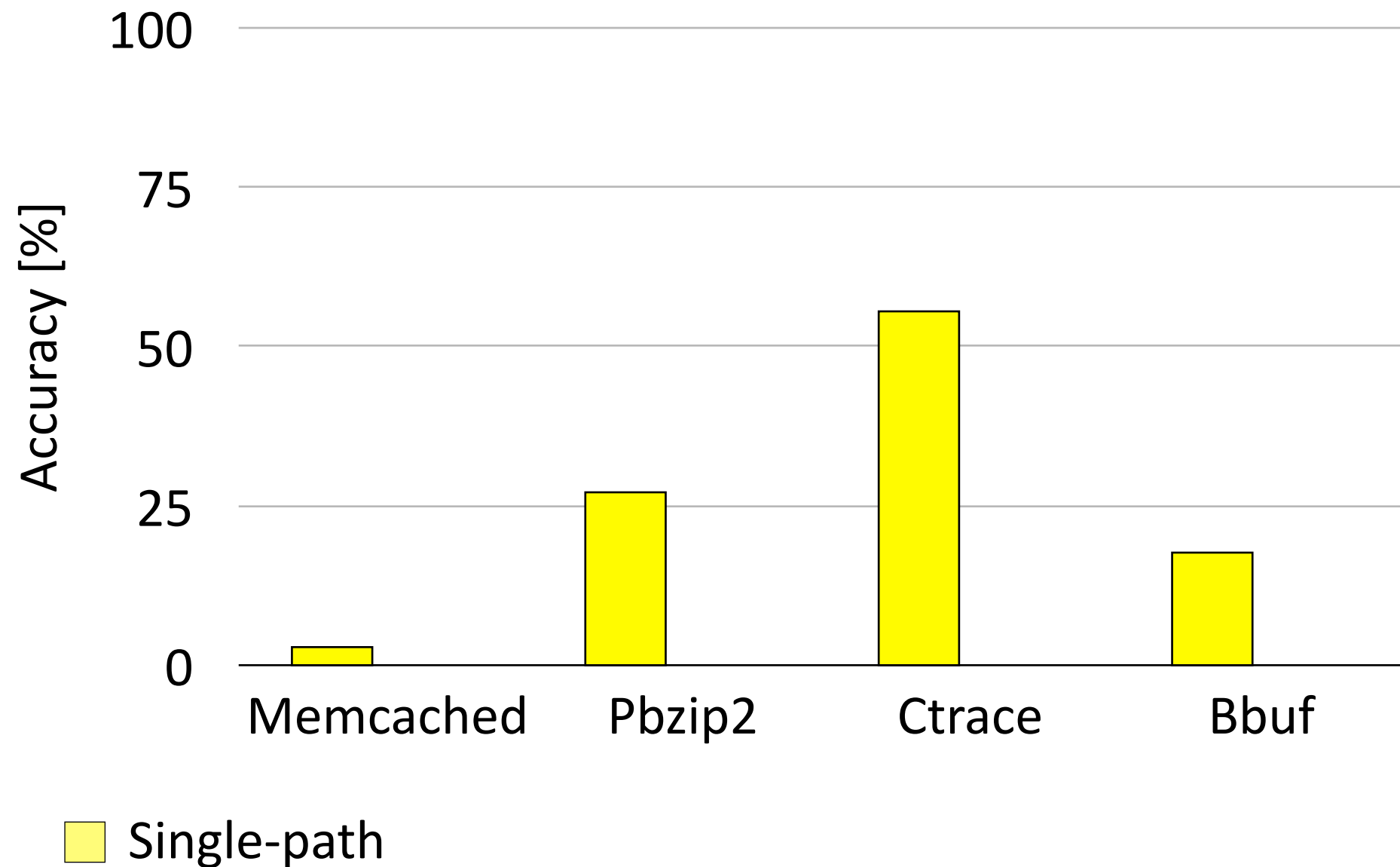
Classification Results



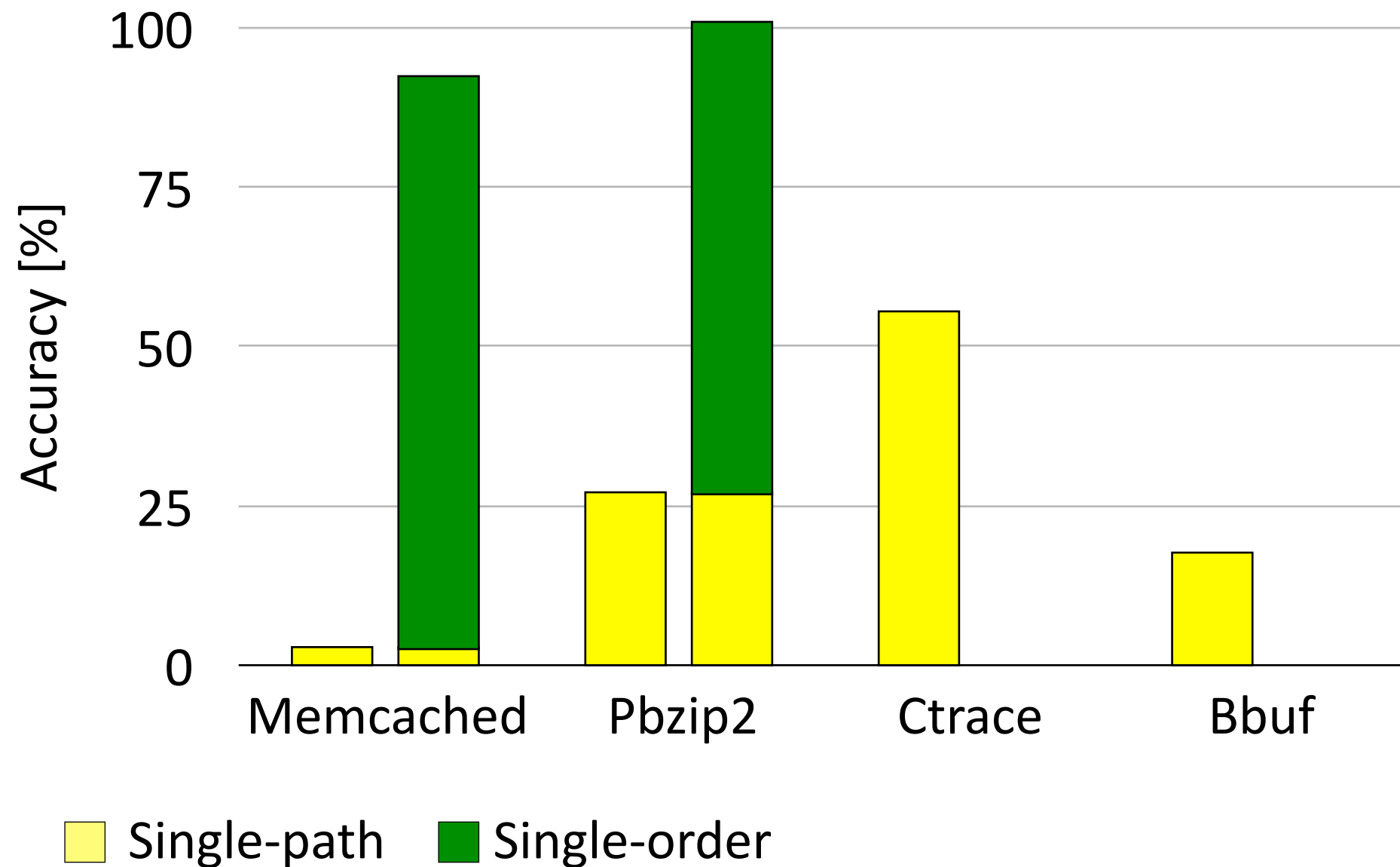
Contribution of Techniques



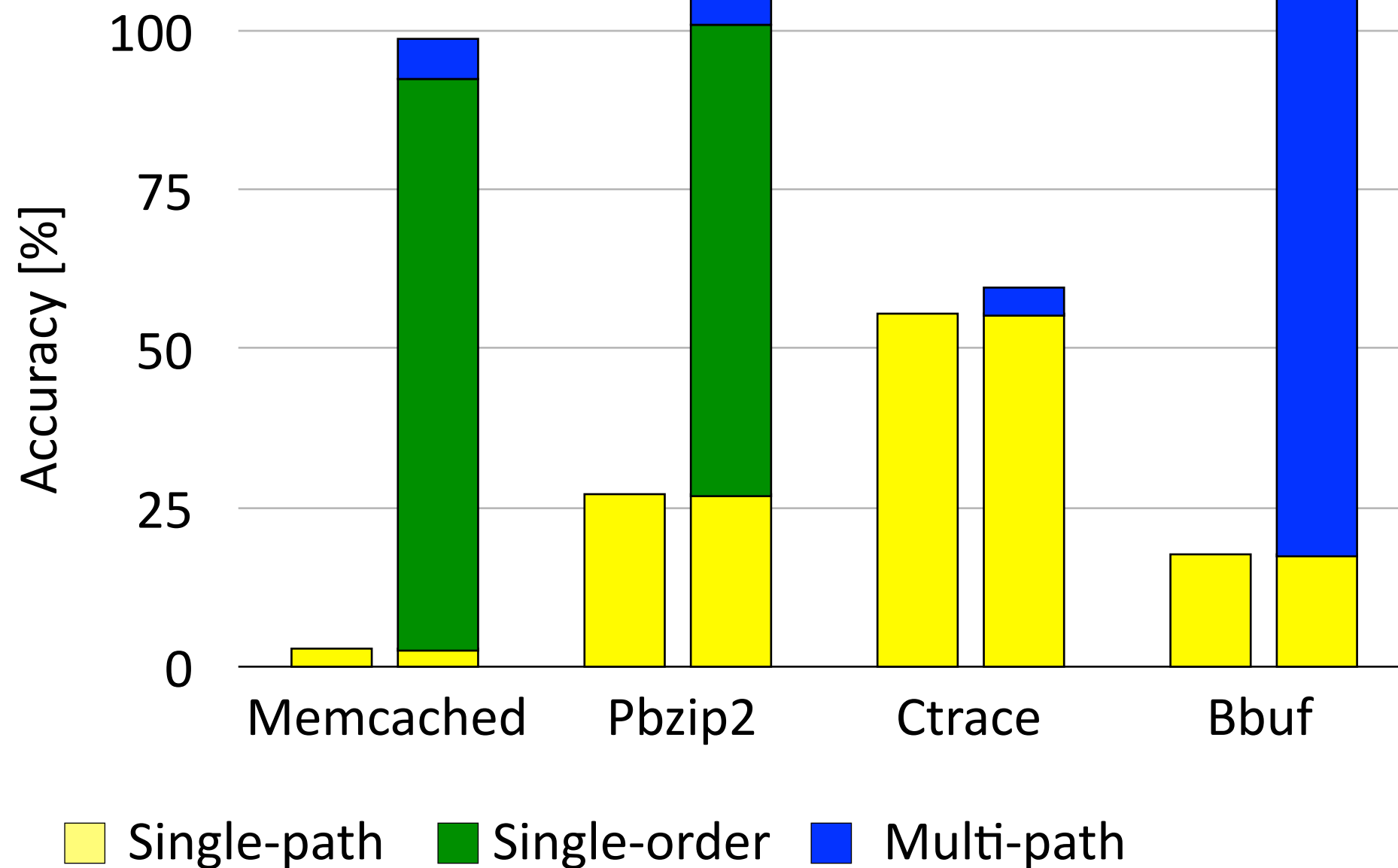
Contribution of Techniques



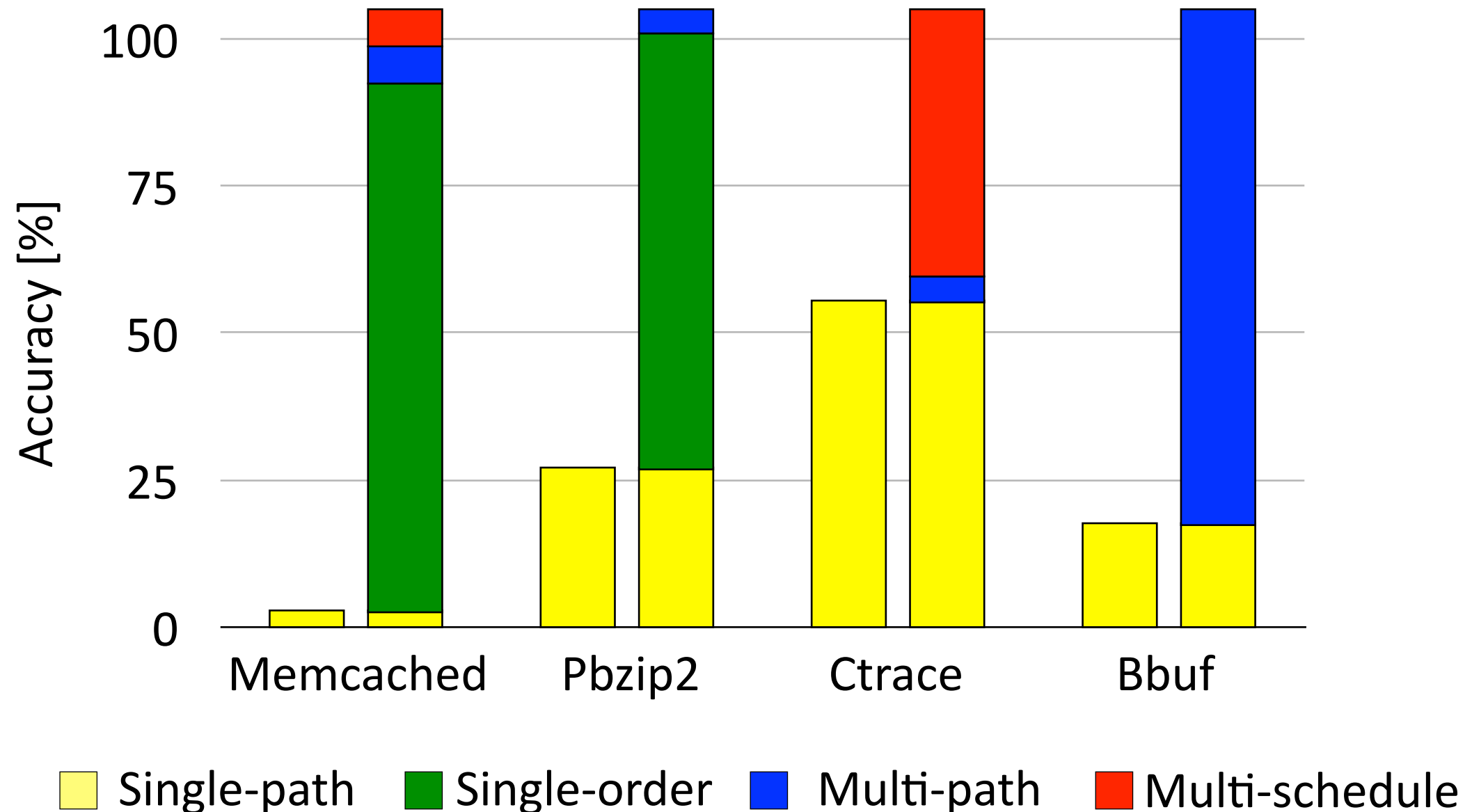
Contribution of Techniques



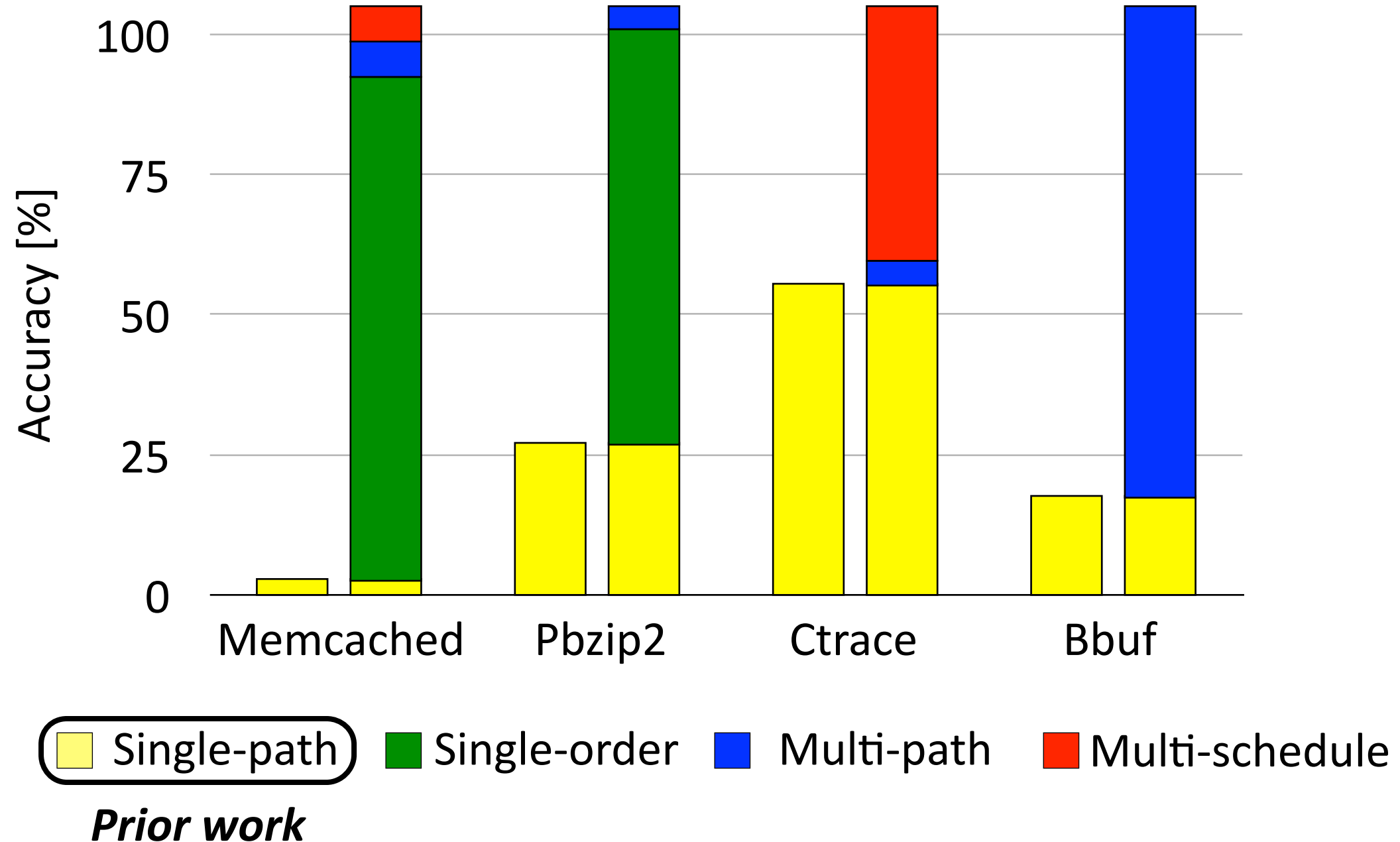
Contribution of Techniques



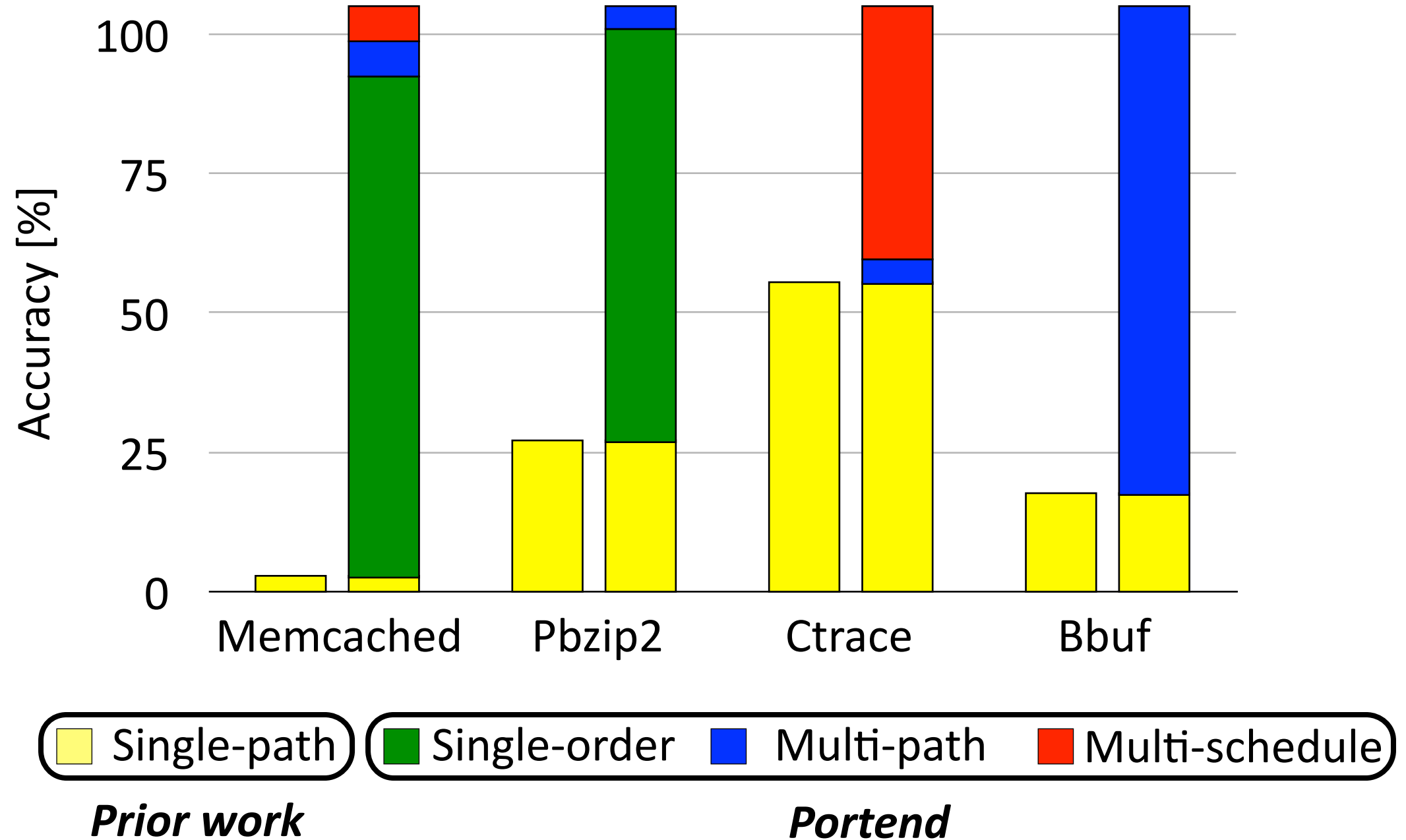
Contribution of Techniques



Contribution of Techniques



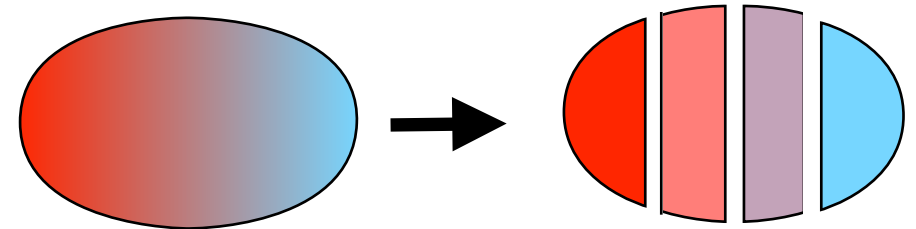
Contribution of Techniques



Conclusion

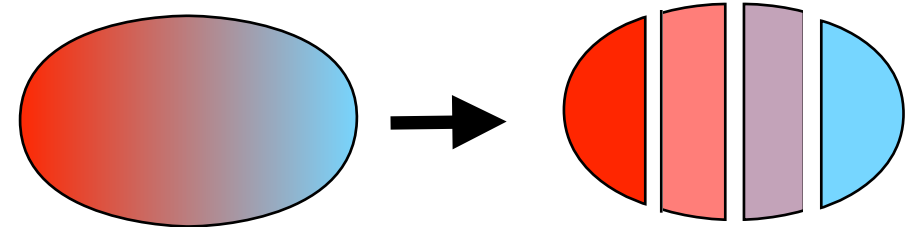
Conclusion

- Finer grained taxonomy

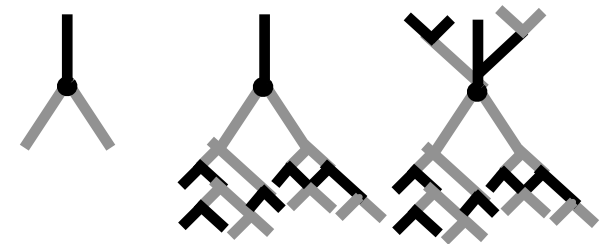


Conclusion

- Finer grained taxonomy



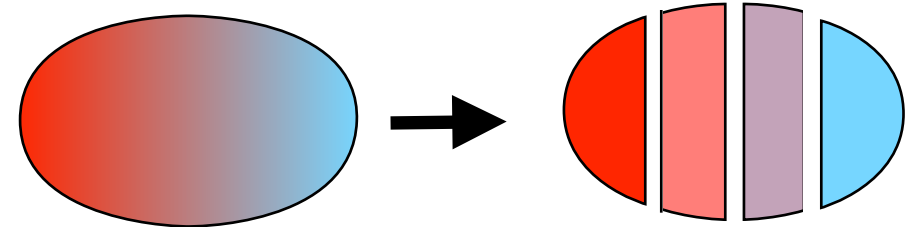
- High precision data race classifier



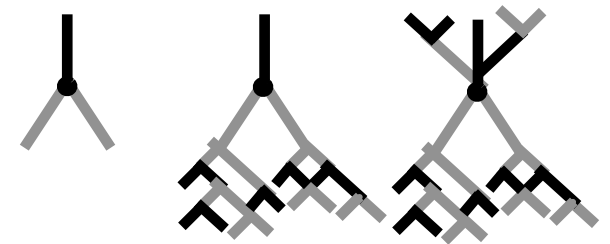
- *Multi-path multi-schedule data race analysis*
- *Symbolic output comparison*

Conclusion

- Finer grained taxonomy



- High precision data race classifier

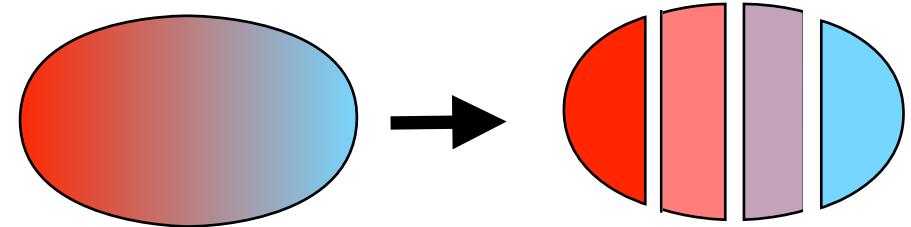


- *Multi-path multi-schedule data race analysis*
- *Symbolic output comparison*

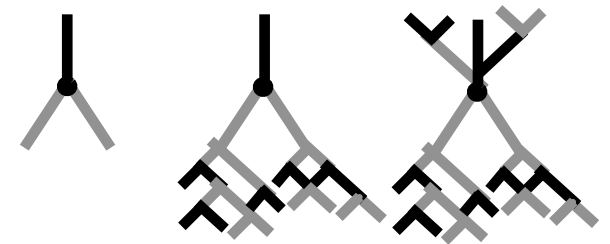
99% classification accuracy on
93 data races in < 5 minutes/race

Conclusion

- Finer grained taxonomy



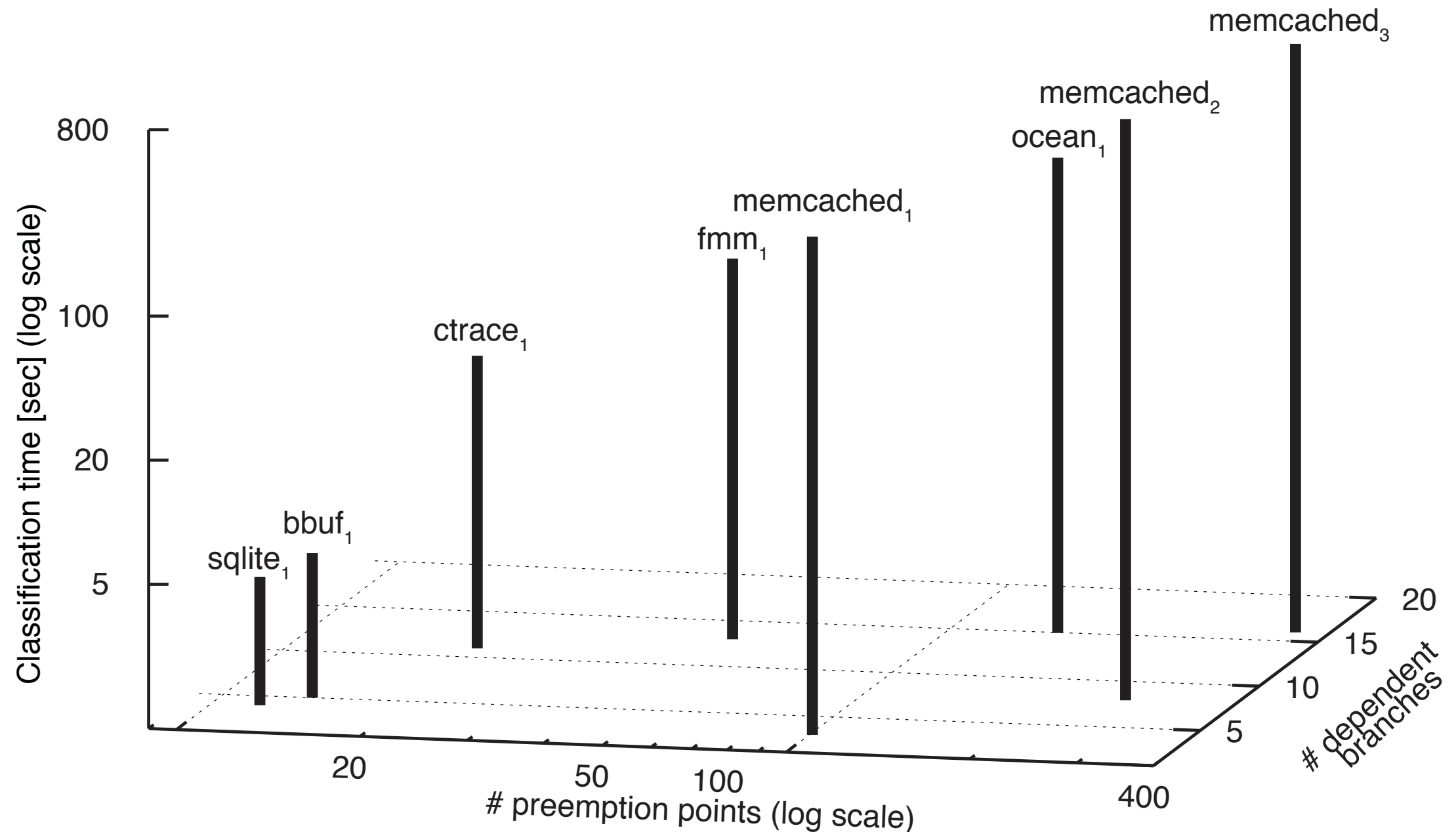
- High precision data race classifier



- *Multi-path multi-schedule data race analysis*
- *Symbolic output comparison*

99% classification accuracy on
93 data races in < 5 minutes/race

What Influences Classification Time?

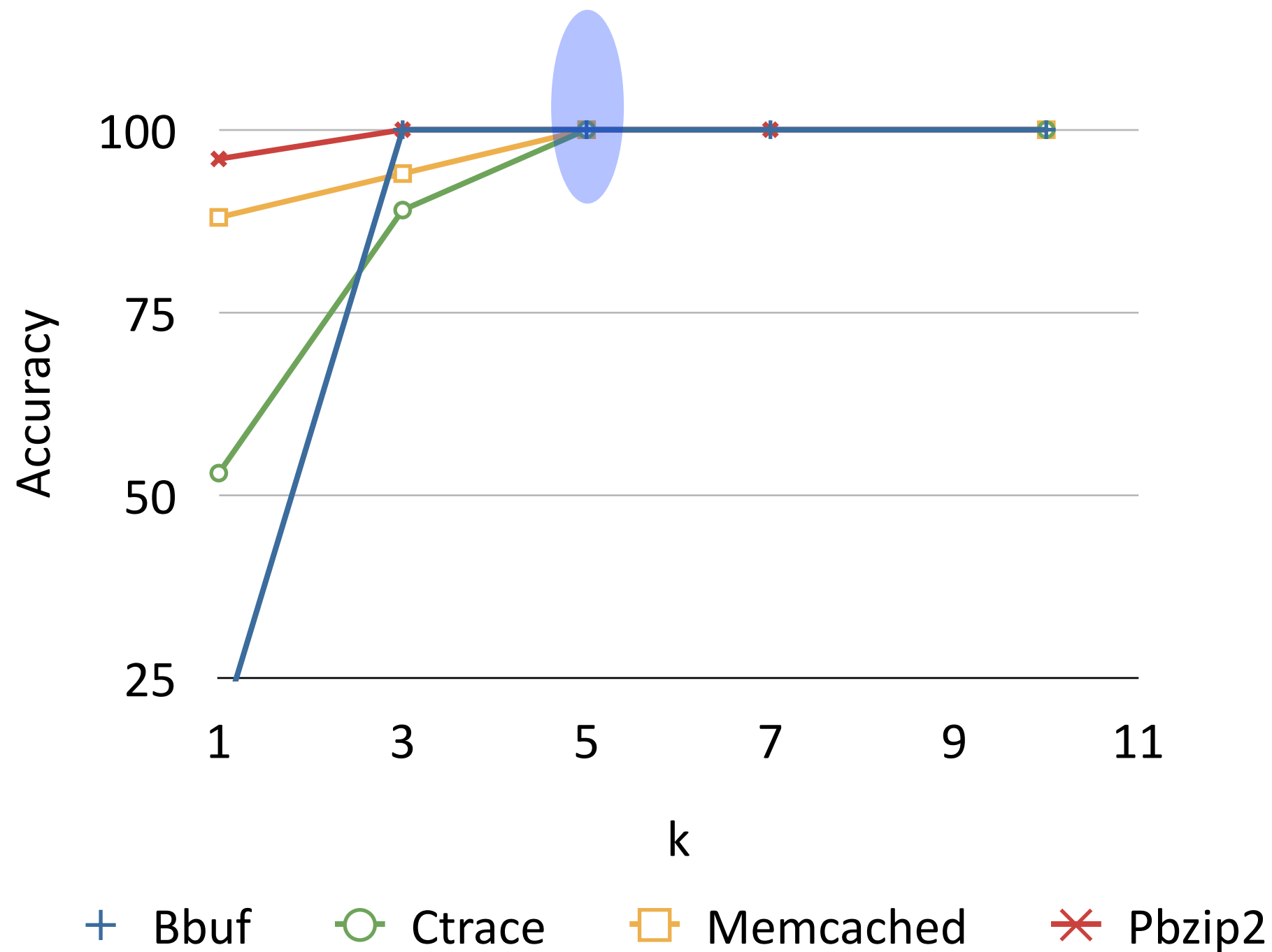


Performance

Program	Concrete Interpretation Time (sec)	Portend Classification Time (sec)		
		Avg	Min	Max
SQLite	3.1	4.2	4.09	4.25
Ocean	19.64	60.02	19.9	207.14
Fmm	24.87	64.45	65.29	72.83
Memcached	73.87	645.99	619.32	730.37
Pbzip2	15.3	360.72	61.36	763.43
Ctrace	3.67	24.29	5.54	41.08
Bbuf	1.81	4.47	4.77	5.82

Avg. classification time per race < 5 min

K vs. Accuracy



Symbolic Output Comparison

```
i = getInput();  
if(i >= 0)  
    print(i);
```

**Symbolic
Primary**

$i = \lambda$

output: $\lambda, \lambda \geq 0$

**Concrete
Alternate**

$i = 5$

output: 5

**Does the concrete output
satisfy the constraints of
the symbolic output?**

Classification Accuracy				
	SpecViol	K-witness	OutDiff	SingleOrd
Ground Truth	100%	100%	100%	100%
Record/Replay Analyzer*	10%	95%	0% (not-classified)	
Portend	100%	99%	99%	100%

*Single-path analysis and state comparison

Portend Trace Format

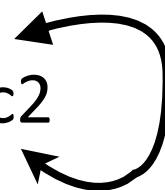
T 0

pc0

T 1

pc1

T 2

pc2  N times

T0:pc₀



T1 → RaceyAccess_{T1}:pc₁

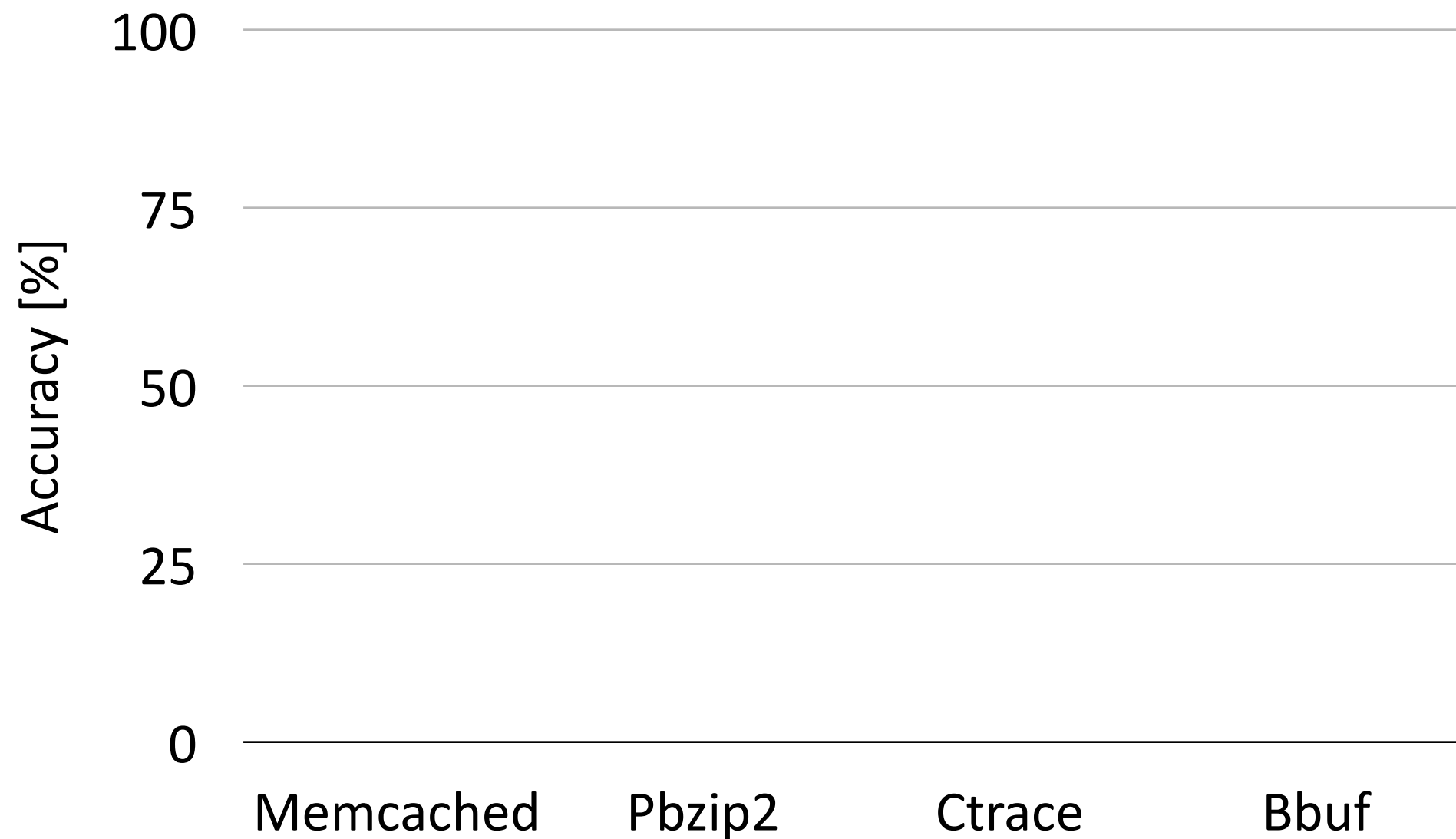


T2 → RaceyAccess_{T2}:pc₂

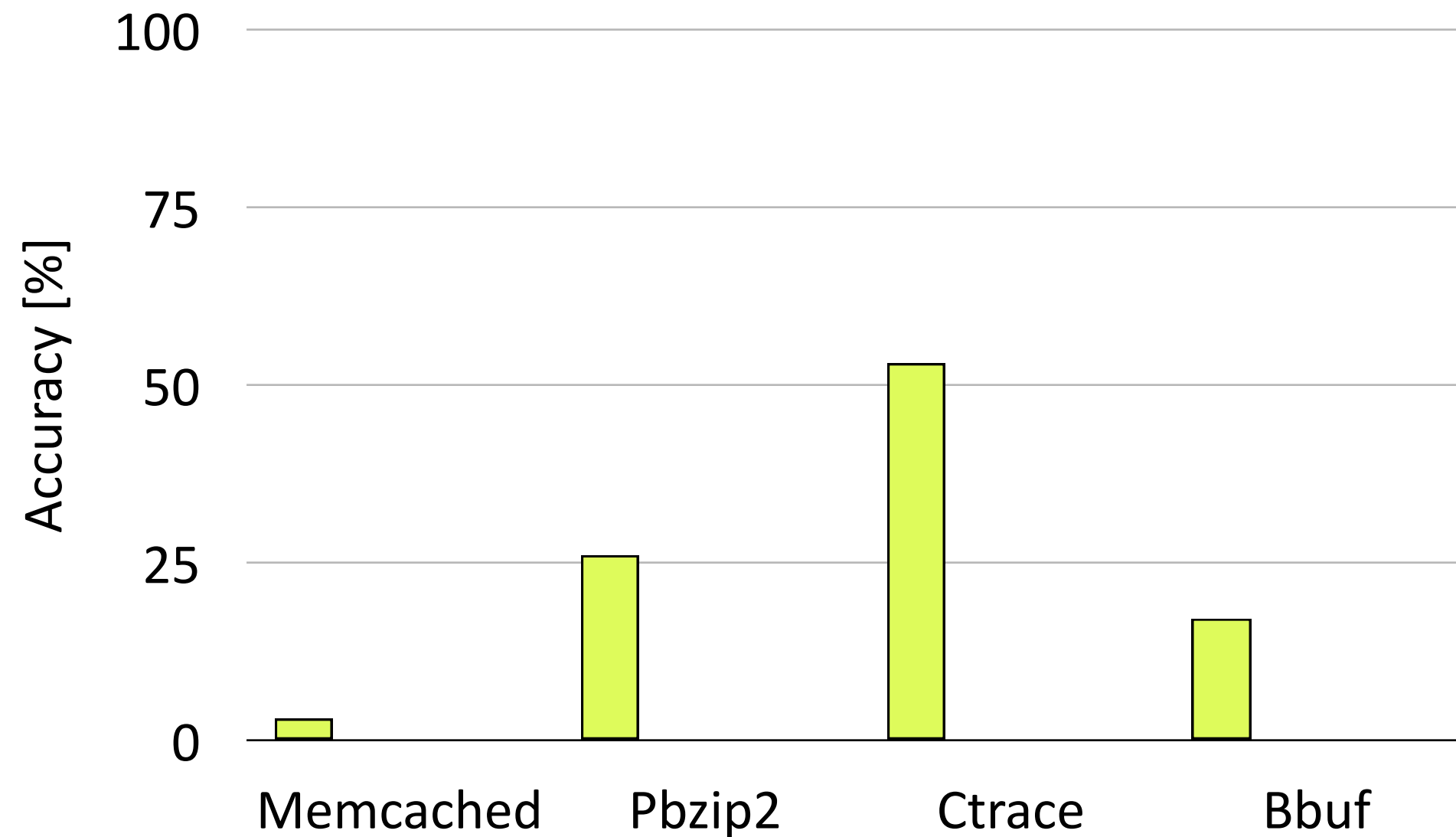


N times

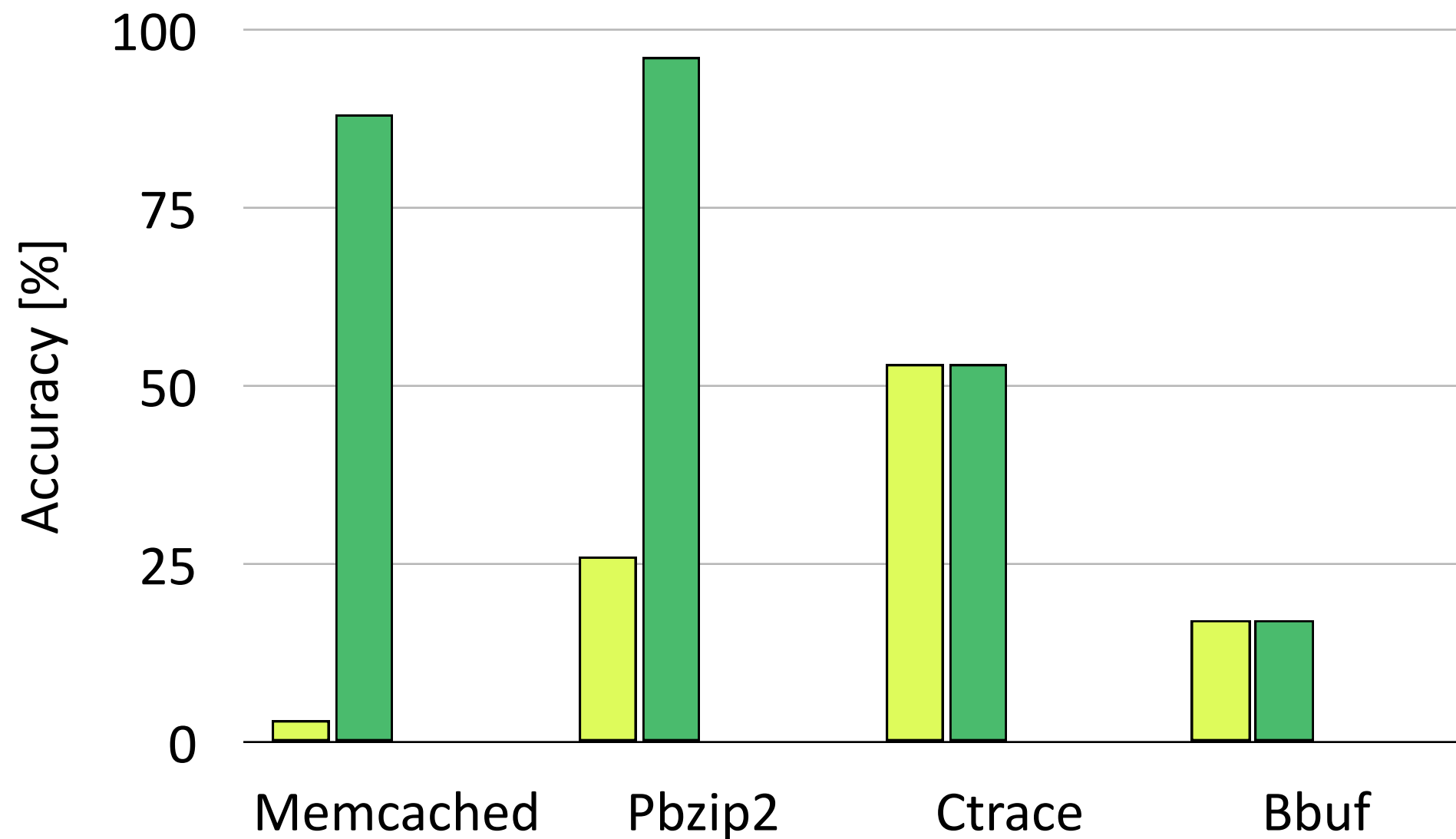
Contribution of Techniques



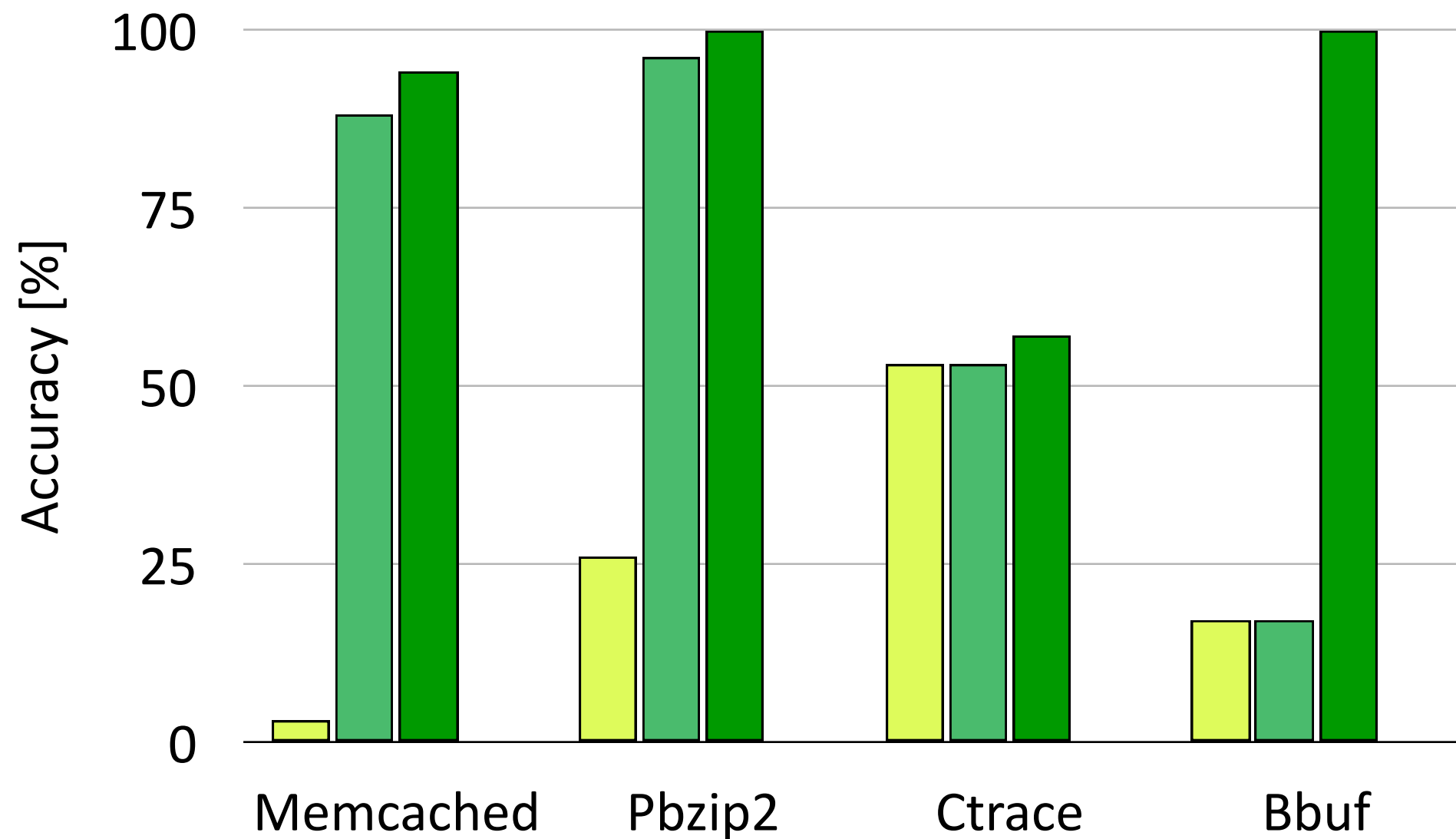
Contribution of Techniques



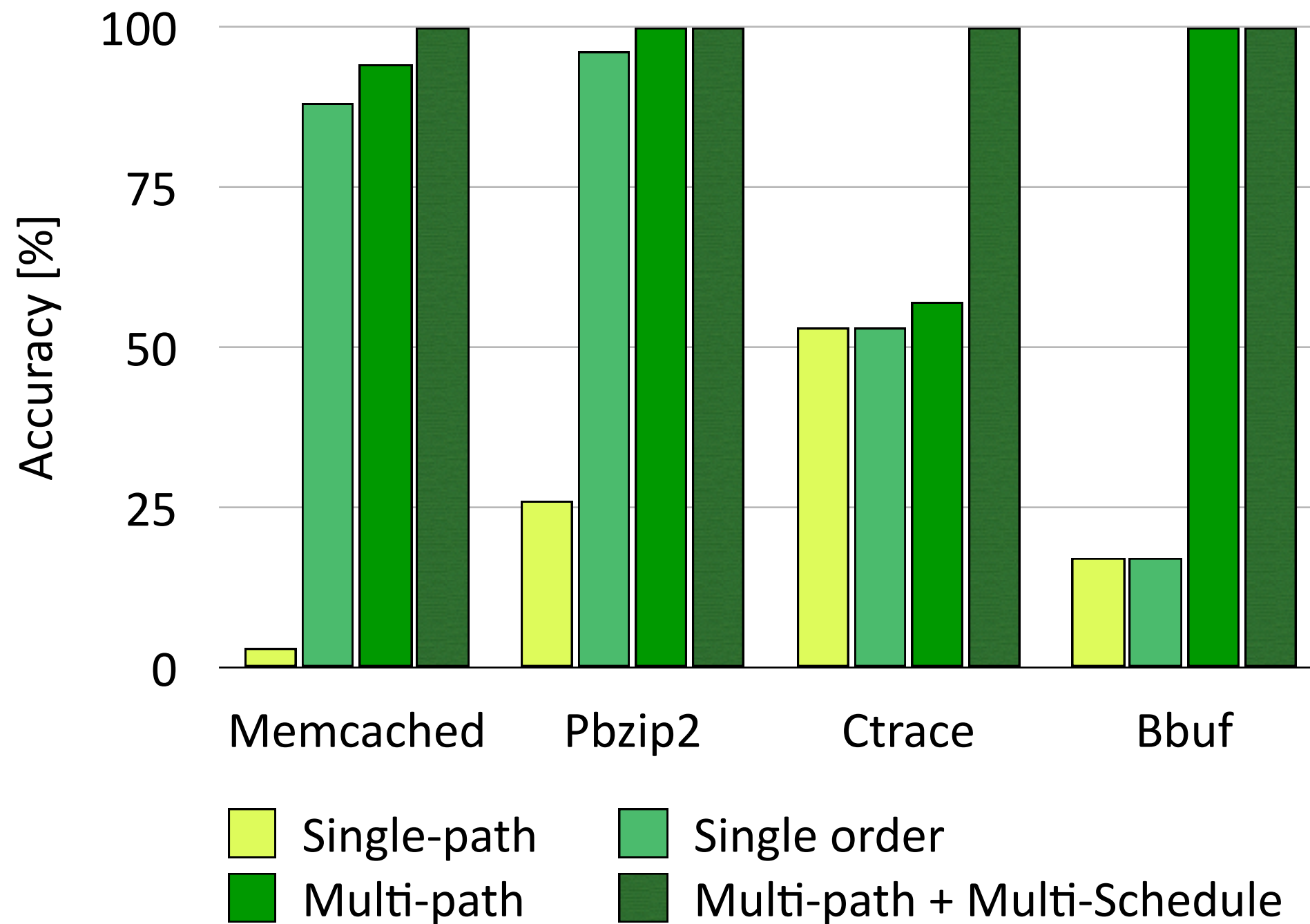
Contribution of Techniques



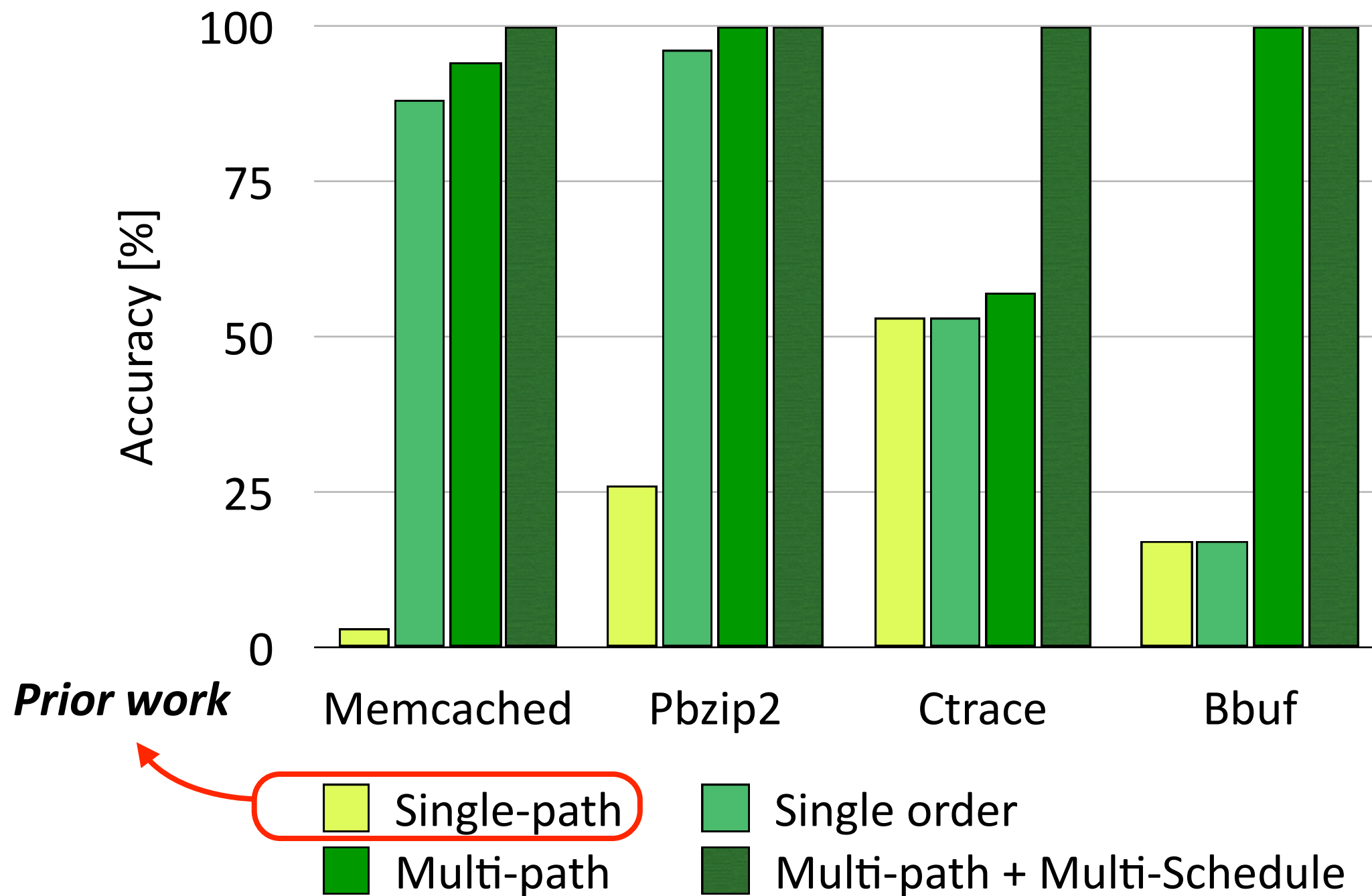
Contribution of Techniques



Contribution of Techniques



Contribution of Techniques



Contribution of Techniques

