Nasa Formal Methods (NFM) 2024, Moffett Field, California (USA)

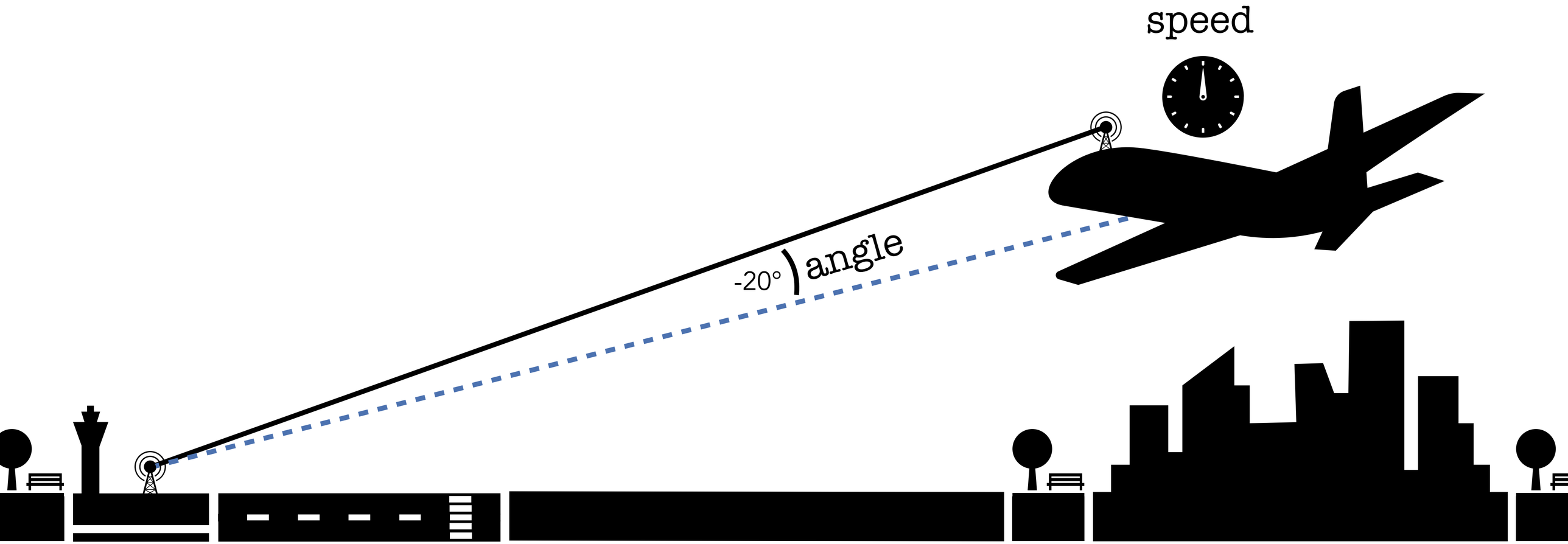
Quantitative Input Usage Static Analysis

Denis Mazzucato, Marco Campion, and Caterina Urban

4 June 2024

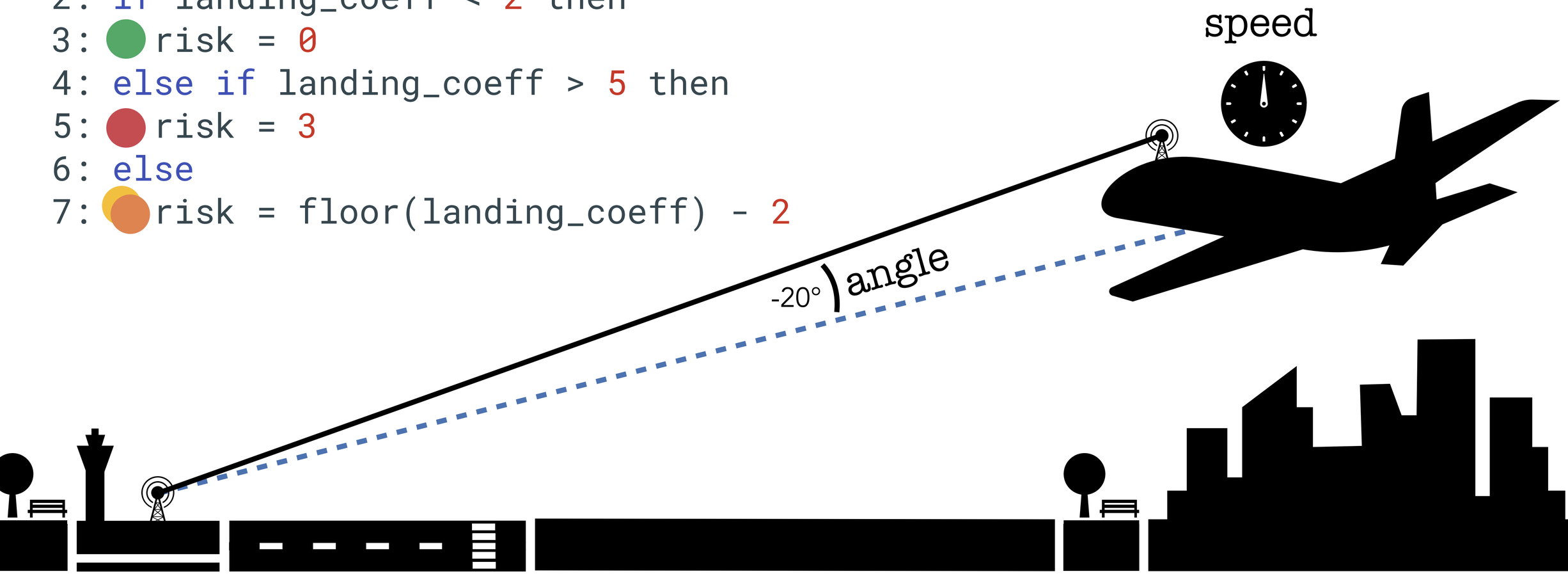
Aircraft Landing Alarm System 🚨

Aircraft Landing Alarm System 🚨



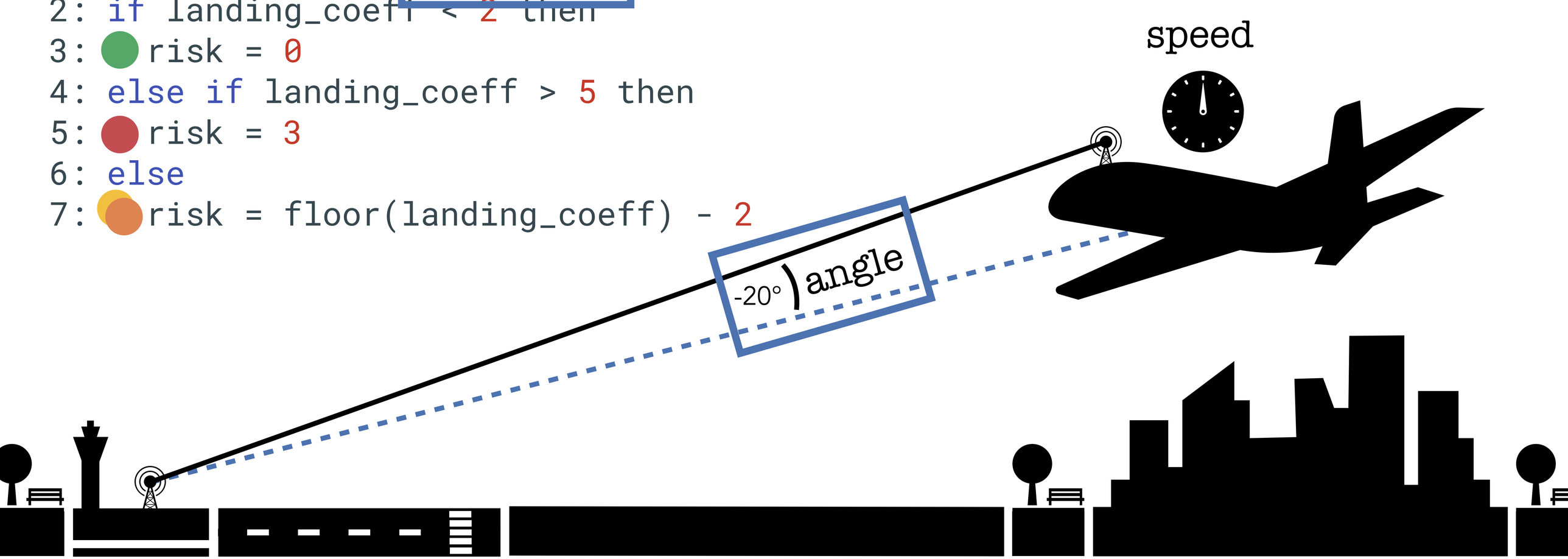
Aircraft Landing Alarm System 🚨

```
1: landing_coeff = abs(angle) + speed
2: if landing_coeff < 2 then
3:    risk = 0
4: else if landing_coeff > 5 then
5:    risk = 3
6: else
7:    risk = floor(landing_coeff) - 2
```



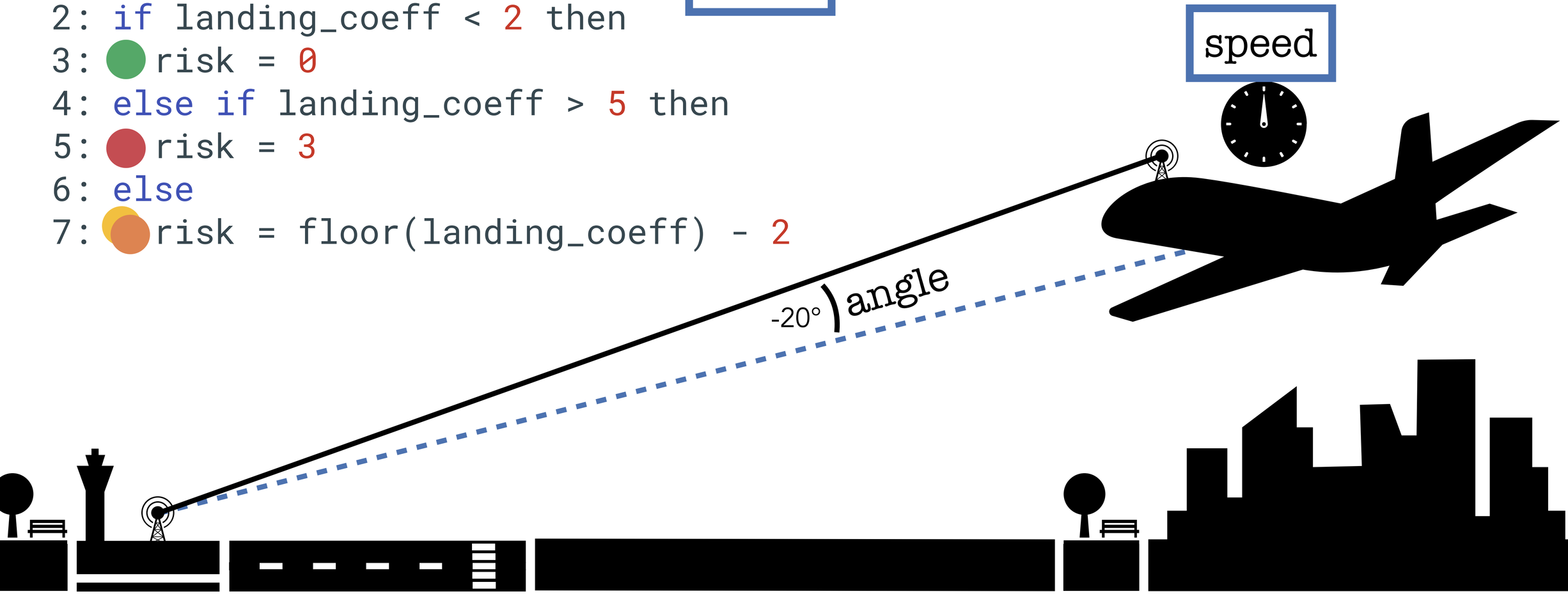
Aircraft Landing Alarm System 🚨

```
1: landing_coeff = abs(angle) + speed
2: if landing_coeff < 2 then
3:     risk = 0
4: else if landing_coeff > 5 then
5:     risk = 3
6: else
7:     risk = floor(landing_coeff) - 2
```



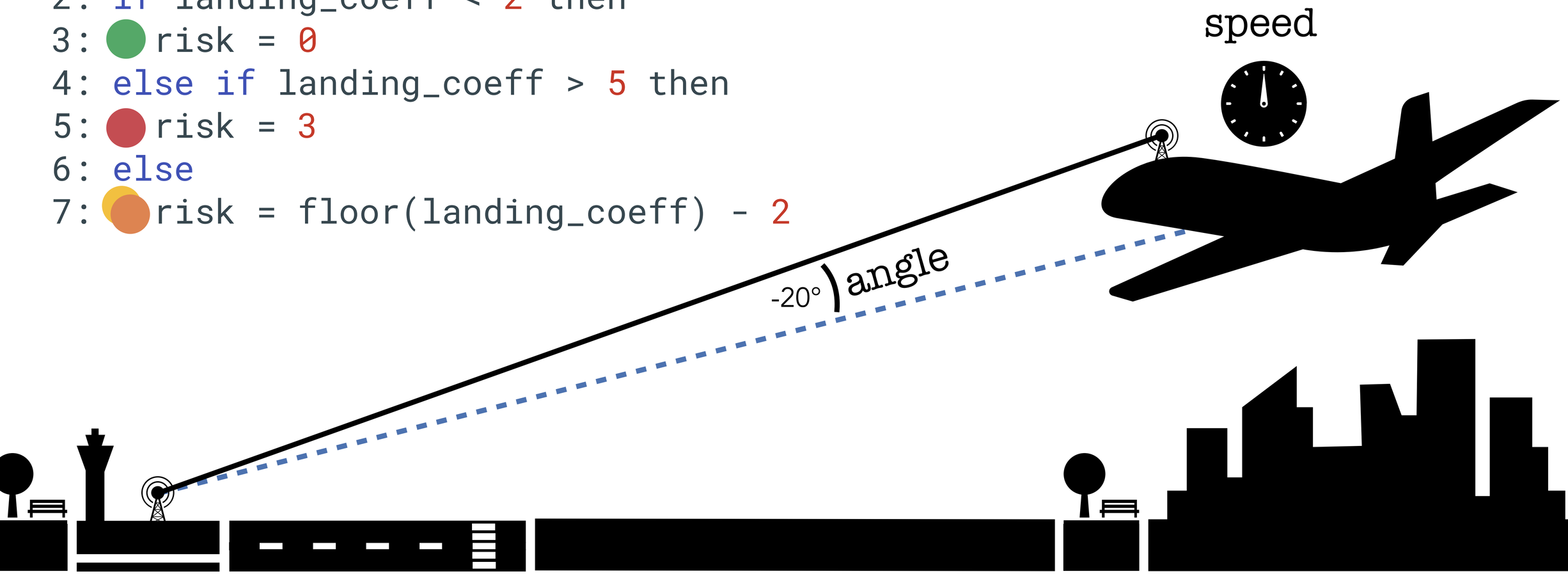
Aircraft Landing Alarm System 🚨

```
1: landing_coeff = abs(angle) + speed
2: if landing_coeff < 2 then
3:    risk = 0
4: else if landing_coeff > 5 then
5:    risk = 3
6: else
7:    risk = floor(landing_coeff) - 2
```



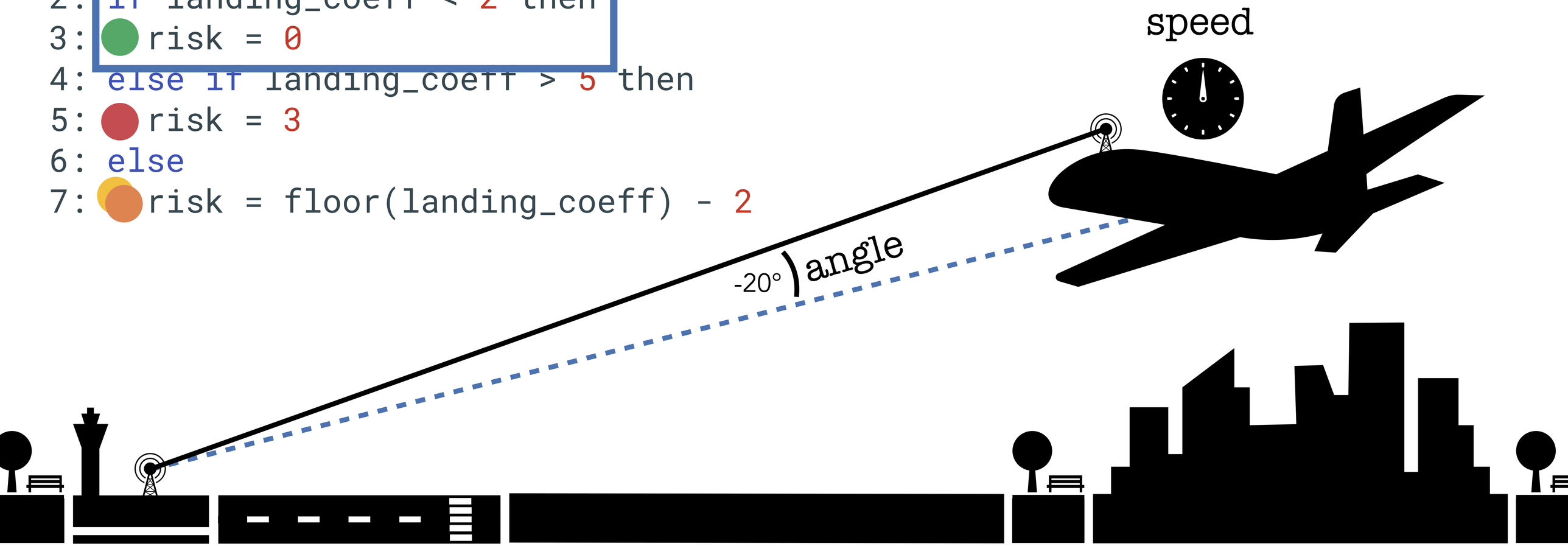
Aircraft Landing Alarm System 🚨

```
1: landing_coeff = abs(angle) + speed
2: if landing_coeff < 2 then
3:     risk = 0
4: else if landing_coeff > 5 then
5:     risk = 3
6: else
7:     risk = floor(landing_coeff) - 2
```



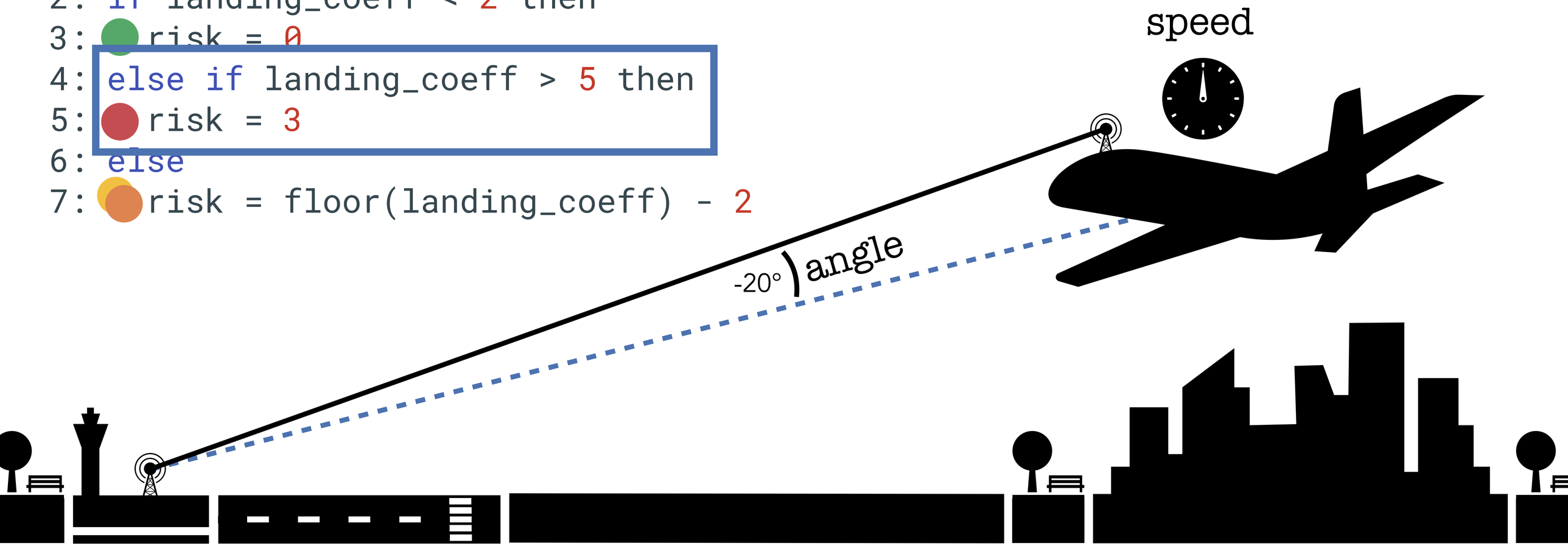
Aircraft Landing Alarm System 🚨

```
1: landing_coeff = abs(angle) + speed
2: if landing_coeff < 2 then
3:   risk = 0
4: else if landing_coeff > 5 then
5:   risk = 3
6: else
7:   risk = floor(landing_coeff) - 2
```



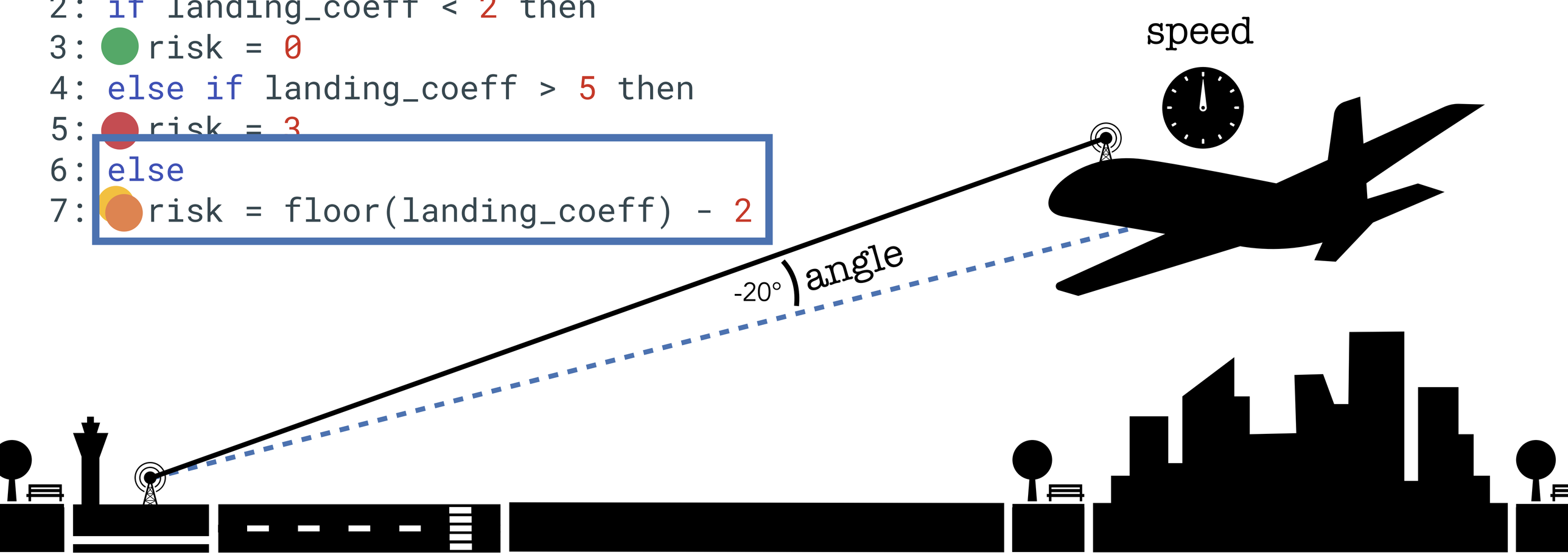
Aircraft Landing Alarm System 🚨

```
1: landing_coeff = abs(angle) + speed
2: if landing_coeff < 2 then
3:     risk = 0
4: else if landing_coeff > 5 then
5:     risk = 3
6: else
7:     risk = floor(landing_coeff) - 2
```



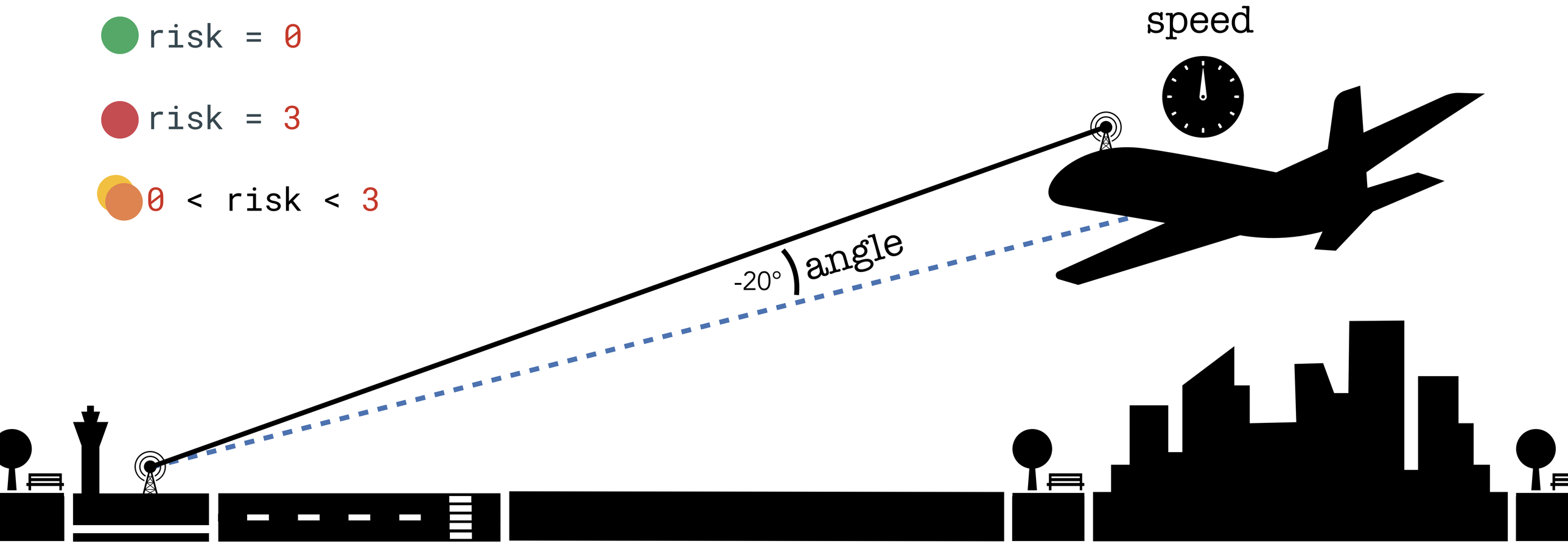
Aircraft Landing Alarm System 🚨

```
1: landing_coeff = abs(angle) + speed
2: if landing_coeff < 2 then
3:     risk = 0
4: else if landing_coeff > 5 then
5:     risk = 3
6: else
7:     risk = floor(landing_coeff) - 2
```



Aircraft Landing Alarm System 🚨

- `risk = 0`
- `risk = 3`
- `0 < risk < 3`

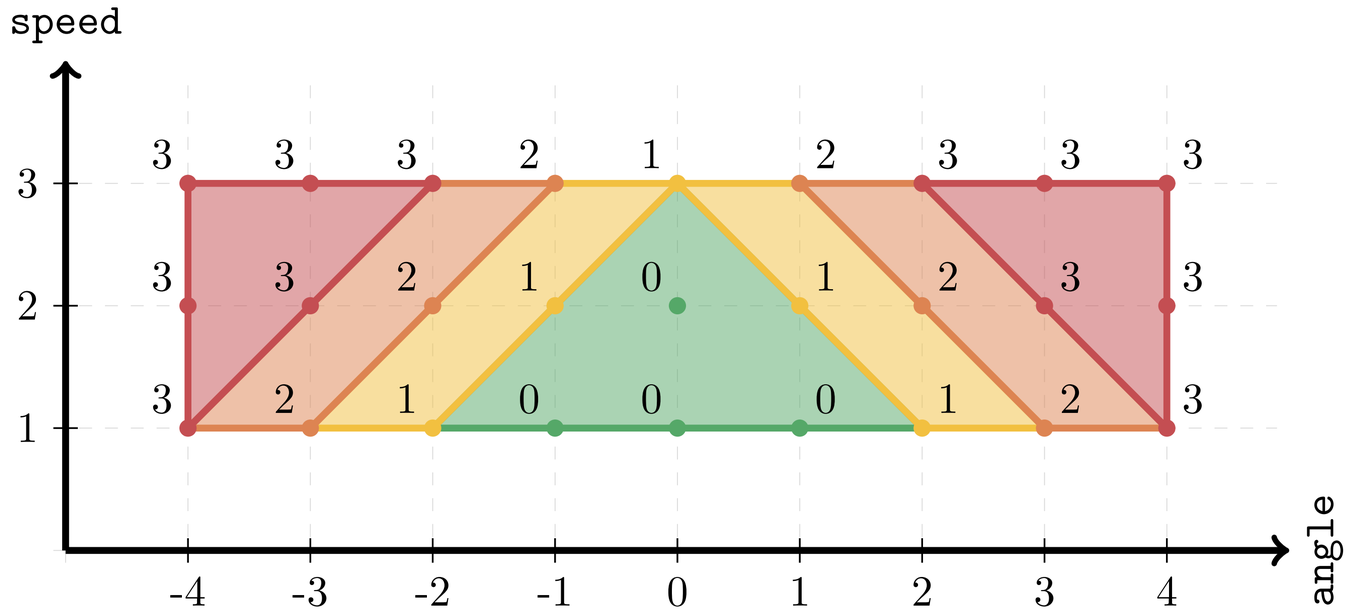


Aircraft Landing Alarm System 🚨

risk = 0

risk = 3

0 < risk < 3



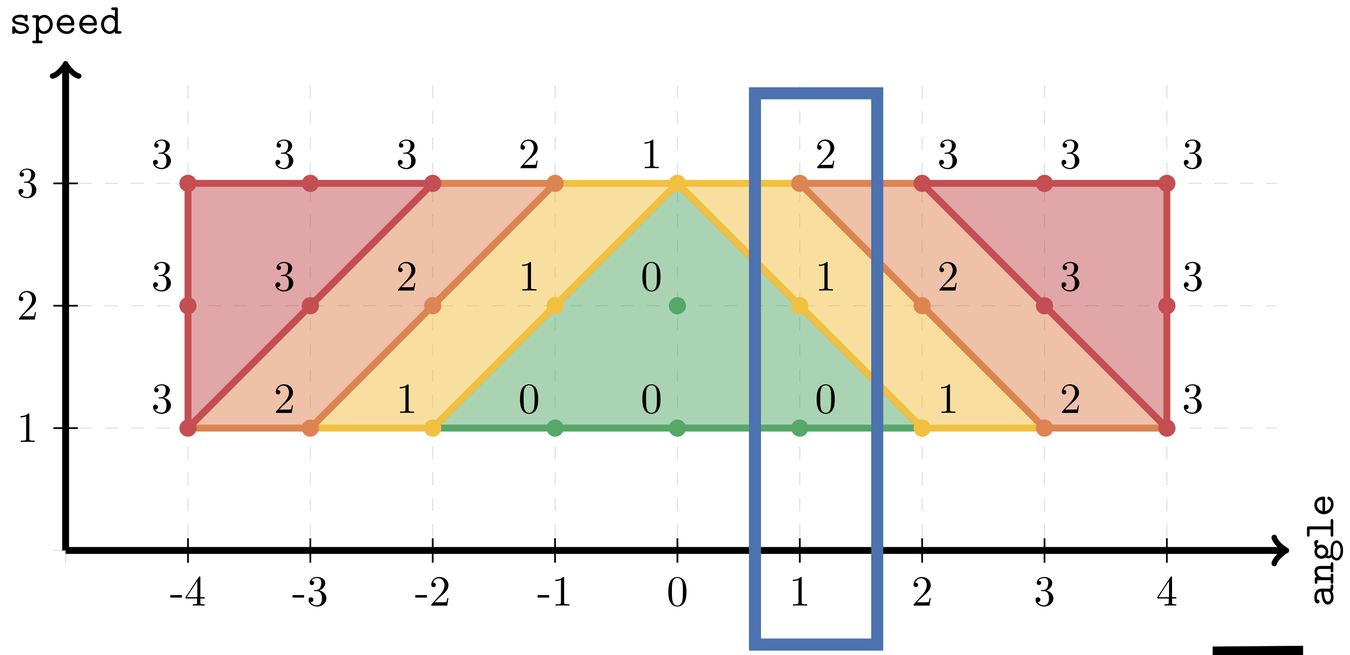
ENS | PSL Inria

Aircraft Landing Alarm System 🚨

risk = 0

risk = 3

0 < risk < 3



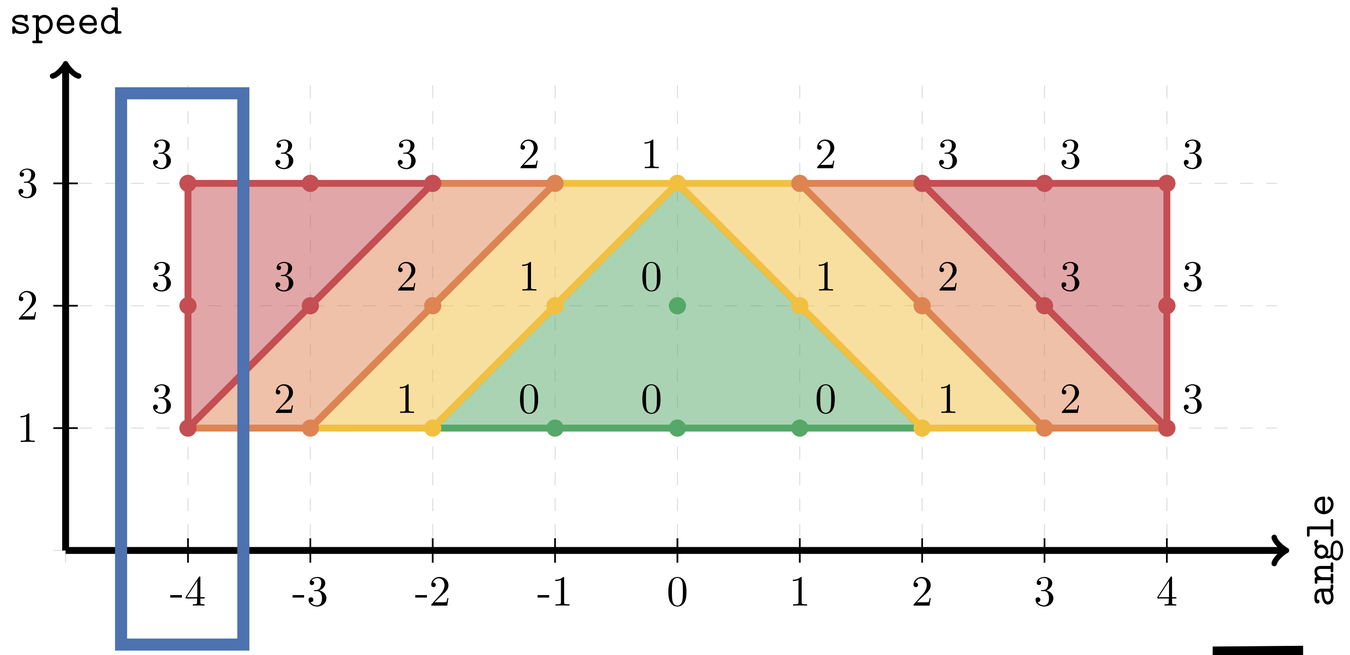
ENS | PSL Inria

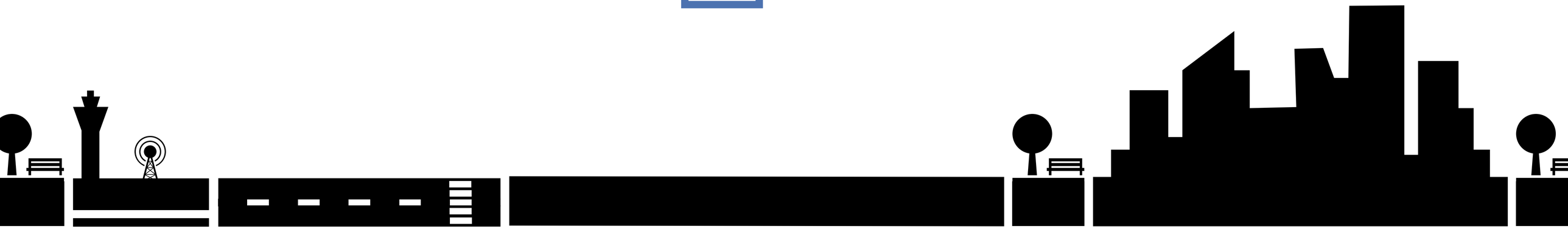
Aircraft Landing Alarm System 🚨

risk = 0

risk = 3

0 < risk < 3

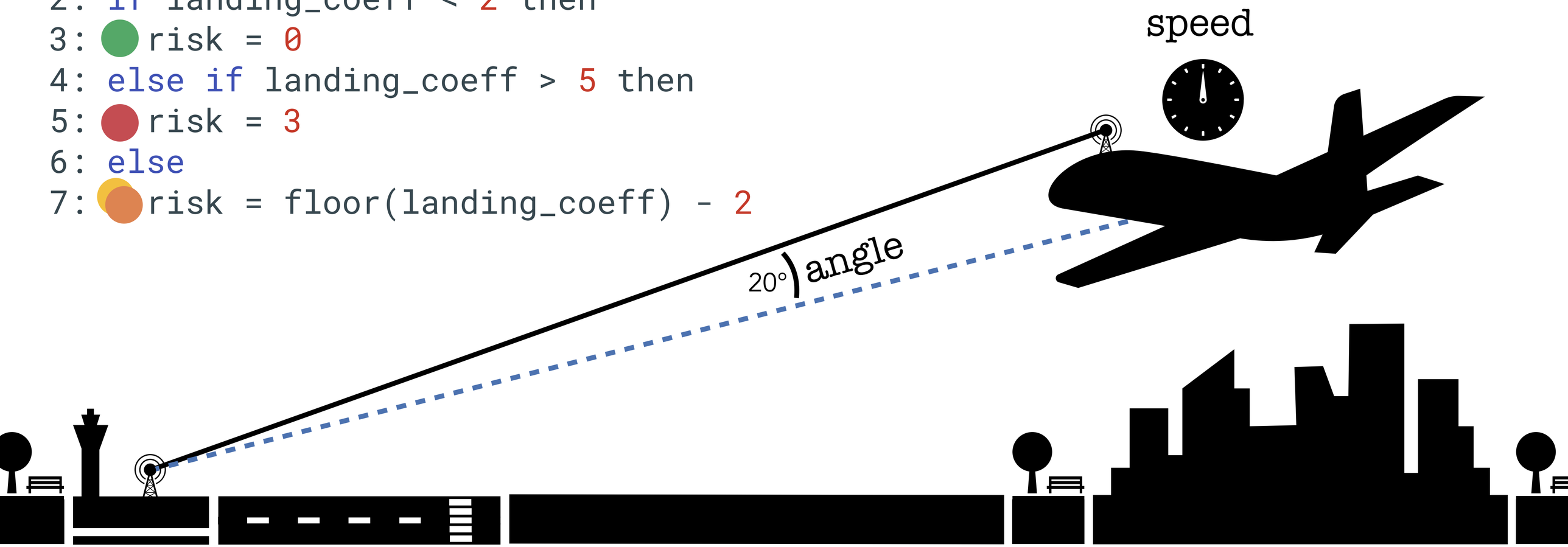




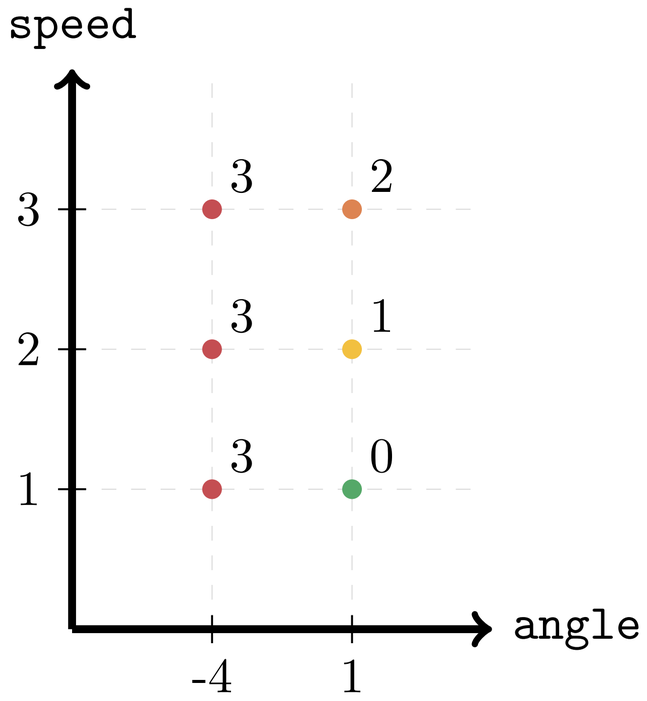
ENS | PSL Inria

Goal: Quantify the impact of speed and angle on risk

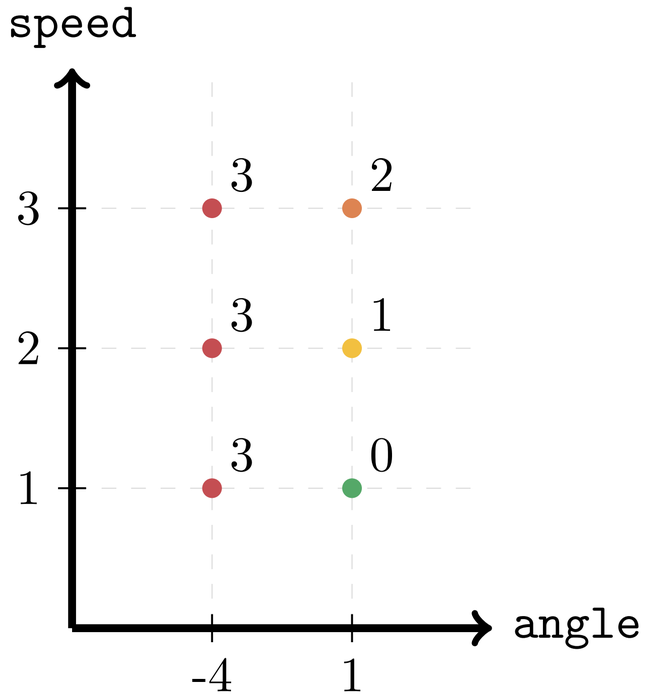
```
1: landing_coeff = abs(angle) + speed
2: if landing_coeff < 2 then
3:     risk = 0
4: else if landing_coeff > 5 then
5:     risk = 3
6: else
7:     risk = floor(landing_coeff) - 2
```



Goal: Quantify the impact of speed and angle on risk



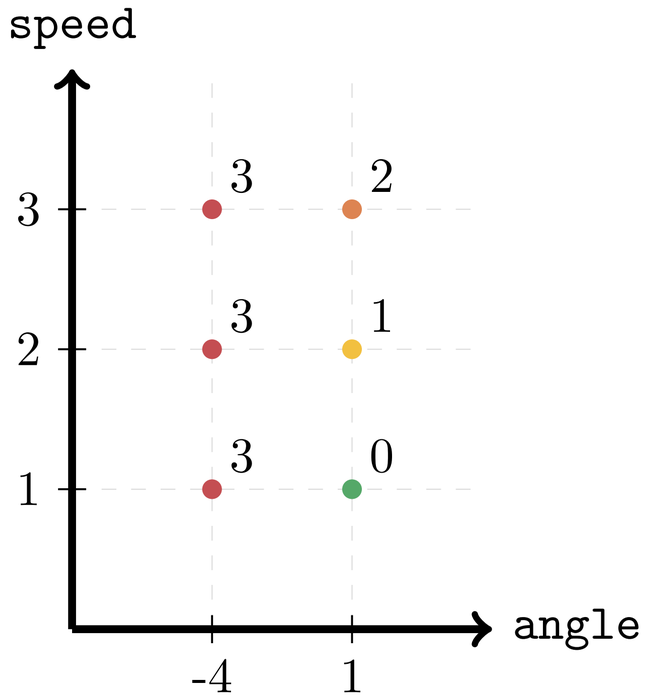
Goal: Quantify the impact of `speed` and `angle` on `risk`



Number of *reachable outcomes*

ENS | PSL Inria

Goal: Quantify the impact of `speed` and `angle` on `risk`

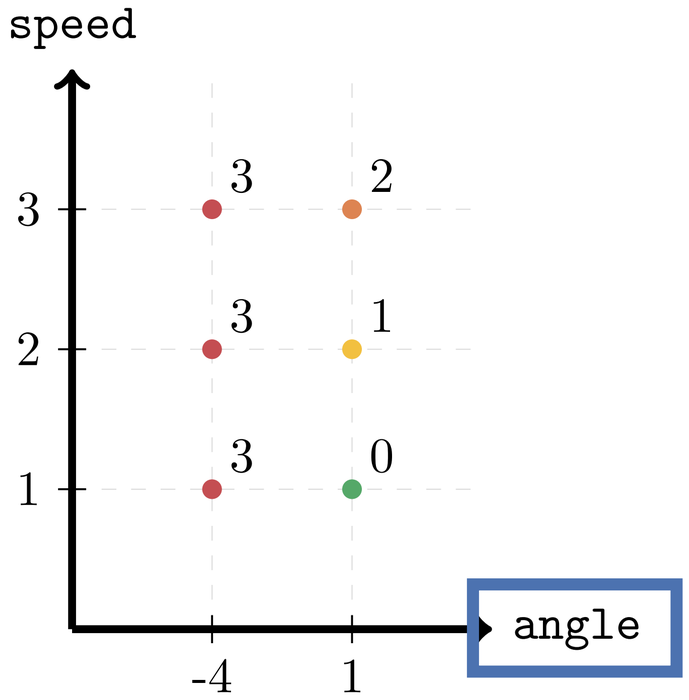


Number of *reachable outcomes*

OUTCOMES

ENS | PSL Inria

Goal: Quantify the impact of `speed` and `angle` on `risk`

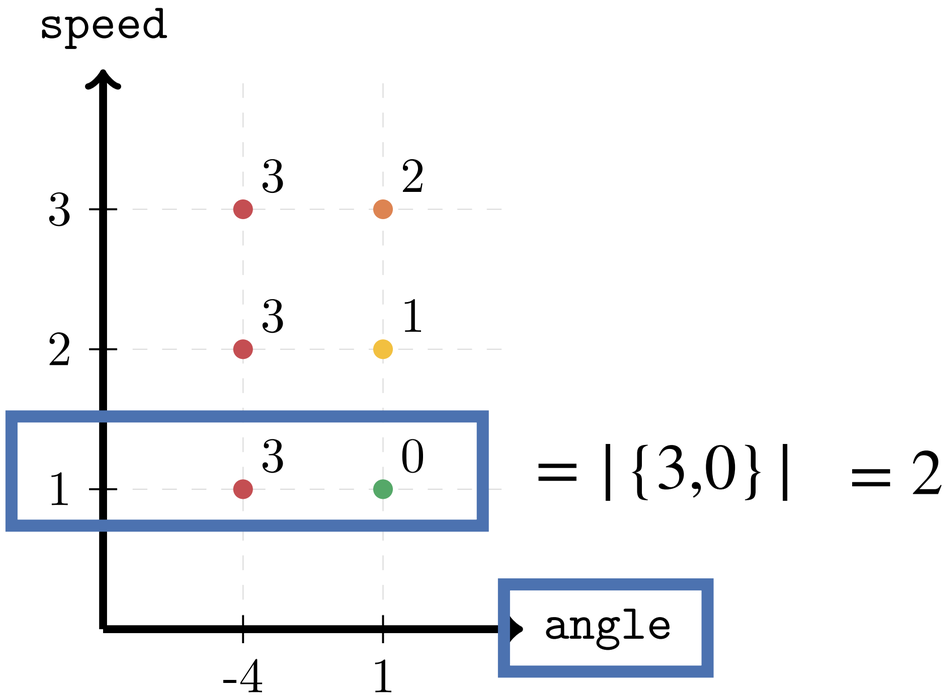


Number of *reachable outcomes*

OUTCOMES

ENS | PSL Inria

Goal: Quantify the impact of `speed` and `angle` on `risk`

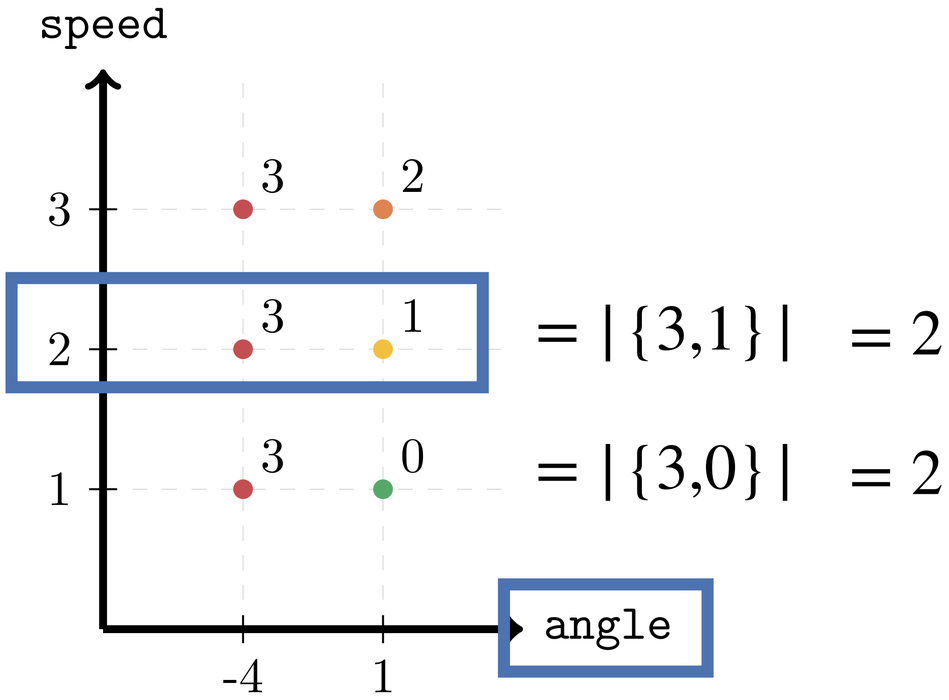


$= |\{3,0\}| \quad = 2$

Number of *reachable outcomes*

OUTCOMES

Goal: Quantify the impact of `speed` and `angle` on `risk`



$= |\{3,1\}| = 2$

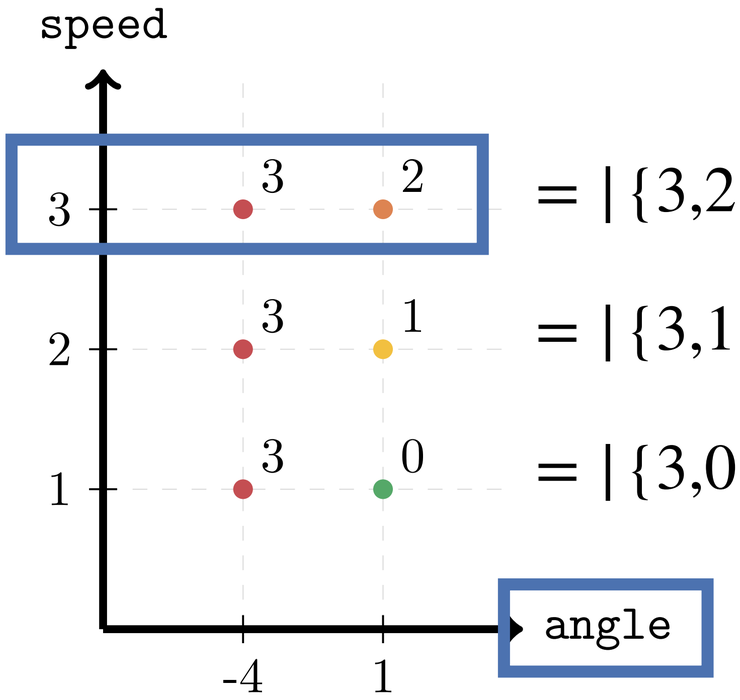
$= |\{3,0\}| = 2$

Number of *reachable outcomes*

OUTCOMES

ENS | PSL Inria

Goal: Quantify the impact of `speed` and `angle` on `risk`



$= |\{3,2\}| = 2$

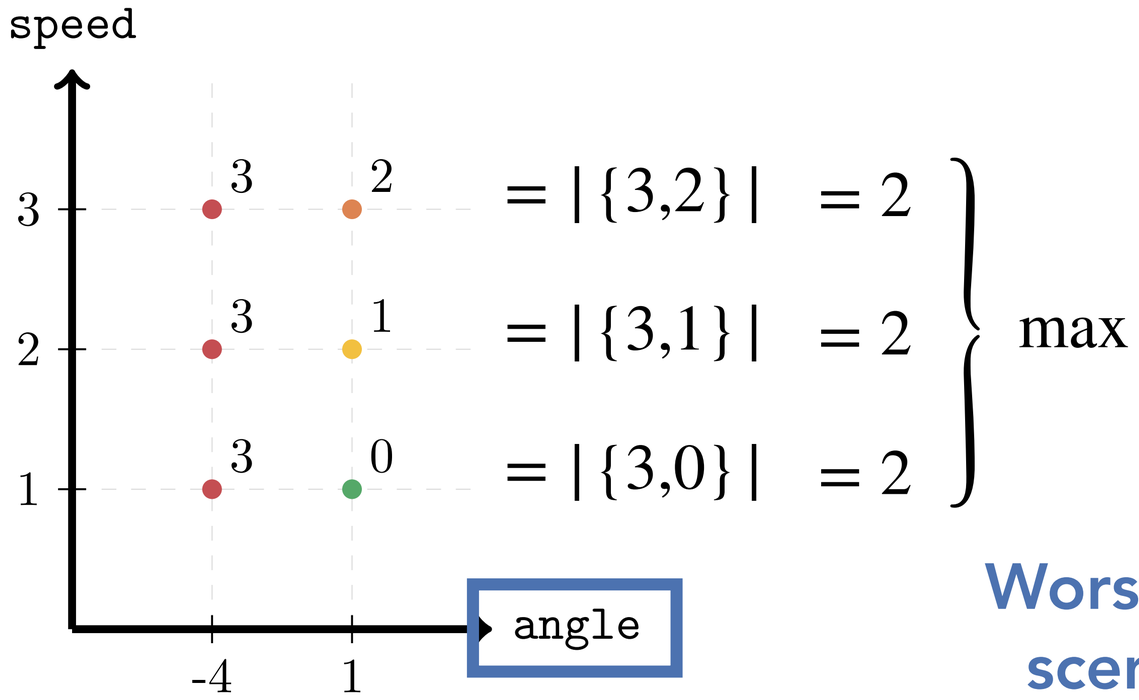
$= |\{3,1\}| = 2$

$= |\{3,0\}| = 2$

Number of *reachable outcomes*

OUTCOMES

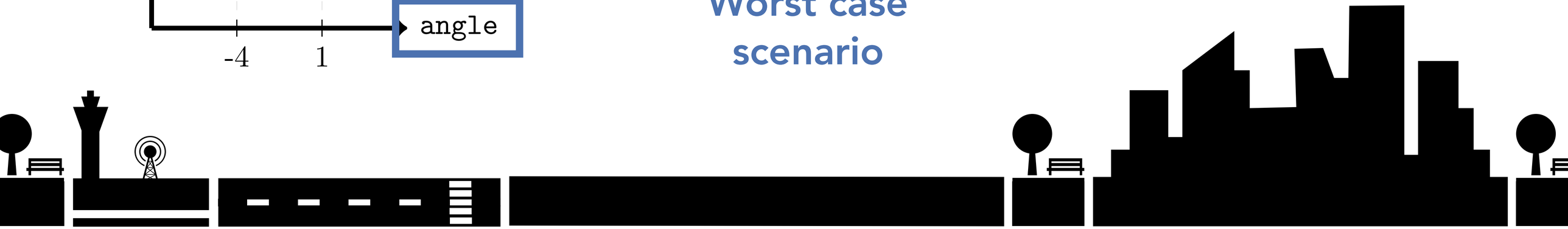
Goal: Quantify the impact of `speed` and `angle` on `risk`



Number of *reachable outcomes*

OUTCOMES

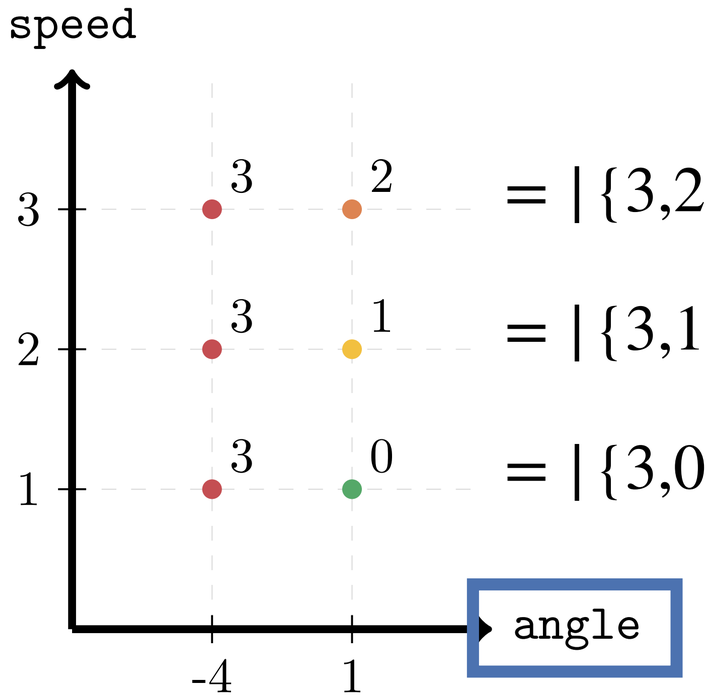
Worst case scenario



Denis Mazzucato et al. *Quantitative Input Usage Static Analysis*, NFM 2024

ENS | PSL Inria

Goal: Quantify the impact of speed and angle on risk

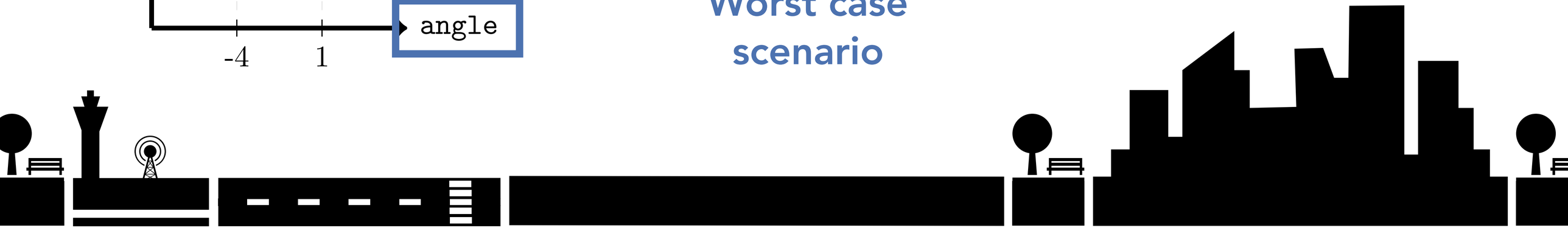


$$\left.\begin{array}{lll} = |\{3,2\}| & = 2 \\ = |\{3,1\}| & = 2 \\ = |\{3,0\}| & = 2 \end{array}\right\} \max = 2$$

Number of *reachable outcomes*

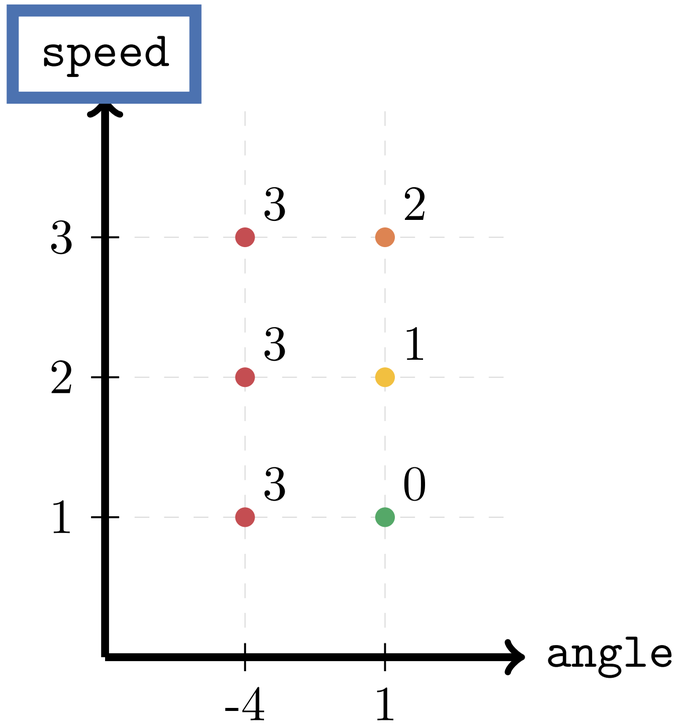
OUTCOMES

Worst case scenario



ENS | PSL Inria

Goal: Quantify the impact of `speed` and `angle` on `risk`

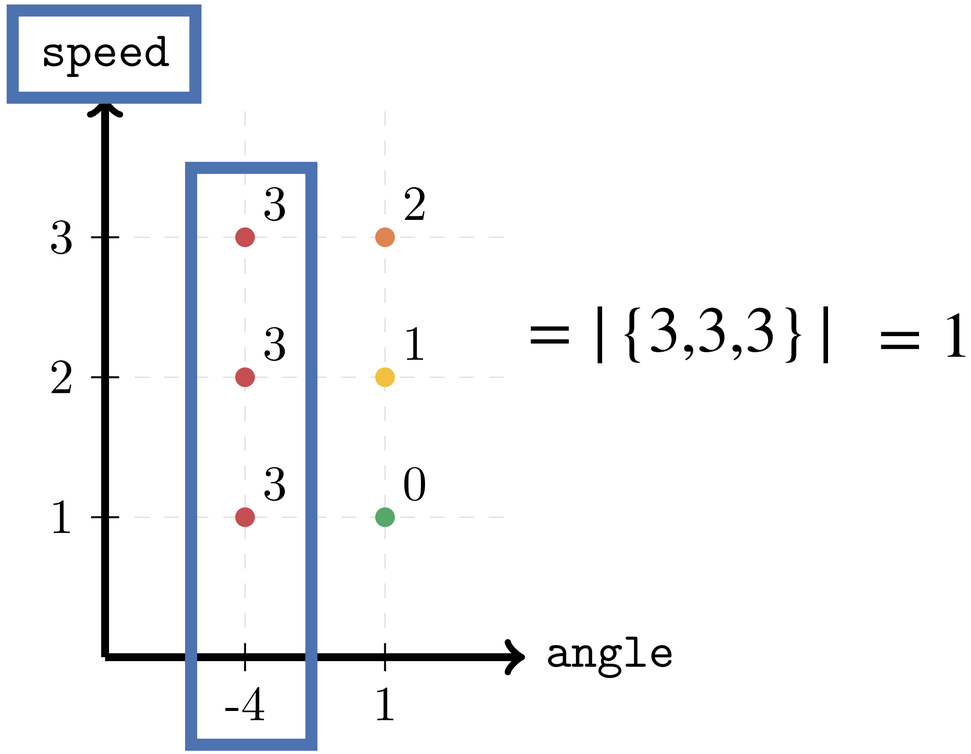


Number of *reachable outcomes*

OUTCOMES

ENS | PSL Inria

Goal: Quantify the impact of `speed` and `angle` on `risk`

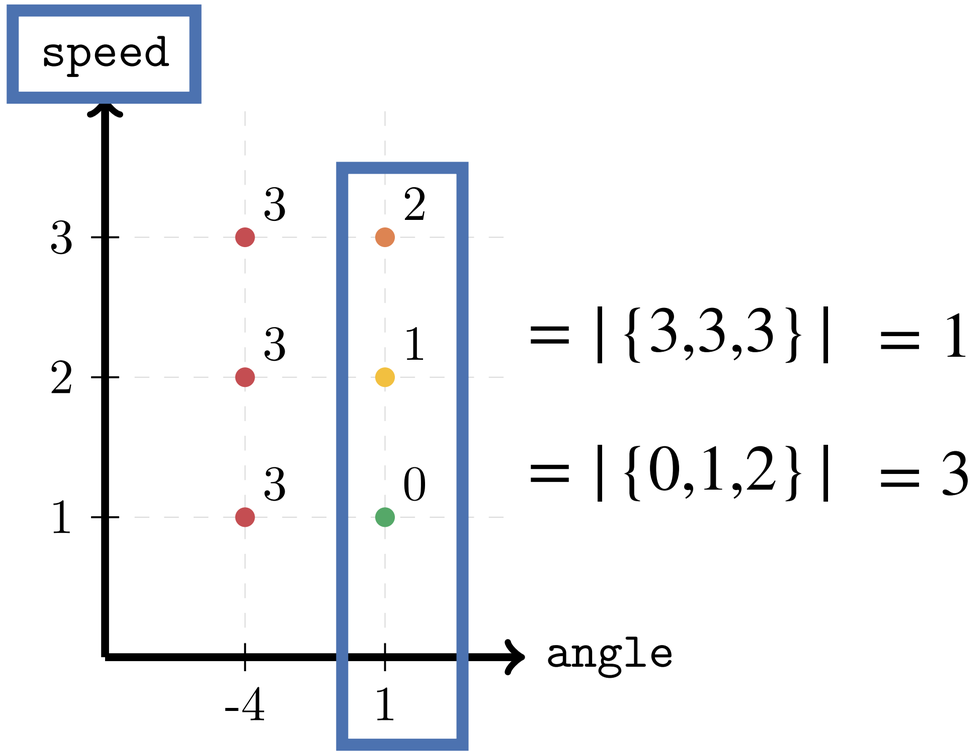


$= |\{3,3,3\}| = 1$

Number of *reachable outcomes*

OUTCOMES

Goal: Quantify the impact of `speed` and `angle` on `risk`



$= |\{3,3,3\}| = 1$

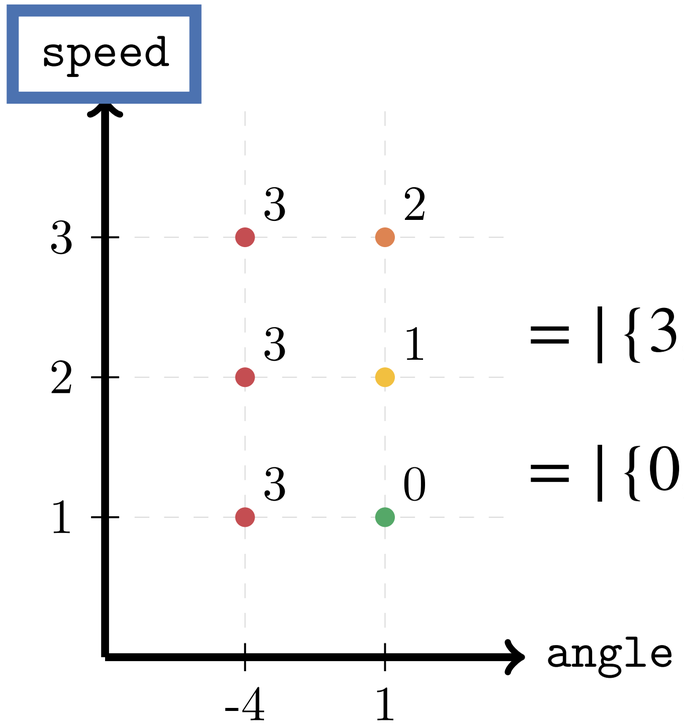
$= |\{0,1,2\}| = 3$

Number of *reachable outcomes*

OUTCOMES

ENS | PSL Inria

Goal: Quantify the impact of speed and angle on risk



$$\left.\begin{array}{l} = |\{3,3,3\}| \;\; = 1 \\ = |\{0,1,2\}| \;\; = 3 \end{array}\right\} \max \;\; = 3$$

Number of *reachable outcomes*

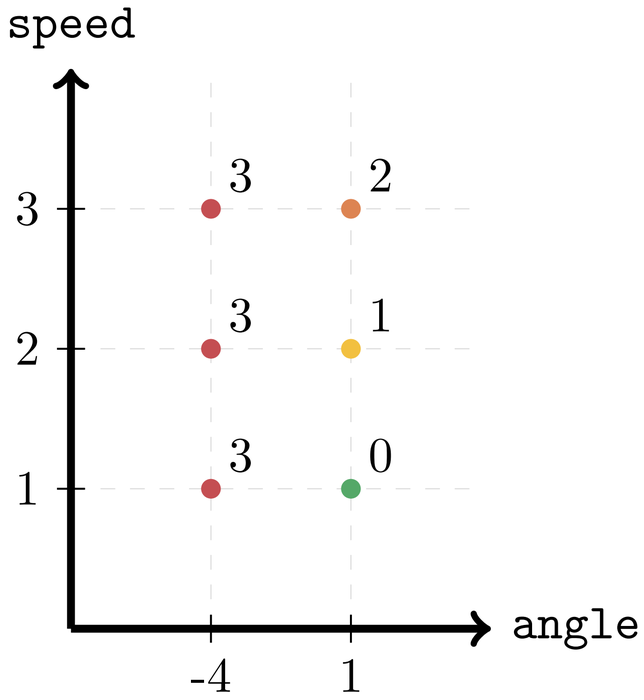
OUTCOMES

ENS | PSL Inria

Goal: Quantify the impact of `speed` and `angle` on `risk`

Distance of *reachable outcomes*

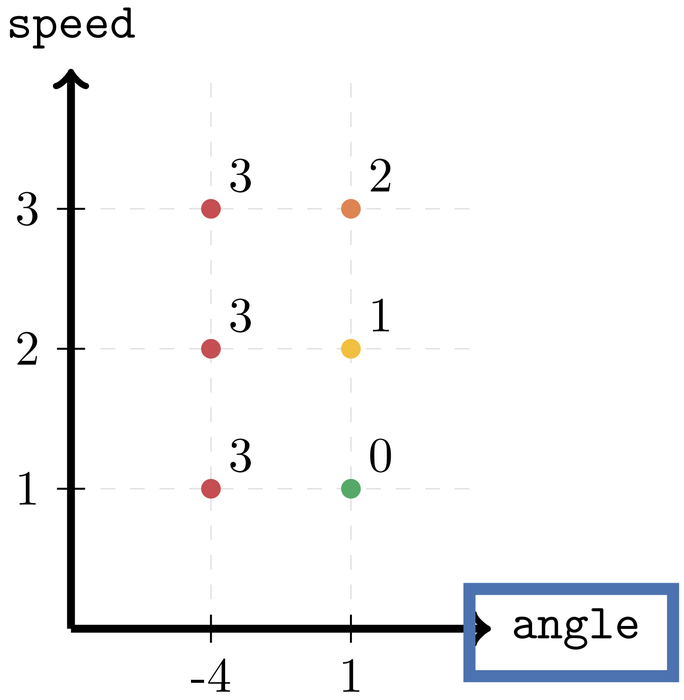
RANGE



Goal: Quantify the impact of `speed` and `angle` on `risk`

Distance of *reachable outcomes*

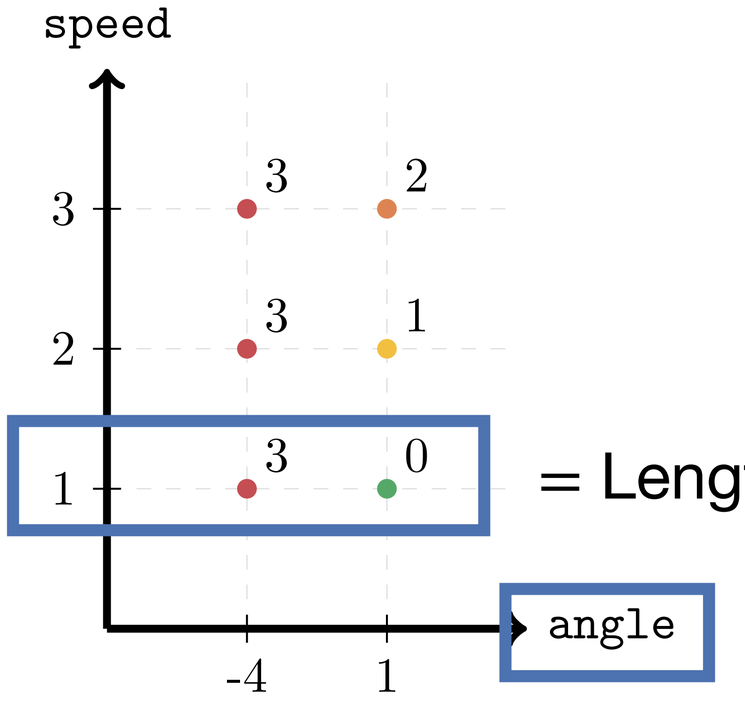
RANGE



Goal: Quantify the impact of speed and angle on risk

Distance of *reachable outcomes*

RANGE

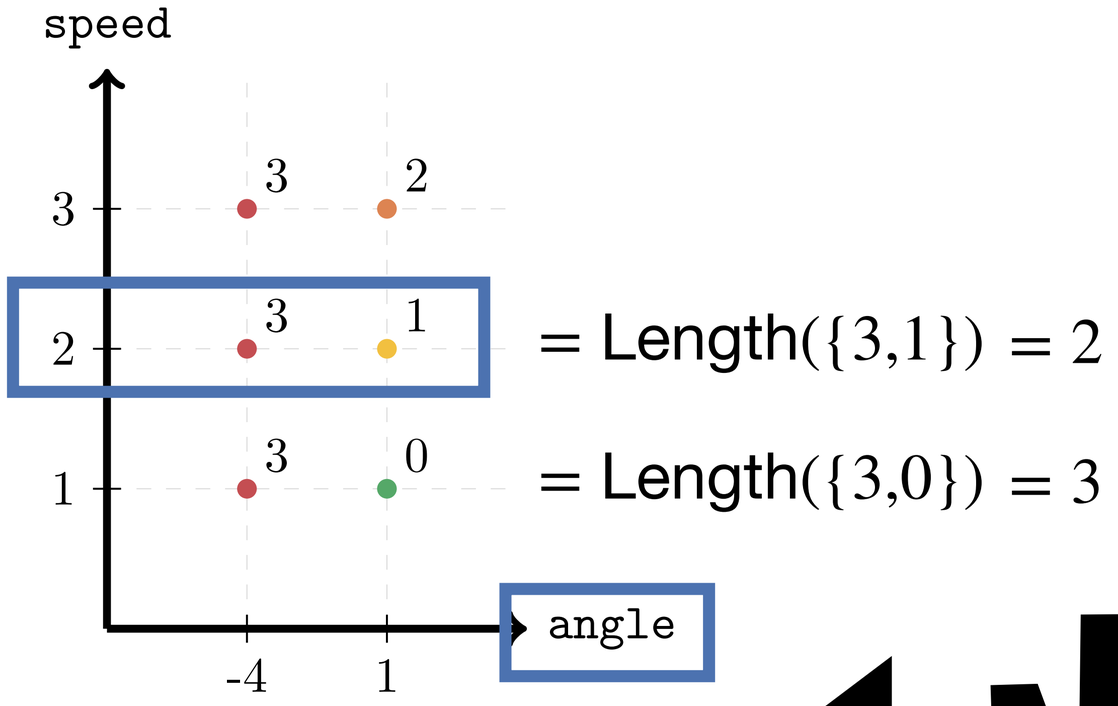


$= \text{Length}(\{3,0\}) = 3$

Goal: Quantify the impact of `speed` and `angle` on `risk`

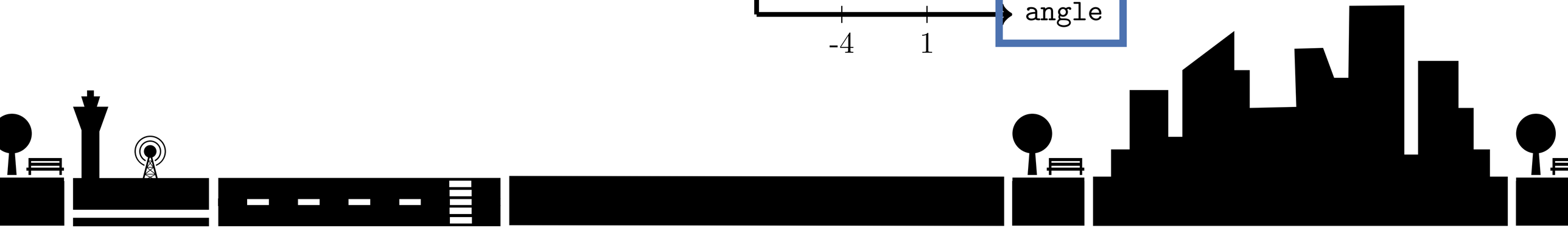
Distance of *reachable outcomes*

RANGE



$= \text{Length}(\{3,1\}) = 2$

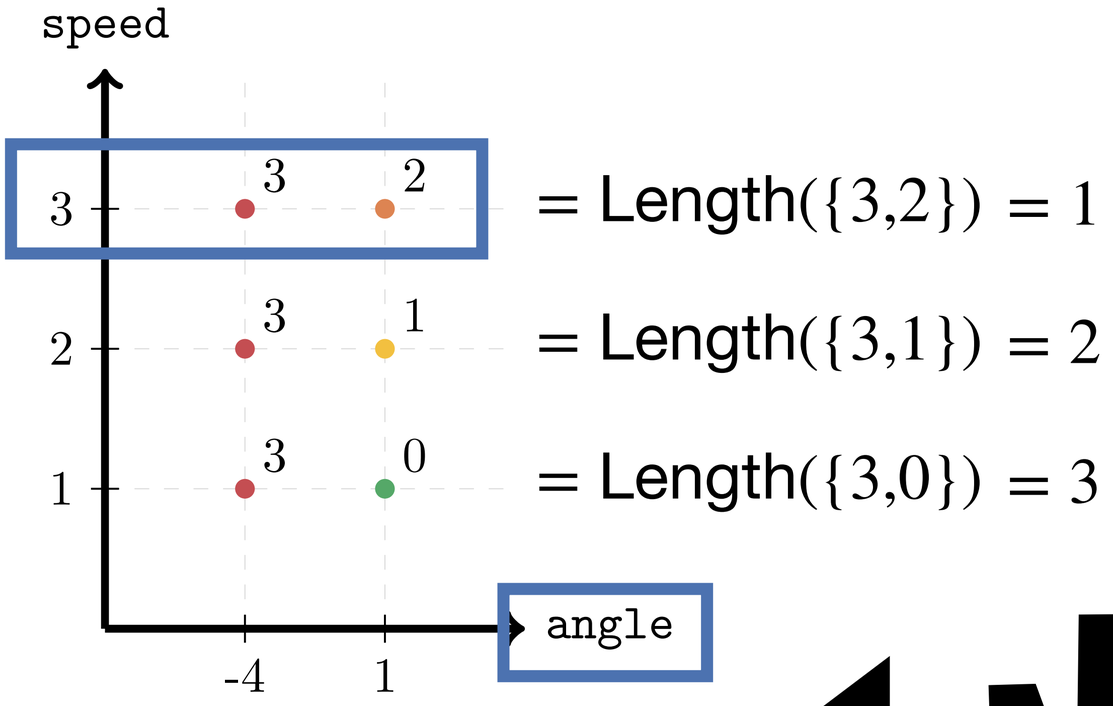
$= \text{Length}(\{3,0\}) = 3$



Goal: Quantify the impact of `speed` and `angle` on `risk`

Distance of *reachable outcomes*

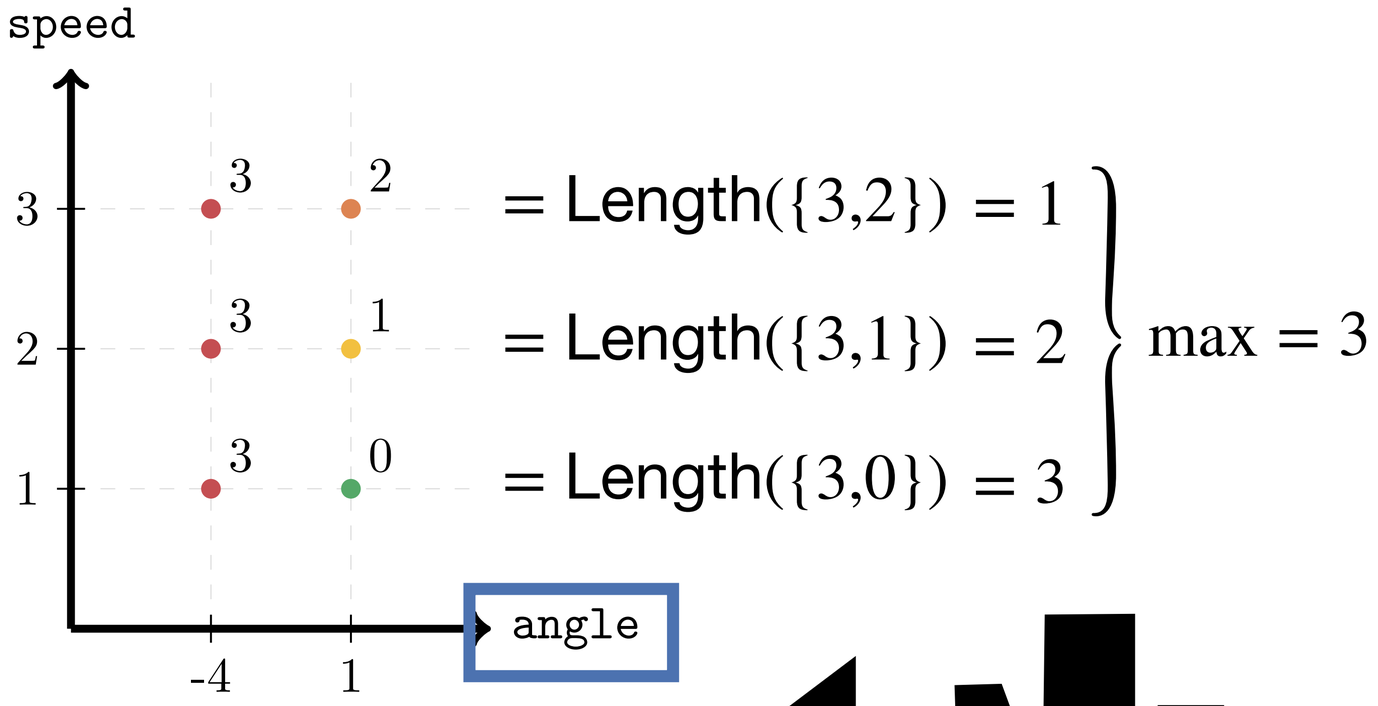
RANGE



Goal: Quantify the impact of `speed` and `angle` on `risk`

Distance of *reachable outcomes*

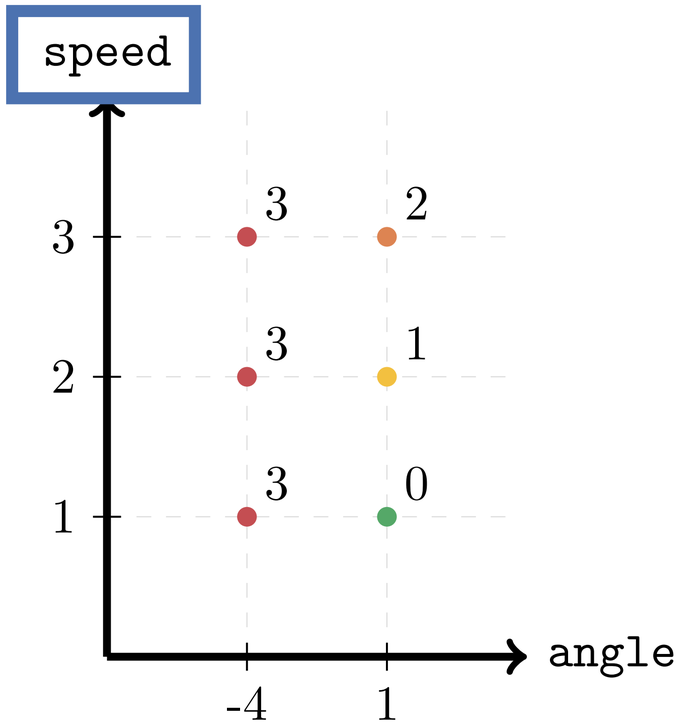
RANGE



Goal: Quantify the impact of `speed` and `angle` on `risk`

Distance of *reachable outcomes*

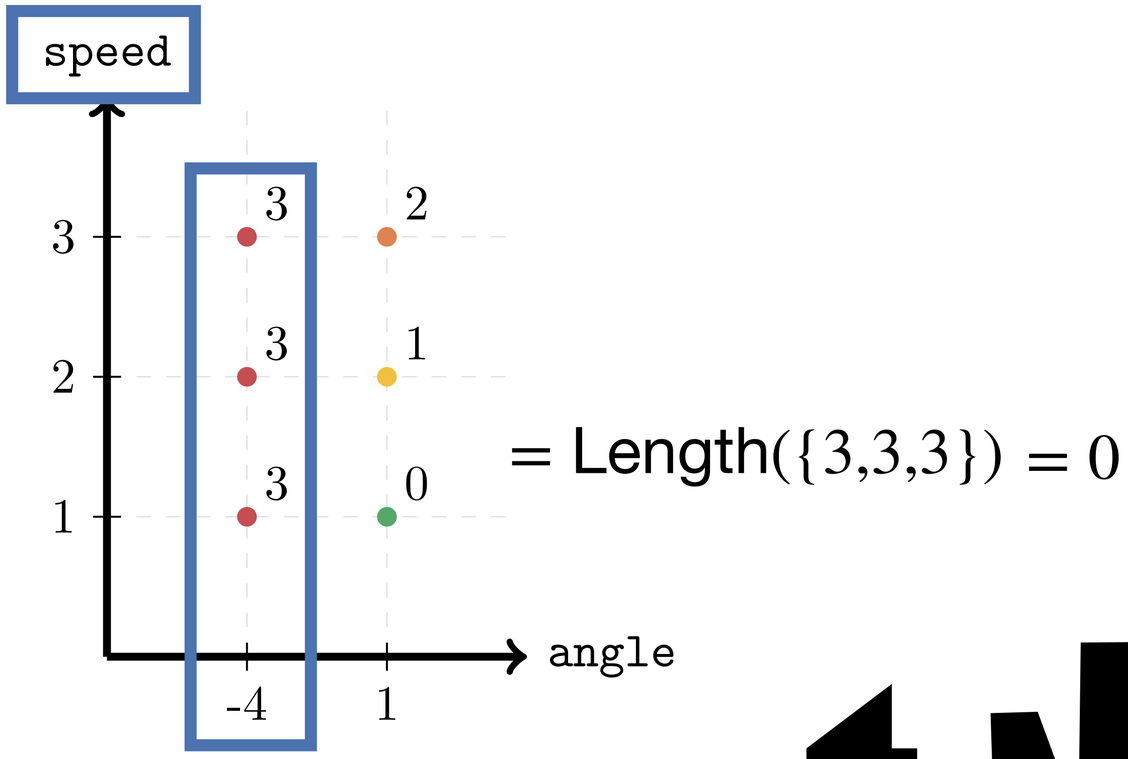
RANGE



Goal: Quantify the impact of `speed` and `angle` on `risk`

Distance of *reachable outcomes*

RANGE

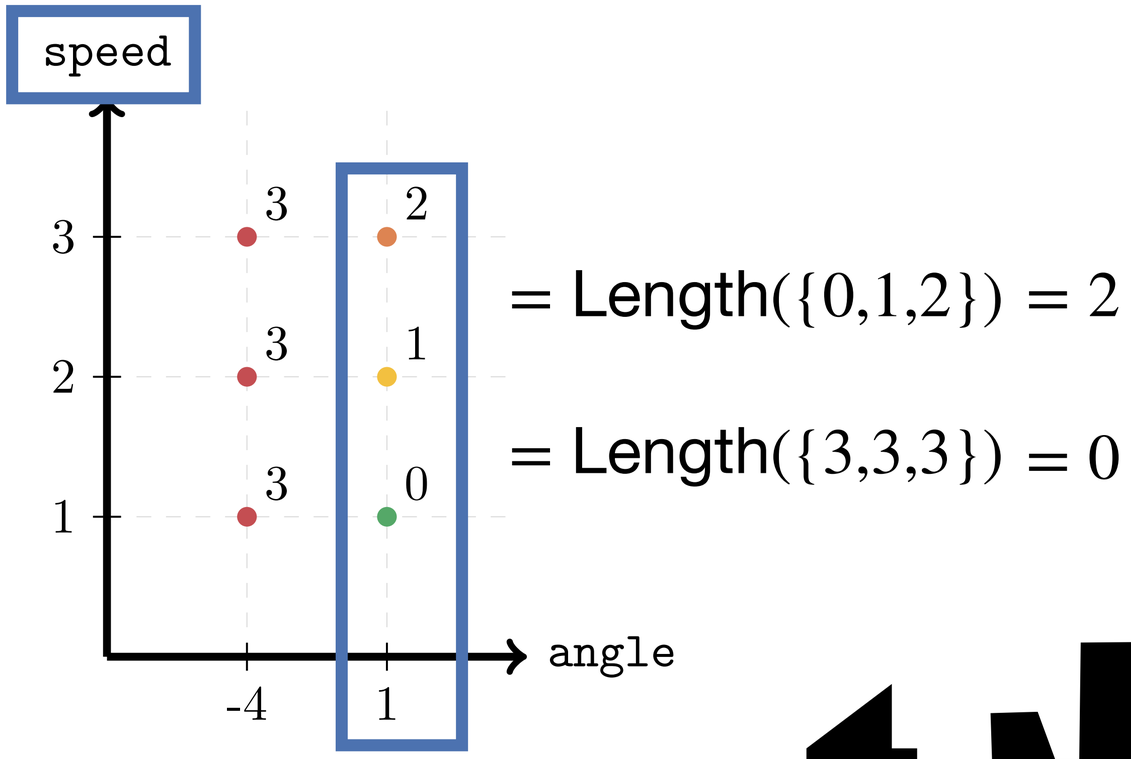


$= \text{Length}(\{3,3,3\}) = 0$

Goal: Quantify the impact of speed and angle on risk

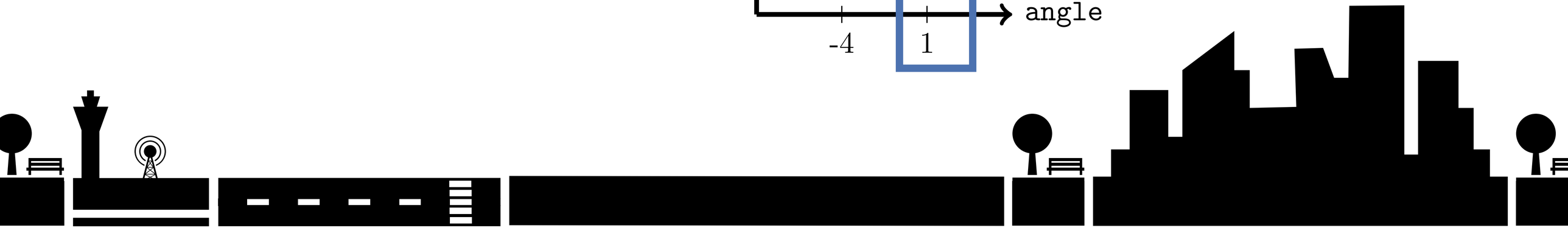
Distance of *reachable outcomes*

RANGE



$= \text{Length}(\{0,1,2\}) = 2$

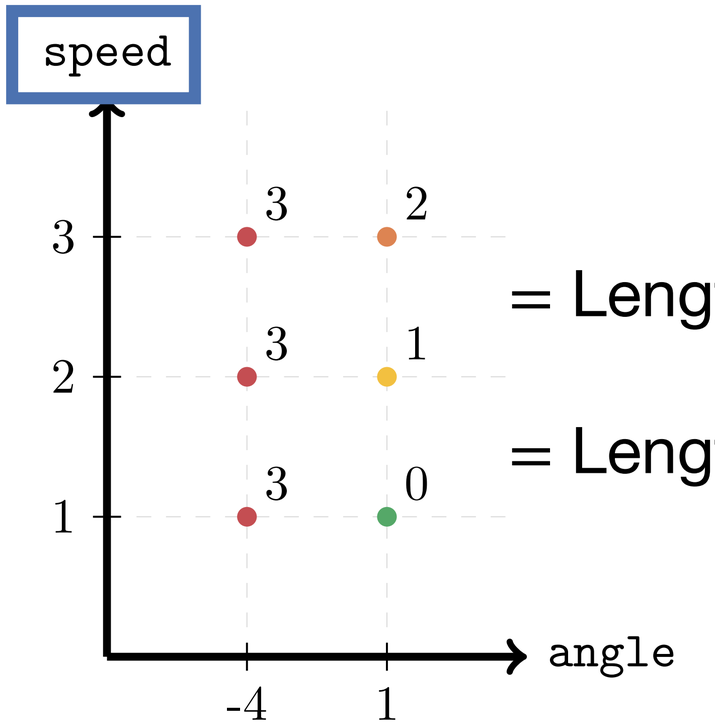
$= \text{Length}(\{3,3,3\}) = 0$



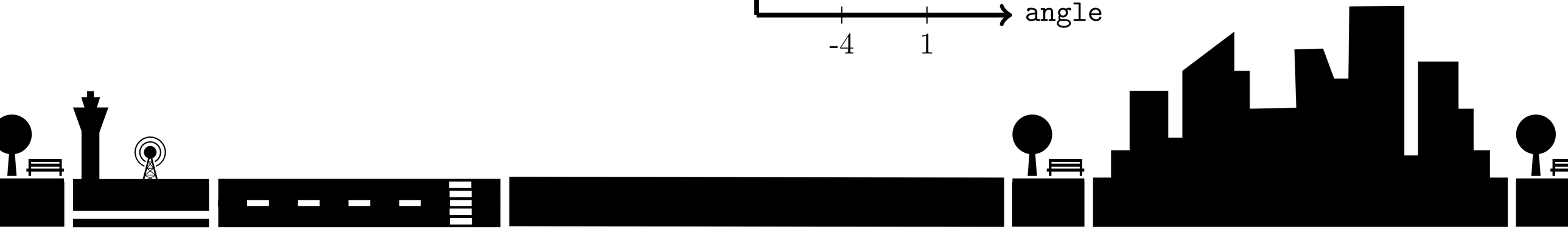
Goal: Quantify the impact of speed and angle on risk

Distance of *reachable outcomes*

RANGE



$$\left.\begin{array}{l} = \text{Length}(\{0,1,2\}) = 2 \\ = \text{Length}(\{3,3,3\}) = 0 \end{array}\right\} \max = 2$$



ENS | PSL Inria

Goal: Quantify the impact of `speed` and `angle` on `risk`

Distance of *reachable outcomes*

Number of *reachable outcomes*

	RANGE	OUTCOMES
angle	3	2
speed	2	3

Automatic & Sound Static Analysis
by Abstract Interpretation

	RANGE	OUTCOMES
angle	3	2
speed	2	3

Automatic & Sound Static Analysis
by Abstract Interpretation

Find k such that

	RANGE	OUTCOMES
angle	$3 \leq k$	$2 \leq k$
speed	$2 \leq k$	$3 \leq k$

Automatic & Sound Static Analysis
by Abstract Interpretation

Find k such that

	RANGE	OUTCOMES
angle	$3 \leq k$	$2 \leq k$
speed	$2 \leq k$	$3 \leq k$

Smallest k permitted by the abstraction!

Automatic & Sound Static Analysis
by Abstract Interpretation

Find k such that

	RANGE	OUTCOMES
angle	$3 \leq k$	$2 \leq k$
speed	$2 \leq k$	$3 \leq k$

Smallest k permitted by the abstraction!

1. Output Buckets

Automatic & Sound Static Analysis
by Abstract Interpretation

Find k such that

	RANGE	OUTCOMES
angle	$3 \leq k$	$2 \leq k$
speed	$2 \leq k$	$3 \leq k$

Smallest k permitted by the abstraction!

1. Output Buckets
2. Backward Abstract Analysis

Automatic & Sound Static Analysis
by Abstract Interpretation

Find k such that

	RANGE	OUTCOMES
angle	$3 \leq k$	$2 \leq k$
speed	$2 \leq k$	$3 \leq k$

Smallest k permitted by the abstraction!

1. Output Buckets
2. Backward Abstract Analysis
3. Abstract Implementations of RANGE and OUTCOMES

Automatic & Sound Static Analysis
by Abstract Interpretation

Find k such that

	RANGE	OUTCOMES
angle	$3 \leq k$	$2 \leq k$
speed	$2 \leq k$	$3 \leq k$

Smallest k permitted by the abstraction!

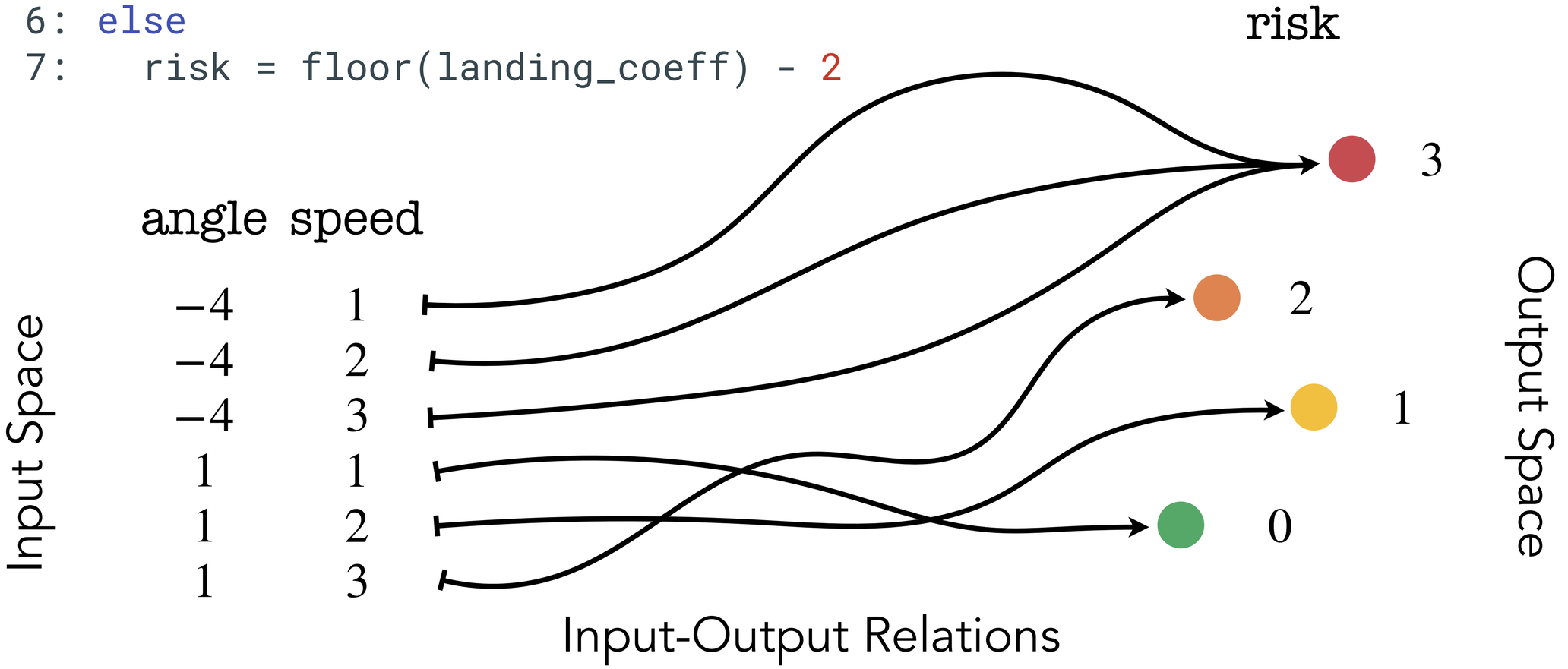
1. Output Buckets
2. Backward Abstract Analysis
3. Abstract Implementations of RANGE and OUTCOMES

RANGE$^\natural$ and OUTCOMES$^\natural$

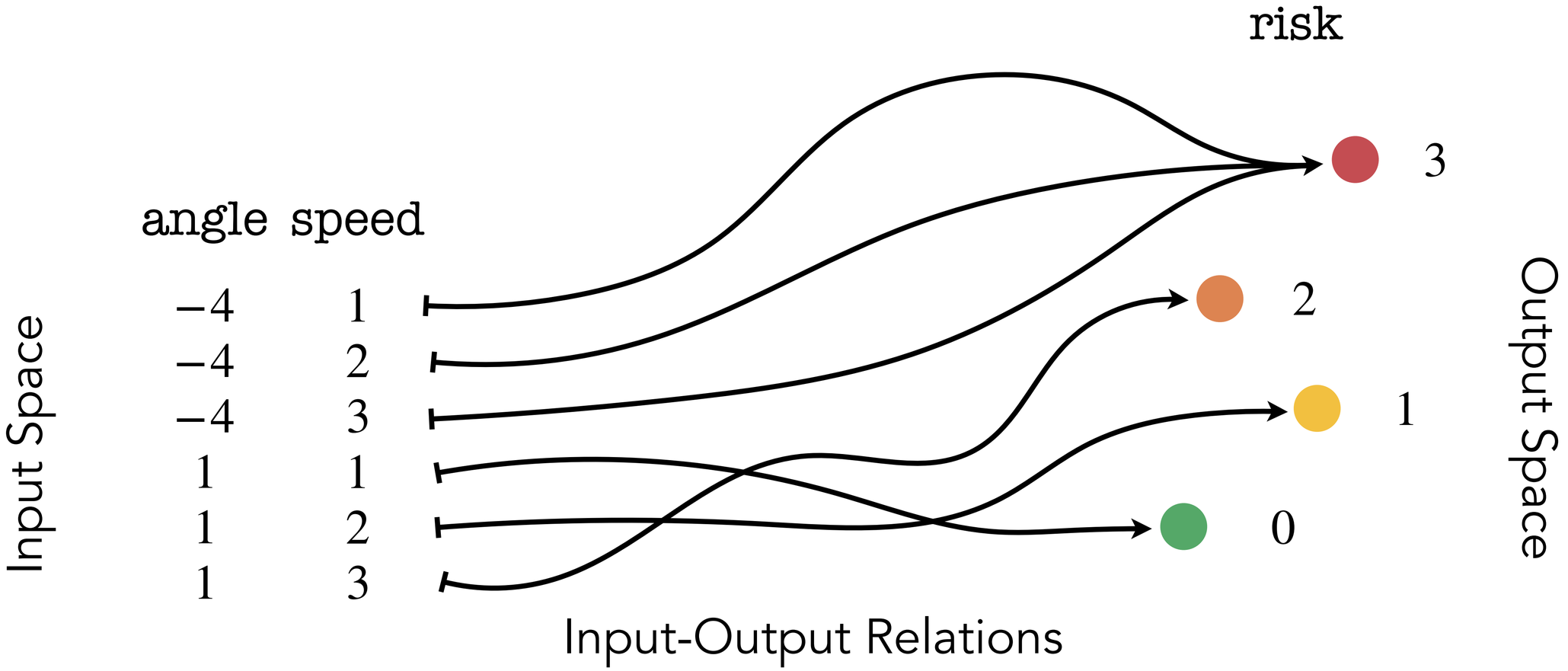
Denis Mazzucato et al. *Quantitative Input Usage Static Analysis*, NFM 2024

ENS | PSL | Inria

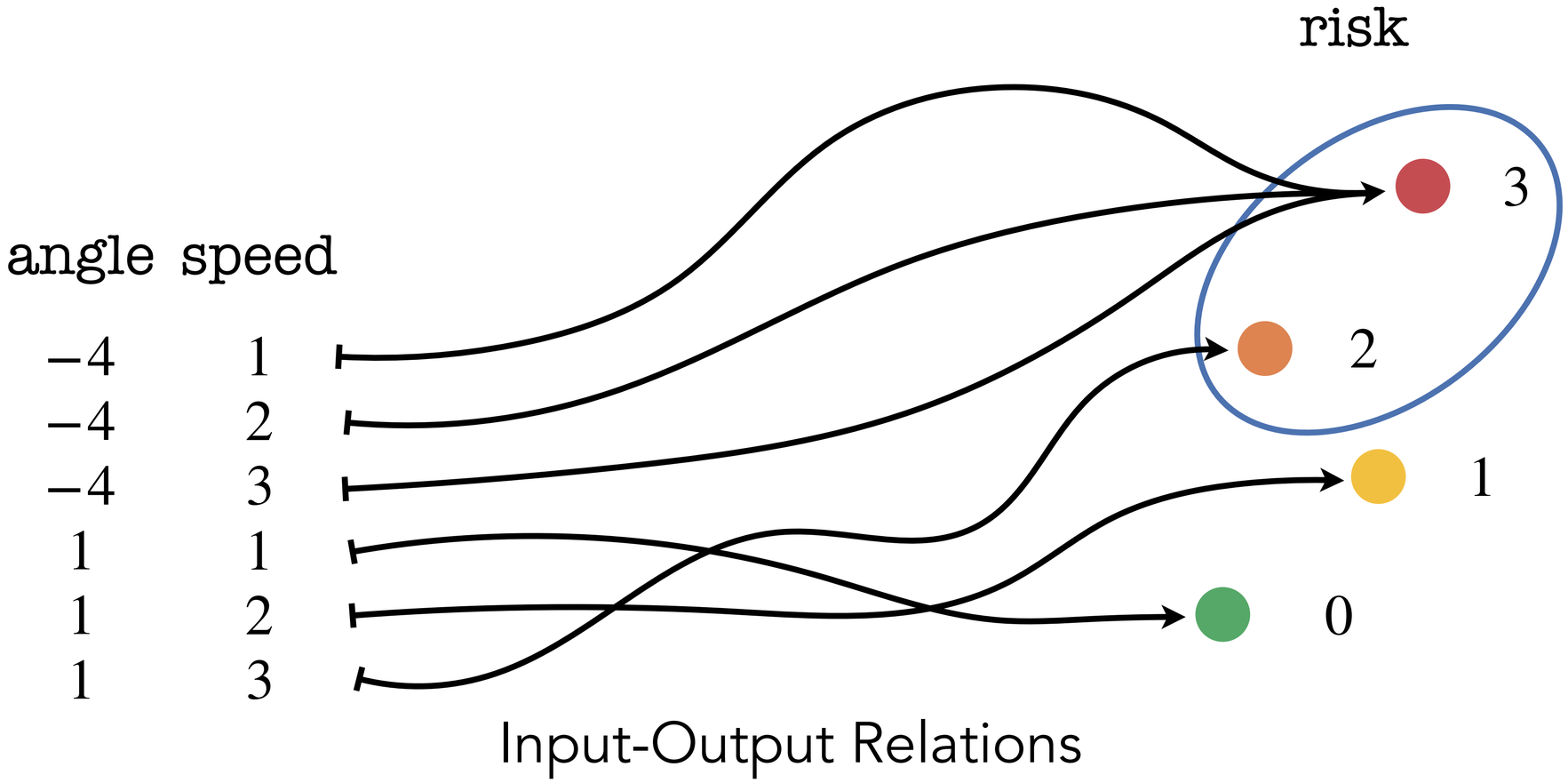
```
1: landing_coeff = abs(angle) + speed
2: if landing_coeff < 2 then
3:   risk = 0
4: else if landing_coeff > 5 then
5:   risk = 3
6: else
7:   risk = floor(landing_coeff) - 2
```



Intuition: OUTCOMES for the variable **angle**

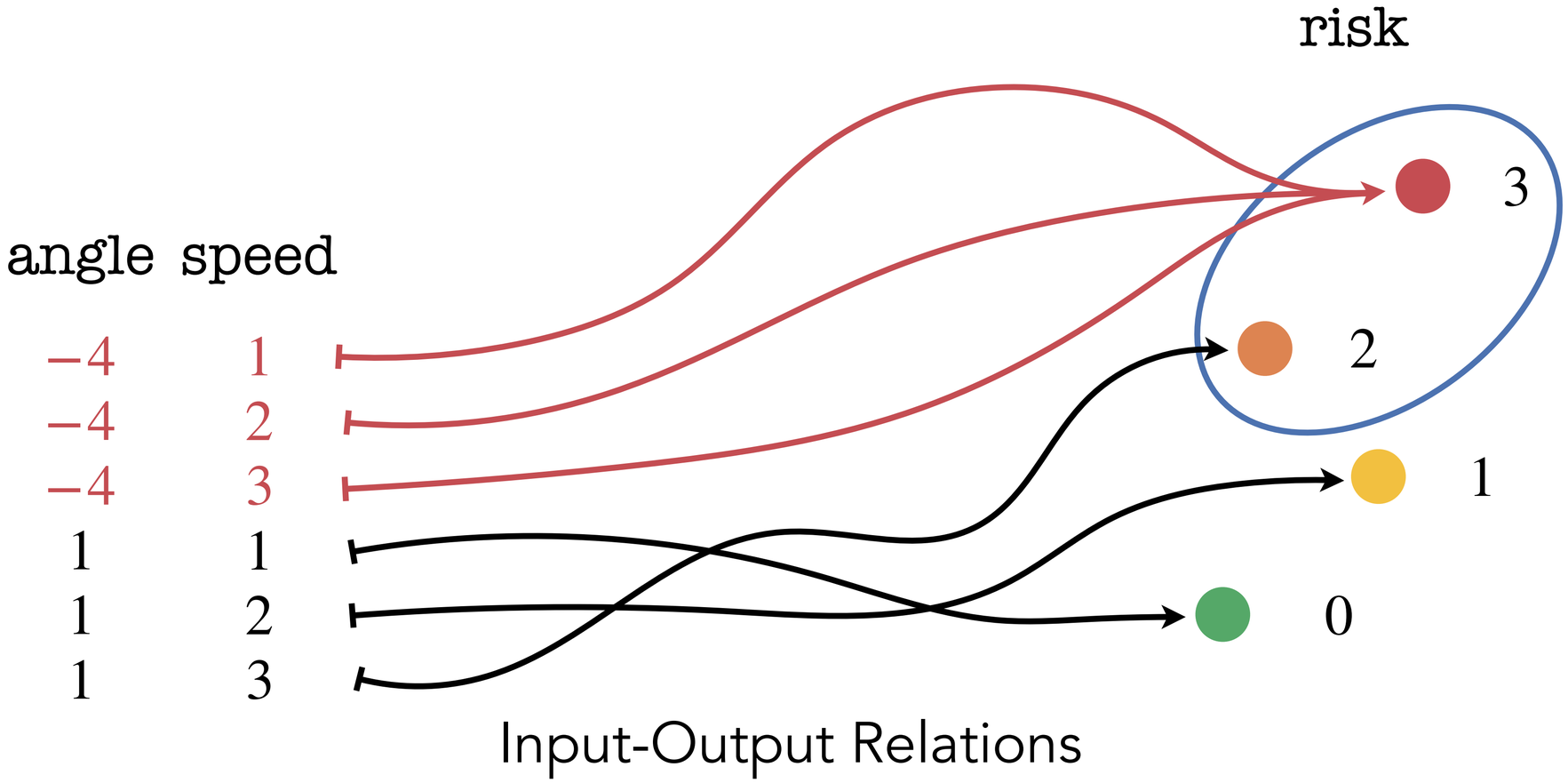


Intuition: OUTCOMES for the variable **angle**

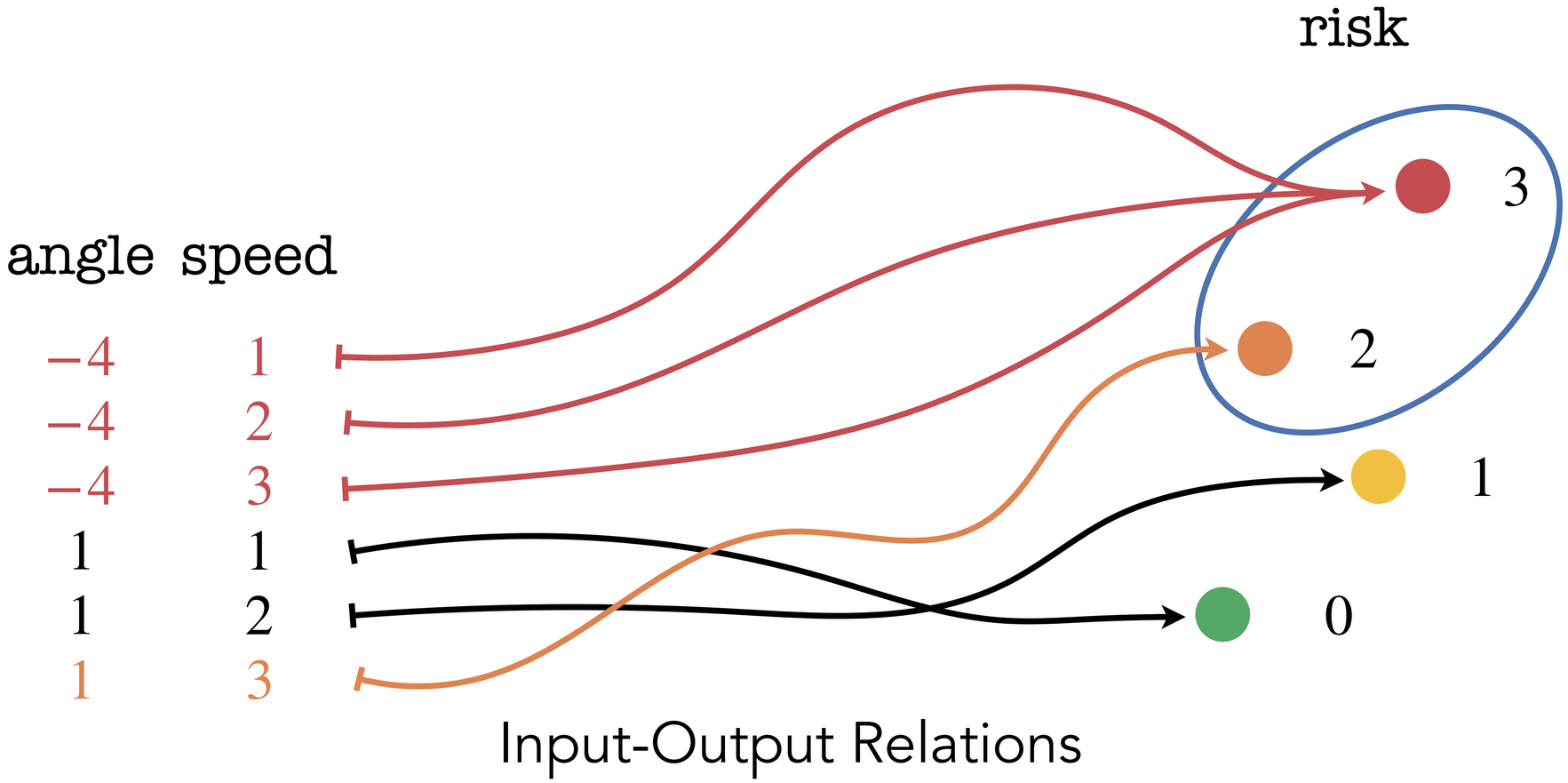


Input-Output Relations

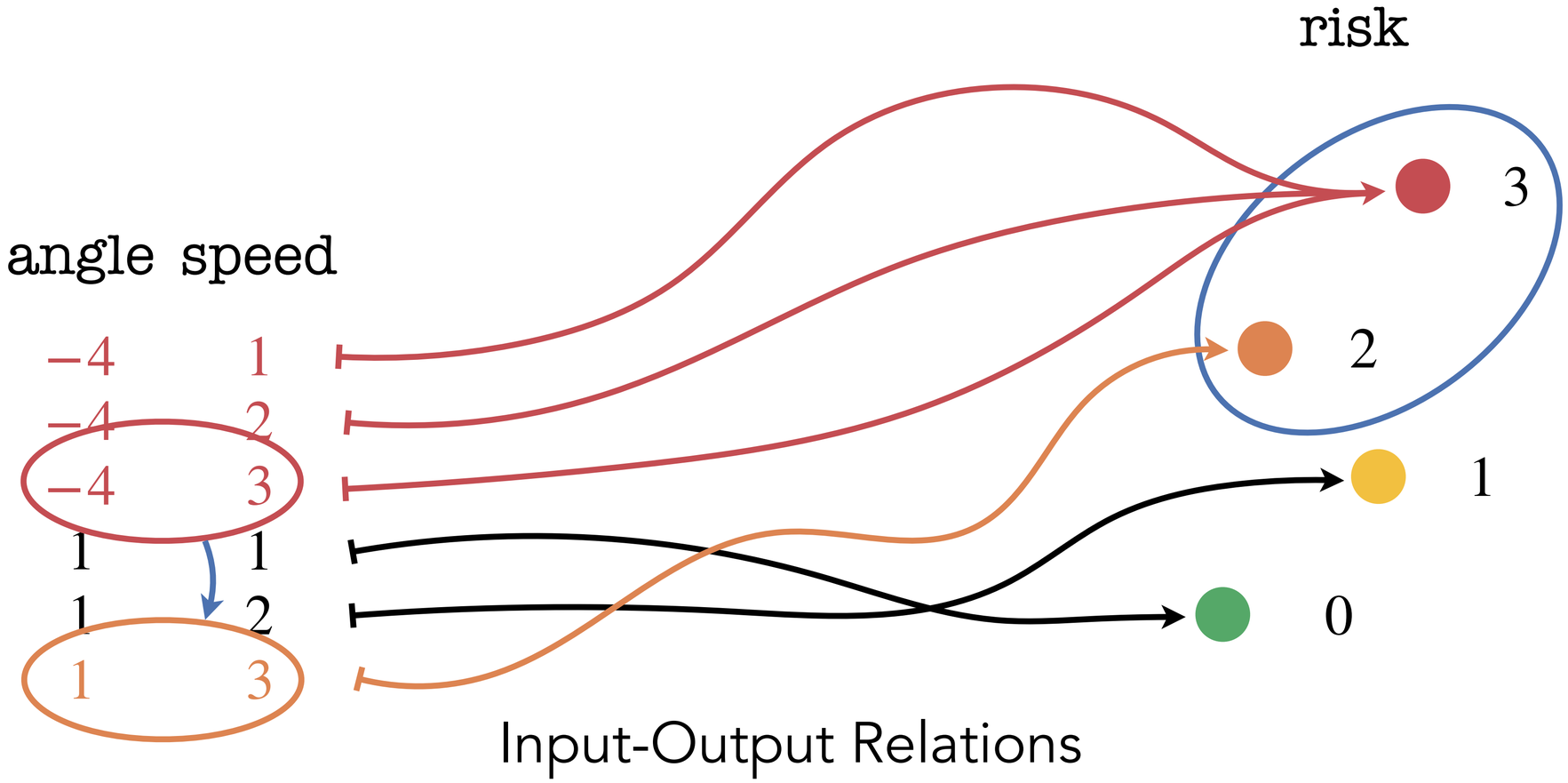
Intuition: OUTCOMES for the variable **angle**



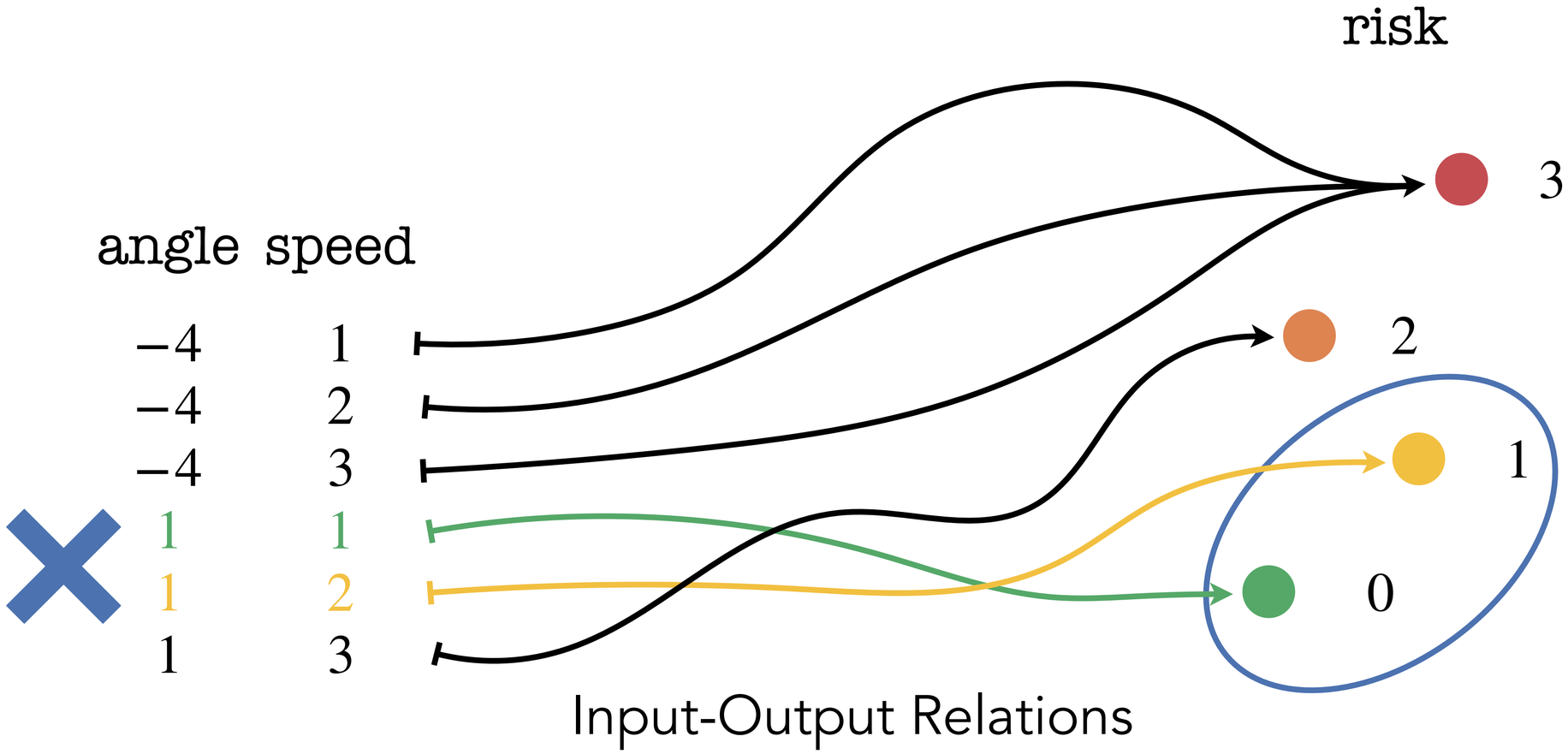
Intuition: OUTCOMES for the variable **angle**



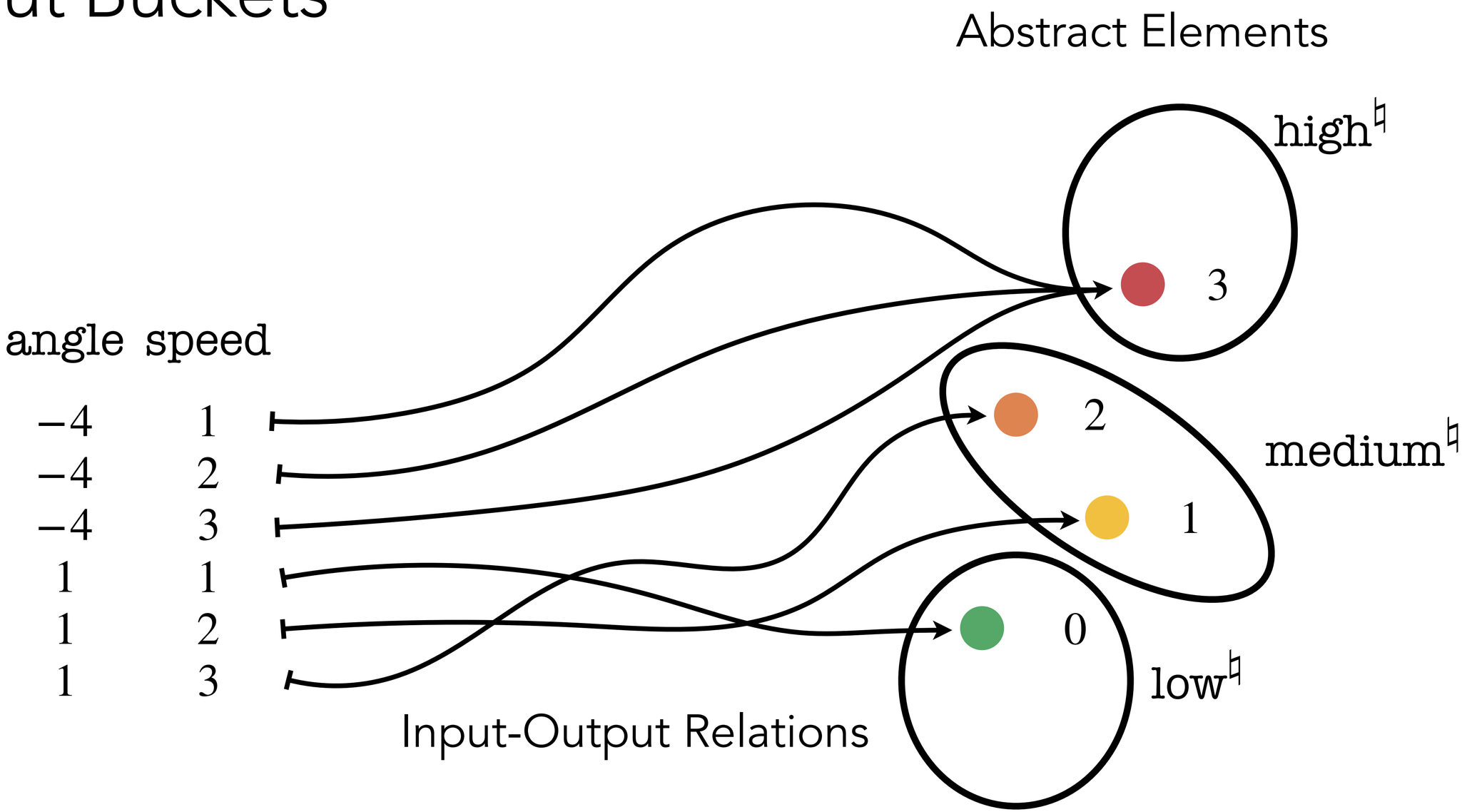
Intuition: OUTCOMES for the variable **angle**



Intuition: OUTCOMES for the variable **angle**



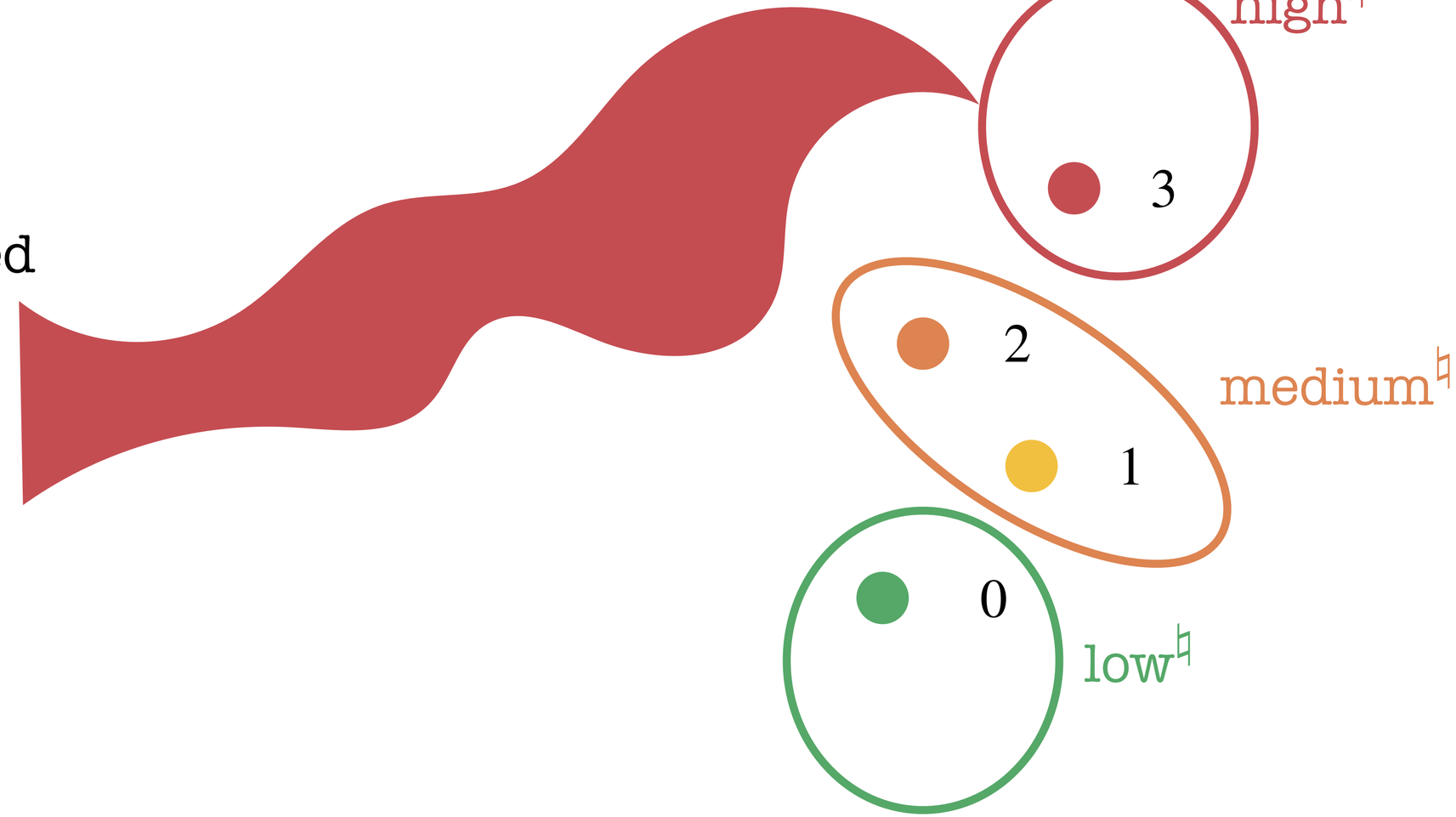
1) Output Buckets



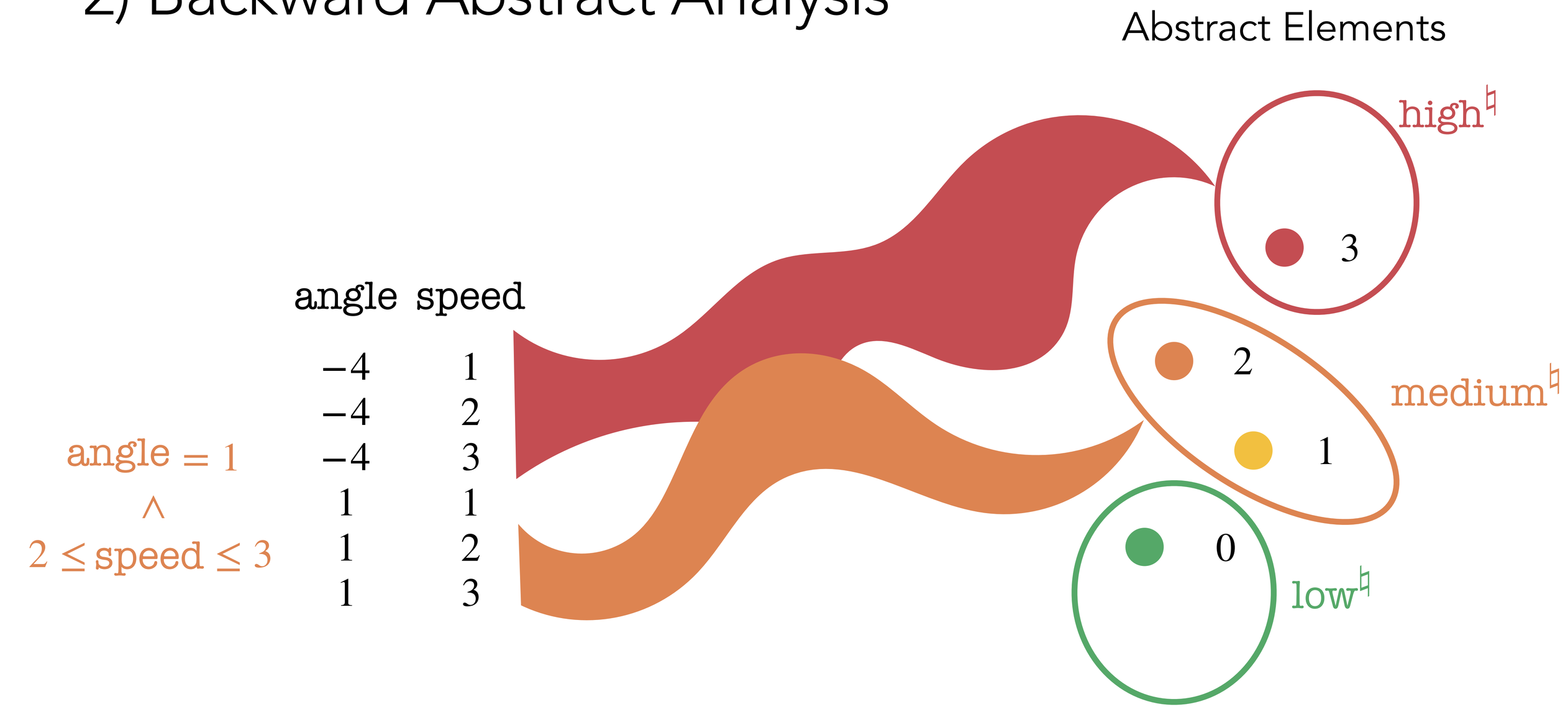
2) Backward Abstract Analysis

$\text{angle} = -4$
$\wedge$
$1 \leq \text{speed} \leq 3$

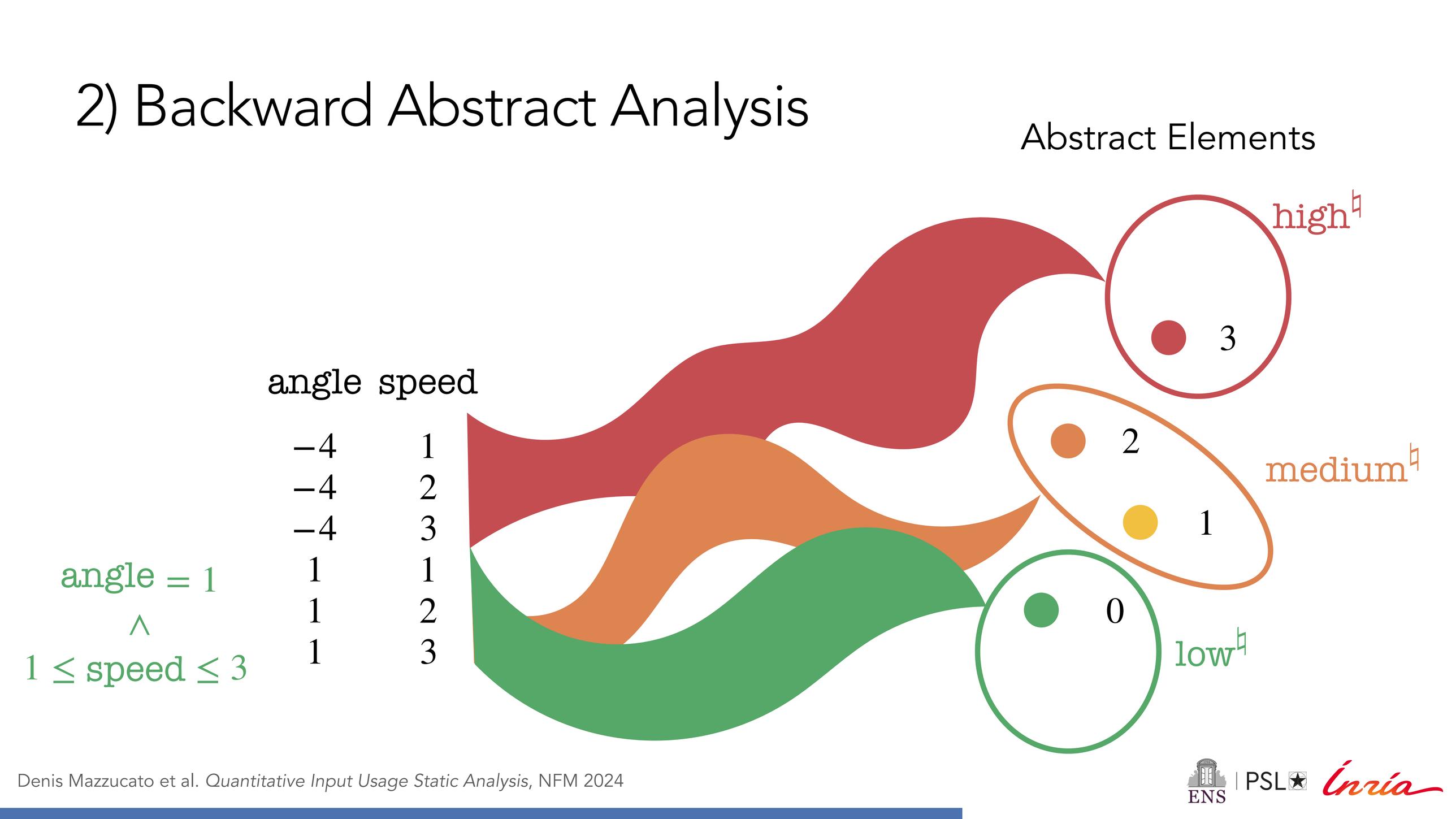
angle	speed
−4	1
−4	2
−4	3
1	1
1	2
1	3



2) Backward Abstract Analysis



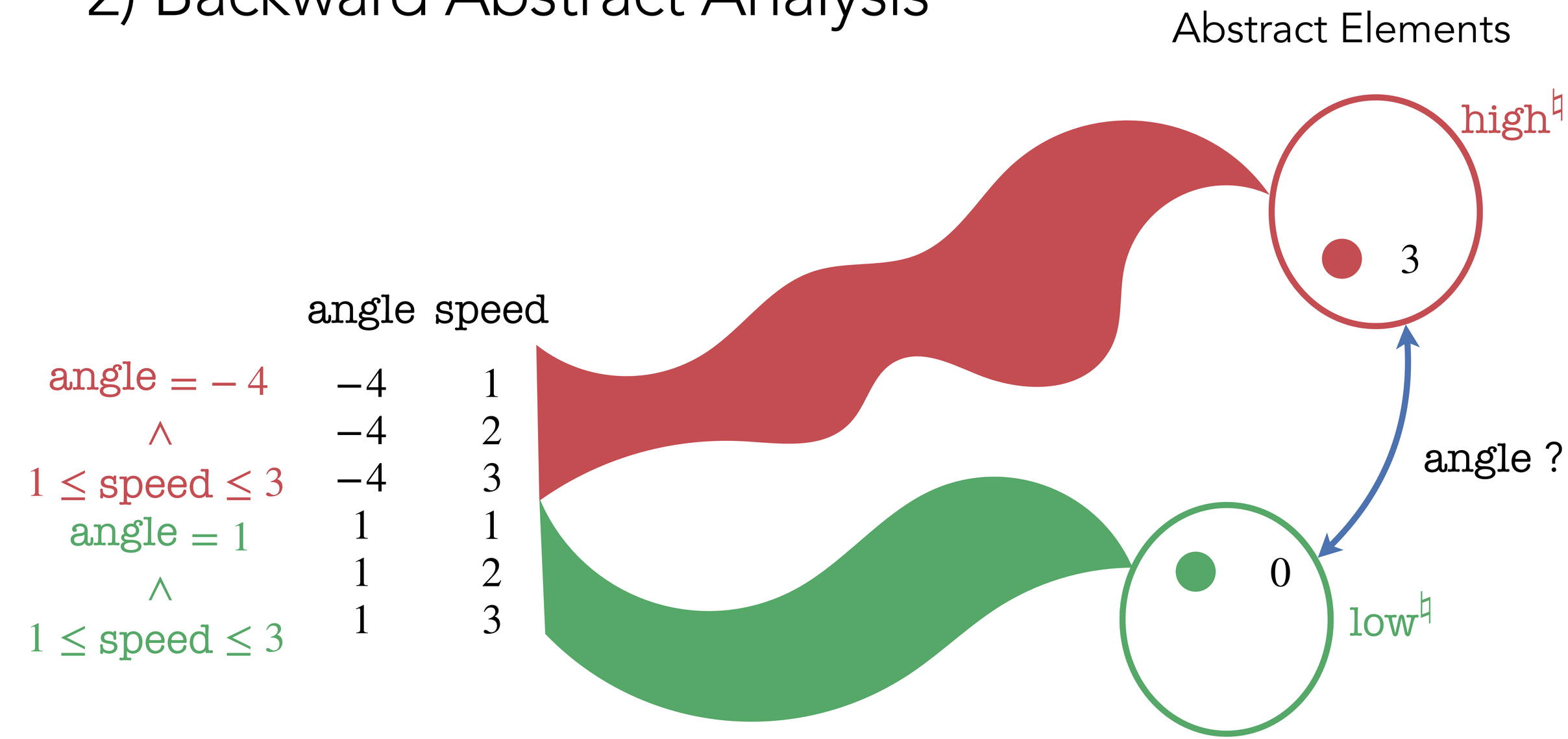
2) Backward Abstract Analysis

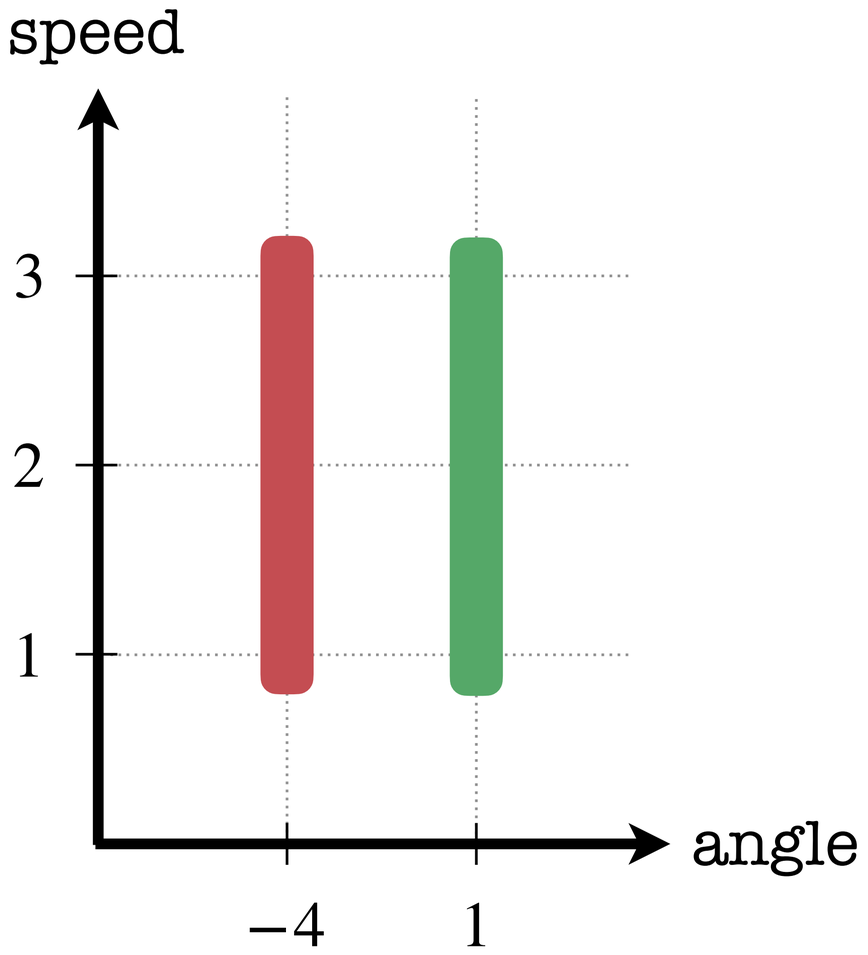


Denis Mazzucato et al. *Quantitative Input Usage Static Analysis*, NFM 2024

ENS | PSL Inria

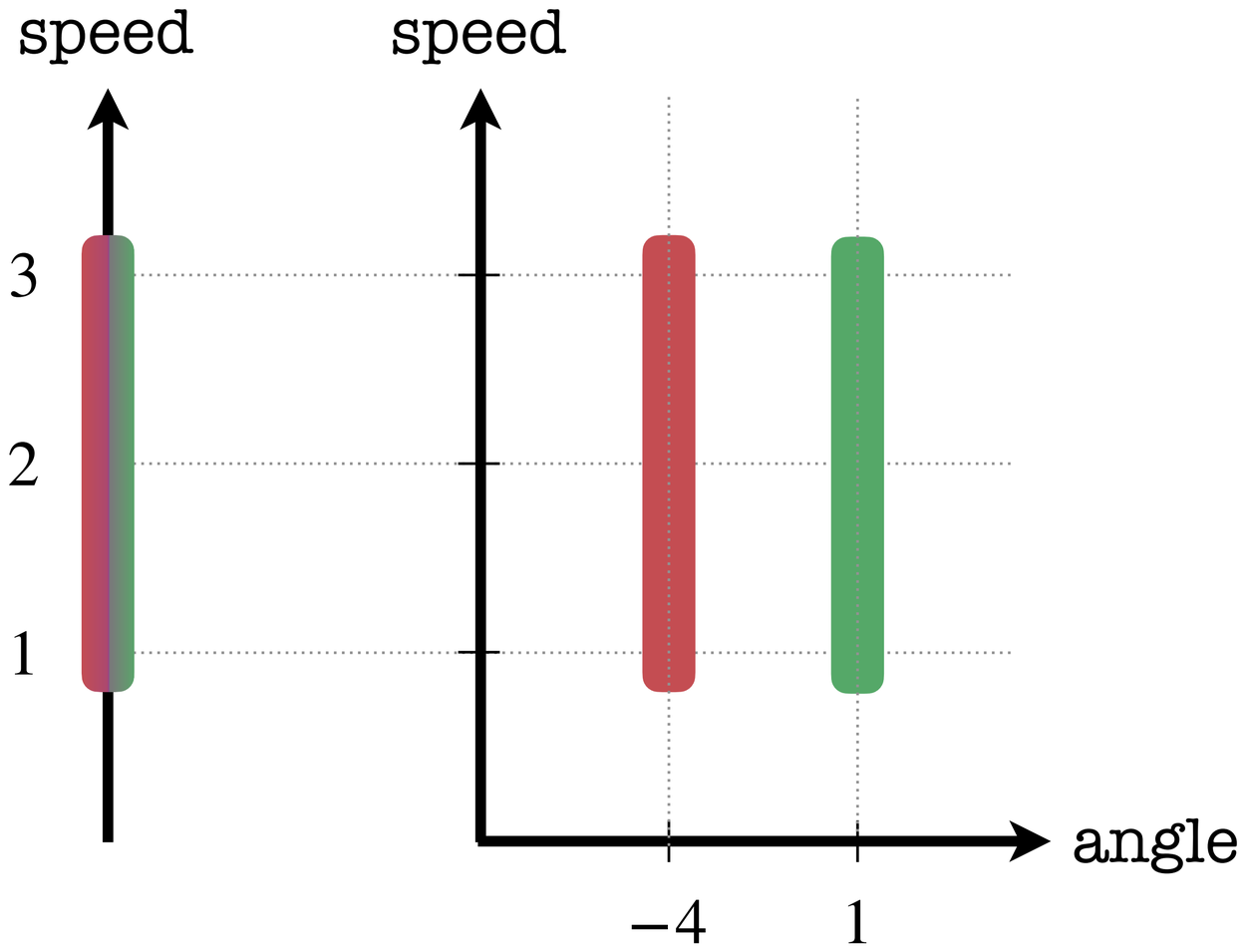
2) Backward Abstract Analysis





$$\text{angle} = -4 \;\wedge\; 1 \leq \text{speed} \leq 3$$

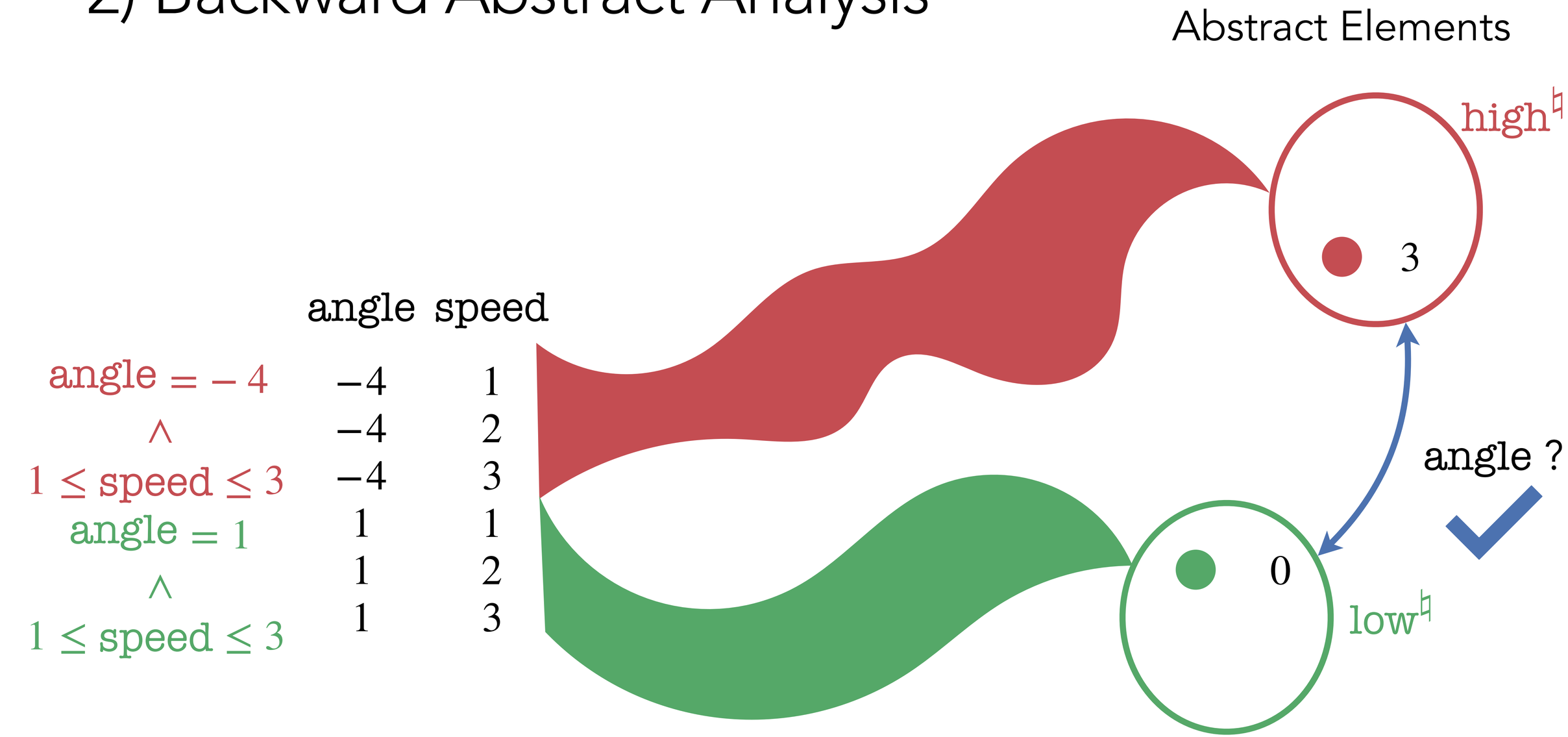
$$\text{angle} = 1 \;\wedge\; 1 \leq \text{speed} \leq 3$$



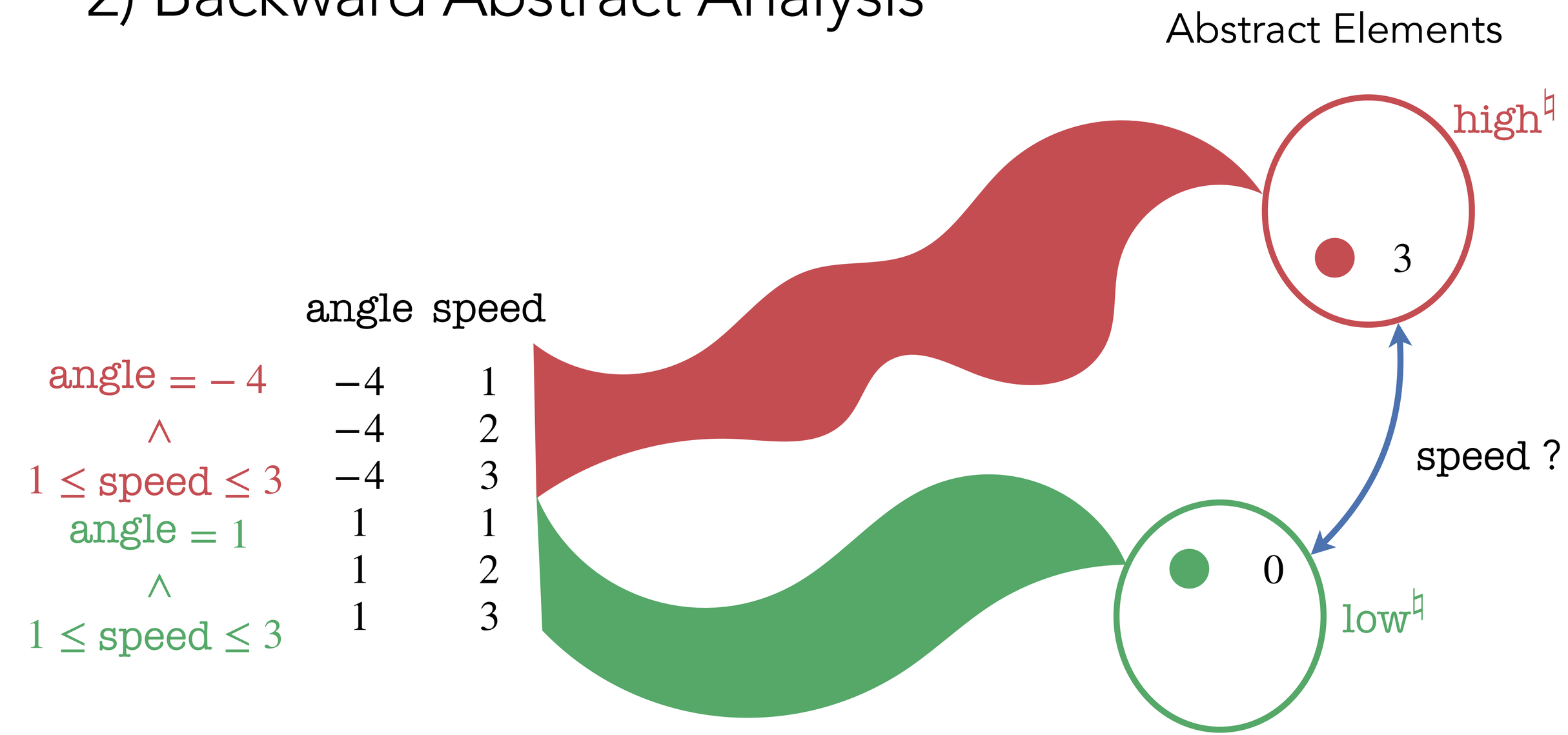
$$\text{angle} = -4 \wedge 1 \leq \text{speed} \leq 3$$

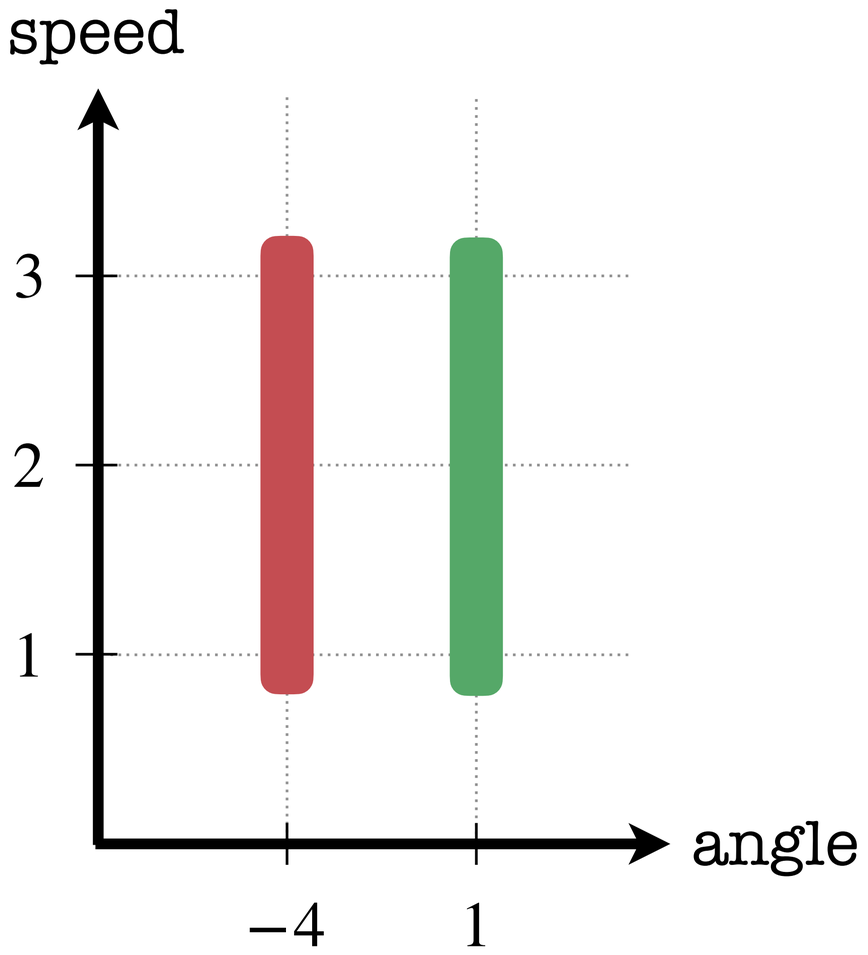
$$\text{angle} = 1 \wedge 1 \leq \text{speed} \leq 3$$

2) Backward Abstract Analysis



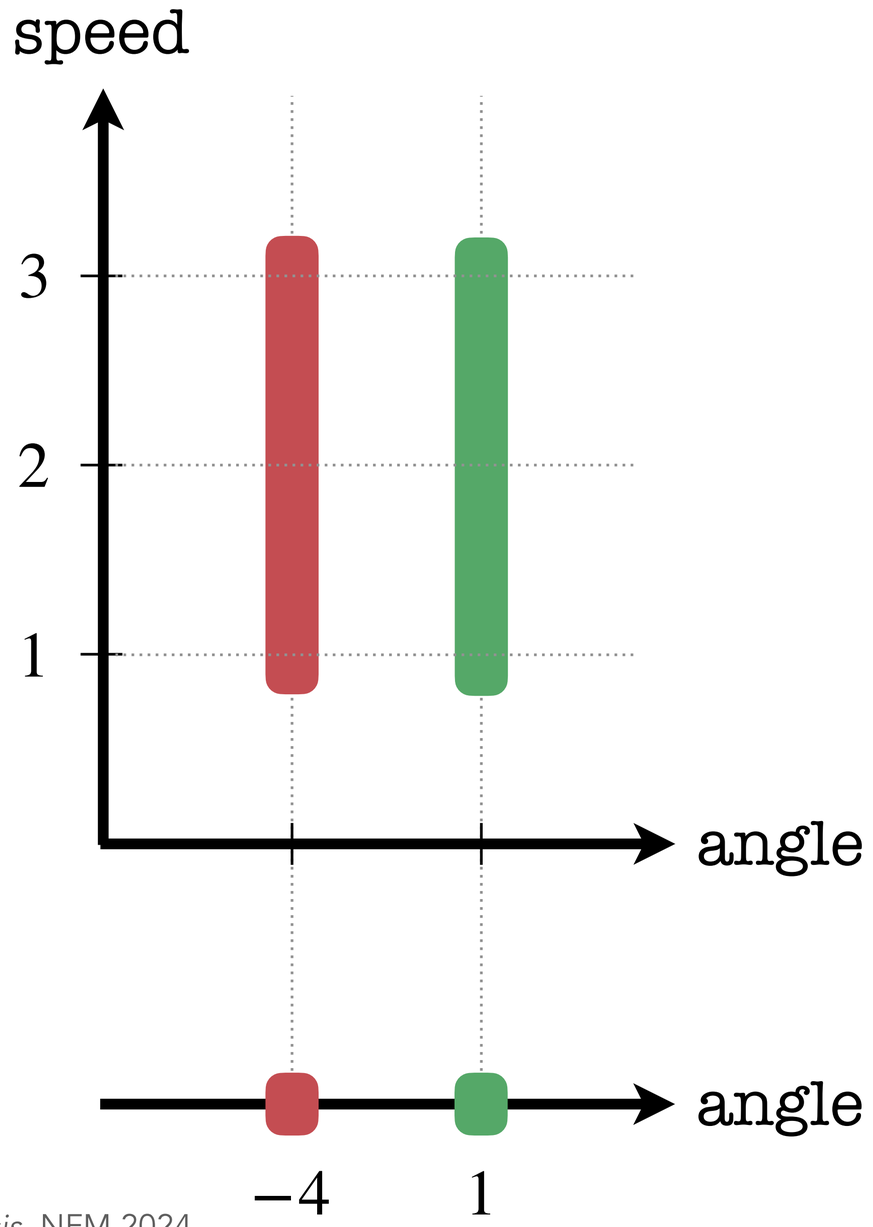
2) Backward Abstract Analysis





$$\text{angle} = -4 \;\wedge\; 1 \leq \text{speed} \leq 3$$

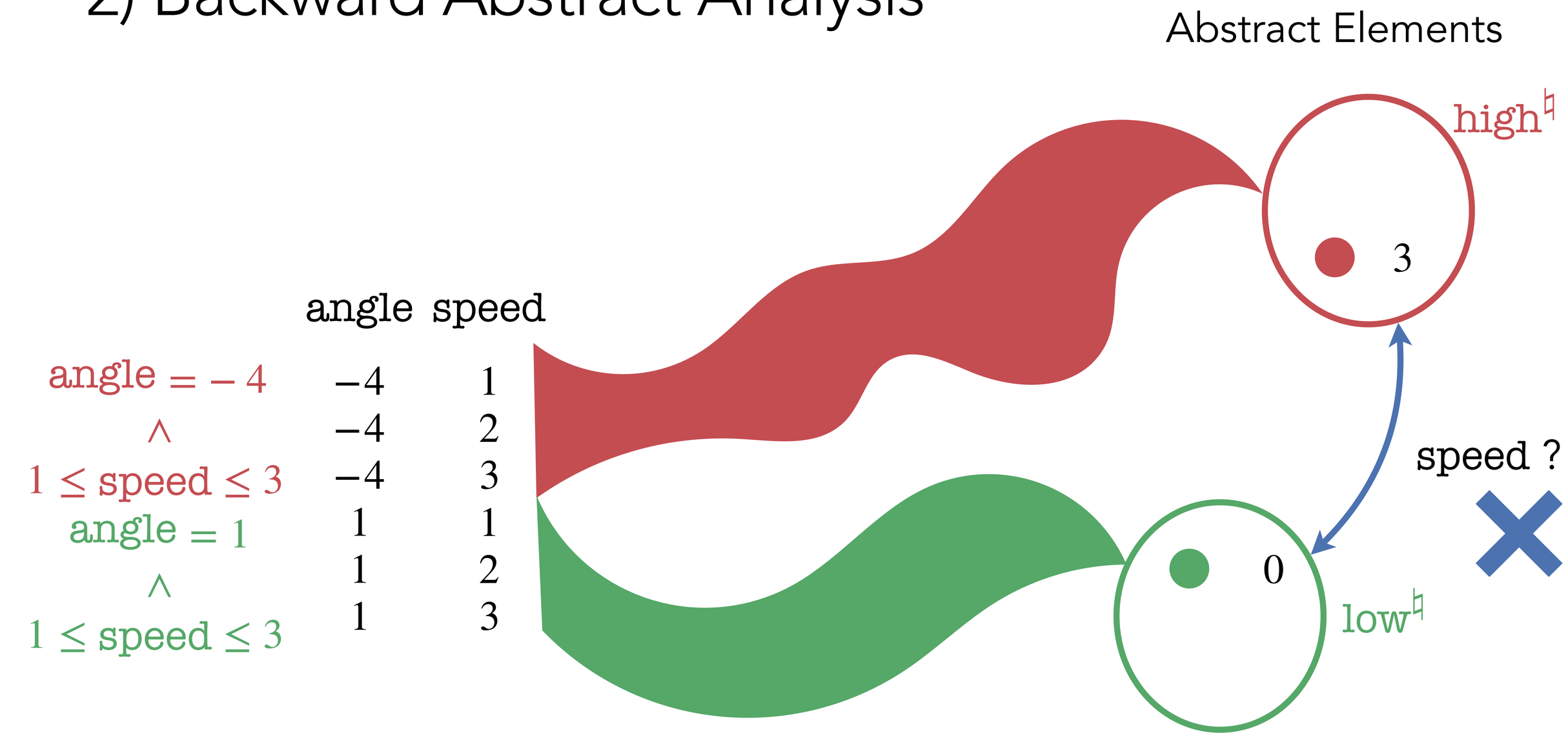
$$\text{angle} = 1 \;\wedge\; 1 \leq \text{speed} \leq 3$$



$$\text{angle} = -4 \wedge 1 \leq \text{speed} \leq 3$$

$$\text{angle} = 1 \wedge 1 \leq \text{speed} \leq 3$$

2) Backward Abstract Analysis

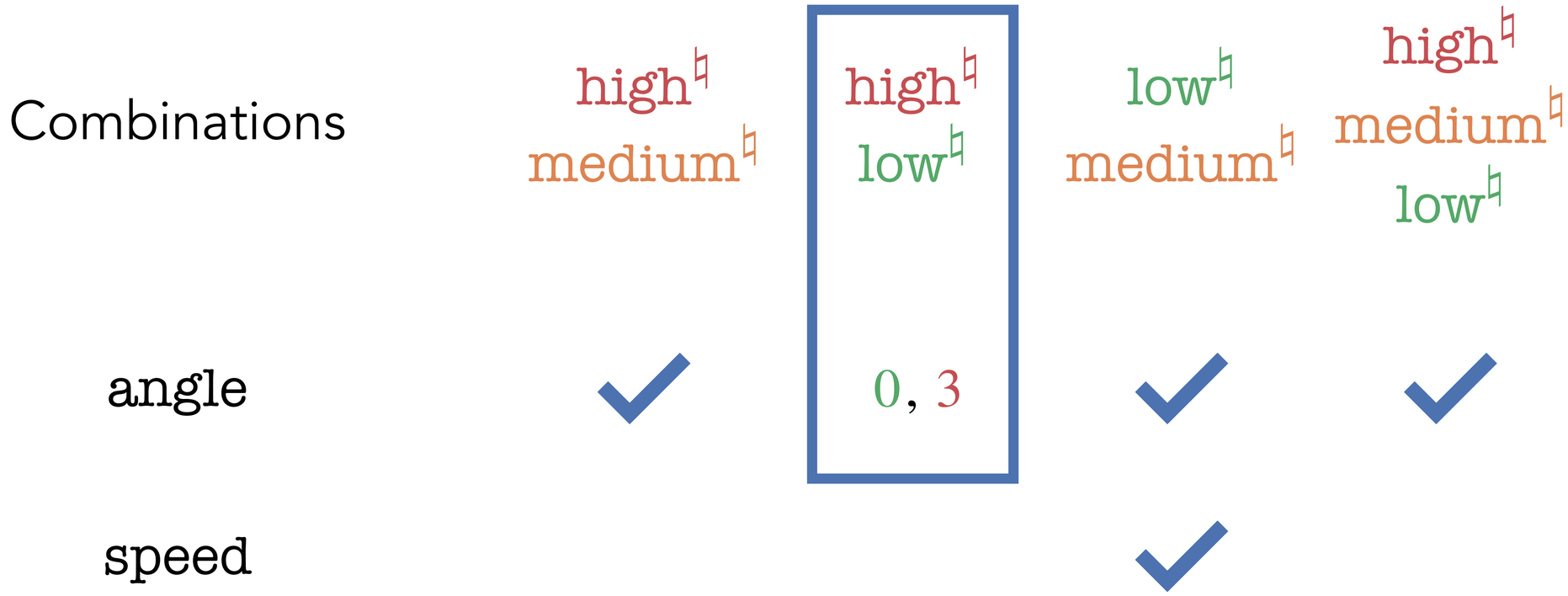


3) Abstract Implementation of Impact Definitions

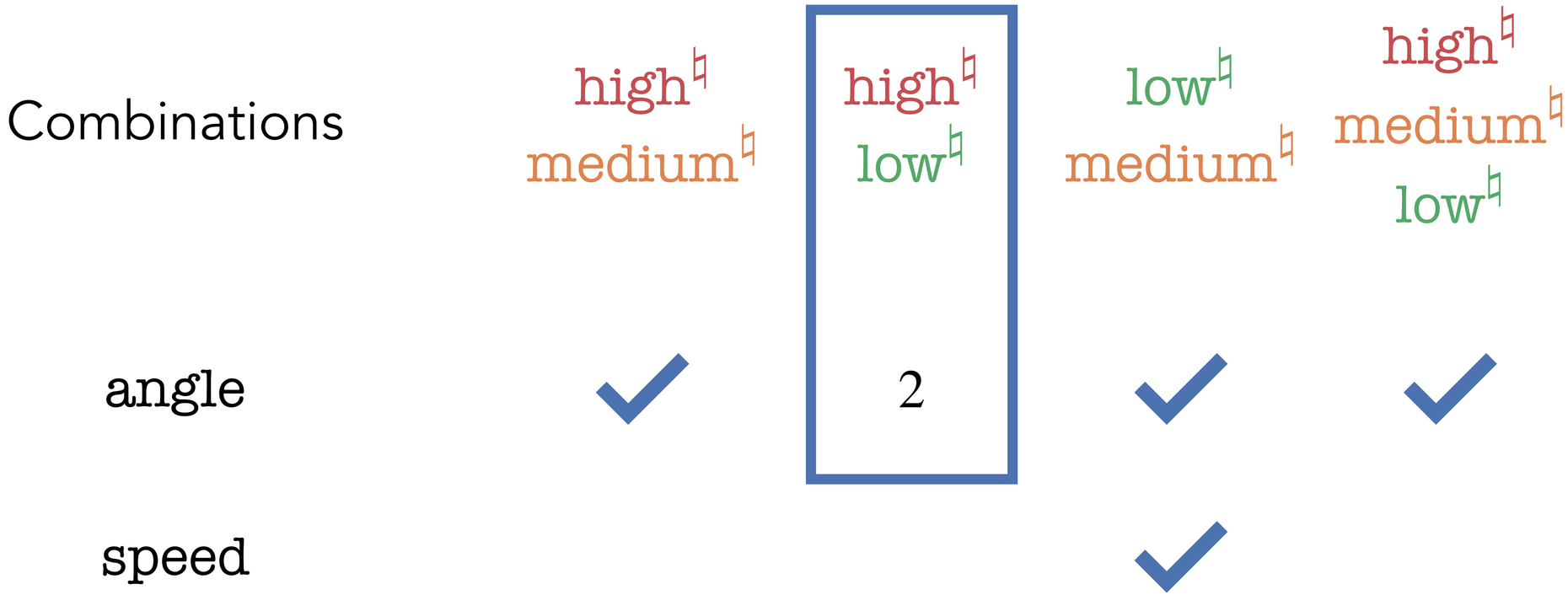
Combinations	high♮ medium♮	high♮ low♮	low♮ medium♮	high♮ medium♮ low♮
angle	✓	✓	✓	✓
speed			✓	

Denis Mazzucato et al. *Quantitative Input Usage Static Analysis*, NFM 2024

Abstract Impact Outcomes♮



Abstract Impact Outcomes♮



Abstract Impact Outcomes♮

Combinations	high♮ medium♮	high♮ low♮	low♮ medium♮	high♮ medium♮ low♮
angle	1,2, 3	2	✓	✓
speed			✓	

Abstract Impact Outcomes♮

Combinations	high♮ medium♮	high♮ low♮	low♮ medium♮	high♮ medium♮ low♮
angle	3	2	✓	✓
speed			✓	

Abstract Impact Outcomes♮

Combinations	high♮ medium♮	high♮ low♮	low♮ medium♮	high♮ medium♮ low♮
angle	3	2	3	4
speed			3	

Abstract Impact Outcomes♮

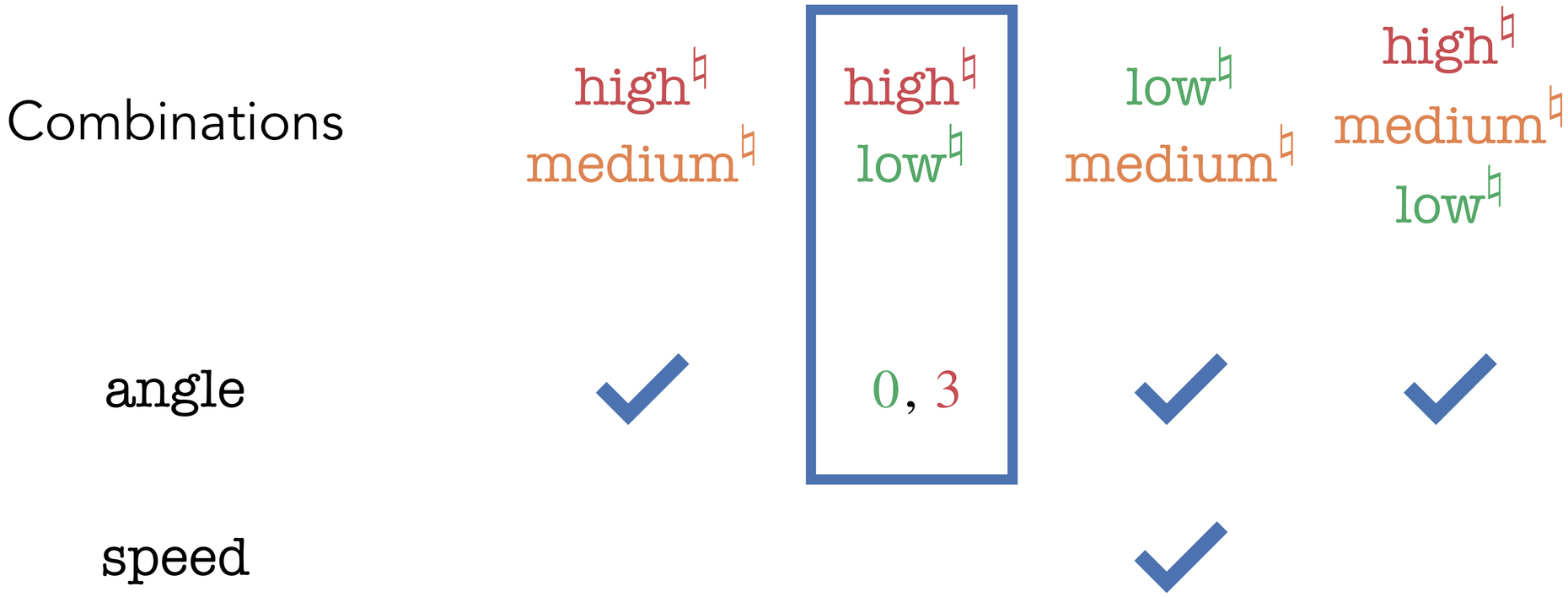
Combinations	high♮ medium♮	high♮ low♮	low♮ medium♮	high♮ medium♮ low♮	
angle	3	2	3	4	$\Longrightarrow$ 4
speed			3		$\Longrightarrow$ 3

Abstract Impact RANGE♭

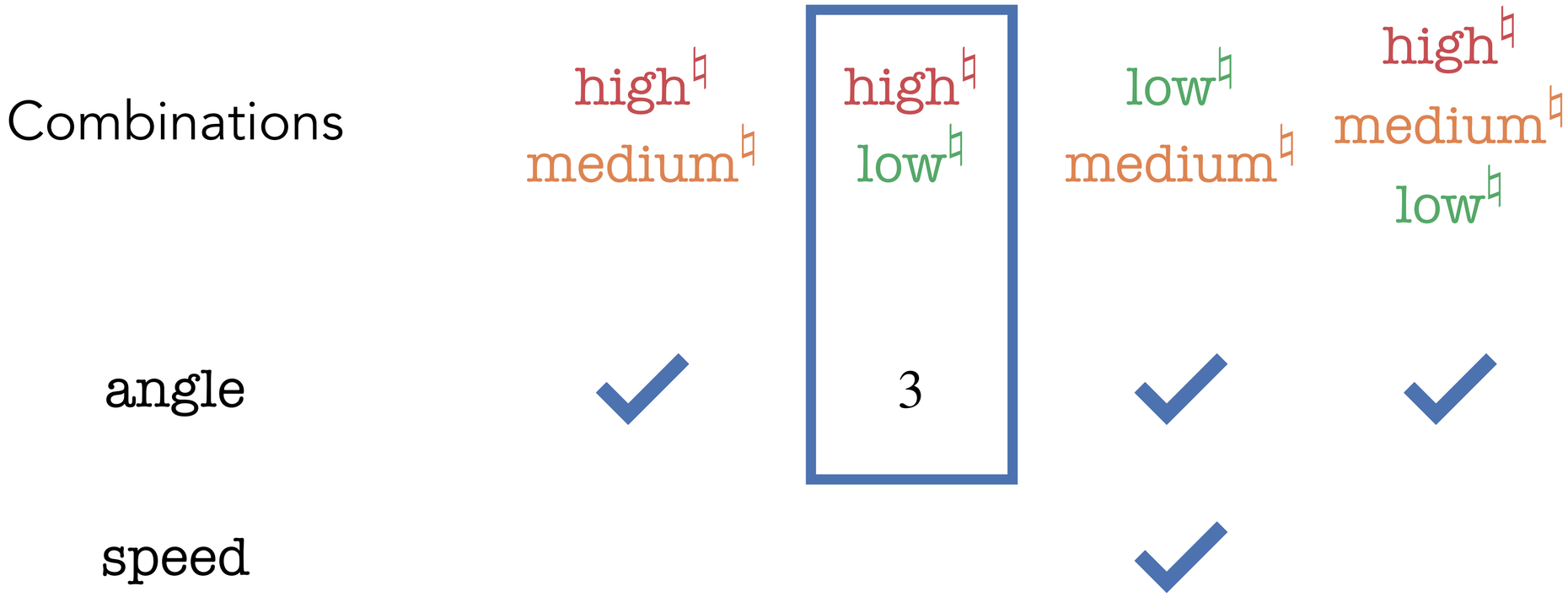
Combinations	high♭ medium♭	high♭ low♭	low♭ medium♭	high♭ medium♭ low♭
angle	✓	✓	✓	✓
speed			✓	

Denis Mazzucato et al. *Quantitative Input Usage Static Analysis*, NFM 2024

Abstract Impact RANGE♭



Abstract Impact RANGE♭



Abstract Impact RANGE♭

Combinations	high♭ medium♭	high♭ low♭	low♭ medium♭	high♭ medium♭ low♭
angle	1,2, 3	3	✓	✓
speed			✓	

Abstract Impact RANGE♭

Combinations	high♭ medium♭	high♭ low♭	low♭ medium♭	high♭ medium♭ low♭
angle	2	3	✓	✓
speed			✓	

Abstract Impact RANGE♭

Combinations	high♭ medium♭	high♭ low♭	low♭ medium♭	high♭ medium♭ low♭
angle	2	3	2	3
speed			2	

Abstract Impact RANGE♭

Combinations	high♭ medium♭	high♭ low♭	low♭ medium♭	high♭ medium♭ low♭	
angle	2	3	2	3	$\Longrightarrow$ 3
speed			2		$\Longrightarrow$ 2

Goal: Quantify the impact of `speed` and `angle` on `risk`

	Range	Outcomes
angle	3	2
speed	2	3

Goal: Quantify the impact of speed and angle on risk

	Range	Outcomes	Range$^\flat$	Outcomes$^\flat$
angle	3	2	3	4
speed	2	3	2	3

Source of Imprecision

Abstraction of the Backward Analysis

Source of Imprecision

Abstraction of the Backward Analysis

Choice of the Output Buckets

Use Case: Reinhart and Rogoff

C. M. Reinhart and K. S. Rogoff. Growth in a time of debt.
American Economic Review 2010.

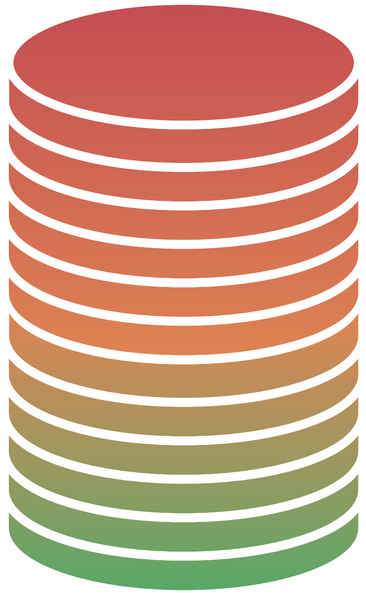
```
 1: def mean_growth_rate_60_90(
 2:     portugal1, portugal2, portugal3,
 3:     norway1,
 4:     uk1, uk2, uk3, uk4,
 5:     usa1, usa2, usa3):
 6:   portugal_avg = avg(portugal1, portugal2, portugal3)
 7:   norway_avg = avg(norway1)
 8:   uk_avg = avg(uk1, uk2, uk3, uk4)
 9:   usa_avg = avg(usa1, usa2, usa3)
10:   return avg(portugal_avg, norway_avg, uk_avg, usa_avg)
```

Use Case: Reinhart and Rogoff

C. M. Reinhart and K. S. Rogoff. Growth in a time of debt.
American Economic Review 2010.

```
 1: def mean_growth_rate_60_90(
 2:     portugal1, portugal2, portugal3,
 3:     norway1,
 4:     uk1, uk2, uk3, uk4,
 5:     usa1, usa2, usa3):
 6:   portugal_avg = avg(portugal1, portugal2, portugal3)
 7:   norway_avg = avg(norway1)
 8:   uk_avg = avg(uk1, uk2, uk3, uk4)
 9:   usa_avg = avg(usa1, usa2, usa3)
10:   return avg(portugal_avg, norway_avg, uk_avg, usa_avg)
```

$\text{avg}^{\natural} = 20\,\%$

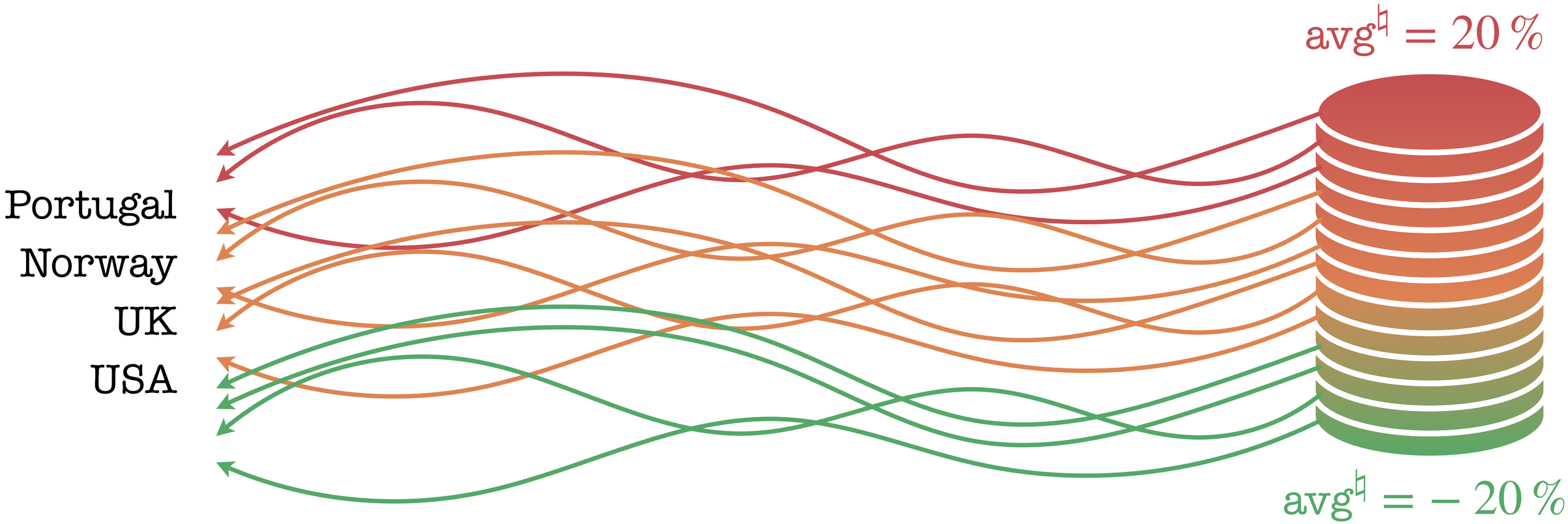


$\text{avg}^{\natural} = -20\,\%$

41 Output Buckets

Use Case: Reinhart and Rogoff

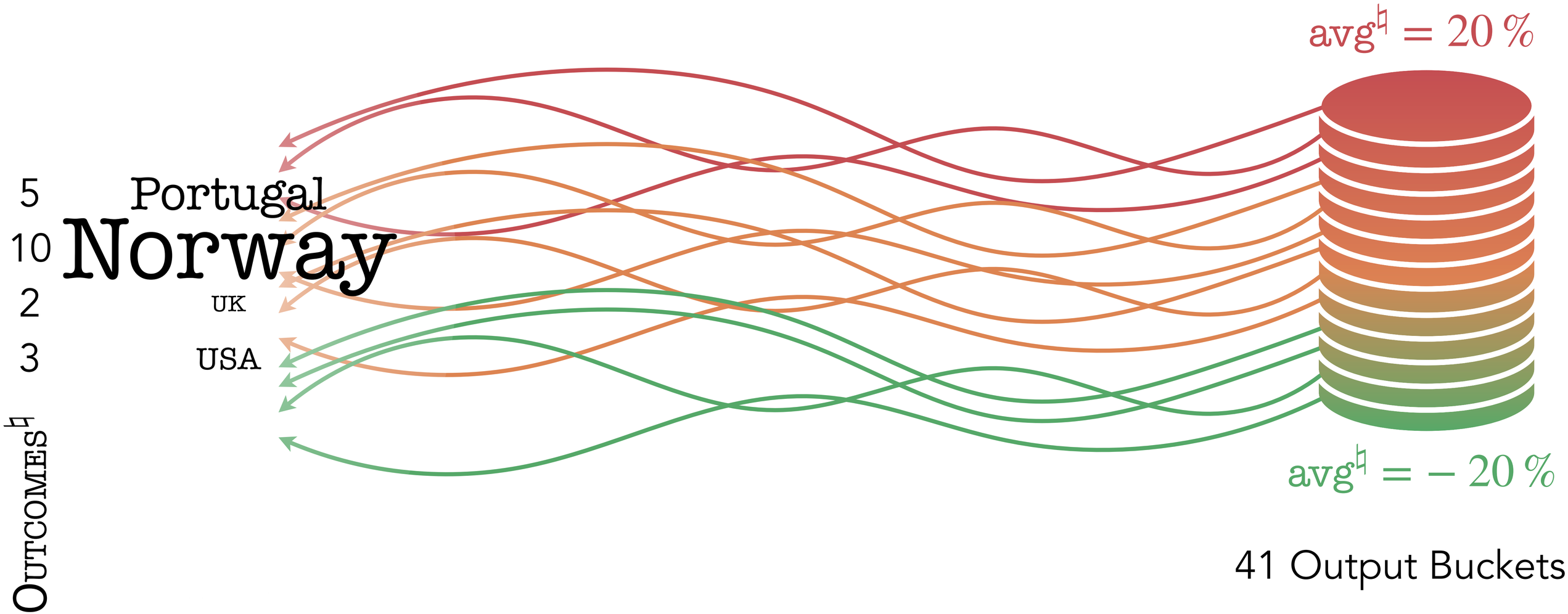
C. M. Reinhart and K. S. Rogoff. Growth in a time of debt.
American Economic Review 2010.



41 Output Buckets

Use Case: Reinhart and Rogoff

C. M. Reinhart and K. S. Rogoff. Growth in a time of debt.
American Economic Review 2010.



41 Output Buckets

ENS | PSL Inria

Use Case: Reinhart and Rogoff

C. M. Reinhart and K. S. Rogoff. Growth in a time of debt.
American Economic Review 2010.

```
 1: def mean_growth_rate_60_90(
 2:     portugal1, portugal2, portugal3,
 3:     norway1,
 4:     uk1, uk2, uk3, uk4,
 5:     usa1, usa2, usa3):
 6:   portugal_avg = avg(portugal1, portugal2, portugal3)
 7:   norway_avg = avg(norway1)
 8:   uk_avg = avg(uk1, uk2, uk3, uk4)
 9:   usa_avg = avg(usa1, usa2, usa3)
10:   return avg(portugal_avg, norway_avg, uk_avg, usa_avg)
```

Use Case: Reinhart and Rogoff

C. M. Reinhart and K. S. Rogoff. Growth in a time of debt. American Economic Review 2010.

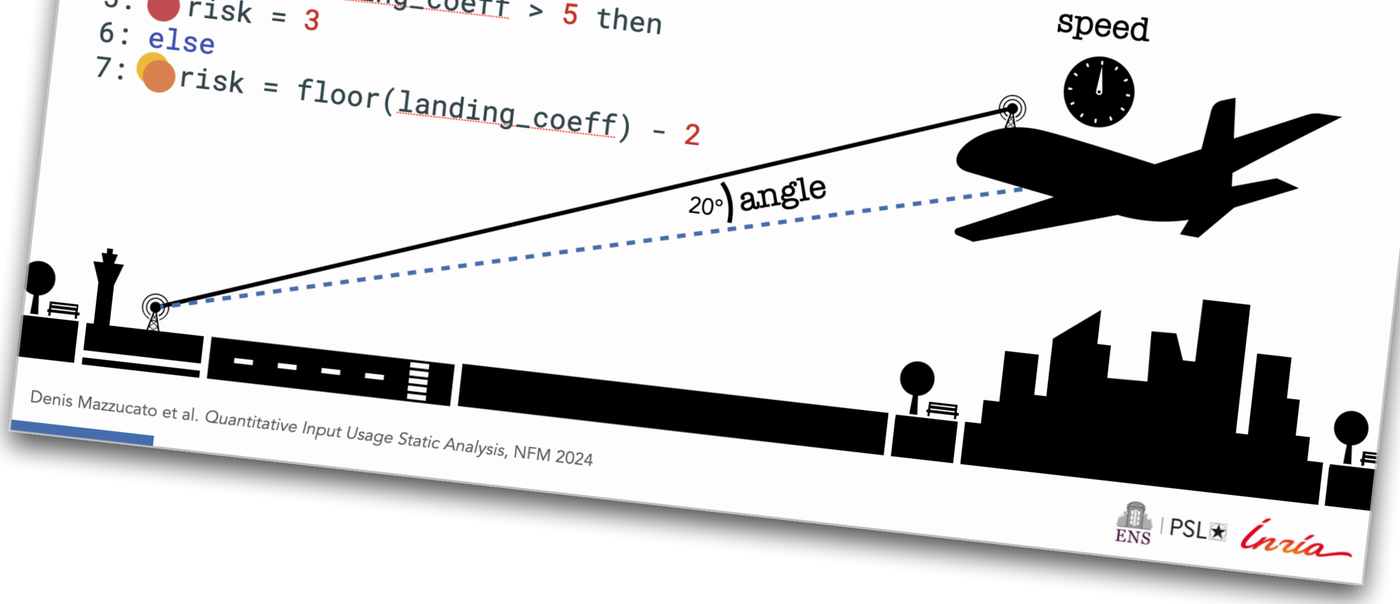
+1.7%

```
 1: def mean_growth_rate_60_90(
 2:     portugal1, portugal2, portugal3,
 3:     norway1,
 4:     uk1, uk2, uk3, uk4,
 5:     usa1, usa2, usa3):
 6:   portugal_avg = avg(portugal1, portugal2, portugal3)
 7:   norway_avg = avg(norway1)
 8:   uk_avg = avg(uk1, uk2, uk3, uk4)
 9:   usa_avg = avg(usa1, usa2, usa3)
10:   return avg(portugal_avg, norway_avg, uk_avg, usa_avg)
```

Conclusion

Goal: Quantify the impact of speed and angle on risk

```
1: landing_coeff = abs(angle) + speed
2: if landing_coeff < 2 then
3:   risk = 0
4: else if landing_coeff > 5 then
5:   risk = 3
6: else
7:   risk = floor(landing_coeff) - 2
```

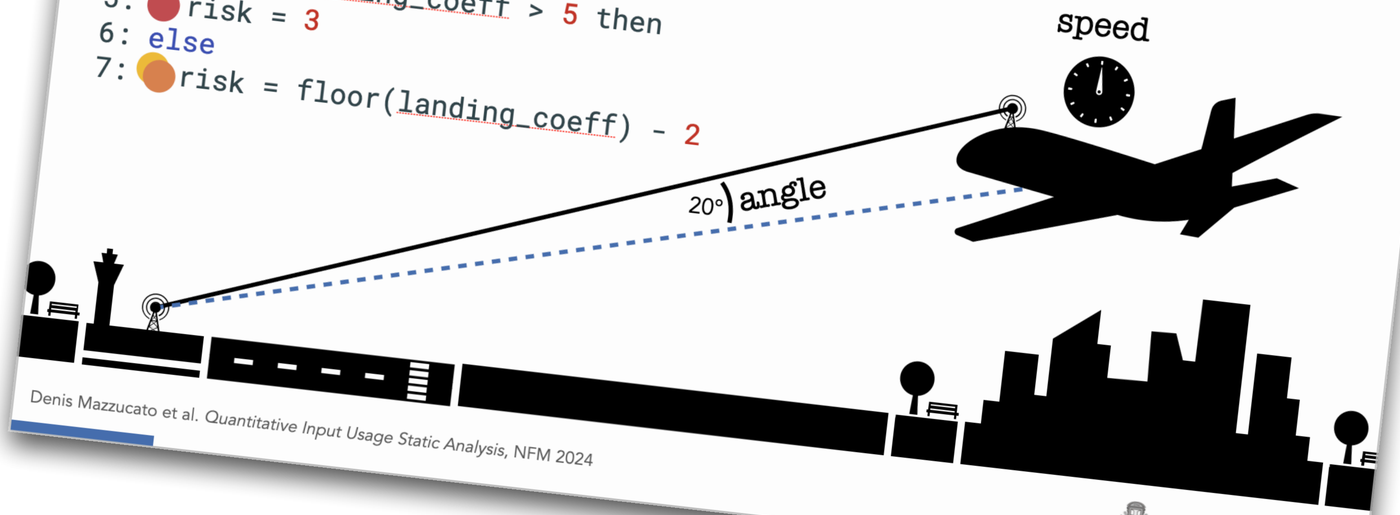


Denis Mazzucato et al. *Quantitative Input Usage Static Analysis*, NFM 2024

Conclusion

Goal: Quantify the impact of speed and angle on risk

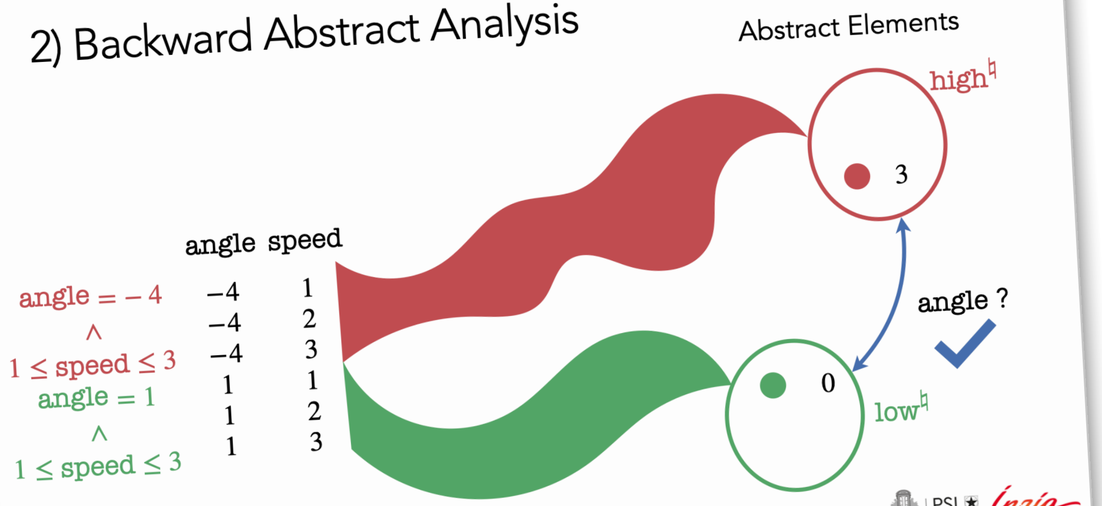
```
1: landing_coeff = abs(angle) + speed
2: if landing_coeff < 2 then
3:     risk = 0
4: else if landing_coeff > 5 then
5:     risk = 3
6: else
7:     risk = floor(landing_coeff) - 2
```



Denis Mazzucato et al. *Quantitative Input Usage Static Analysis*, NFM 2024

ENS | PSL | Inria

2) Backward Abstract Analysis



Denis Mazzucato et al. *Quantitative Input Usage Static Analysis*, NFM 2024

ENS | PSL | Inria

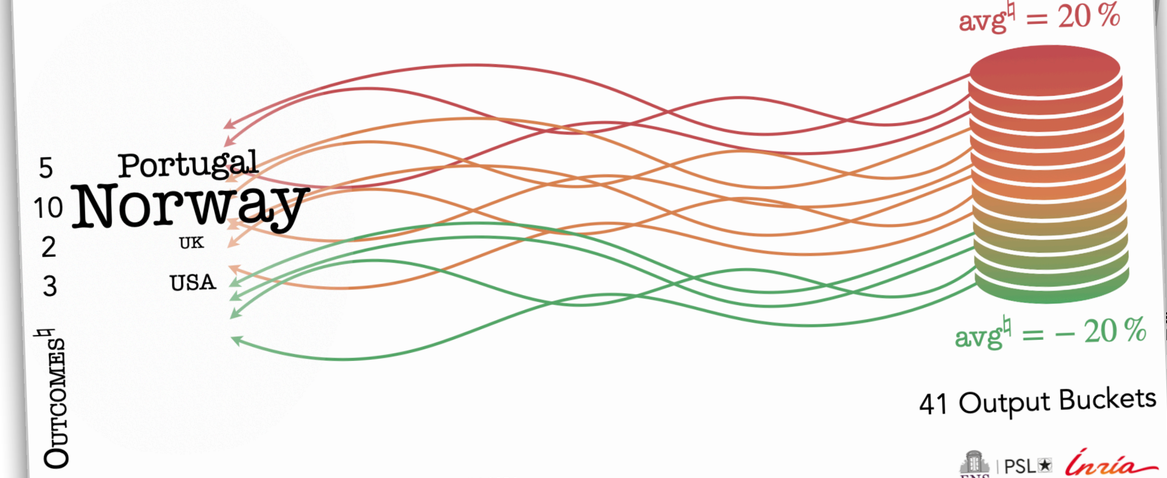
Denis Mazzucato et al. *Quantitative Input Usage Static Analysis*, NFM 2024

ENS | PSL | Inria

Conclusion

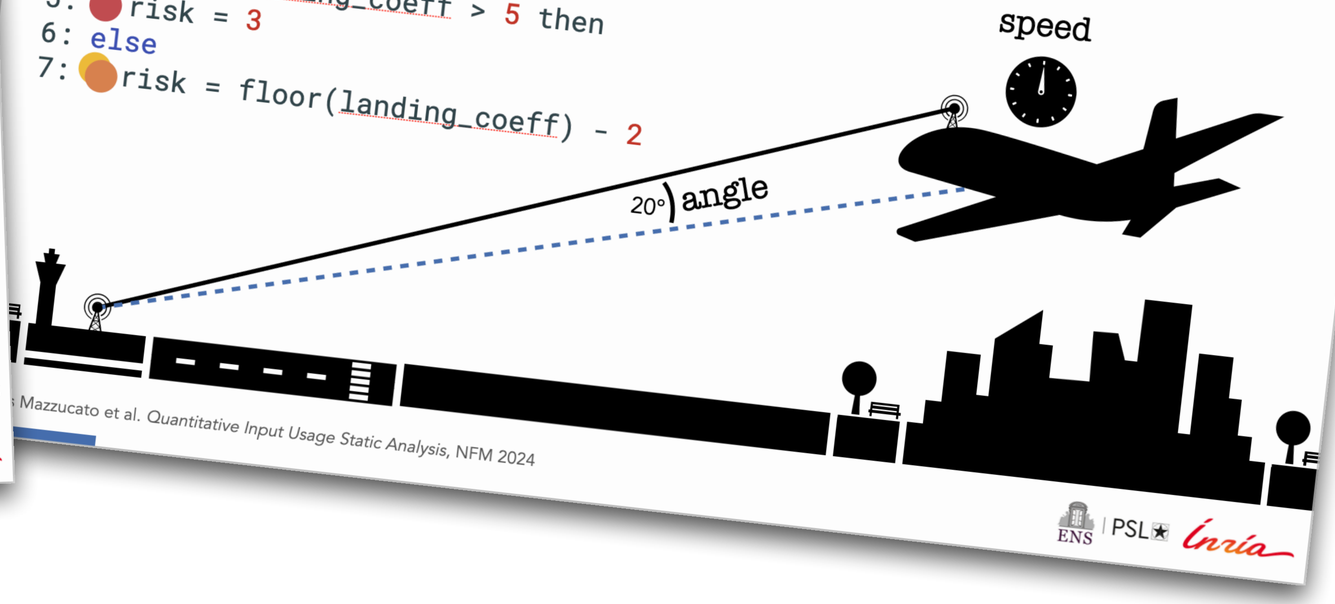
Use Case: Reinhart and Rogoff

C. M. Reinhart and K. S. Rogoff. Growth in a time of debt. American Economic Review 2010.

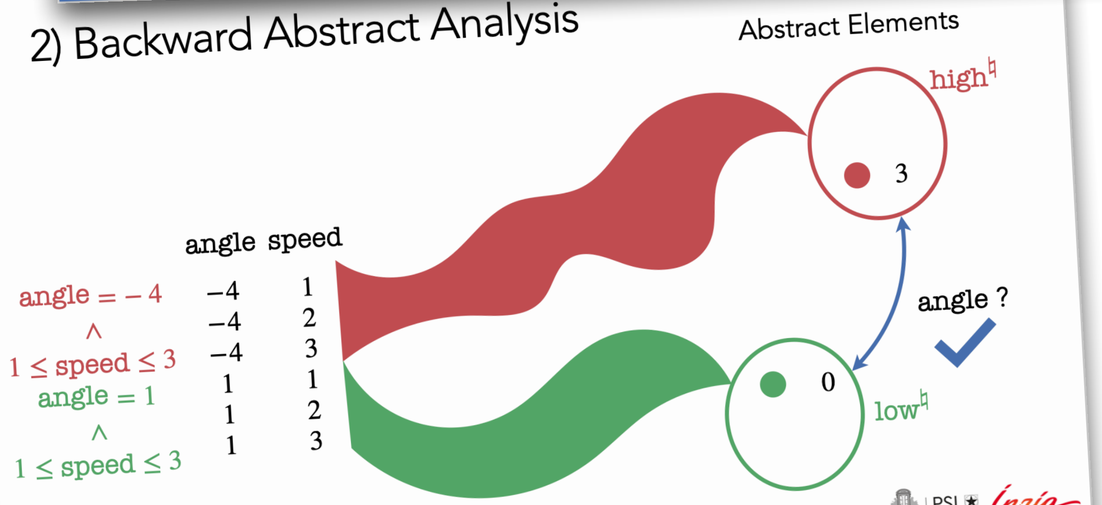


Goal: Quantify the impact of speed and angle on risk

```
1: landing_coeff = abs(angle) + speed
2: if landing_coeff < 2 then
3:     risk = 0
4: else if landing_coeff > 5 then
5:     risk = 3
6: else
7:     risk = floor(landing_coeff) - 2
```



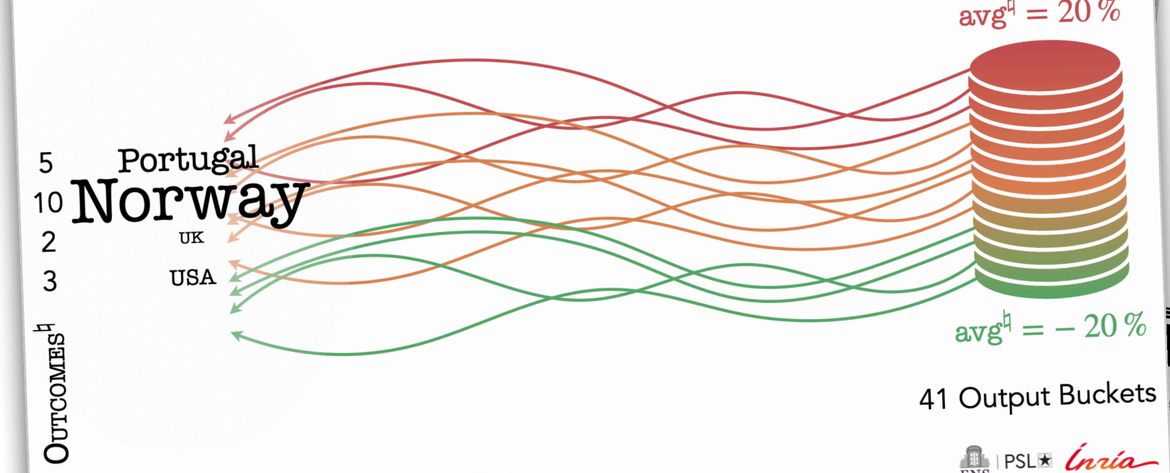
2) Backward Abstract Analysis



Conclusion

Use Case: Reinhart and Rogoff

C. M. Reinhart and K. S. Rogoff. Growth in a time of debt. American Economic Review 2010.

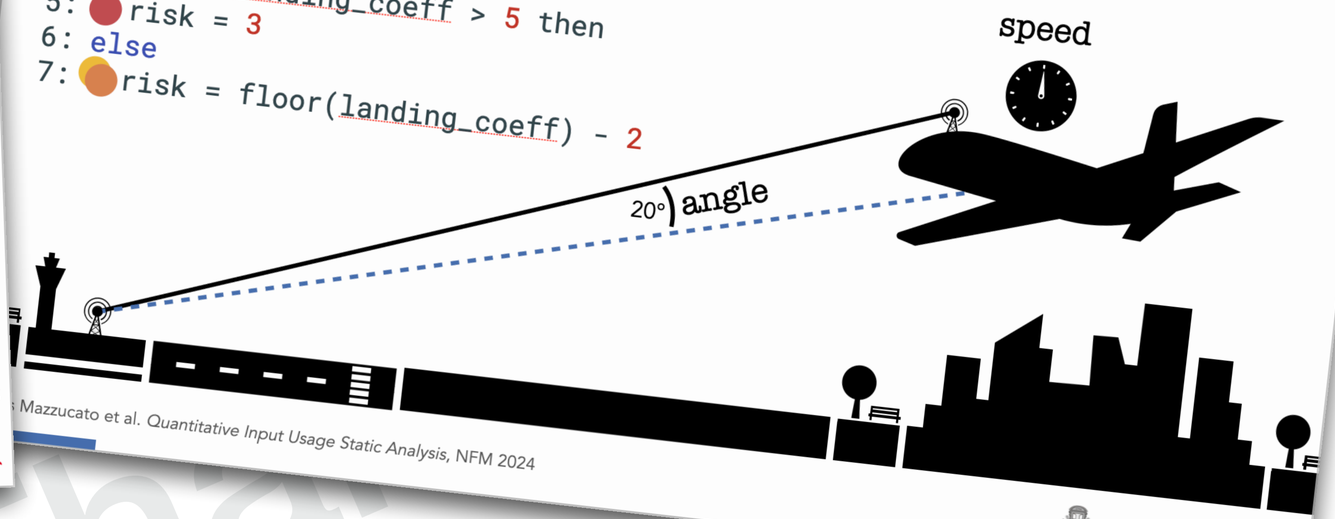


Denis Mazzucato et al. *Quantitative Input Usage Static Analysis*, NFM 2024

ENS | PSL ★ Inria

Goal: Quantify the impact of speed and angle on risk

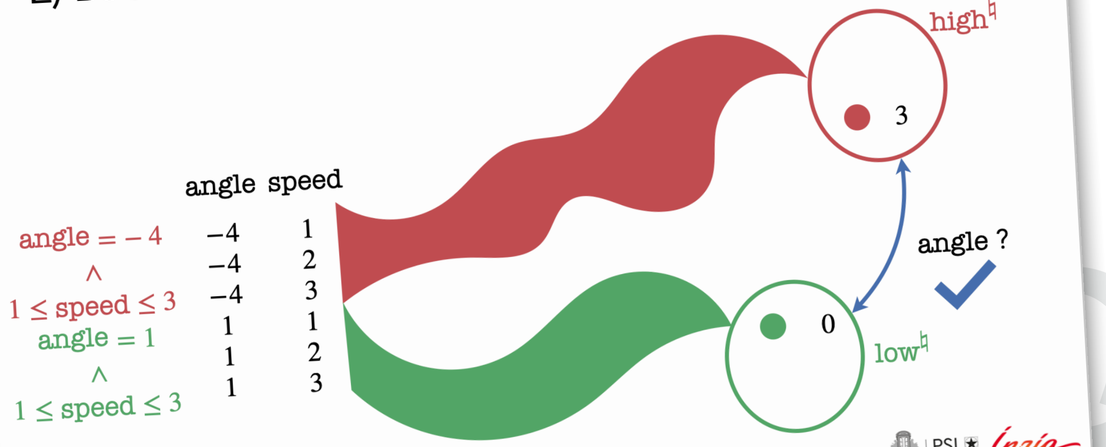
```
1: landing_coeff = abs(angle) + speed
2: if landing_coeff < 2 then
3:     risk = 0
4: else if landing_coeff > 5 then
5:     risk = 3
6: else
7:     risk = floor(landing_coeff) - 2
```



Denis Mazzucato et al. *Quantitative Input Usage Static Analysis*, NFM 2024

ENS | PSL ★ Inria

2) Backward Abstract Analysis



Denis Mazzucato et al. *Quantitative Input Usage Static Analysis*, NFM 2024

ENS | PSL ★ Inria

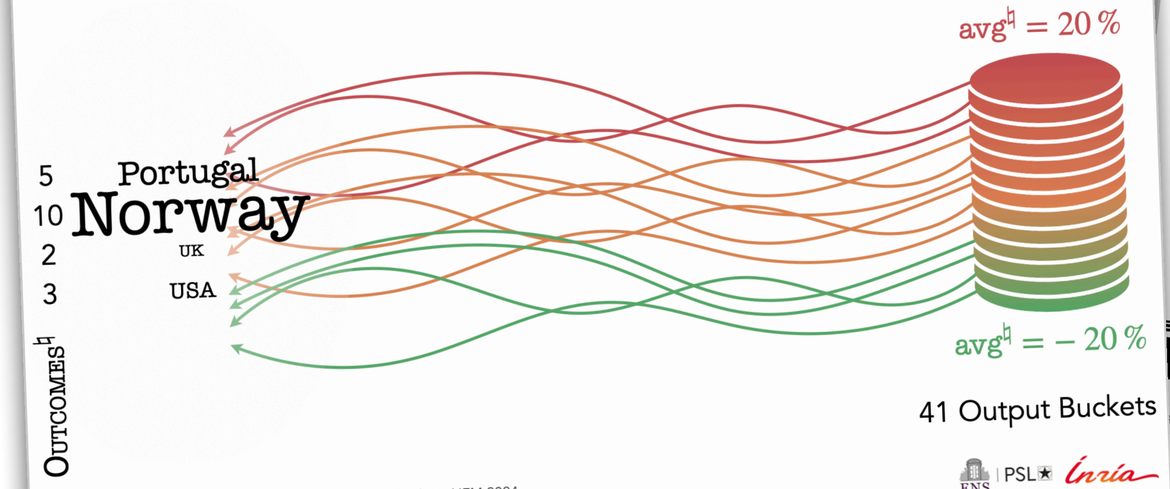
Denis Mazzucato et al. *Quantitative Input Usage Static Analysis*, NFM 2024

ENS | PSL ★ Inria

Conclusion

Use Case: Reinhart and Rogoff

C. M. Reinhart and K. S. Rogoff. Growth in a time of debt. American Economic Review 2010.

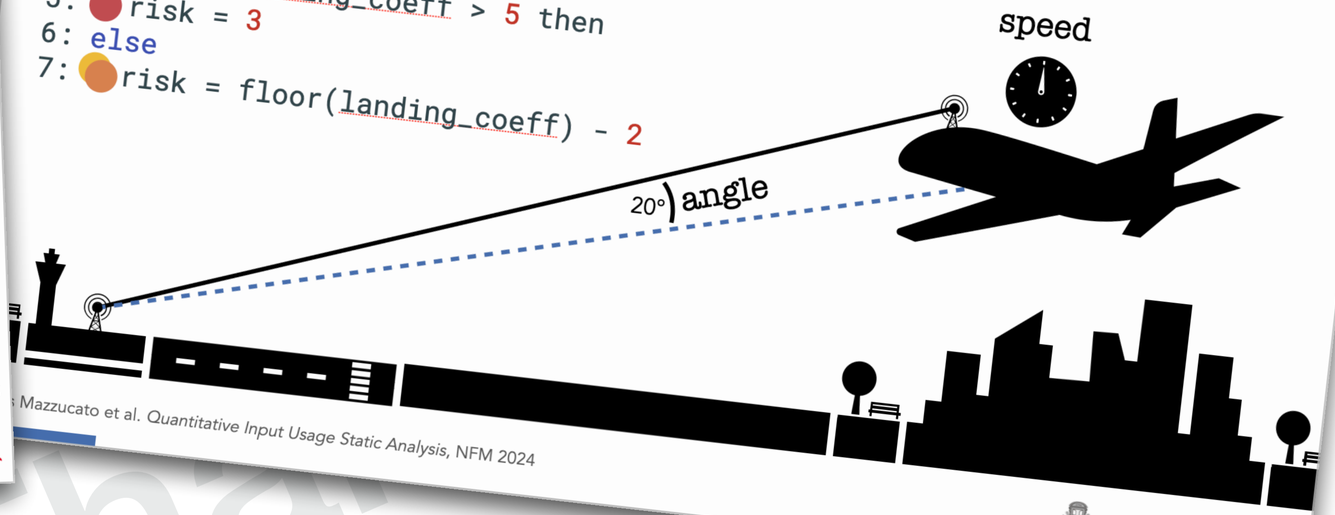


41 Output Buckets

Denis Mazzucato et al. *Quantitative Input Usage Static Analysis*, NFM 2024

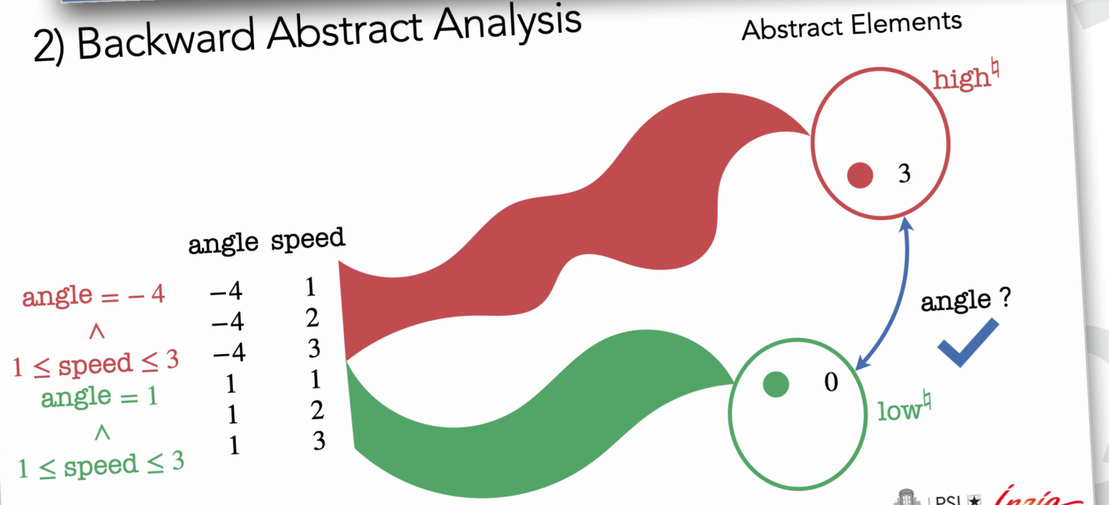
Goal: Quantify the impact of speed and angle on risk

```
1: landing_coeff = abs(angle) + speed
2: if landing_coeff < 2 then
3:     risk = 0
4: else if landing_coeff > 5 then
5:     risk = 3
6: else
7:     risk = floor(landing_coeff) - 2
```



Denis Mazzucato et al. *Quantitative Input Usage Static Analysis*, NFM 2024

2) Backward Abstract Analysis



Denis Mazzucato et al. *Quantitative Input Usage Static Analysis*, NFM 2024

Spoiler (Submitted)

Quantify the Impact on Timing Behavior

ENS | PSL | Inria