

# Diagnosis, Synthesis and Analysis of Probabilistic Models

Tingting Han

University of Twente, The Netherlands

September 25, 2009

# What do I do?

# What do I do?

Mom



Fixing computers

# What do I do?

Mom



Programming

# What do I do?

A college mate



Mom



$$\int f(x)dx$$
$$f(x), \left( \sum_{j=1}^n a_j u_j(x) \right)' = \sum_{j=1}^n a_j u_j'(x) \quad c = \lim_{x \rightarrow \infty} f(x), d = \lim_{x \rightarrow -\infty} f(x)$$
$$\Delta F = F(x_0 + \Delta x_0) - F(x_0) \quad I_1 = \int_{x_0}^c \frac{x}{x_0} \xrightarrow{x \rightarrow a} \frac{x}{a}$$
$$\{X_n \pm y_n\} = \{X_1 \pm y_1, \dots, X_n \pm y_n\} \quad (\sqrt[n+2]{n+2})^3 - (\sqrt[n]{n})^2$$
$$\lim_{n \rightarrow \infty} \frac{(\sqrt[n+2]{n+2})^3 - (\sqrt[n]{n})^2}{(\sqrt[n+2]{n+2})^2 + (\sqrt[n+2]{n+2})} \sum_{k=0}^n a_k z^k \quad \lim_{n \rightarrow \infty} (\sqrt[n+2]{n+2} - \sqrt[n]{n})$$
$$\left(1 + \frac{1}{n+1}\right)^{n+1} < \left(1 + \frac{1}{n}\right)^n \quad a = \psi\left(\frac{1}{q}\right) = [\psi\left(\frac{1}{q}\right)]^q$$
$$\int \pi f^2(x)dx = \int \pi \left(\frac{x}{x_0}\right)^2 dx = \int \frac{2\pi}{h^2} x^2 dx \int [u_1(x) + u_2(x) + \dots + u_n(x)] dx$$
$$\lim_{x \rightarrow \infty} x^3 \left[ \frac{a_0}{3} + \frac{a_1}{x} + \frac{a_2}{x^2} + \frac{a_3}{x^3} \right] = \lim_{x \rightarrow \infty} a_k z_0^k = 0 \quad \lim_{x \rightarrow \infty} f(x) = 1$$
$$a_j \int f_j(x)dx + C \quad (a+x)^n = \sum_{k=0}^n c_{n,k} a^{n-k} x^k \int \left( \sum_{j=1}^n a_j f_j(x) \right) dx = \sum_{j=1}^n a_j \int f_j(x)dx$$
$$z^{n-1} + a_1 z^{n-2} + \dots + a_{n-1} z \quad I_1 = \int_{x_0}^c dx z^{n-1} - a^n = (z-a)(z-a_1)$$
$$a_0 + a_1 z + \dots + a_n z^n \quad \sum_{k=0}^n a_k z^k \quad P_n(z) = a_0 + a_1 z + \dots + a_n z^n$$
$$\frac{a(x+h) - a(x)}{h} = \frac{a(x+h) - a(x)}{h} \quad a = \psi\left(\frac{1}{q}\right) \quad (\log_a x)' = \lim_{h \rightarrow 0} \frac{\log_a(x+h) - \log_a x}{h}$$
$$\lim_{h \rightarrow 0} \log_a\left(\frac{x+h}{x}\right)^{1/h} = \lim_{h \rightarrow 0} \log_a \frac{x+h}{x} (1 + \frac{h}{x})^{1/h} = \lim_{x \rightarrow 0} \frac{1}{x} \log_a (1 + \frac{1}{x})$$
$$\int u_j(x)dx \quad P_n(z_0) = \sum_{k=0}^n a_k z_0^k = 0 \quad I_1 = \int_{x_0}^c dx \dots \int_{x_0}^c dx \dots \int_{x_0}^c dx$$

Applied mathematics, Formal methods

# What do I do?

A college mate



Mom



# What do I do?

A college mate



Mom



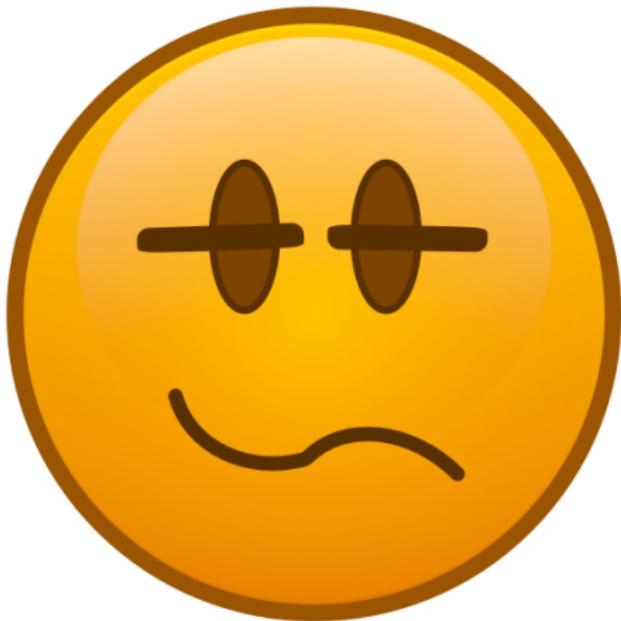
Correctness!

# What do I do?

A college mate



Mom



# What do I do?

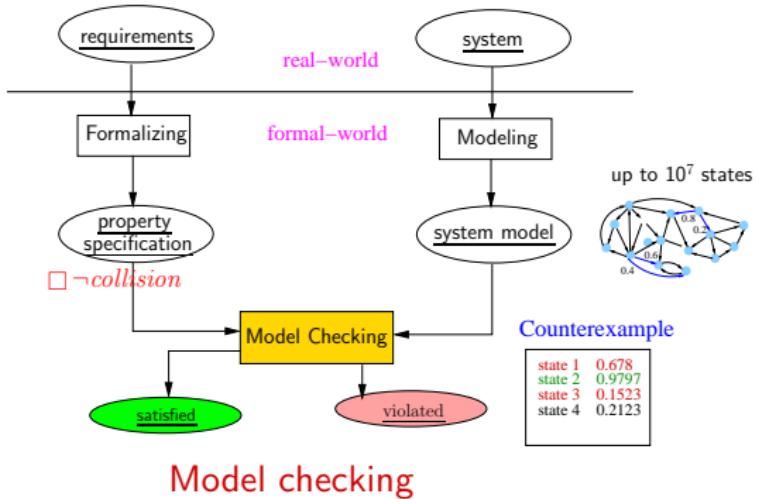
A college mate



Mom



There should be no collisions!



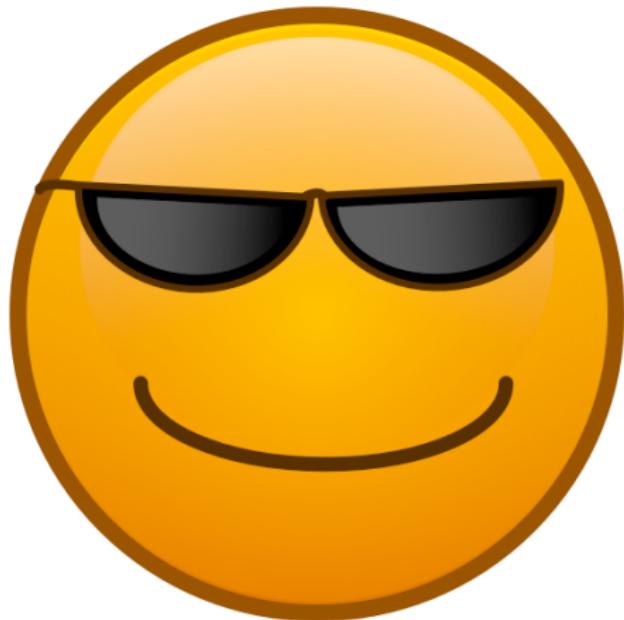
Model checking

# What do I do?

A college mate



Mom



# What do I do?

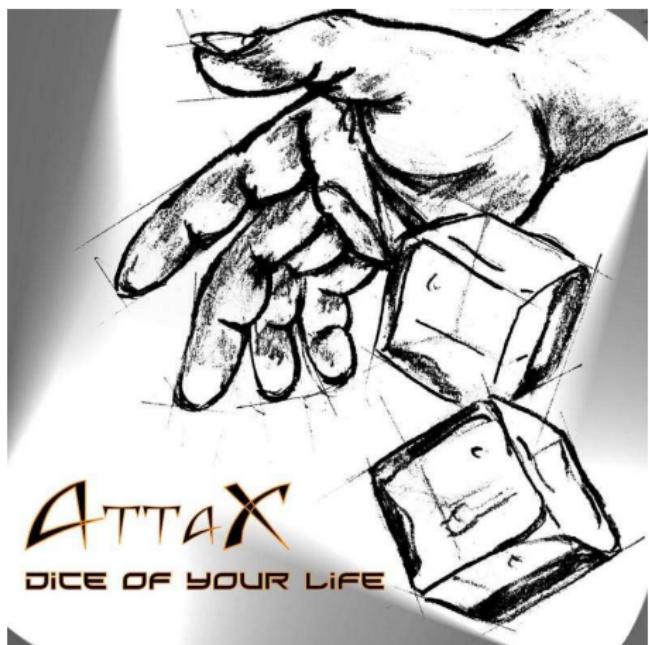
A researcher in a workshop



A college mate



Mom



add Probability!

# What do I do?

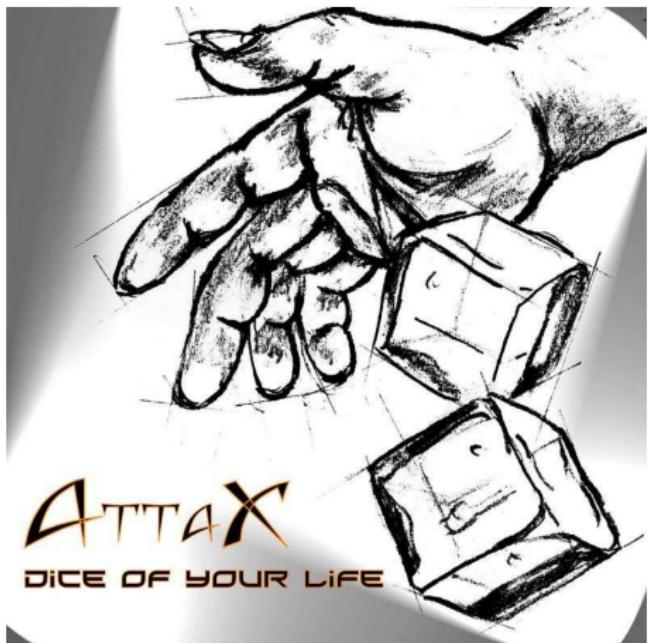
A researcher in a workshop



A college mate



Mom



**add Probability!**  $\Rightarrow$  probabilistic model checking

# What do I do?

Boss



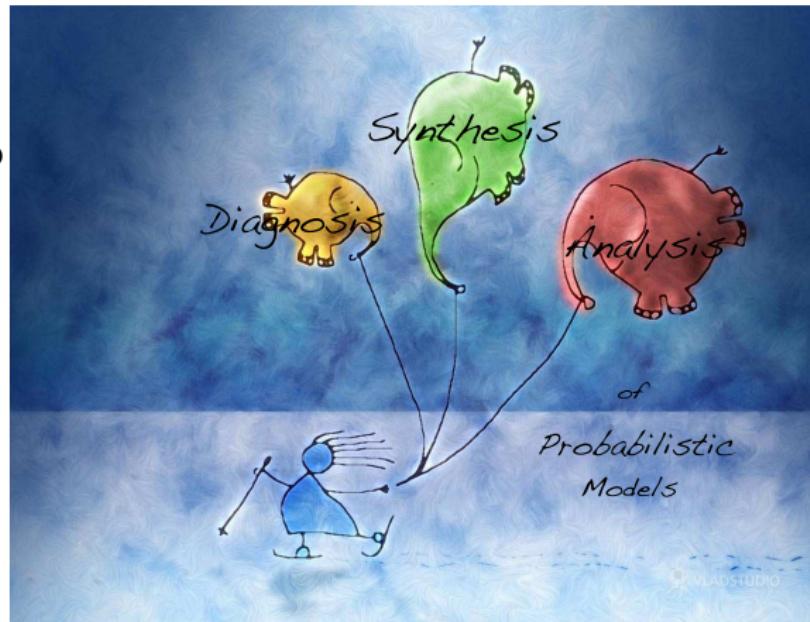
A researcher in a workshop



A college mate



Mom



# Analysis

# Analysis

## Specifications

	branching-time	linear-time		
logic				
automata				
	untimed	real-time	untimed	real-time

# Analysis

How to model check  $\overbrace{\text{CTMC}}$  against ?

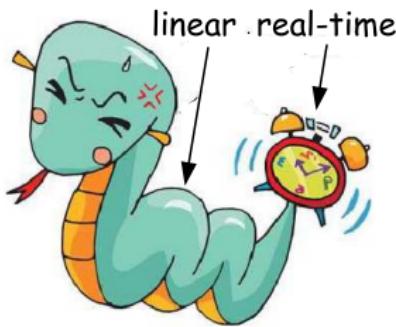
For CTMC model:

	branching-time		linear-time	
logic				
automata				
	untimed	real-time	untimed	real-time

# Analysis

How to model check  $\text{CTMC}$  against  $\text{linear real-time specification}$ ?

For  $\text{CTMC}$  model:

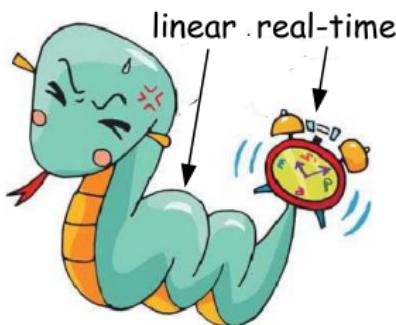


	branching-time	linear-time		
logic	😊	😊	😊	
automata			😊	
	untimed	real-time	untimed	real-time

# Analysis

How to model check  $\text{CTMC}$  against  $\text{linear real-time specification}$ ?

For  $\text{CTMC}$  model:



	branching-time	linear-time		
logic	😊	😊	😊	
automata			😊	
	untimed	real-time	untimed	real-time

$\text{CTMC} \implies \text{probabilistic model checking} \iff \text{deterministic timed automata}$

# Diagnosis

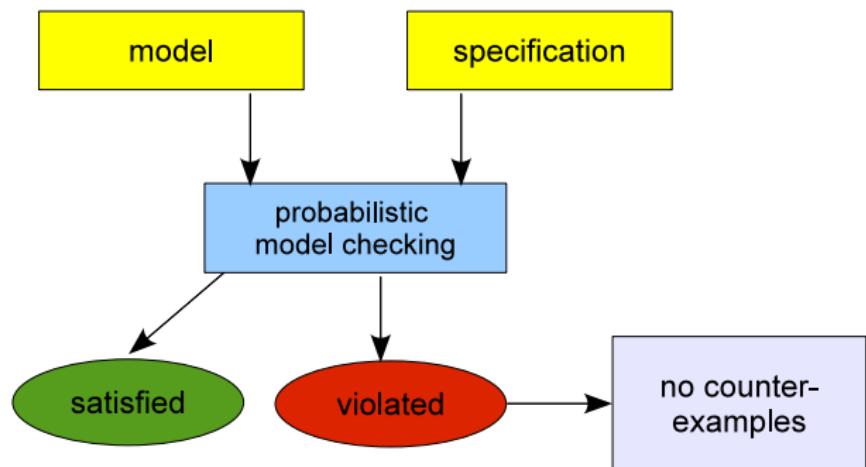
# Diagnosis



What's wrong with your model?

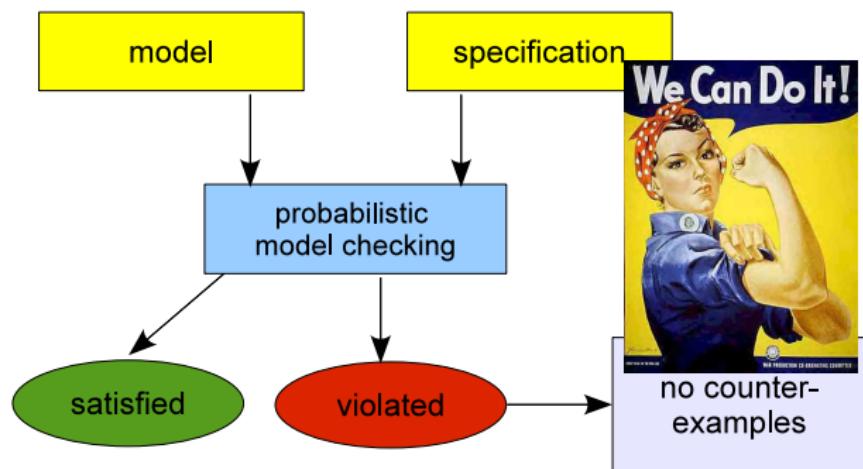
# Diagnosis

What's wrong with your model?



# Diagnosis

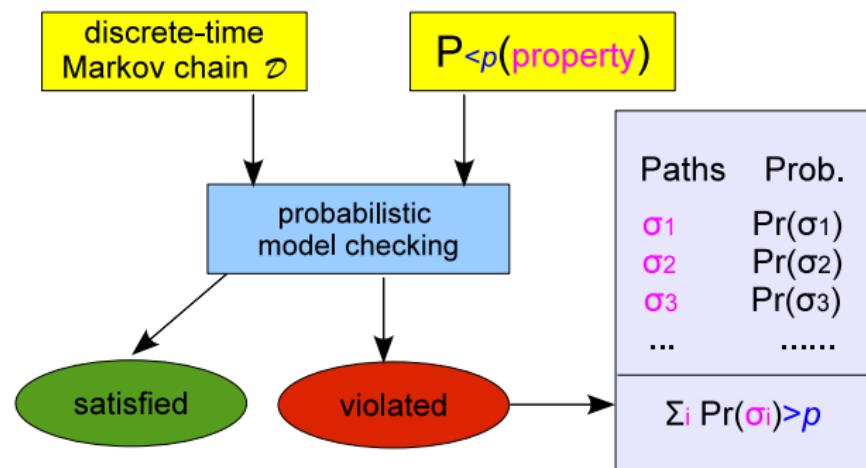
What's wrong with your model?



# Diagnosis



What's wrong with your model?



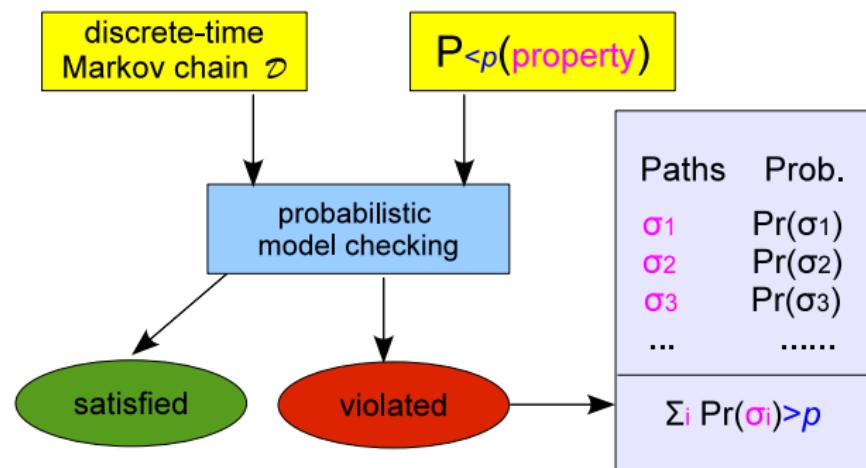
What has been done?

- Define a counterexample

# Diagnosis



What's wrong with your model?



What has been done?

- Define a counterexample
- Design algorithms

# Diagnosis



What's wrong with your model?

Compact representation

Before:



After:

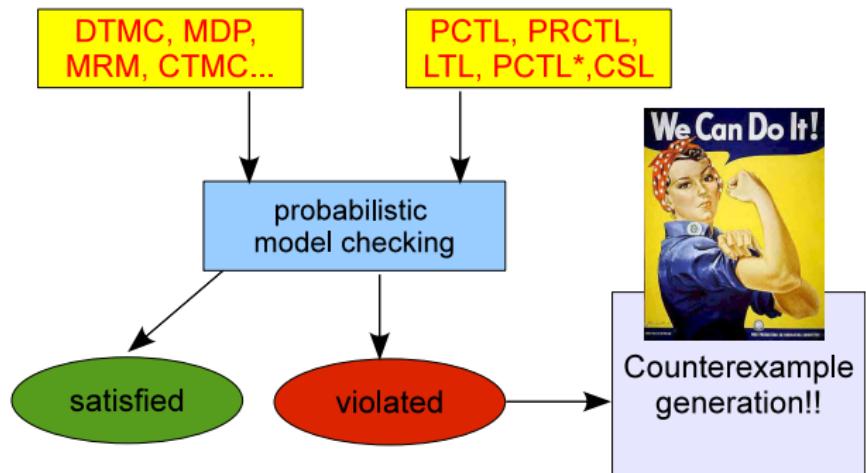


What has been done?

- Define a counterexample
- Design algorithms
- Compact representation

# Diagnosis

What's wrong with your model?



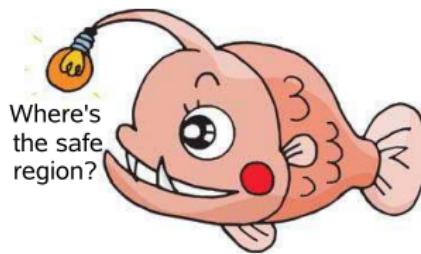
What has been done?

- Define a counterexample
- Compact representation
- Design algorithms
- Generalization

# Synthesis

# Synthesis

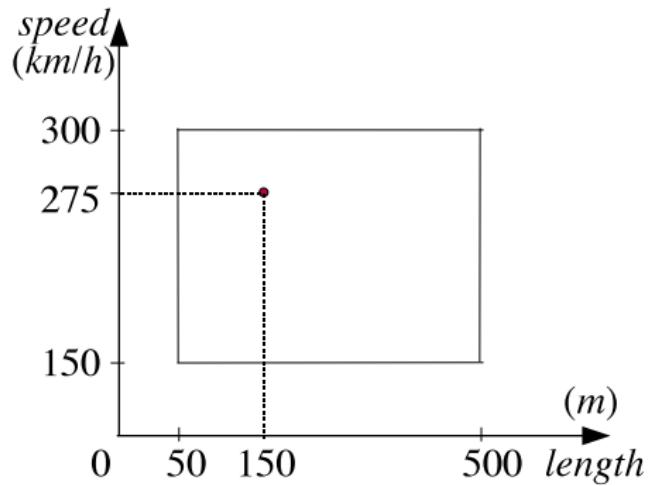
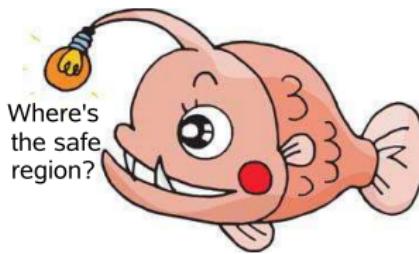
What parameter values can make the model “safe”?



# Synthesis

What parameter values can make the model “safe”?

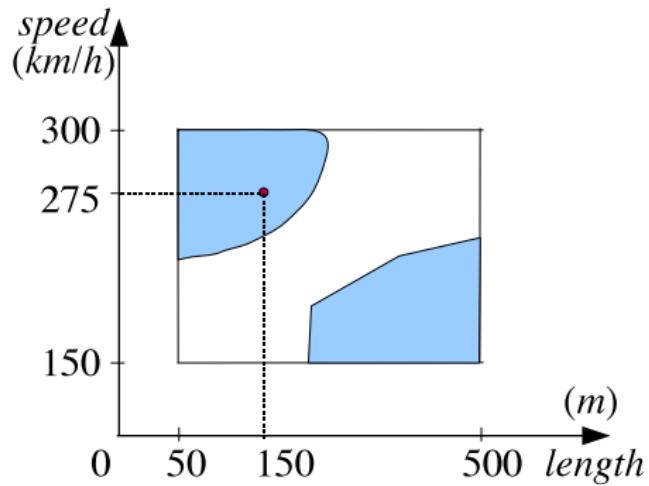
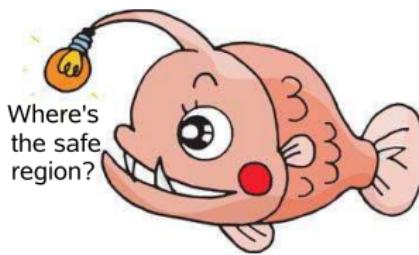
*trains*[*speed* = ?, *length* = ?] satisfies  $\mathcal{P}_{>0.9999}(\text{no collision})$



# Synthesis

What parameter values can make the model “safe”?

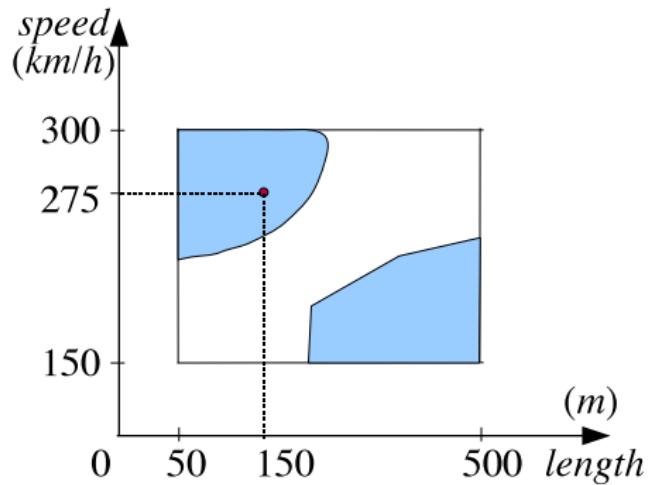
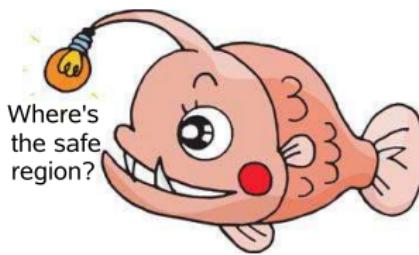
*trains*[*speed* = ?, *length* = ?] satisfies  $\mathcal{P}_{>0.9999}(\text{no collision})$



# Synthesis

What parameter values can make the model “safe”?

*trains*[*speed* = ?, *length* = ?] satisfies  $\mathcal{P}_{>0.9999}(\text{no collision})$



Parameter synthesis is much harder than model checking!



*köszönöm !תודה dekuji*

*mahalo 고맙습니다*

*thank you*

*merci 谢谢 danke*

*Ευχαριστώ شكرًا*

*／どうもありがとう gracias*

*Bedankt*