
AWS
re:Invent
DECEMBER 2 – 6, 2024 | LAS VEGAS, NV

AIM393

Introducing Automated Reasoning checks in Amazon Bedrock Guardrails

Stefano Buliani
(he/him)
Product Manager
Amazon Web Services

Byron Cook
(he/him)
VP, Distinguished Scientist
Amazon Web Services

Agenda

01 How we got here – finding a gen AI strategy

02 Automated Reasoning checks

03 What is Automated Reasoning anyway?

04 Getting started with Automated Reasoning checks and demo

05 Next steps

How we got here

Ninety-five percent of CIOs surveyed believe in the moderate or extensive potential value of gen AI, with top areas of value being in productivity, customer experience and digital business transformation

Gartner®

Gartner, Key findings from the 2024 Gartner CIO Generative AI Survey, August 2024.

aws

Leaders are asking – what is our gen AI strategy?

- **Understand** large language models (LLMs)
- **Educate** leaders
- Identify **use cases**

Experiment, experiment, experiment

Understand LLMs

Educate leaders

Identify **use cases**

Onboard employees

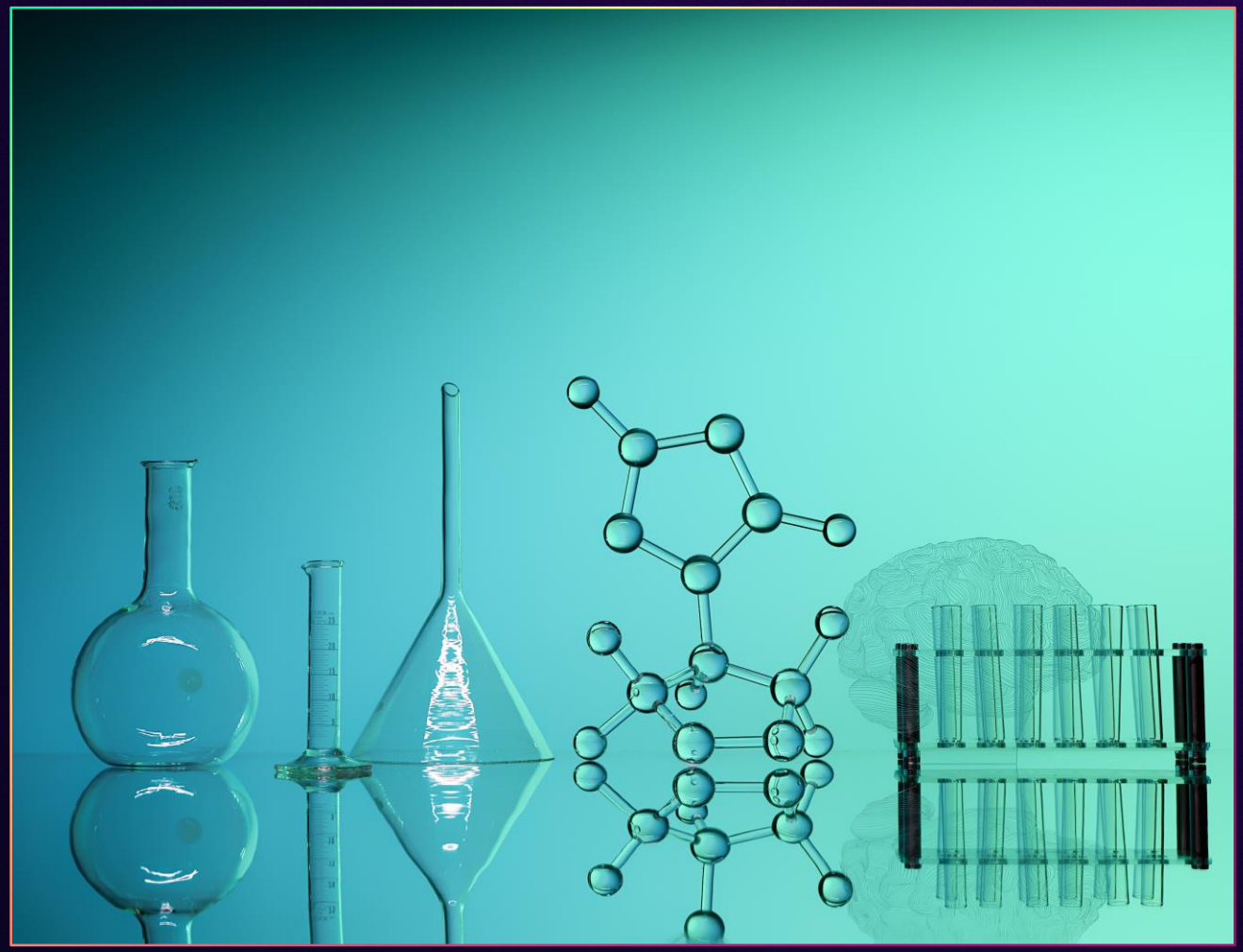
Simplify **customer support**

Automate decisions

Wow comes first when experimenting

First reaction is always **wow**

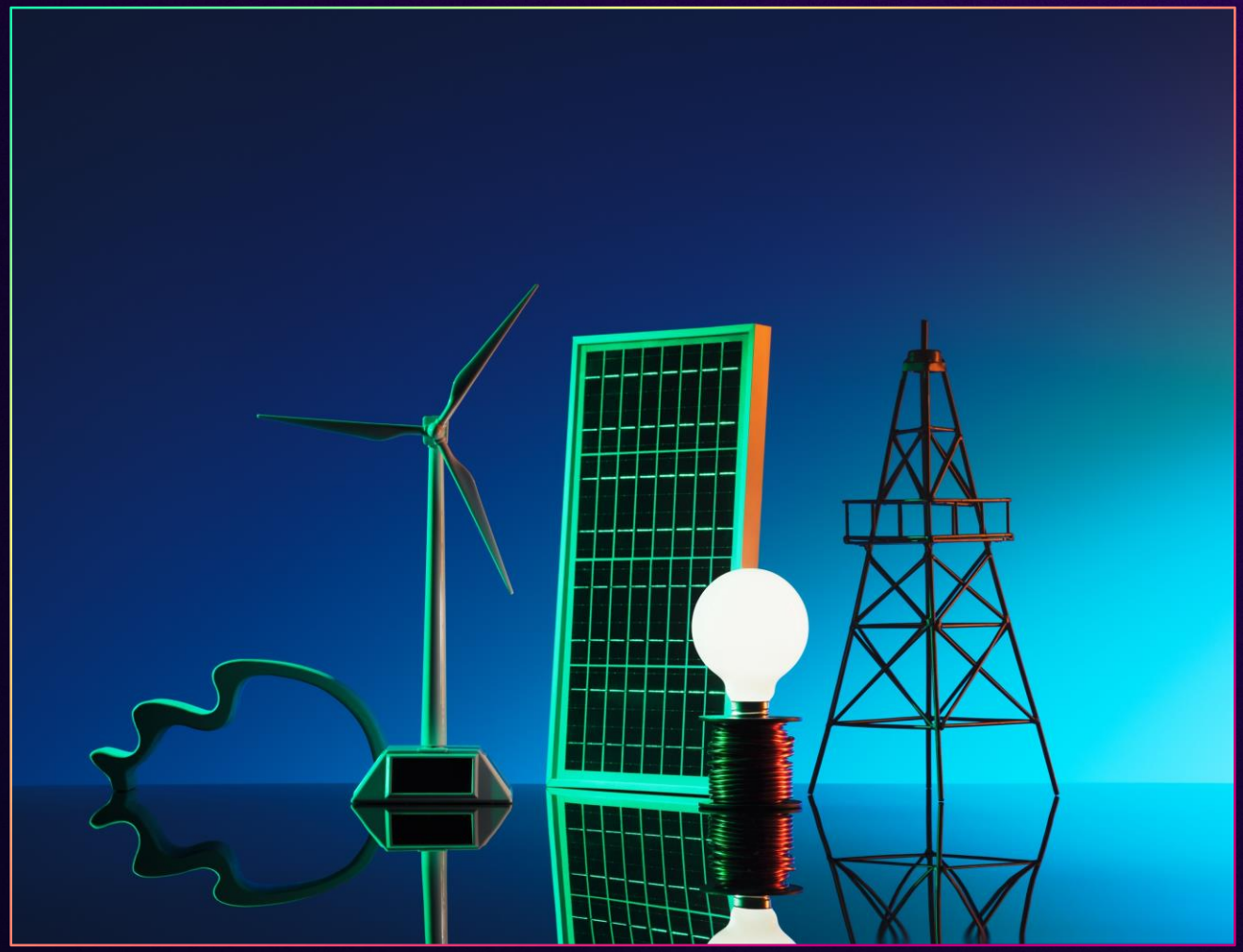
We can build so fast



Then we test for production

From experiment to production

Lacks accuracy



Hallucinations can be subtle

Ground truth

My friend Sam and I enjoy solving Advent of Code puzzles. We spend hours on Slack discussing the trade offs between different algorithms to solve the problem. Our passion for this activity brings us closer as good friends.

LLM summary

Ben and I love solving Advent of Code puzzles, and this makes us good friends.

Hallucinations can be subtle

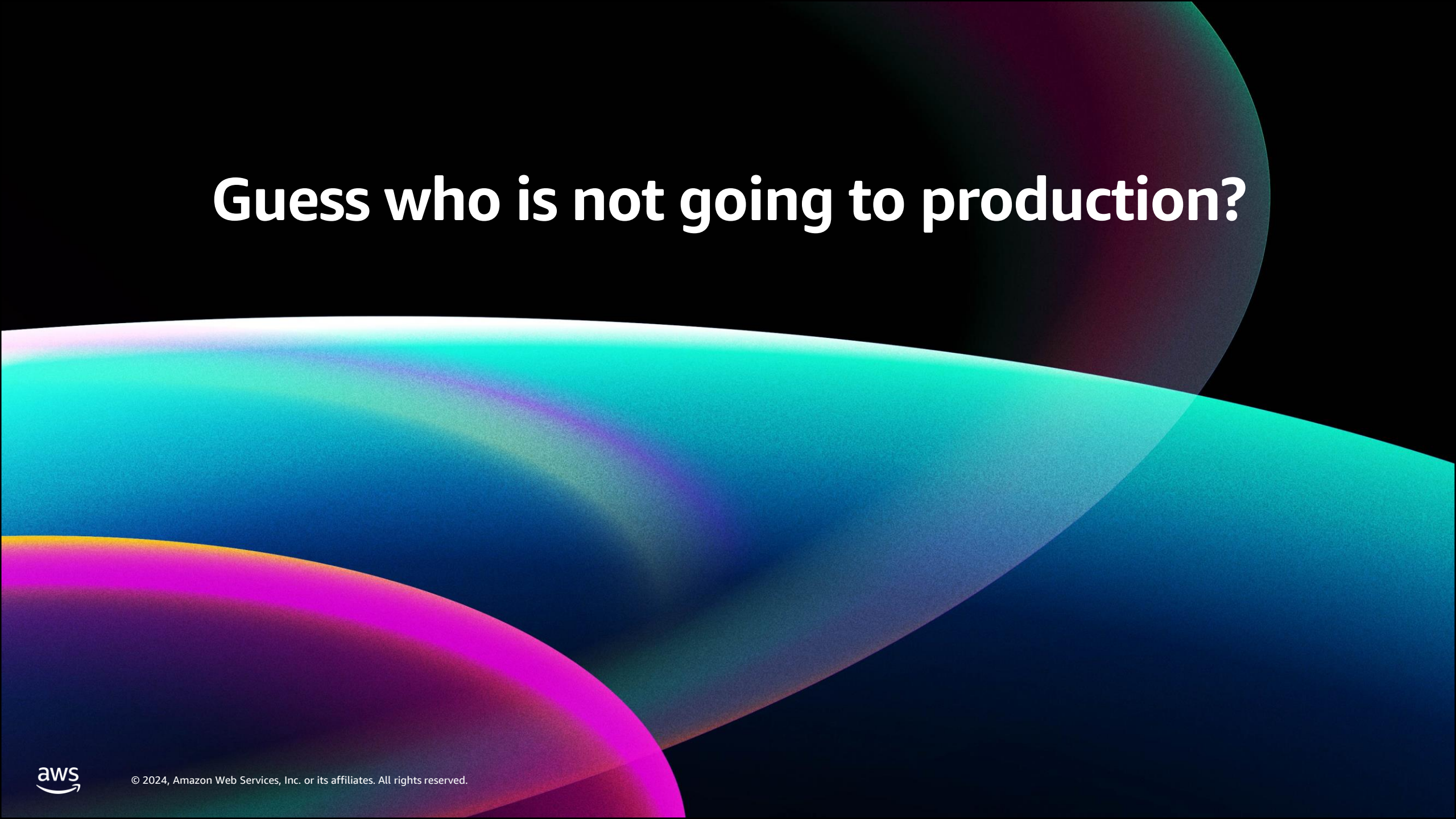
Ground truth

My friend **Sam** and I enjoy solving Advent of Code puzzles. We spend hours on Slack discussing the trade offs between different algorithms to solve the problem. Our passion for this activity brings us closer as good friends.

LLM summary

Ben and I love solving Advent of Code puzzles, and this makes us good friends.

Guess who is not going to production?



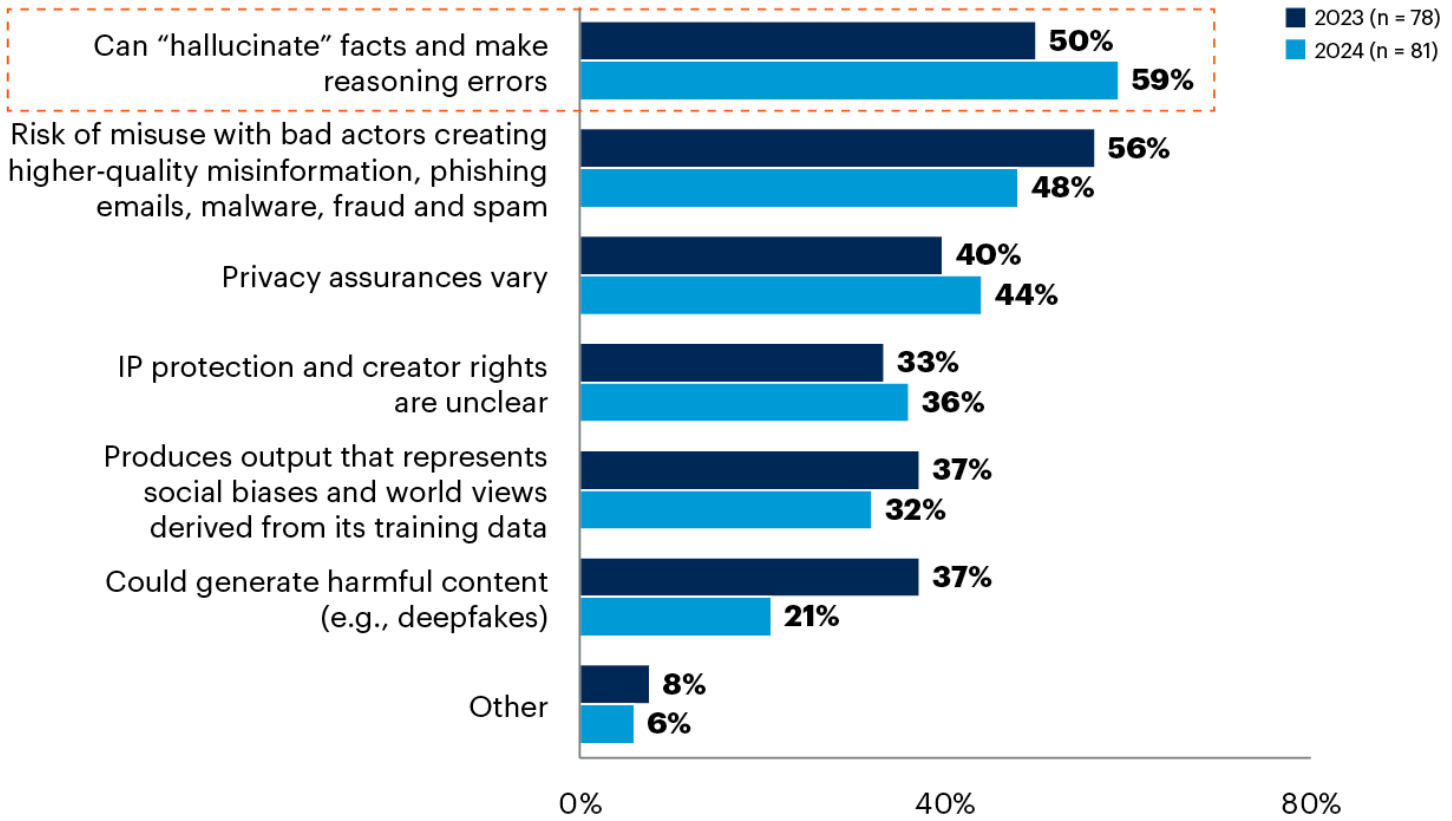
The concern of hallucinations that result in reasoning errors was the top-rated potential risk (59%), followed by bad actors creating misinformation (48%) and privacy assurances (44%).

Gartner®

Gartner, Key Findings From the 2024 Gartner CIO Generative AI Survey, August 2024.

You are in good company

Gartner, Key Findings From the 2024 Gartner CIO Generative AI Survey, August 2024.



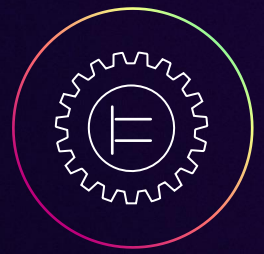
Hallucinations are not a bug. It’s creativity.

Automated Reasoning checks

We have three objectives

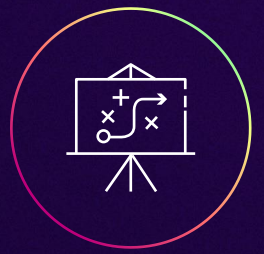
Accurate

Identifies and suggests corrections for inaccurate factual claims on supported knowledge



Sound

When it says something is incorrect – it is; if we cannot make a claim one way or another, we'll tell you



Transparent

We can explain exactly why we believe a claim is accurate or not

When it works best

- HR policies
- Laws and regulation
- Operational workflows

It’s not suited for

- Marketing messaging best practices
- Probabilistic calculations (what are the chances of?)
- Qualitative descriptions

Amazon Bedrock Guardrails

Evaluate prompts and model responses for agents, knowledge bases, FMs in Amazon Bedrock, and self-managed or third-party FMs

Configure thresholds to filter harmful content, jailbreaks, and prompt injection attacks

Define and disallow denied topics with short natural language descriptions

Remove personally identifiable information (PII) and sensitive information in generative AI applications

Filter hallucinations by detecting groundedness and relevance of model responses based on context

Amazon Bedrock Guardrails

Evaluate prompts and model responses for agents, knowledge bases, FMs in Amazon Bedrock, and self-managed or third-party FMs

Configure thresholds to filter harmful content, jailbreaks, and prompt injection attacks

Define and disallow denied topics with short natural language descriptions

Remove personally identifiable information (PII) and sensitive information in generative AI applications

Filter hallucinations by detecting groundedness and relevance of model responses based on context

Amazon Bedrock Guardrails

Evaluate prompts and model responses for agents, knowledge bases, FMs in Amazon Bedrock, and self-managed or third-party FMs

Configure thresholds to filter harmful content, jailbreaks, and prompt injection attacks

Define and disallow denied topics with short natural language descriptions

Remove personally identifiable information (PII) and sensitive information in generative AI applications

Filter hallucinations by detecting groundedness and relevance of model responses based on context

Amazon Bedrock Guardrails

Evaluate prompts and model responses for agents, knowledge bases, FMs in Amazon Bedrock, and self-managed or third-party FMs

Configure thresholds to filter harmful content, jailbreaks, and prompt injection attacks

Define and disallow denied topics with short natural language descriptions

Remove personally identifiable information (PII) and sensitive information in generative AI applications

Filter hallucinations by detecting groundedness and relevance of model responses based on context

Amazon Bedrock Guardrails

Evaluate prompts and model responses for agents, knowledge bases, FMs in Amazon Bedrock, and self-managed or third-party FMs

Configure thresholds to filter harmful content, jailbreaks, and prompt injection attacks

Define and disallow denied topics with short natural language descriptions

Remove personally identifiable information (PII) and sensitive information in generative AI applications

Filter hallucinations by detecting groundedness and relevance of model responses based on context

Amazon Bedrock Guardrails

Evaluate prompts and model responses for agents, knowledge bases, FMs in Amazon Bedrock, and self-managed or third-party FMs

Configure thresholds to filter harmful content, jailbreaks, and prompt injection attacks

Define and disallow denied topics with short natural language descriptions

Remove personally identifiable information (PII) and sensitive information in generative AI applications

Filter hallucinations by detecting groundedness and relevance of model responses based on context

Even more complete

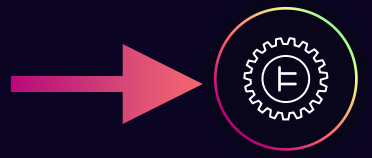
Evaluate prompts and model responses for agents, knowledge bases, FMs in Amazon Bedrock, and self-managed or third-party FMs

Configure thresholds to filter harmful content, jailbreaks, and prompt injection attacks

Define and disallow denied topics with short natural language descriptions

Remove personally identifiable information (PII) and sensitive information in generative AI applications

Filter hallucinations by detecting groundedness and relevance of model responses based on context



Identify, correct, and explain factual claims in responses based on ground truth formal logic

Even more complete

Evaluate prompts and model responses for agents, knowledge bases, FMs in Amazon Bedrock, and self-managed or third-party FMs

Configure thresholds to filter harmful content, jailbreaks, and prompt injection attacks

Define and disallow denied topics with short natural language descriptions

Remove personally identifiable information (PII) and sensitive information in generative AI applications

Filter hallucinations by detecting groundedness and relevance of model responses based on context

Identify, correct, and explain factual claims in responses based on ground truth formal logic

AIM393

Introduction to Automated Reasoning checks in Amazon Bedrock Guardrails

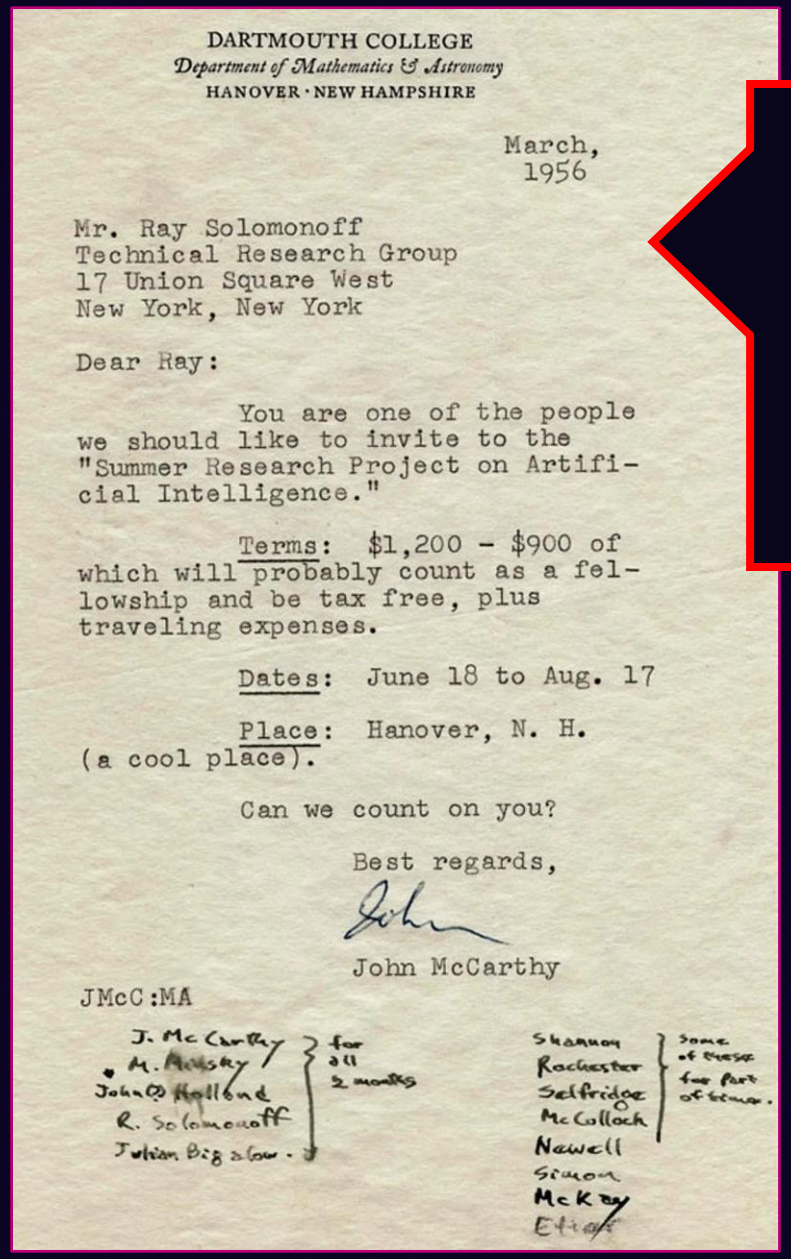
Stefano Buliani
(he/him)
Product Manager
Amazon Web Services

Byron Cook
(he/him)
VP, Distinguished Scientist
Amazon Web Services

What *is* automated reasoning?

a.k.a. *symbolic* AI

What *is* automated reasoning?



DARTMOUTH COLLEGE
Department of Mathematics & Astronomy
HANOVER · NEW HAMPSHIRE

March,
1956

Mr. Ray Solomonoff
Technical Research Group
17 Union Square West
New York, New York

Dear Ray:

You are one of the people we should like to invite to the "Summer Research Project on Artificial Intelligence."

Terms: $1,200 - $900 of which will probably count as a fellowship and be tax free, plus traveling expenses.

Dates: June 18 to Aug. 17

Place: Hanover, N. H. (a cool place).

Can we count on you?

Best regards,

John

John McCarthy

JMcC:MA

J. McCarthy
M. Minsky
John Holland
R. Solomonoff
Julian Bigelow
} for all 2 months

Shannon
Rochester
Selfridge
McCulloch
Newell
Simon
McKay
Ethaf
} some of these for part of time.

Dartmouth, 1956: The term *Artificial Intelligence* is coined

DARTMOUTH COLLEGE
Department of Mathematics & Astronomy
HANOVER · NEW HAMPSHIRE

March,
1956

Mr. Ray Solomonoff
Technical Research Group
17 Union Square West
New York, New York

Dear Ray:

You are one of the people we should like to invite to the "Summer Research Project on Artificial Intelligence."

Terms: $1,200 - $900 of which will probably count as a fellowship and be tax free, plus traveling expenses.

Dates: June 18 to Aug. 17

Place: Hanover, N. H. (a cool place).

Can we count on you?

Best regards,

John

John McCarthy

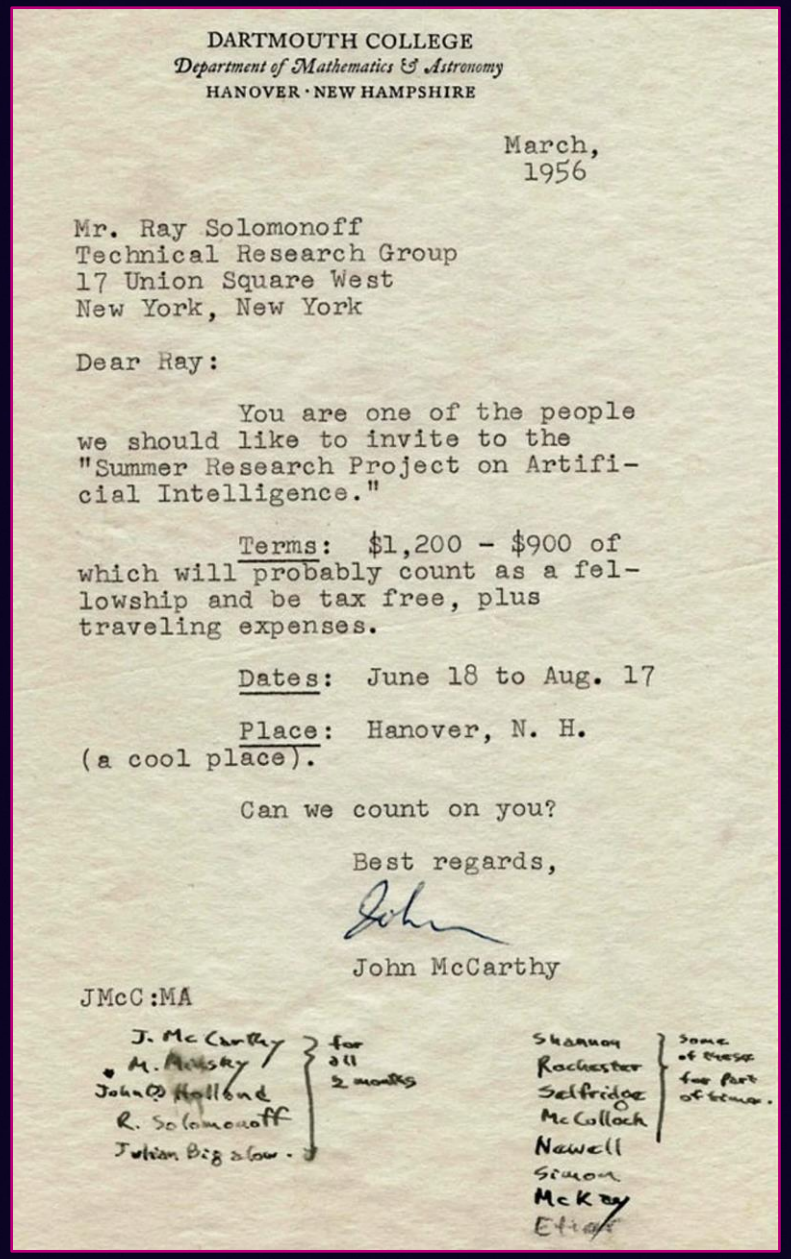
JMcC:MA

J. McCarthy
M. Minsky
John Holland
R. Solomonoff
Julian Bigelow
} for all 2 months

Shannon
Rochester
Selfridge
McCulloch
Newell
Simon
McKay
Ethaf
} some of these for part of time.

Oliver Selfridge | Nathaniel Rochester | Marvin Minsky | John McCarthy

Ray Solomonoff | Peter Milner | Claude Shannon



DARTMOUTH COLLEGE
Department of Mathematics & Astronomy
HANOVER · NEW HAMPSHIRE

March,
1956

Mr. Ray Solomonoff
Technical Research Group
17 Union Square West
New York, New York

Dear Ray:

You are one of the people we should like to invite to the "Summer Research Project on Artificial Intelligence."

Terms: $1,200 - $900 of which will probably count as a fellowship and be tax free, plus traveling expenses.

Dates: June 18 to Aug. 17

Place: Hanover, N. H. (a cool place).

Can we count on you?

Best regards,

John McCarthy

JMcC:MA

J. McCarthy
M. Minsky
John Holland
R. Solomonoff
Julian Bigelow
} for all 2 months

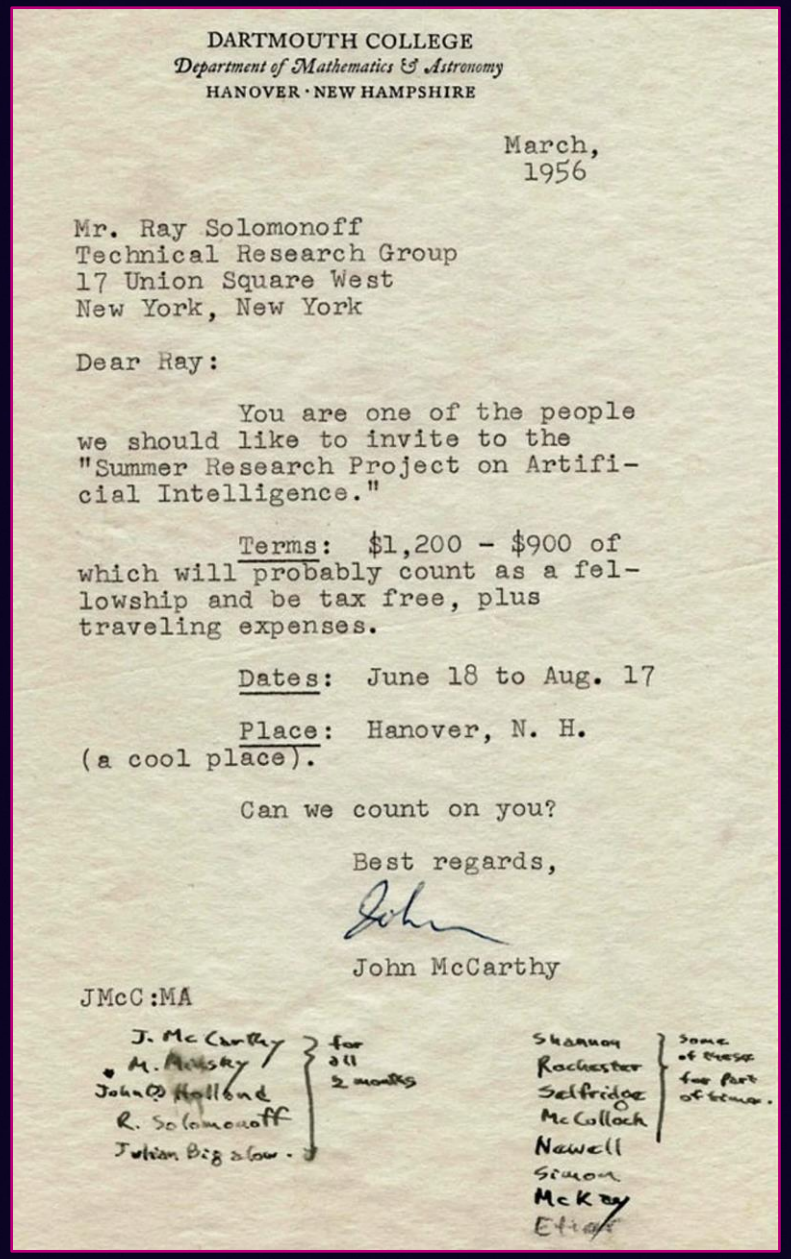
Shannon
Rochester
Selfridge
McCulloch
Newell
Simon
McKay
Ethan
} some of these for part of time.

AI

Connectionist AI

Symbolic AI

Probabilistic AI



DARTMOUTH COLLEGE
Department of Mathematics & Astronomy
HANOVER · NEW HAMPSHIRE

March,
1956

Mr. Ray Solomonoff
Technical Research Group
17 Union Square West
New York, New York

Dear Ray:

You are one of the people we should like to invite to the "Summer Research Project on Artificial Intelligence."

Terms: $1,200 - $900 of which will probably count as a fellowship and be tax free, plus traveling expenses.

Dates: June 18 to Aug. 17

Place: Hanover, N. H. (a cool place).

Can we count on you?

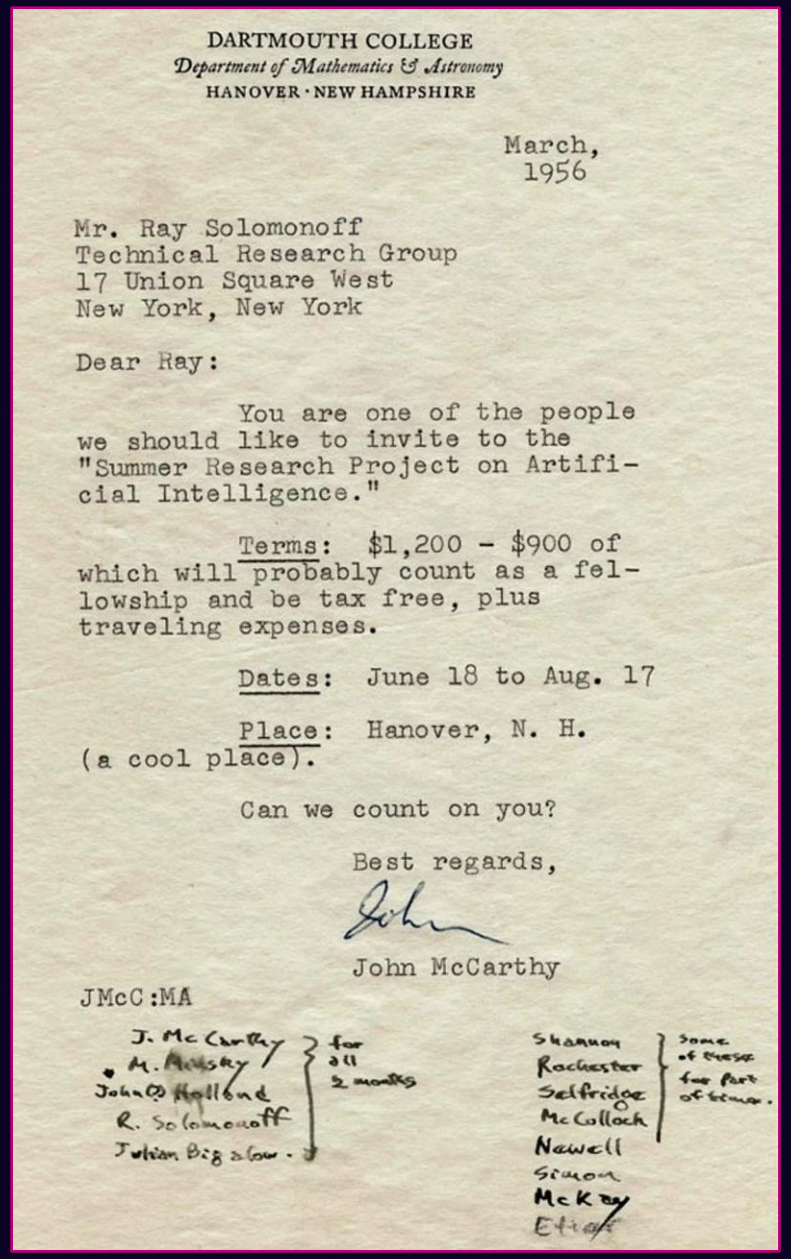
Best regards,

John McCarthy

JMcC:MA

J. McCarthy
M. Minsky
John Holland
R. Solomonoff
Julian Bigelow
} for all 2 months

Shannon
Rochester
Selfridge
McCulloch
Newell
Simon
McKay
Ethan
} some of these for part of time.



DARTMOUTH COLLEGE
Department of Mathematics & Astronomy
HANOVER · NEW HAMPSHIRE

March,
1956

Mr. Ray Solomonoff
Technical Research Group
17 Union Square West
New York, New York

Dear Ray:

You are one of the people we should like to invite to the "Summer Research Project on Artificial Intelligence."

Terms: $1,200 - $900 of which will probably count as a fellowship and be tax free, plus traveling expenses.

Dates: June 18 to Aug. 17

Place: Hanover, N. H. (a cool place).

Can we count on you?

Best regards,

John McCarthy

JMcC:MA

J. McCarthy
M. Minsky
John Holland
R. Solomonoff
Julian Bigelow
} for all 2 months

Shannon
Rochester
Selfridge
McCulloch
Newell
Simon
McKay
Ethan
} some of these for part of time.

AI

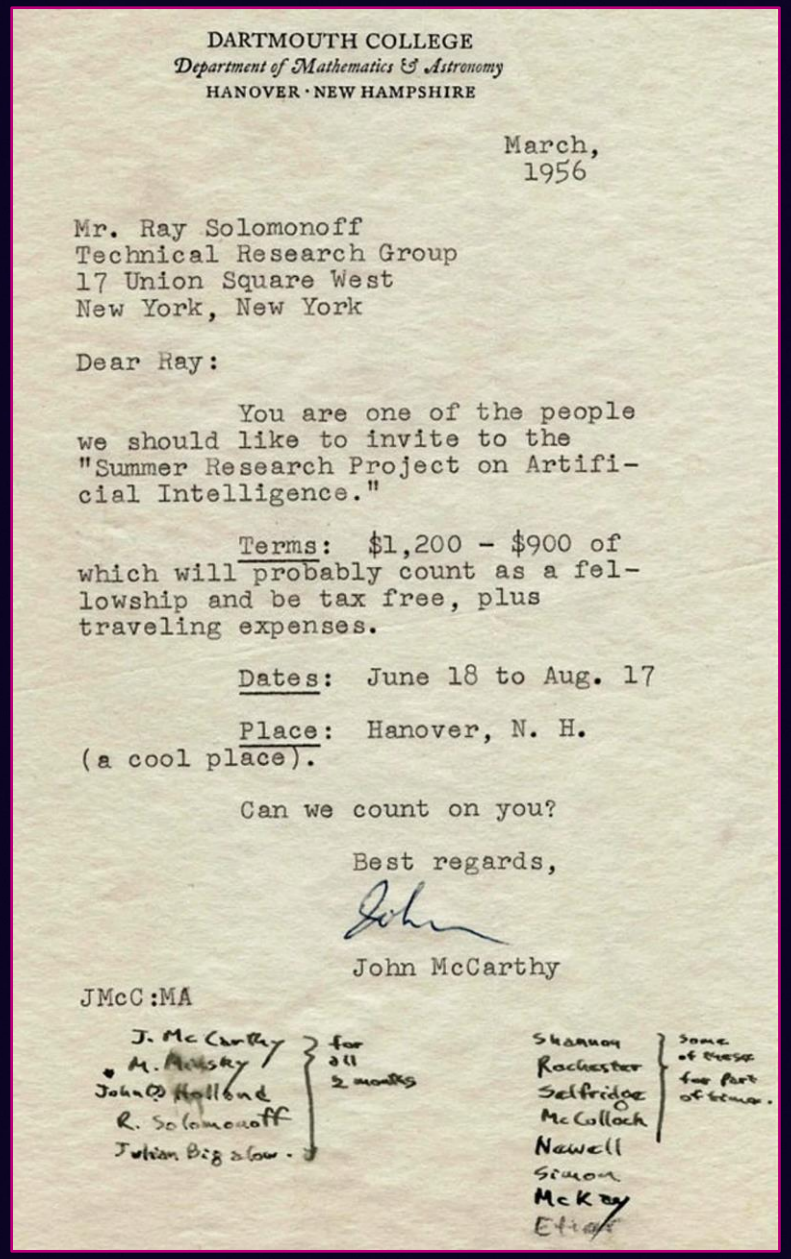
Connectionist AI

Symbolic AI

Probabilistic AI

"Machine Learning"

"Automated Reasoning"



DARTMOUTH COLLEGE
Department of Mathematics & Astronomy
HANOVER · NEW HAMPSHIRE

March,
1956

Mr. Ray Solomonoff
Technical Research Group
17 Union Square West
New York, New York

Dear Ray:

You are one of the people we should like to invite to the "Summer Research Project on Artificial Intelligence."

Terms: $1,200 - $900 of which will probably count as a fellowship and be tax free, plus traveling expenses.

Dates: June 18 to Aug. 17

Place: Hanover, N. H. (a cool place).

Can we count on you?

Best regards,

John McCarthy

JMcC:MA

J. McCarthy
M. Minsky
John Holland
R. Solomonoff
Julian Bigelow
} for all 2 months

Shannon
Rochester
Selfridge
McCulloch
Newell
Simon
McKay
Ethan
} some of these for part of time.

AI

Connectionist AI

Symbolic AI

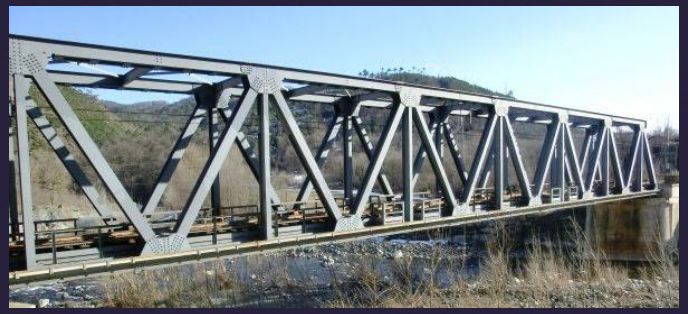
Probabilistic AI

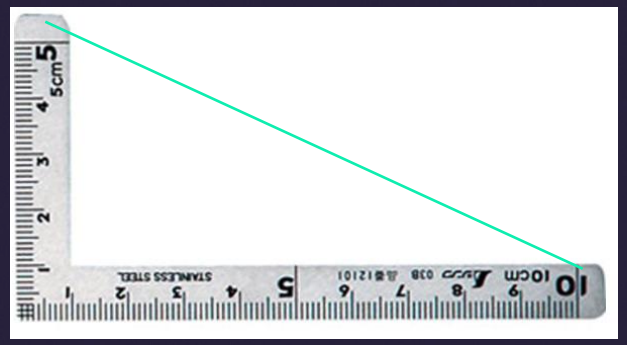
"Machine Learning"

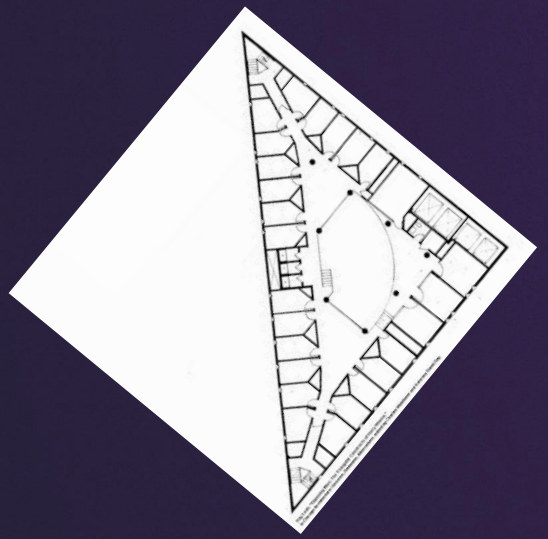
"Automated Reasoning"

Today's lingo

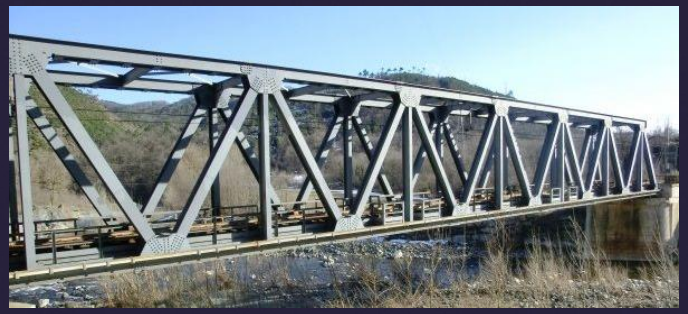
Today's lingo

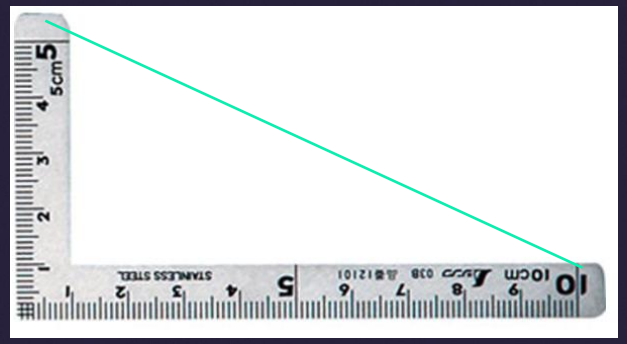


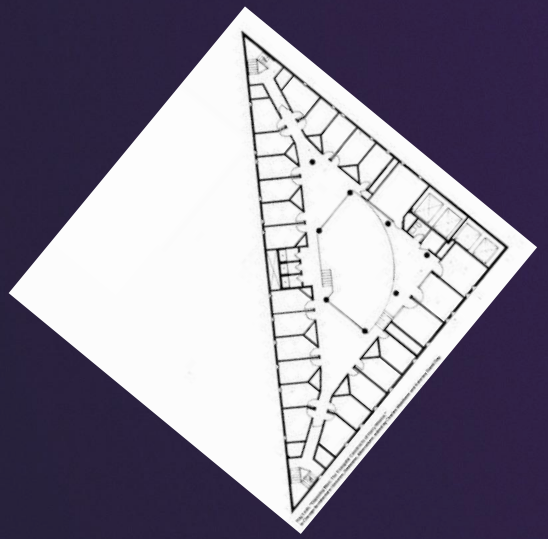




Machine learning takes some data and tries to find a **model** that hopefully will fit the remaining expected data

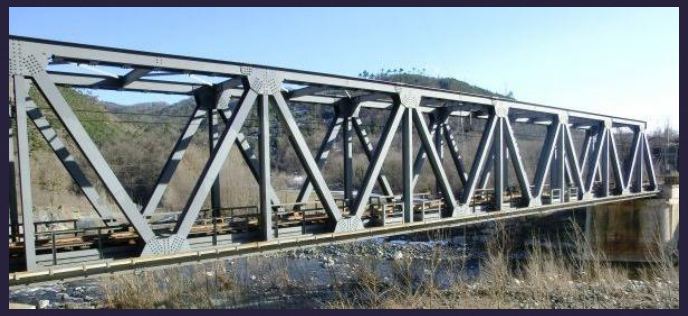


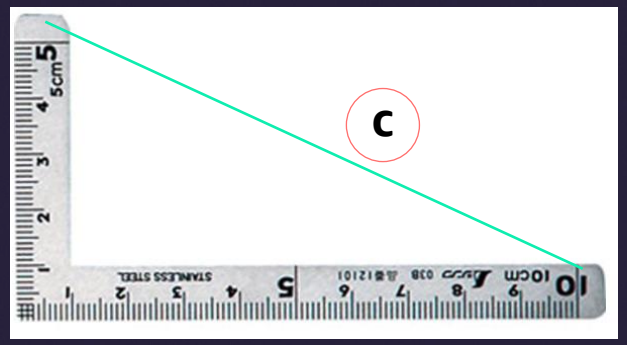


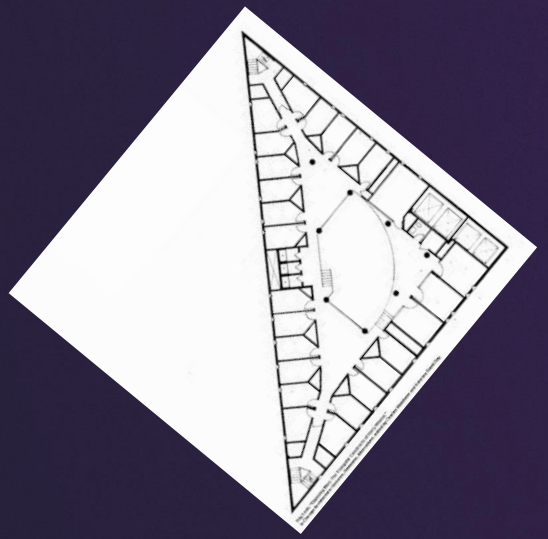


Machine learning takes some data and tries to find a **model** that hopefully will fit the remaining expected data

$$a^2 + b^2 = c^2$$

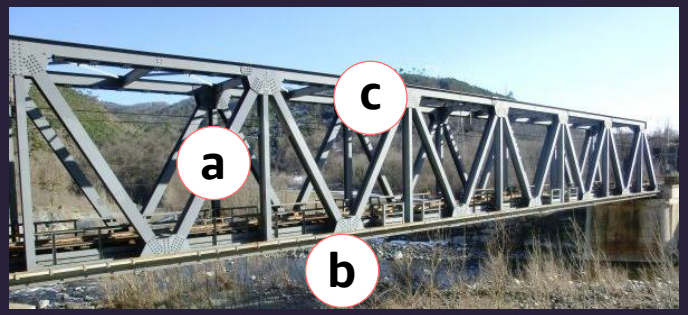


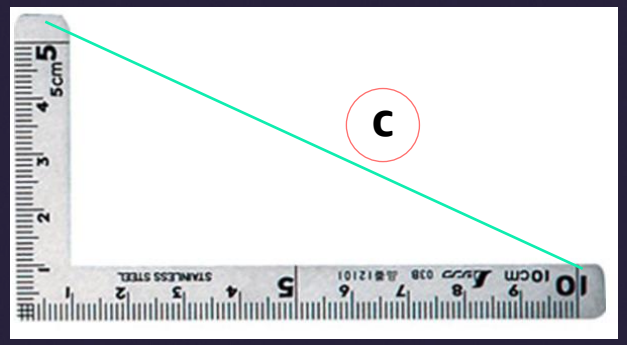


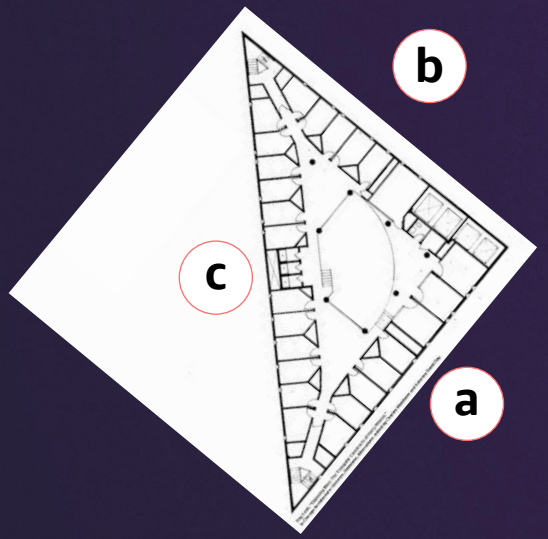


Machine learning takes some data and tries to find a **model** that hopefully will fit the remaining expected data

$$a^2 + b^2 = c^2$$

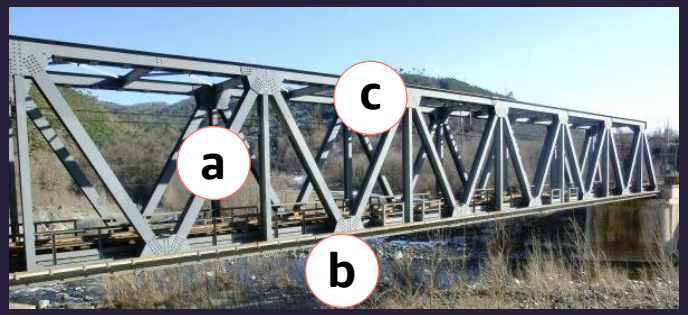


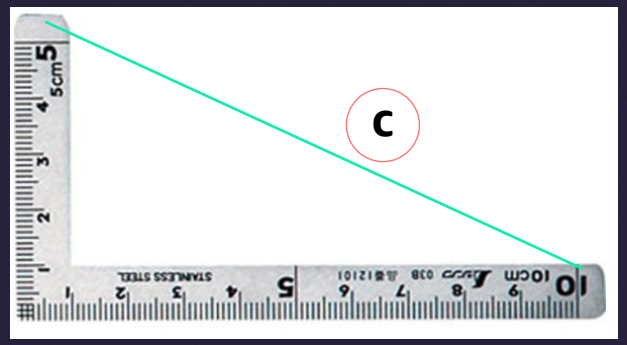


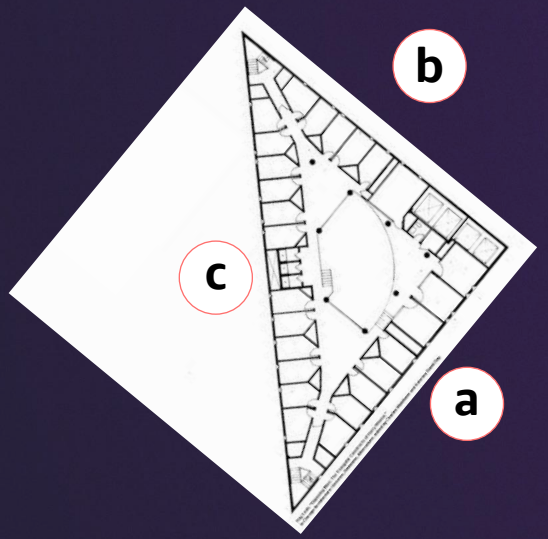


Machine learning takes some data and tries to find a **model** that hopefully will fit the remaining expected data

$$a^2 + b^2 = c^2$$

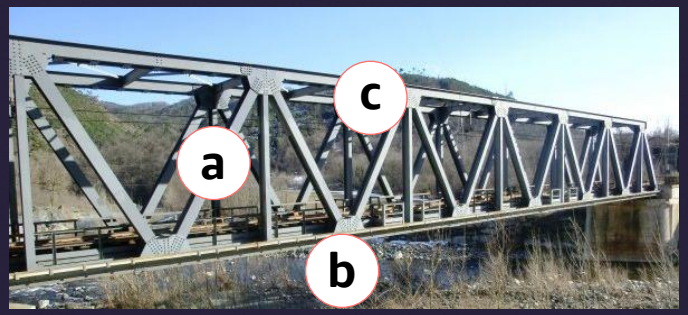


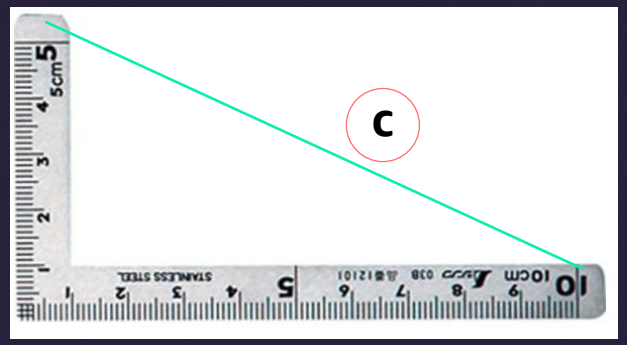


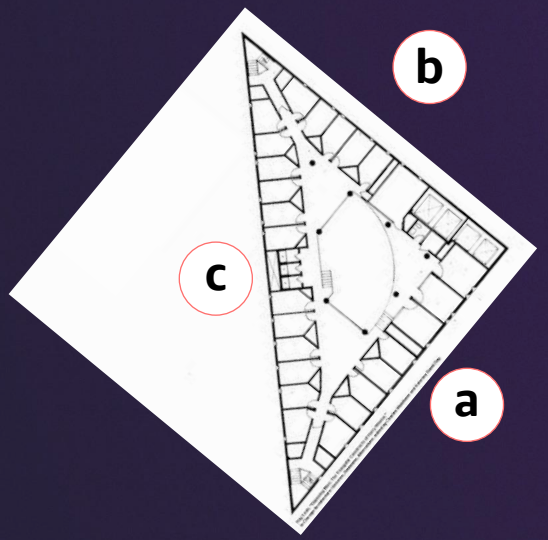


Machine learning takes some data and tries to find a **model** that hopefully will fit the remaining expected data

$$a^2 + b^2 = c^2$$





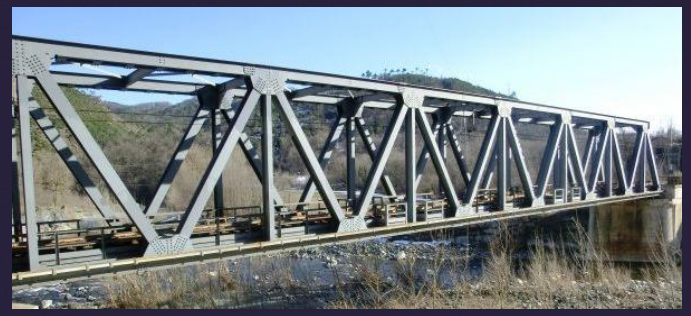


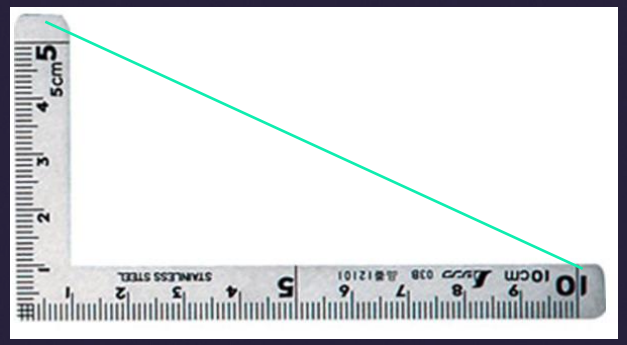
Machine learning takes some data and tries to find a **model** that hopefully will fit the remaining expected data

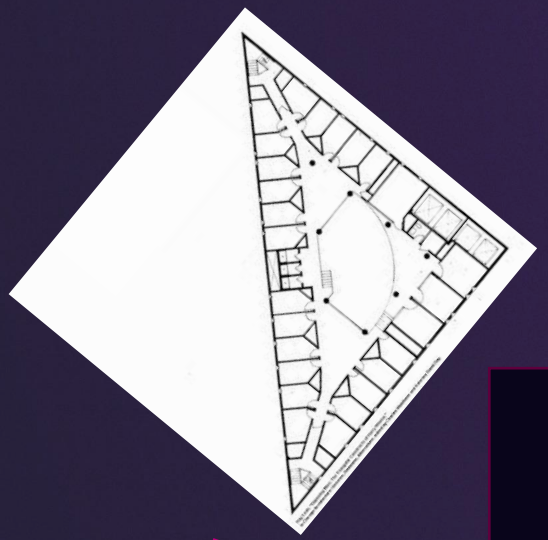
$a^2 + b^2 = c^2$

$a^2 + b^2 = c^{2.1}$

Sometimes inaccurate





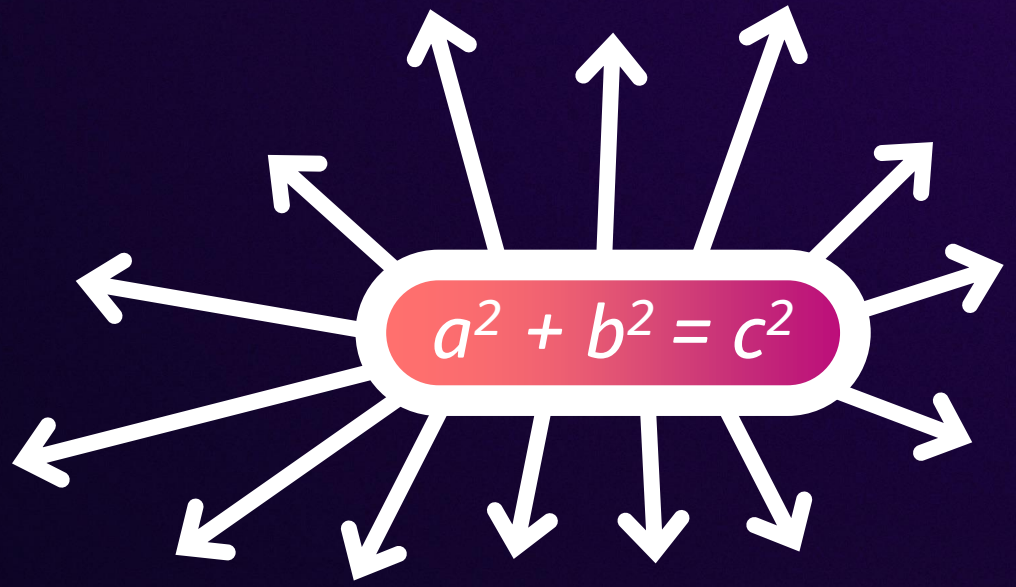


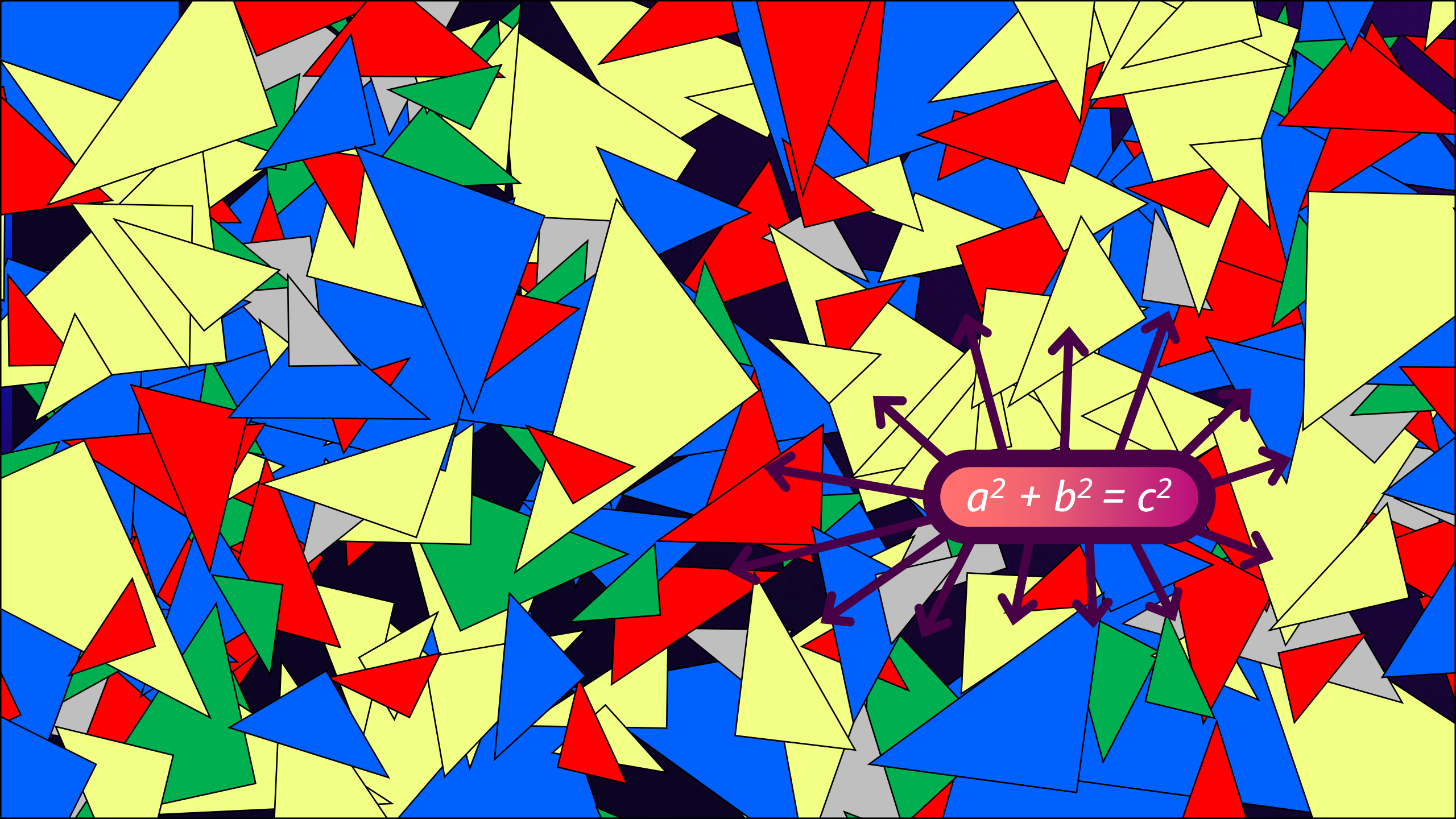
Inference/Testing

$a^2 + b^2 = c^2$

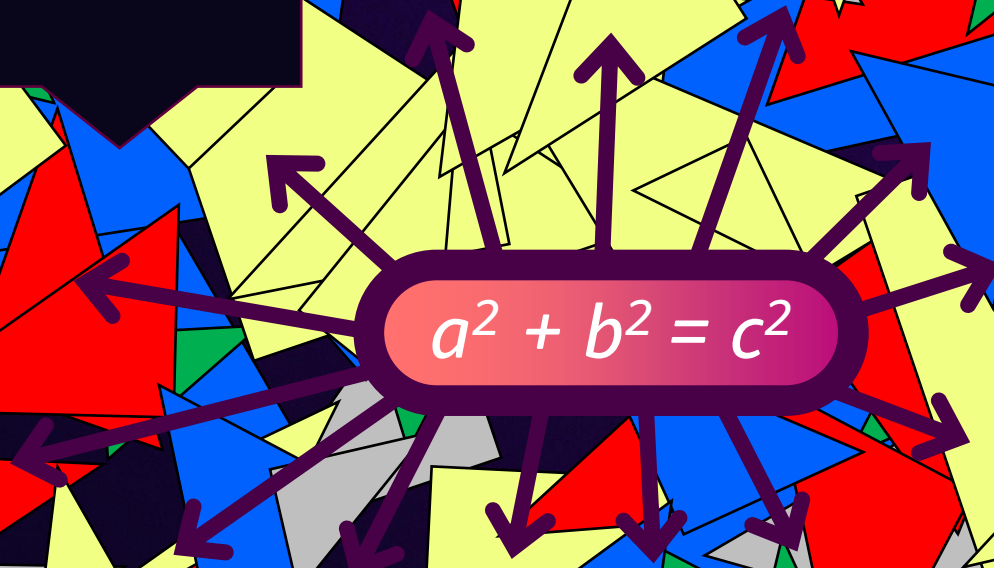
Training

Infinite set



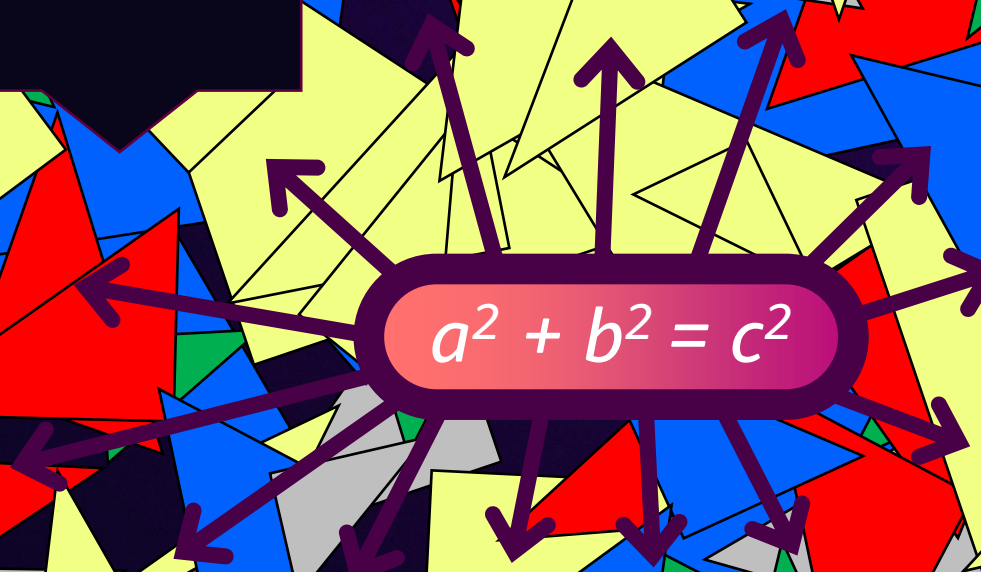

$a^2 + b^2 = c^2$

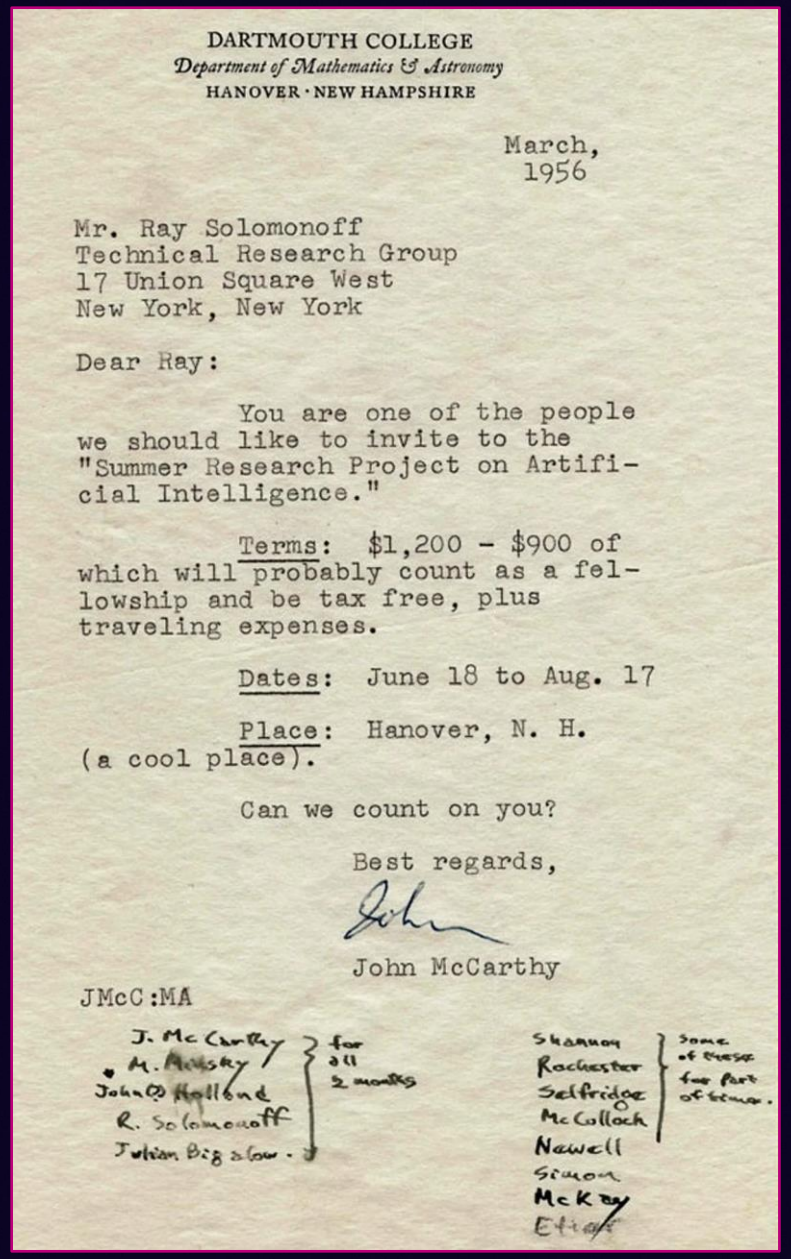
Reasoning is the act of talking ***accurately*** about ***all possible*** data a model can produce



Reasoning is the act of talking ***accurately*** about ***all possible*** data a model can produce

Even when infinite or intractably large





DARTMOUTH COLLEGE
Department of Mathematics & Astronomy
HANOVER · NEW HAMPSHIRE

March,
1956

Mr. Ray Solomonoff
Technical Research Group
17 Union Square West
New York, New York

Dear Ray:

You are one of the people we should like to invite to the "Summer Research Project on Artificial Intelligence."

Terms: $1,200 - $900 of which will probably count as a fellowship and be tax free, plus traveling expenses.

Dates: June 18 to Aug. 17

Place: Hanover, N. H. (a cool place).

Can we count on you?

Best regards,

John McCarthy

JMcC:MA

J. McCarthy
M. Minsky
John Holland
R. Solomonoff
Julian Bigelow
} for all 2 months

Shannon
Rochester
Selfridge
McCulloch
Newell
Simon
McKay
Ethe
} some of these for part of time.

AI

Connectionist AI

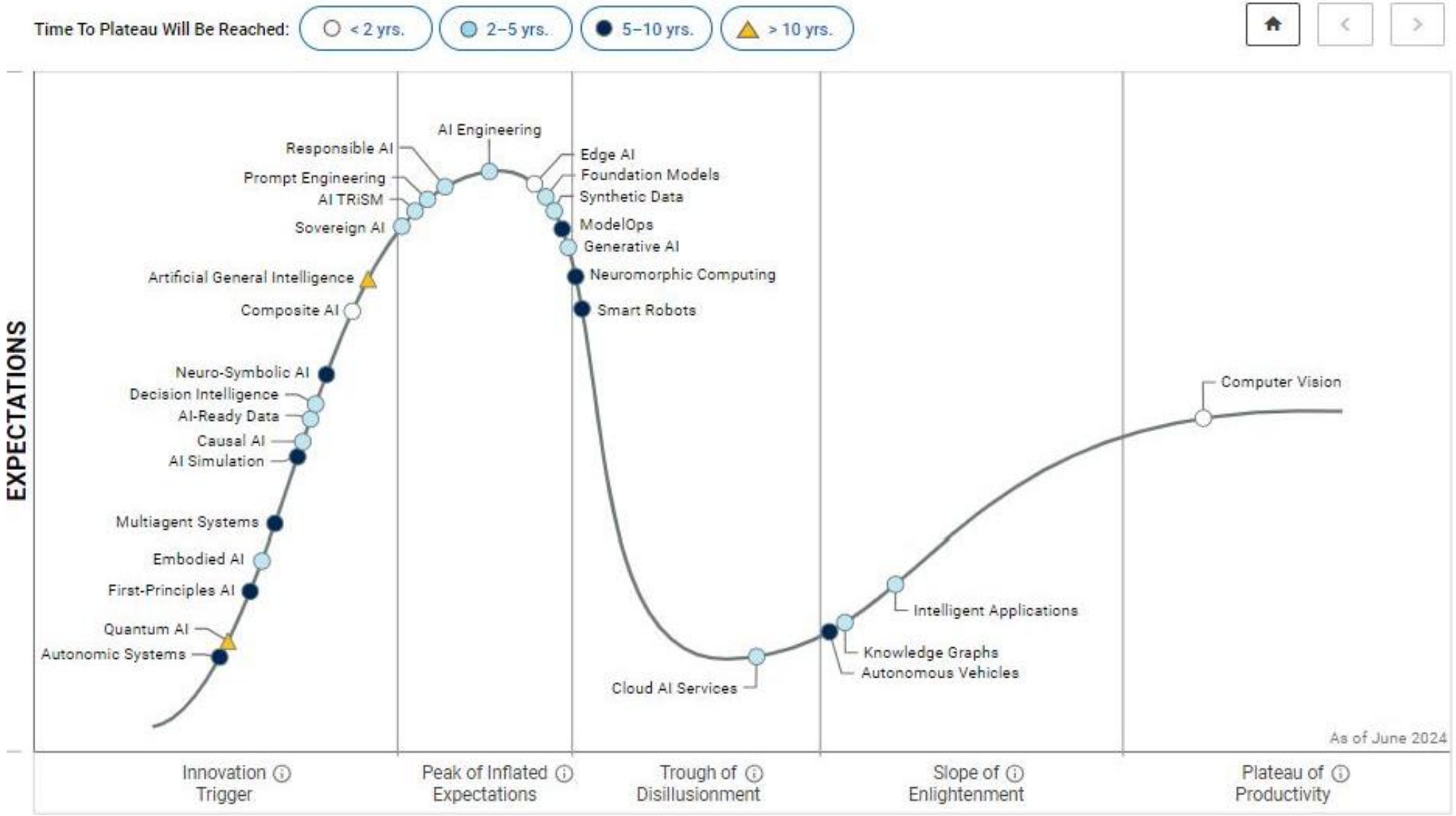
Symbolic AI

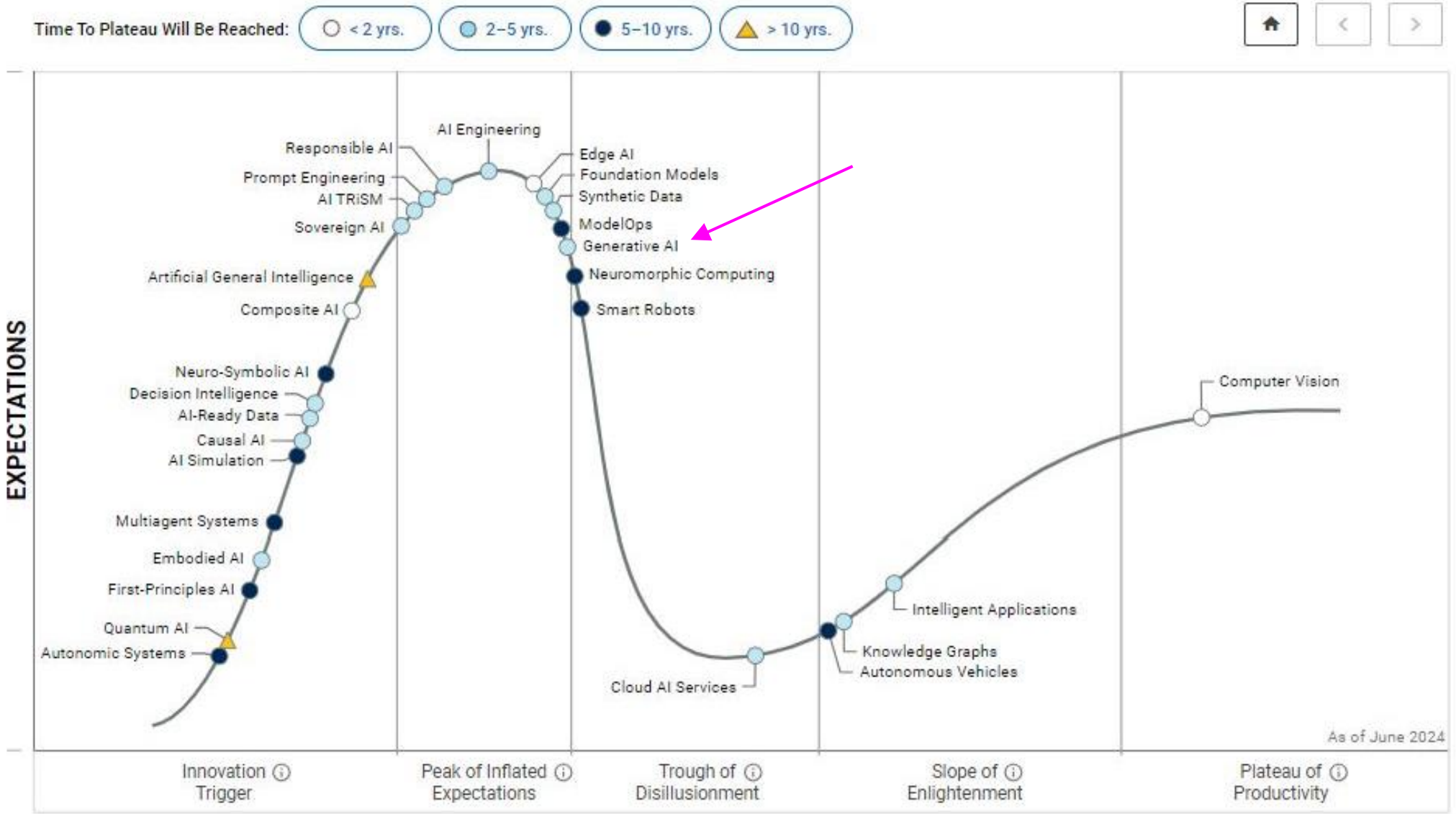
Probabilistic AI

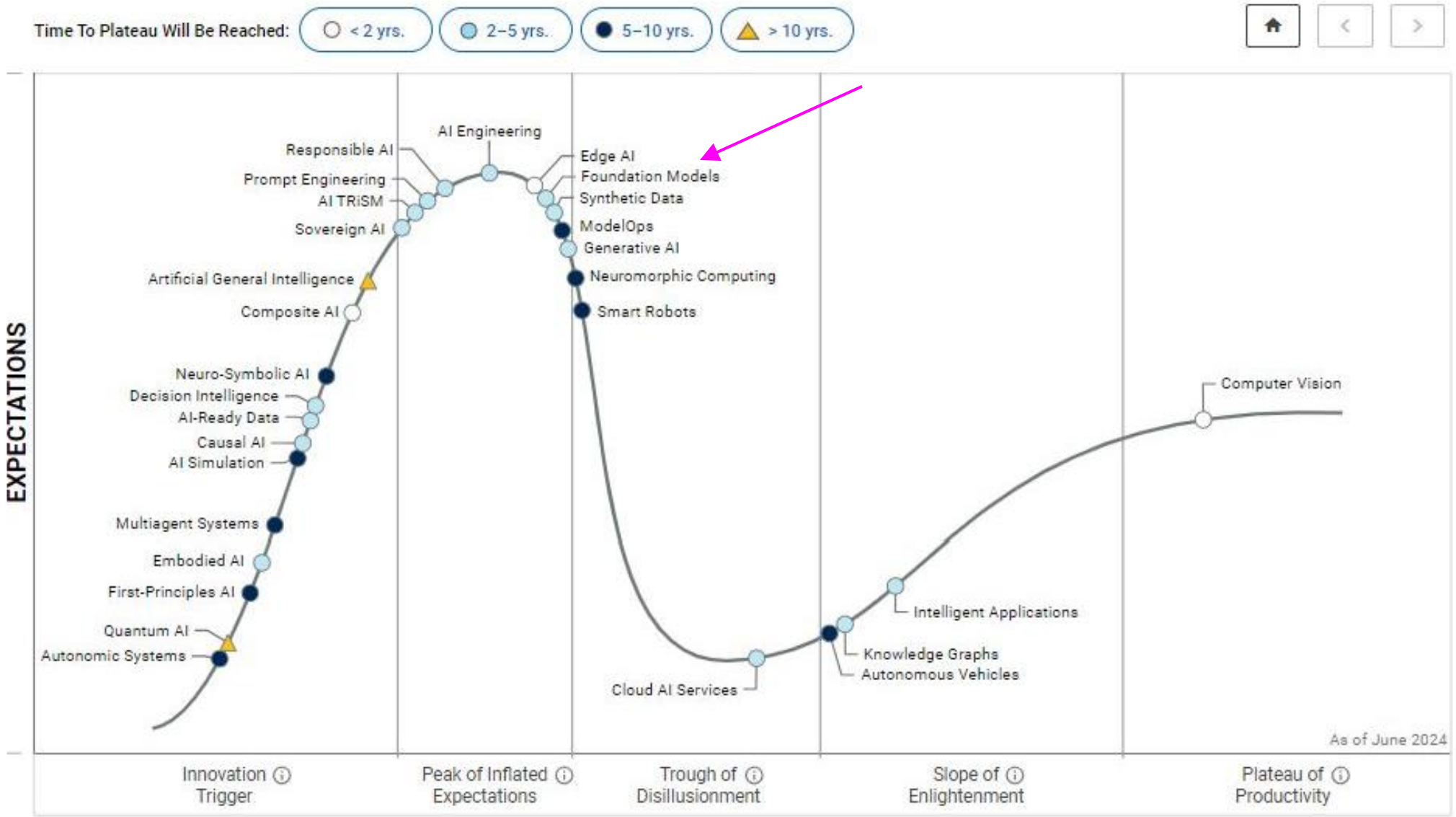
"Machine Learning"

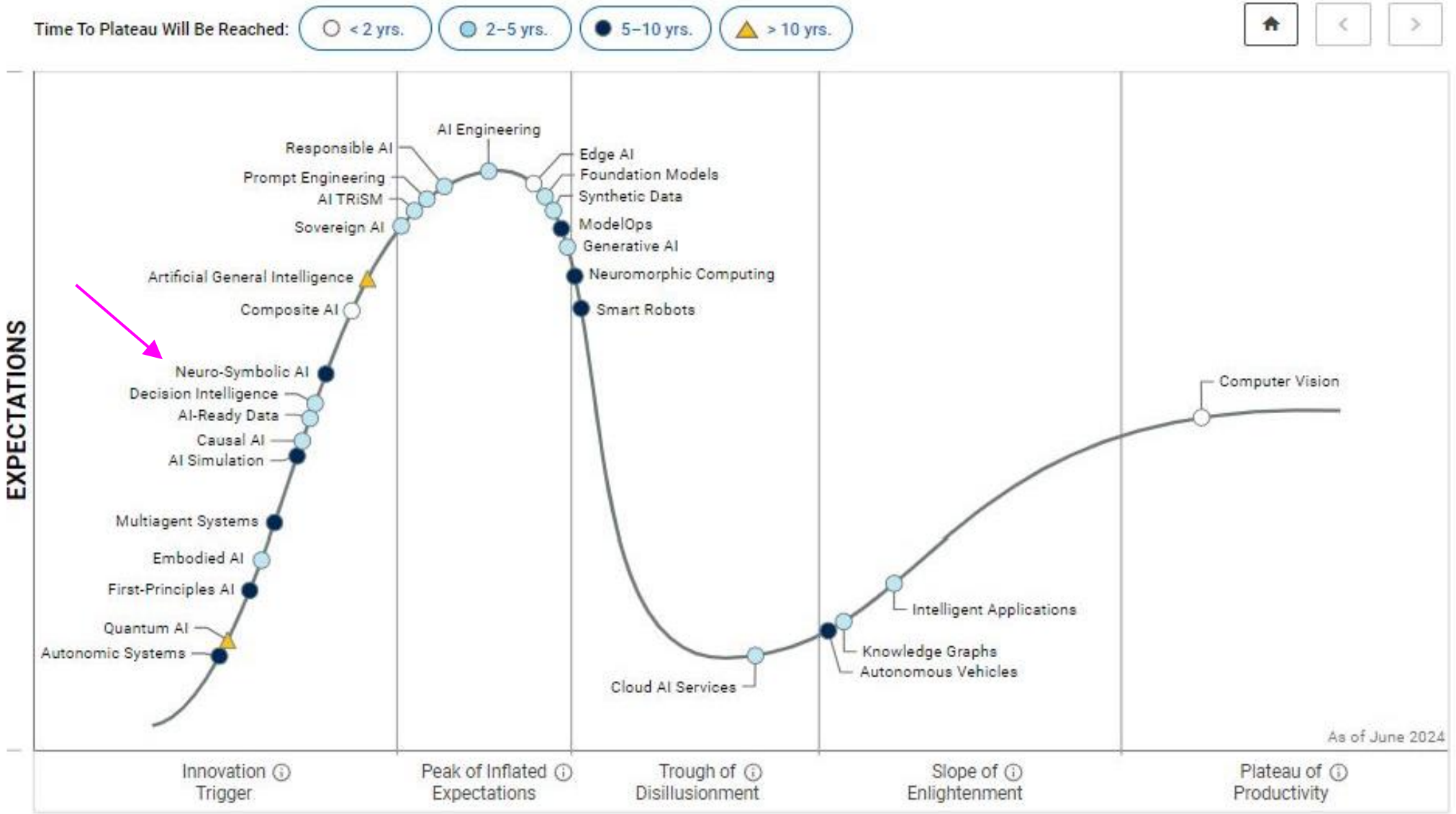
"Automated Reasoning"

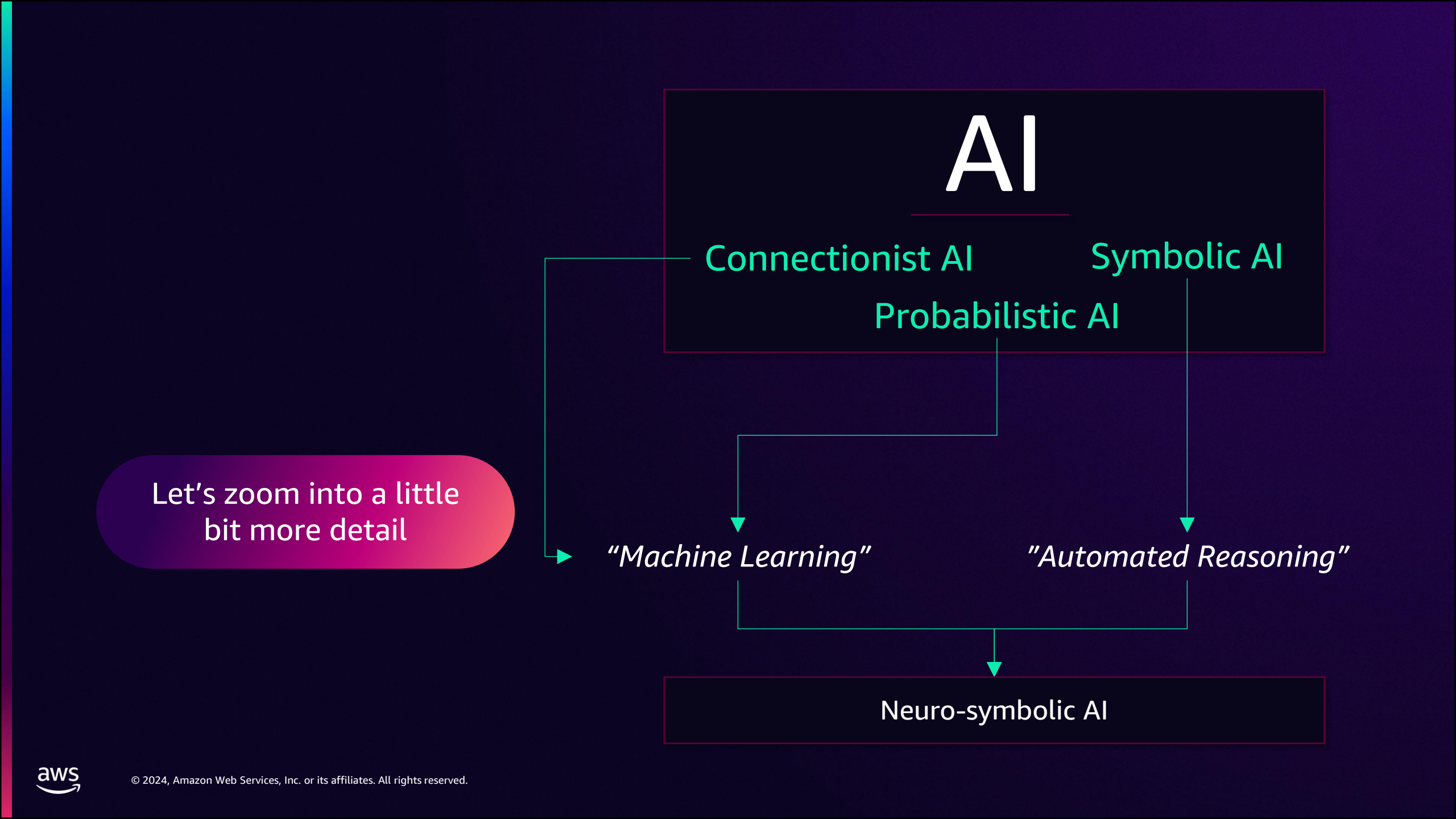
Neuro-symbolic AI

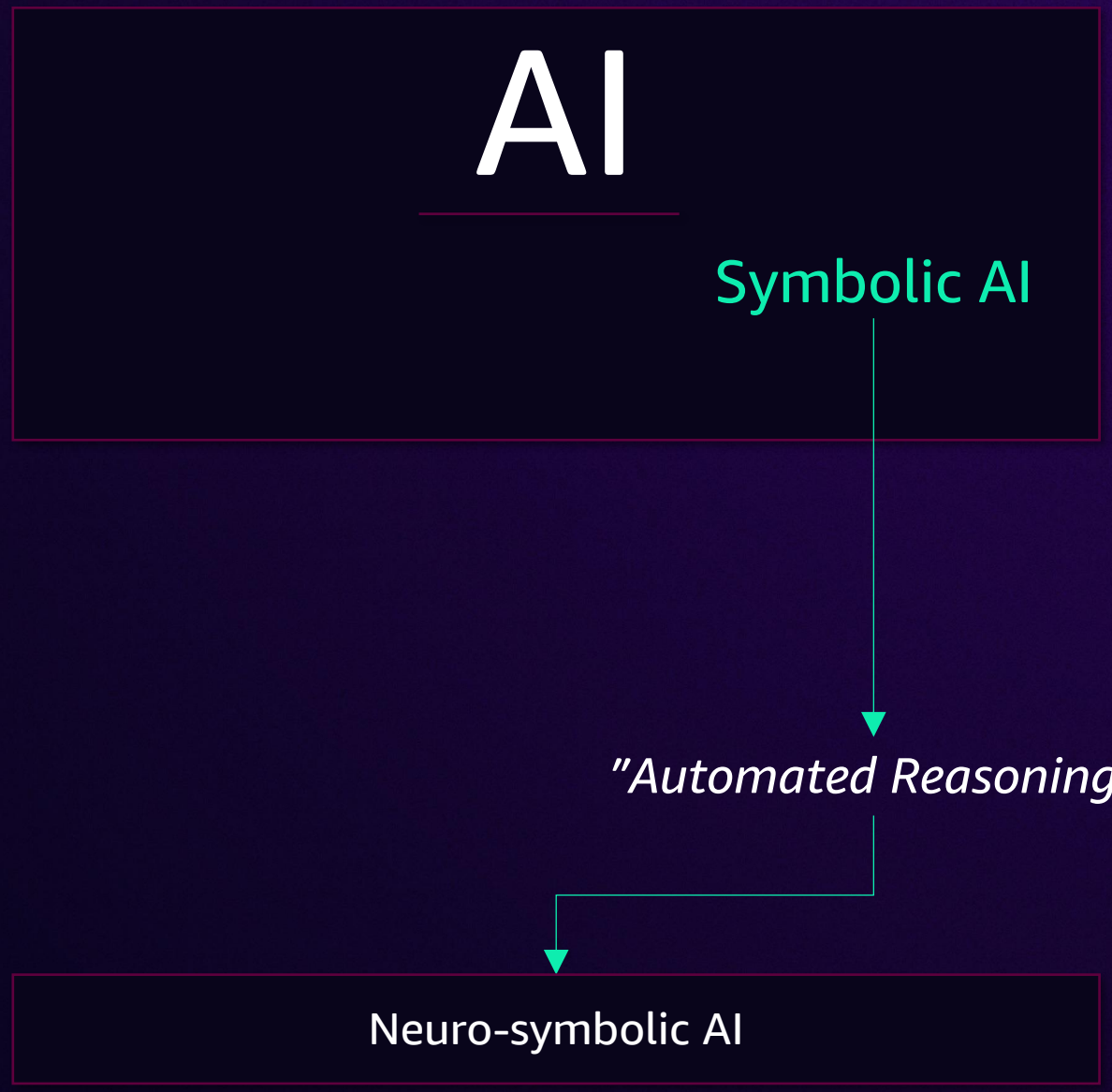




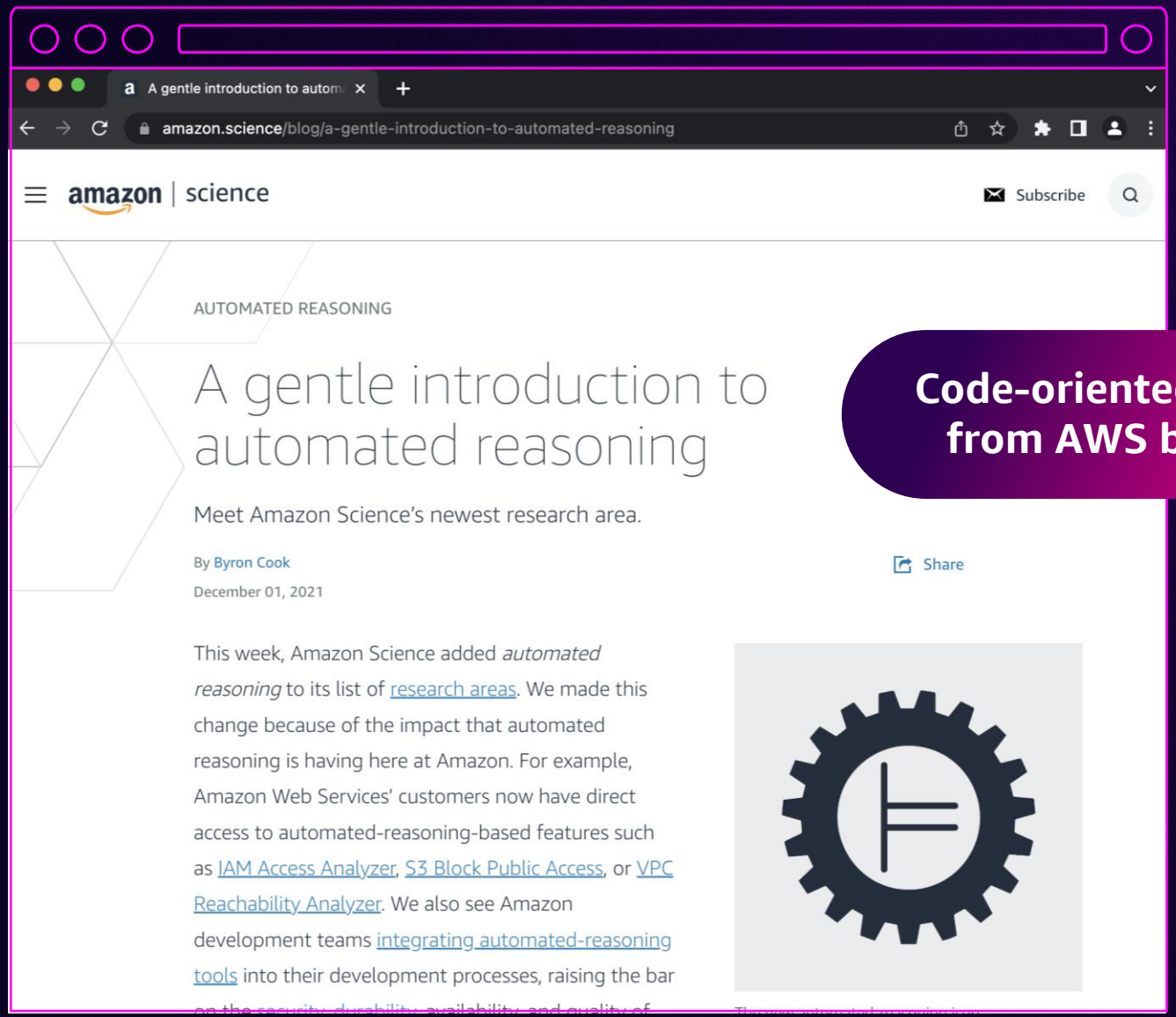








Let’s zoom into a little bit more detail



Code-oriented example from AWS blog post

```
assert isinstance(x,int) and isinstance(y,int)

if y > 0:
  while x > y:
    x = x - y
```

```
assert isinstance(x,int) and isinstance(y,int)

if y > 0:
  while x > y:
    x = x - y
```

Could this run infinitely?

```
assert isinstance(x,int) and isinstance(y,int)

if y > 0:
  while x > y:
    x = x - y
```

Could this run infinitely?

Assume the processor and interpreter are operating correctly

```
if y > 0:
  while x > y:
    x = x - y
```

Will eventually fail (no matter the initial values of x and y

```
if y > 0:
  while x > y:
    x = x - y
```

Will eventually fail (no matter the initial values of x and y

Reason: x-y is decreasing

```
if y > 0:
  while x > y:
    x = x - y
```

Reason: x-y is decreasing

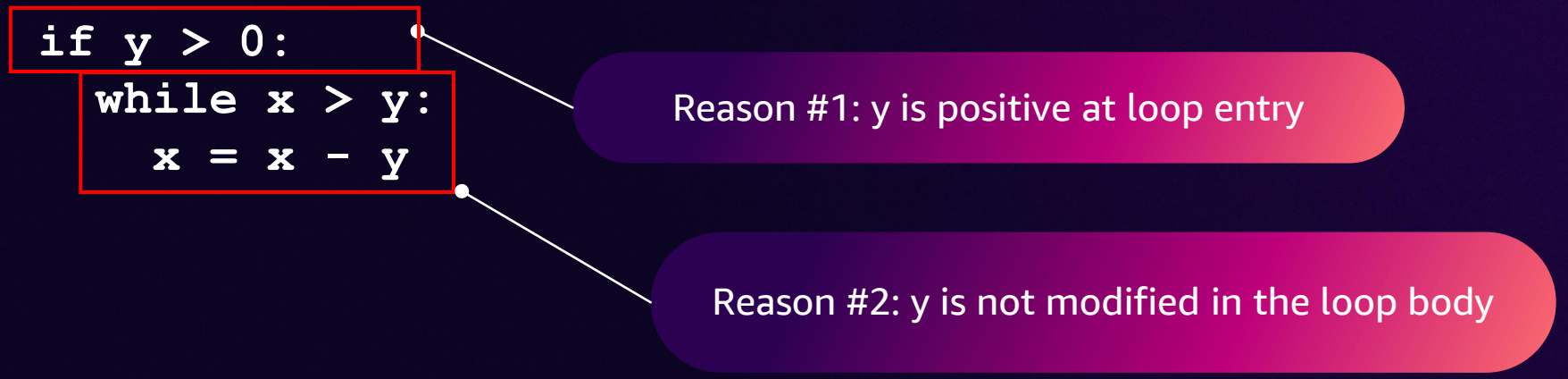
```
if y > 0:
  while x > y:
    x = x - y
```

Reason: y is positive and constant

Reason: x-y is decreasing

```
if y > 0:
  while x > y:
    x = x - y
```

Reason: y is positive and constant



```
if y > 0:
  while x > y:
    x = x - y
```

Thus: loop always terminates for all values of x and y

```
if y > 0:
  while x > y:
    x = x - y
```

Thus: loop always terminates for all values of x and y

Termination cannot be exhaustively tested

a.k.a. *symbolic* AI

What *is* automated reasoning?

a.k.a. *symbolic* AI

What *is* automated reasoning?

Let’s zoom even deeper into detail

```
1: if y > 0:
2:   while x > y:
3:     x = x - y
4:
```

Let's zoom into even more detail

The *semantics* of the loop in mathematical logic / set theory

$$
\begin{aligned}
R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) > 0) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) \leq 0) && \Rightarrow (t(\mathrm{p}) = 4 \ \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) > s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) \leq s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\
& \}
\end{aligned}
$$

```
1: if y > 0:
2:   while x > y:
3:     x = x - y
4:
```

We transition between two states

$$
\begin{aligned}
R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) > 0) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) \leq 0) && \Rightarrow (t(\mathrm{p}) = 4 \ \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) > s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) \leq s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\
& \}
\end{aligned}
$$

```
1: if y > 0:
2:   while x > y:
3:     x = x - y
4:
```

The case where we enter the loop

$$
\begin{aligned}
R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1\ \wedge s(\mathrm{y}) > 0) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 1\ \wedge s(\mathrm{y}) \leq 0) && \Rightarrow (t(\mathrm{p}) = 4\ \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 2\ \wedge s(\mathrm{x}) > s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\
& [(s(\mathrm{p}) = 2\ \wedge s(\mathrm{x}) \leq s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x})\ )] \\
& \} &&
\end{aligned}
$$

```
1: if y > 0:
2:   while x > y:
3:     x = x - y
4:
```

In the if statement

$$
\begin{aligned}
R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) > 0) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) \leq 0) && \Rightarrow (t(\mathrm{p}) = 4 \ \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) > s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) \leq s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\
& \}
\end{aligned}
$$

```
1: if y > 0:
2:   while x > y:
3:     x = x - y
4:
```

Going into the if branch

$$
\begin{aligned}
R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) > 0) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) \leq 0) && \Rightarrow (t(\mathrm{p}) = 4 \ \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) > s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) \leq s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\
& \} &&
\end{aligned}
$$

```
1: if y > 0:
2:   while x > y:
3:     x = x - y
4:
```

Post state is in the loop

$$
\begin{aligned}
R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) > 0) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) \leq 0) && \Rightarrow (t(\mathrm{p}) = 4 \ \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) > s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) \leq s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\
& \} &&
\end{aligned}
$$

```
1: if y > 0:
2:   while x > y:
3:     x = x - y
4:
```

y is unchanged

$$
\begin{aligned}
R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) > 0) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) \leq 0) && \Rightarrow (t(\mathrm{p}) = 4 \ \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) > s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) \leq s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\
& \} &&
\end{aligned}
$$

```
1: if y > 0:
2:   while x > y:
3:     x = x - y
4:
```

x is unchanged

$$
\begin{aligned}
R = \{(s,t) \mid & [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) > 0) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) \leq 0) && \Rightarrow (t(\mathrm{p}) = 4 \ \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) > s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) \leq s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\
& \} &&
\end{aligned}
$$

```
1: if y > 0:
2:   while x > y:
3:     x = x - y
4:
```

The case where we don't enter the loop

$$
\begin{aligned}
R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) > 0) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) \leq 0) && \Rightarrow (t(\mathrm{p}) = 4 \ \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) > s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) \leq s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\
\}&
\end{aligned}
$$

```
1: if y > 0:
2:   while x > y:
3:     x = x - y
4:
```

We skip the loop

$$
\begin{aligned}
R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) > 0) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) \leq 0) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) > s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) \leq s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\
& \} &&
\end{aligned}
$$

```
1: if y > 0:
2:   while x > y:
3:     x = x - y
4:
```

y is unchanged

$$
\begin{aligned}
R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) > 0) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) \leq 0) && \Rightarrow (t(\mathrm{p}) = 4 \ \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) > s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) \leq s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\
& \} &&
\end{aligned}
$$

```
1: if y > 0:
2:   while x > y:
3:     x = x - y
4:
```

x is unchanged

$$
\begin{aligned}
R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) > 0) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) \leq 0) && \Rightarrow (t(\mathrm{p}) = 4 \ \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) > s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) \leq s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\
& \}
\end{aligned}
$$

```
1: if y > 0:
2:   while x > y:
3:     x = x - y
4:
```

The case where we stay in the loop

$$
\begin{aligned}
R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) > 0) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) \leq 0) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) > s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\
& [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) \leq s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\
& \}
\end{aligned}
$$

```
1: if y > 0:
2:   while x > y:
3:     x = x - y
4:
```

We stay in the loop

$$
\begin{aligned}
R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) > 0) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) \leq 0) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) > s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) \leq s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\
& \} &&
\end{aligned}
$$

```
1: if y > 0:
2:   while x > y:
3:     x = x - y
4:
```

y is unchanged

$$
\begin{aligned}
R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) > 0) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) \leq 0) && \Rightarrow (t(\mathrm{p}) = 4 \ \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) > s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) \leq s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\
& \} &&
\end{aligned}
$$

```
1: if y > 0:
2:   while x > y:
3:     x = x - y
4:
```

x = x - y

$$
\begin{aligned}
R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) > 0) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) \leq 0) && \Rightarrow (t(\mathrm{p}) = 4 \ \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) > s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] && \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) \leq s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\
& \} &&
\end{aligned}
$$

```
1: if y > 0:
2:   while x > y:
3:     x = x - y
4:
```

The case where we exit the loop

$$
\begin{aligned}
R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) > 0) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) \leq 0) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) > s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\
& [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) \leq s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\
& \}
\end{aligned}
$$

```
if y > 0:
  while x > y:
    x = x - y
```

Text

Meaning

$$
\begin{aligned}
R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) > 0) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) \leq 0) && \Rightarrow (t(\mathrm{p}) = 4 \ \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) > s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) \leq s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\
& \}
\end{aligned}
$$

```
if y > 0:
  while x > y:
    x = x - y
```

Could this run infinitely? = Is this relation *well-founded*?

$$
\begin{aligned}
R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) > 0) && \Rightarrow \big(t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x})\big)] && \wedge \\
& [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) \leq 0) && \Rightarrow \big(t(\mathrm{p}) = 4 \ \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x})\big)] && \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) > s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] && \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) \leq s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\
& \}
\end{aligned}
$$

$R(a, b)$

Is this relation *well-founded*?

$$
\begin{aligned}
R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) > 0) && \Rightarrow \big(t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x})\big)] && \wedge \\
& [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) \leq 0) && \Rightarrow \big(t(\mathrm{p}) = 4 \ \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x})\big)] && \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) > s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) \leq s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\
& \}
\end{aligned}
$$

Entering loop

$R(a,b) \wedge a(\mathrm{p}) = 1$

Is this relation *well-founded*?

$$
\begin{aligned}
R = \{(s,t) \mid & [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) > 0) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) \leq 0) && \Rightarrow (t(\mathrm{p}) = 4 \ \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) > s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) \leq s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\
\} &
\end{aligned}
$$

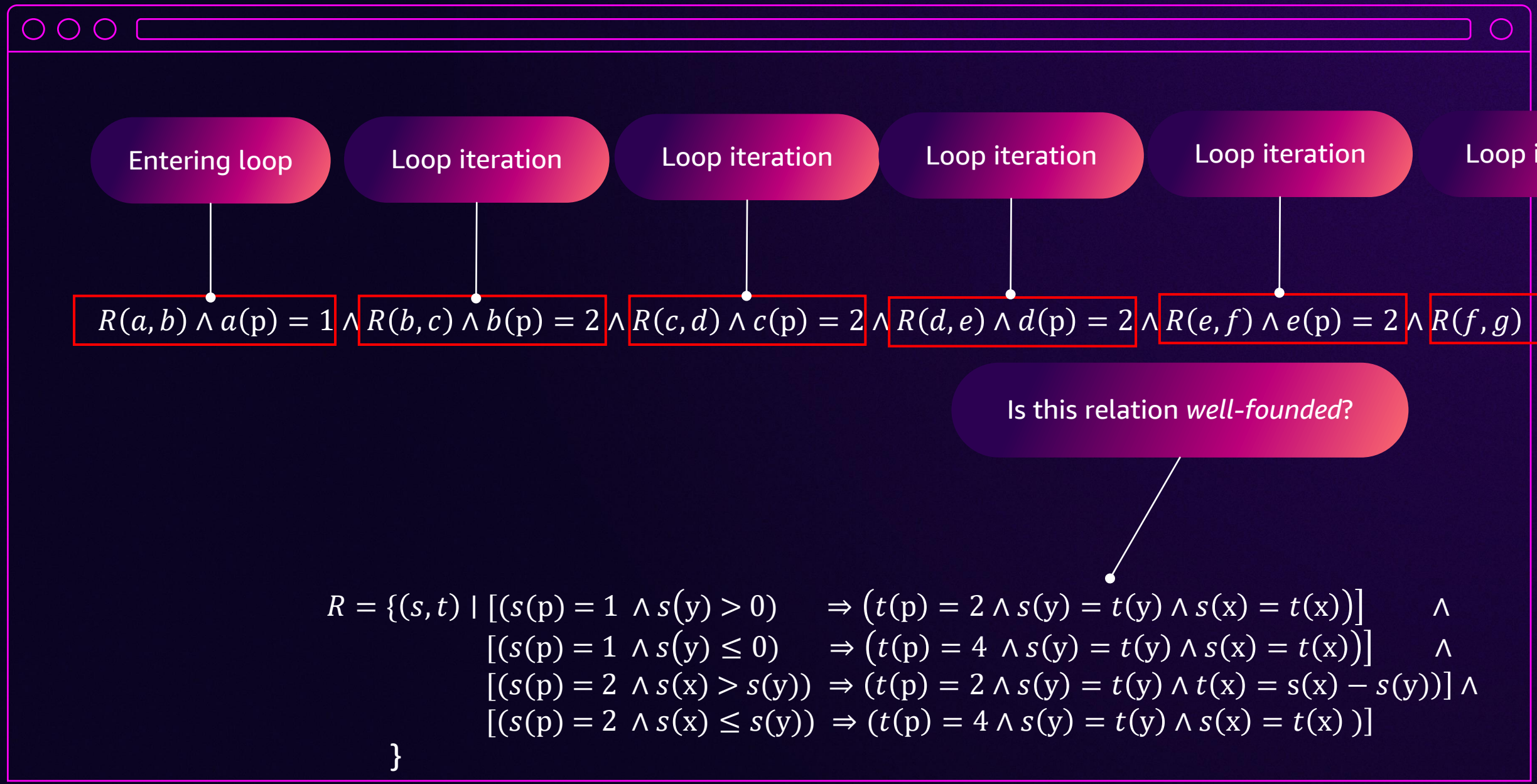
Entering loop

Loop iteration

$$R(a,b) \wedge a(\mathrm{p}) = 1 \wedge R(b,c) \wedge b(\mathrm{p}) = 2$$

Is this relation *well-founded*?

$$\begin{aligned} R = \{(s,t) \mid & [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) > 0) \ \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \ \wedge \\ & [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) \leq 0) \ \Rightarrow (t(\mathrm{p}) = 4 \ \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \ \wedge \\ & [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) > s(\mathrm{y})) \ \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\ & [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) \leq s(\mathrm{y})) \ \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\ \} & \end{aligned}$$



```
if y > 0:
  while x > y:
    x = x - y
```

Will eventually fail

=

Composition will eventually fail

$$
\begin{aligned}
R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) > 0) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) \leq 0) && \Rightarrow (t(\mathrm{p}) = 4 \ \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) > s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) \leq s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\
& \}
\end{aligned}
$$

```
if y > 0:
  while x > y:
    x = x - y
```

Composition

$$R(a,b) \wedge a(\mathrm{p}) = 1 \wedge R(b,c) \wedge b(\mathrm{p}) = 2$$

Will eventually fail

=

Composition will eventually fail

$$\begin{aligned} R = \{(s,t) \mid & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) > 0) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) \leq 0) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) > s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) \leq s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\ \} & \end{aligned}$$

```
if y > 0:
  while x > y:
    x = x - y
```

y is positive ~~and constant~~

$$
\begin{aligned}
R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) > 0) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) \leq 0) && \Rightarrow (t(\mathrm{p}) = 4 \ \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) > s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) \leq s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\
& \}
\end{aligned}
$$

```
if y > 0:
  while x > y:
    x = x - y
```

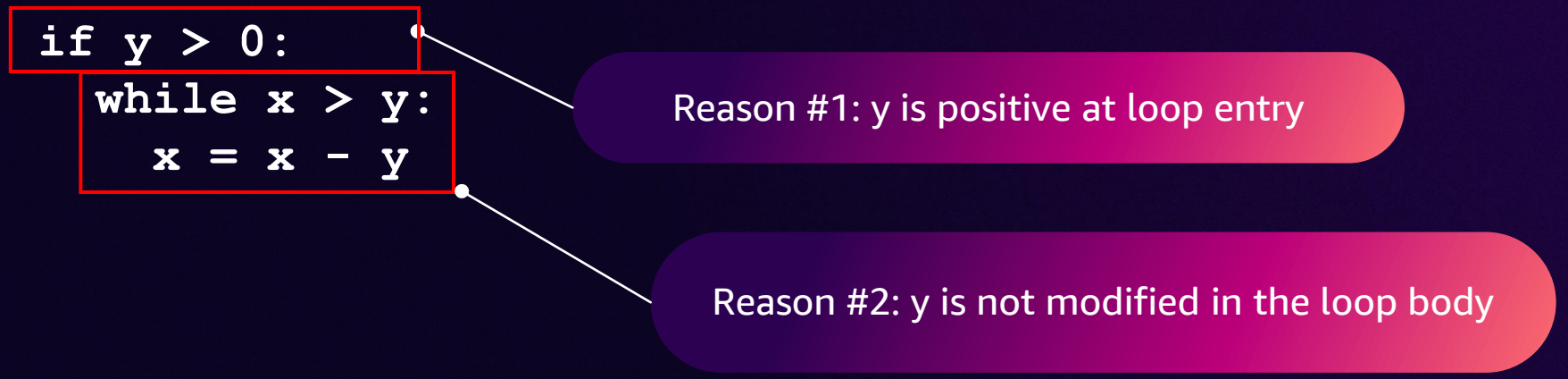
y is positive ~~and constant~~

Proof by induction

$$\forall s,t.\ [s(\mathrm{p}) \neq 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow t(\mathrm{y}) > 0$$

$$\forall s,t.\ [s(\mathrm{p}) = 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow s(\mathrm{y}) > 0 \Rightarrow t(\mathrm{y}) > 0$$

$$\begin{aligned} R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) > 0) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) \leq 0) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) > s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) \leq s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\ \} & \end{aligned}$$



```
if y > 0:
  while x > y:
    x = x - y
```

Reason #1:
Base case

$$\forall s,t.\ [s(\mathrm{p}) \neq 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow t(\mathrm{y}) > 0$$

$$\forall s,t.\ [s(\mathrm{p}) = 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow s(\mathrm{y}) > 0 \Rightarrow t(\mathrm{y}) > 0$$

$$\begin{aligned} R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) > 0) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) \leq 0) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) > s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) \leq s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\ \} & \end{aligned}$$

```
if y > 0:
  while x > y:
    x = x - y
```

We are not already in the loop

$$\forall s,t.\ [s(\mathrm{p}) \neq 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow t(\mathrm{y}) > 0$$

$$\forall s,t.\ [s(\mathrm{p}) = 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow s(\mathrm{y}) > 0 \Rightarrow t(\mathrm{y}) > 0$$

$$\begin{aligned} R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) > 0) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) \leq 0) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) > s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) \leq s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\ \} & \end{aligned}$$

```
if y > 0:
  while x > y:
    x = x - y
```

We have entered into the loop

$$\forall s,t.\ [s(\mathrm{p}) \neq 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow t(\mathrm{y}) > 0$$

$$\forall s,t.\ [s(\mathrm{p}) = 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow s(\mathrm{y}) > 0 \Rightarrow t(\mathrm{y}) > 0$$

$$\begin{aligned} R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) > 0) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) \leq 0) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) > s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) \leq s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\ \} & \end{aligned}$$

```
if y > 0:
  while x > y:
    x = x - y
```

We have taken a step in the program

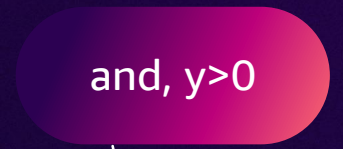
$$\forall s,t.\ [s(\mathrm{p}) \neq 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow t(\mathrm{y}) > 0$$

$$\forall s,t.\ [s(\mathrm{p}) = 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow s(\mathrm{y}) > 0 \Rightarrow t(\mathrm{y}) > 0$$

R defined here

$$\begin{aligned} R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) > 0) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) \leq 0) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) > s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) \leq s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\ \} & \end{aligned}$$

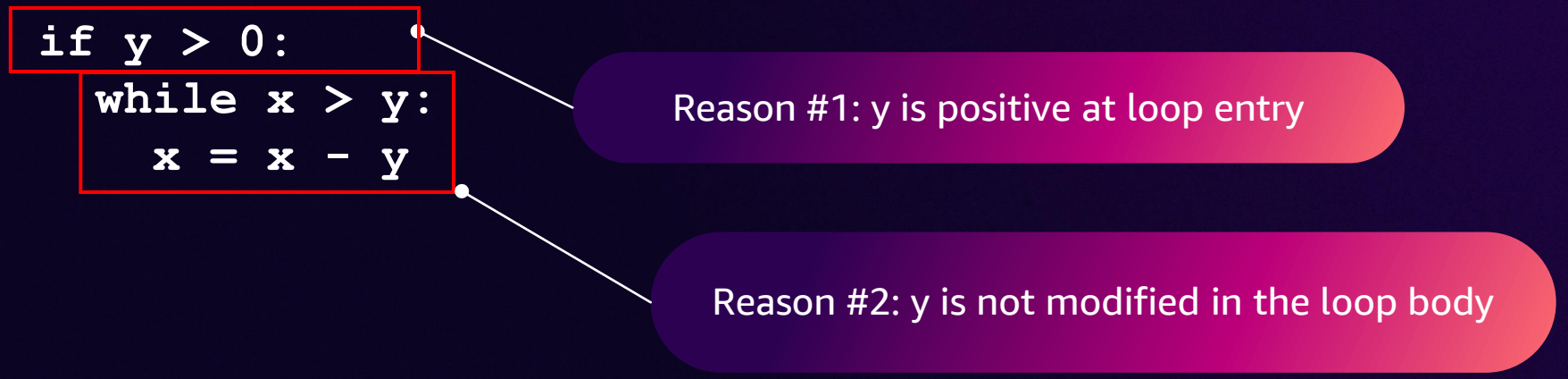
```
if y > 0:
  while x > y:
    x = x - y
```



$$\forall s,t.\ [s(\mathrm{p}) \neq 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow t(\mathrm{y}) > 0$$

$$\forall s,t.\ [s(\mathrm{p}) = 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow s(\mathrm{y}) > 0 \Rightarrow t(\mathrm{y}) > 0$$

$$\begin{aligned} R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) > 0) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) \leq 0) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) > s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) \leq s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\ \} & \end{aligned}$$



```
if y > 0:
  while x > y:
    x = x - y
```

Reason #2:
Step case

$$\forall s,t.\ [s(\mathrm{p}) \neq 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow t(\mathrm{y}) > 0$$

$$\forall s,t.\ [s(\mathrm{p}) = 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow s(\mathrm{y}) > 0 \Rightarrow t(\mathrm{y}) > 0$$

$$\begin{aligned} R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) > 0) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) \leq 0) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) > s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) \leq s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\ \} & \end{aligned}$$

```
if y > 0:
  while x > y:
    x = x - y
```

We are already in the loop

$$\forall s,t.\ [s(\mathrm{p}) \neq 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow t(\mathrm{y}) > 0$$

$$\forall s,t.\ [s(\mathrm{p}) = 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow s(\mathrm{y}) > 0 \Rightarrow t(\mathrm{y}) > 0$$

$$\begin{aligned} R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) > 0) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) \leq 0) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) > s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) \leq s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\ \} & \end{aligned}$$

```
if y > 0:
  while x > y:
    x = x - y
```

We are staying in the loop

$$\forall s,t.\ [s(\mathrm{p}) \neq 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow t(\mathrm{y}) > 0$$

$$\forall s,t.\ [s(\mathrm{p}) = 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow s(\mathrm{y}) > 0 \Rightarrow t(\mathrm{y}) > 0$$

$$\begin{aligned} R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) > 0) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) \leq 0) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) > s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) \leq s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\ \} & \end{aligned}$$

```
if y > 0:
  while x > y:
    x = x - y
```

We have taken a step in the program

$$\forall s,t.\ [s(\mathrm{p}) \neq 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow t(\mathrm{y}) > 0$$

$$\forall s,t.\ [s(\mathrm{p}) = 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow s(\mathrm{y}) > 0 \Rightarrow t(\mathrm{y}) > 0$$

R defined here

$$\begin{aligned} R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) > 0) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) \leq 0) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) > s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) \leq s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\ \} & \end{aligned}$$

```
if y > 0:
  while x > y:
    x = x - y
```

y>0 implies that it *stays* y>0

$$\forall s,t.\ [s(\mathrm{p}) \neq 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow t(\mathrm{y}) > 0$$

$$\forall s,t.\ [s(\mathrm{p}) = 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow s(\mathrm{y}) > 0 \Rightarrow t(\mathrm{y}) > 0$$

$$\begin{aligned} R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) > 0) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) \leq 0) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) > s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) \leq s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\ \} & \end{aligned}$$

```
if y > 0:
  while x > y:
    x = x - y
```

y is positive ***and constant***

Constant

$$\forall s,t.\ [s(\mathrm{p}) \neq 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow t(\mathrm{y}) > 0$$
$$\forall s,t.\ [s(\mathrm{p}) = 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow s(\mathrm{y}) > 0 \Rightarrow t(\mathrm{y}) > 0$$
$$\forall s,t.\ [s(\mathrm{p}) = 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow s(\mathrm{y}) = t(\mathrm{y})$$

$$\begin{aligned} R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) > 0) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) \leq 0) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) > s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) \leq s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\ \} & \end{aligned}$$

```
if y > 0:
  while x > y:
    x = x - y
```

Can all be automatically discharged with a mechanical theorem prover

$$\forall s,t.\ [s(\mathrm{p}) \neq 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow t(\mathrm{y}) > 0$$
$$\forall s,t.\ [s(\mathrm{p}) = 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow s(\mathrm{y}) > 0 \Rightarrow t(\mathrm{y}) > 0$$
$$\forall s,t.\ [s(\mathrm{p}) = 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow s(\mathrm{y}) = t(\mathrm{y})$$

$$\begin{aligned} R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) > 0) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) \leq 0) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) > s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) \leq s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\ \} & \end{aligned}$$

```
if y > 0:
  while x > y:
    x = x - y
```

Symbolic AI

Can all be automatically discharged with a mechanical theorem prover

$$\forall s,t.\ [s(\mathrm{p}) \neq 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow t(\mathrm{y}) > 0$$
$$\forall s,t.\ [s(\mathrm{p}) = 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow s(\mathrm{y}) > 0 \Rightarrow t(\mathrm{y}) > 0$$
$$\forall s,t.\ [s(\mathrm{p}) = 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow s(\mathrm{y}) = t(\mathrm{y})$$

$$\begin{aligned} R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) > 0) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) \leq 0) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) > s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) \leq s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\ \} & \end{aligned}$$

```
if y > 0:
  while x > y:
    x = x - y
```

Reasoning accurately about infinite sets

$$\forall s,t.\ [s(\mathrm{p}) \neq 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow t(\mathrm{y}) > 0$$

$$\forall s,t.\ [s(\mathrm{p}) = 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow s(\mathrm{y}) > 0 \Rightarrow t(\mathrm{y}) > 0$$

$$\forall s,t.\ [s(\mathrm{p}) = 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow s(\mathrm{y}) = t(\mathrm{y})$$

$$\begin{aligned} R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) > 0) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) \leq 0) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) > s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) \leq s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\ \} & \end{aligned}$$

Symbolic AI

```
if y > 0:
  while x > y:
    x = x - y
```

Reasoning accurately about infinite sets

$$\forall s,t.\ [s(\mathrm{p}) \neq 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow t(\mathrm{y}) > 0$$

$$\forall s,t.\ [s(\mathrm{p}) = 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow s(\mathrm{y}) > 0 \Rightarrow t(\mathrm{y}) > 0$$

$$\forall s,t.\ [s(\mathrm{p}) = 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t)] \Rightarrow s(\mathrm{y}) = t(\mathrm{y})$$

$$\begin{aligned} R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) > 0) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) \leq 0) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) > s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) \leq s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\ \} & \end{aligned}$$

```
if y > 0:
  while x > y:
    x = x - y
```

x-y is decreasing

$$
\begin{aligned}
R = \{(s,t) \mid & [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) > 0) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) \leq 0) && \Rightarrow (t(\mathrm{p}) = 4 \ \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) > s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) \leq s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\
& \}
\end{aligned}
$$

```
if y > 0:
  while x > y:
    x = x - y
```

x-y is decreasing

$$\forall s,t.\ [s(\mathrm{p}) = 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t) \wedge Q(s,t))] \Rightarrow s(\mathrm{x}) - s(\mathrm{y}) > t(\mathrm{x}) - t(\mathrm{y})$$

x-y is decreasing

$$\begin{aligned} R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) > 0) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) \leq 0) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) > s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) \leq s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\ \} & \end{aligned}$$

```
if y > 0:
  while x > y:
    x = x - y
```

$$\forall s,t.\ [s(\mathrm{p}) = 2 \land t(\mathrm{p}) = 2 \land R(s,t) \land Q(s,t))] \Rightarrow s(\mathrm{x}) - s(\mathrm{y}) > t(\mathrm{x}) - t(\mathrm{y})$$

Q:

$$\forall s,t.\ [s(\mathrm{p}) \neq 2 \land t(\mathrm{p}) = 2 \land R(s,t)] \Rightarrow t(\mathrm{y}) > 0$$
$$\forall s,t.\ [s(\mathrm{p}) = 2 \land t(\mathrm{p}) = 2 \land R(s,t)] \Rightarrow s(y) > 0 \Rightarrow t(\mathrm{y}) > 0$$
$$\forall s,t.\ [s(\mathrm{p}) = 2 \land t(\mathrm{p}) = 2 \land R(s,t)] \Rightarrow s(\mathrm{y}) = t(\mathrm{y})$$

$$\begin{aligned} R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1\ \land s(\mathrm{y}) > 0) && \Rightarrow (t(\mathrm{p}) = 2 \land s(\mathrm{y}) = t(\mathrm{y}) \land s(\mathrm{x}) = t(\mathrm{x}))] && \land \\ & [(s(\mathrm{p}) = 1\ \land s(\mathrm{y}) \leq 0) && \Rightarrow (t(\mathrm{p}) = 4\ \land s(\mathrm{y}) = t(\mathrm{y}) \land s(\mathrm{x}) = t(\mathrm{x}))] && \land \\ & [(s(\mathrm{p}) = 2\ \land s(\mathrm{x}) > s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 2 \land s(\mathrm{y}) = t(\mathrm{y}) \land t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \land \\ & [(s(\mathrm{p}) = 2\ \land s(\mathrm{x}) \leq s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 4 \land s(\mathrm{y}) = t(\mathrm{y}) \land s(\mathrm{x}) = t(\mathrm{x})\ )] \\ \} & \end{aligned}$$

```
if y > 0:
  while x > y:
    x = x - y
```

Can be automatically discharged with a mechanical theorem prover

$$\forall s,t.\ [s(\mathrm{p}) = 2 \land t(\mathrm{p}) = 2 \land R(s,t) \land Q(s,t))] \Rightarrow s(\mathrm{x}) - s(\mathrm{y}) > t(\mathrm{x}) - t(\mathrm{y})$$

$$\begin{aligned} R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \land s(\mathrm{y}) > 0) \Rightarrow (t(\mathrm{p}) = 2 \land s(\mathrm{y}) = t(\mathrm{y}) \land s(\mathrm{x}) = t(\mathrm{x}))] \land \\ & [(s(\mathrm{p}) = 1 \land s(\mathrm{y}) \leq 0) \Rightarrow (t(\mathrm{p}) = 4 \land s(\mathrm{y}) = t(\mathrm{y}) \land s(\mathrm{x}) = t(\mathrm{x}))] \land \\ & [(s(\mathrm{p}) = 2 \land s(\mathrm{x}) > s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 2 \land s(\mathrm{y}) = t(\mathrm{y}) \land t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \land \\ & [(s(\mathrm{p}) = 2 \land s(\mathrm{x}) \leq s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 4 \land s(\mathrm{y}) = t(\mathrm{y}) \land s(\mathrm{x}) = t(\mathrm{x}))] \\ \} & \end{aligned}$$

```
if y > 0:
  while x > y:
    x = x - y
```

Reasoning accurately about infinite sets

$$\forall s,t.\ [s(\mathrm{p}) = 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t) \wedge Q(s,t))] \Rightarrow s(\mathrm{x}) - s(\mathrm{y}) > t(\mathrm{x}) - t(\mathrm{y})$$

$$\begin{aligned} R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) > 0) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) \leq 0) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) > s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) \leq s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\ \} & \end{aligned}$$

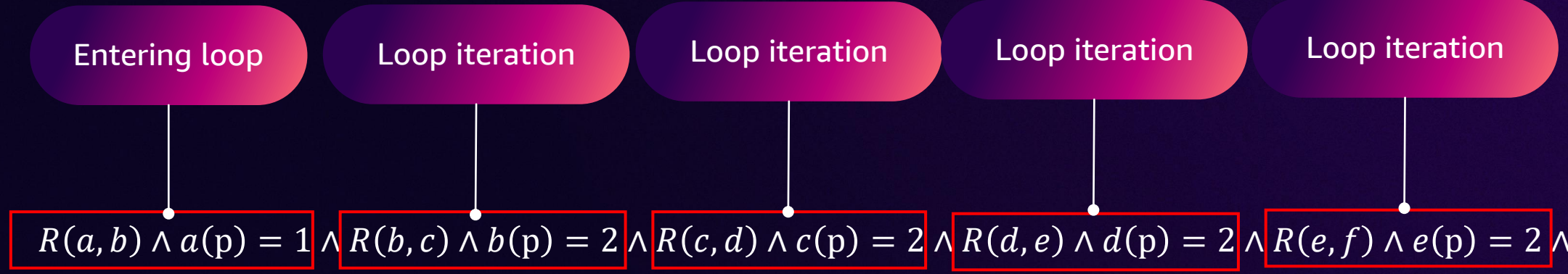
Symbolic AI

Reasoning accurately about infinite sets

```
if y > 0:
  while x > y:
    x = x - y
```

$$\forall s,t.\ [s(\mathrm{p}) = 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t) \wedge Q(s,t))] \Rightarrow s(\mathrm{x}) - s(\mathrm{y}) > t(\mathrm{x}) - t(\mathrm{y})$$

$$\begin{aligned} R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) > 0) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 1 \wedge s(\mathrm{y}) \leq 0) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) > s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\ & [(s(\mathrm{p}) = 2 \wedge s(\mathrm{x}) \leq s(\mathrm{y})) \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\ \} & \end{aligned}$$



x-y is decreasing

$$\forall s,t.\ [s(\mathrm{p}) = 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t) \wedge Q(s,t))] \Rightarrow s(\mathrm{x}) - s(\mathrm{y}) > t(\mathrm{x}) - t(\mathrm{y})$$

$$R(a,b) \wedge a(\mathrm{p}) = 1 \wedge R(b,c) \wedge b(\mathrm{p}) = 2 \wedge R(c,d) \wedge c(\mathrm{p}) = 2 \wedge R(d,e) \wedge d(\mathrm{p}) = 2 \wedge R(e,f) \wedge e(\mathrm{p}) = 2 \wedge \cdots$$

x-y is decreasing

$$\forall s,t.\ [s(\mathrm{p}) = 2 \wedge t(\mathrm{p}) = 2 \wedge R(s,t) \wedge Q(s,t))] \Rightarrow s(\mathrm{x}) - s(\mathrm{y}) > t(\mathrm{x}) - t(\mathrm{y})$$

$$R(a,b) \wedge a(\mathrm{p}) = 1 \wedge R(b,c) \wedge b(\mathrm{p}) = 2 \wedge R(c,d) \wedge c(\mathrm{p}) = 2 \wedge R(d,e) \wedge d(\mathrm{p}) = 2 \wedge R(e,f) \wedge e(\mathrm{p}) = 2 \wedge \cdots$$

$$b(\mathrm{y}) - b(\mathrm{x}) \quad > \quad c(\mathrm{y}) - c(\mathrm{x}) \quad > \quad d(\mathrm{y}) - d(\mathrm{x}) \quad > \quad e(\mathrm{y}) - e(\mathrm{x}) \quad > \quad \cdots$$

R is isomorphic to a sub-relation over (>,p-ints)

$$
\begin{aligned}
R = \{(s,t) \mid & [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) > 0) \ \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \ \wedge \\
& [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) \leq 0) \ \Rightarrow (t(\mathrm{p}) = 4 \ \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \ \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) > s(\mathrm{y})) \ \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) \leq s(\mathrm{y})) \ \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\
\}
\end{aligned}
$$

R is isomorphic to a sub-relation over (>,p-ints)

(>,p-ints) is well-founded

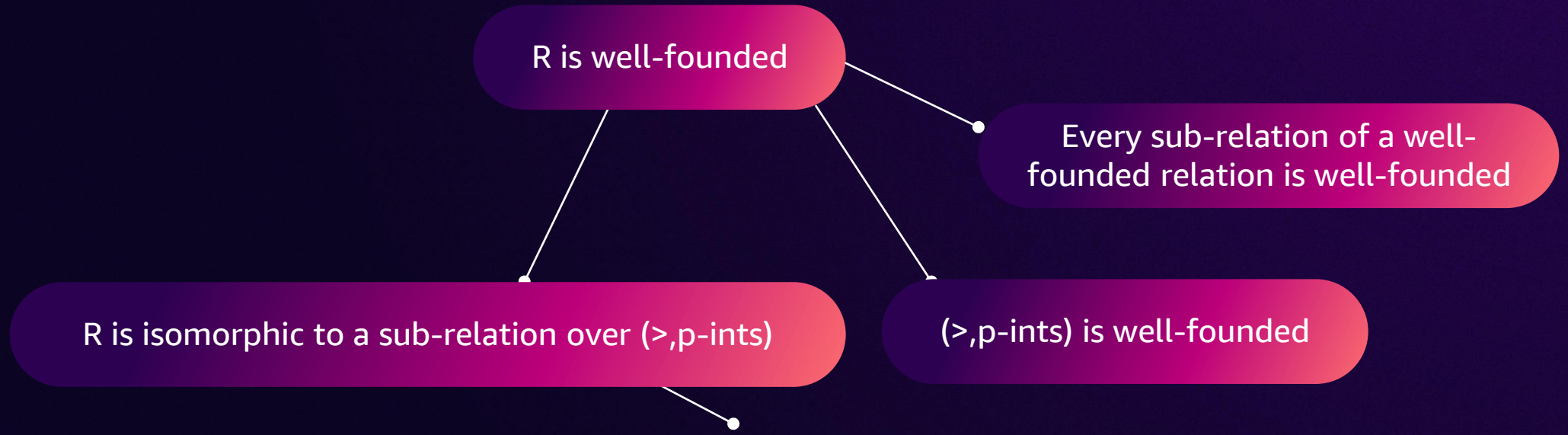
$$
\begin{aligned}
R = \{(s,t) \mid & [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) > 0) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) \leq 0) && \Rightarrow (t(\mathrm{p}) = 4 \ \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) > s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) \leq s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\
\}
\end{aligned}
$$

Every sub-relation of a well-founded relation is well-founded

R is isomorphic to a sub-relation over (>,p-ints)

(>,p-ints) is well-founded

$$
\begin{aligned}
R = \{(s,t) \mid & [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) > 0) \ \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \ \wedge \\
& [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) \leq 0) \ \Rightarrow (t(\mathrm{p}) = 4 \ \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \ \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) > s(\mathrm{y})) \ \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) \leq s(\mathrm{y})) \ \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\
\}
\end{aligned}
$$



$$
\begin{aligned}
R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) > 0) && \Rightarrow \big(t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x})\big)] && \wedge \\
& [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) \leq 0) && \Rightarrow \big(t(\mathrm{p}) = 4 \ \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x})\big)] && \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) > s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] && \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) \leq s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\
& \}
\end{aligned}
$$

R *is* a well-founded relation

$$
\begin{aligned}
R = \{(s,t) \mid & [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) > 0) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) \leq 0) && \Rightarrow (t(\mathrm{p}) = 4 \ \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) > s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) \leq s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] \\
\} &
\end{aligned}
$$

```
if y > 0:
  while x > y:
    x = x - y
```

The code *does* guarantee termination

R *is* a well-founded relation

$$
\begin{aligned}
R = \{(s,t) \mid\ & [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) > 0) && \Rightarrow \big(t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x})\big)] && \wedge \\
& [(s(\mathrm{p}) = 1 \ \wedge s(\mathrm{y}) \leq 0) && \Rightarrow \big(t(\mathrm{p}) = 4 \ \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x})\big)] && \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) > s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 2 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge t(\mathrm{x}) = s(\mathrm{x}) - s(\mathrm{y}))] && \wedge \\
& [(s(\mathrm{p}) = 2 \ \wedge s(\mathrm{x}) \leq s(\mathrm{y})) && \Rightarrow (t(\mathrm{p}) = 4 \wedge s(\mathrm{y}) = t(\mathrm{y}) \wedge s(\mathrm{x}) = t(\mathrm{x}))] && \\
& \} &&
\end{aligned}
$$

a.k.a. *symbolic* AI

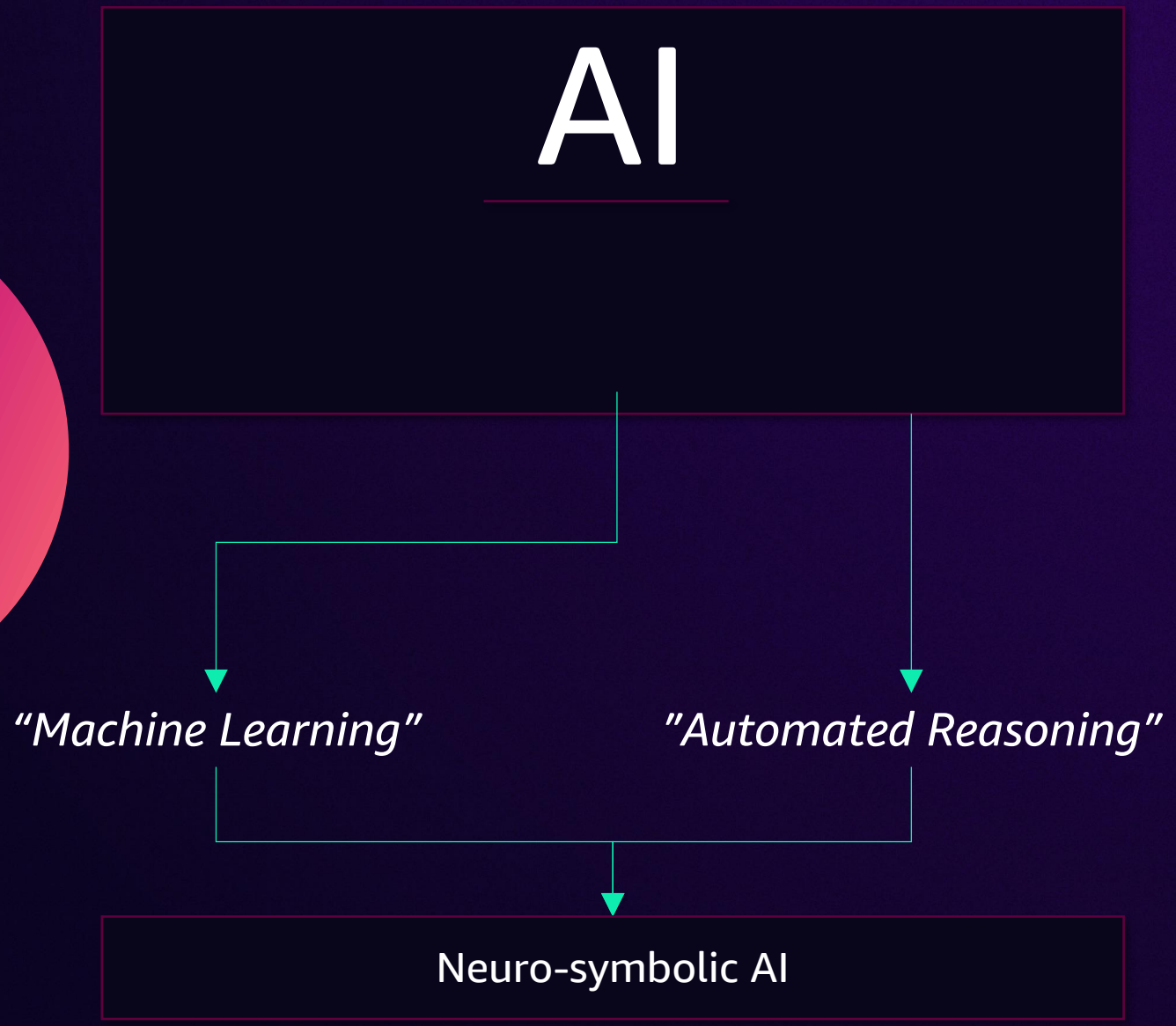
What *is* automated reasoning?

a.k.a. *symbolic* AI

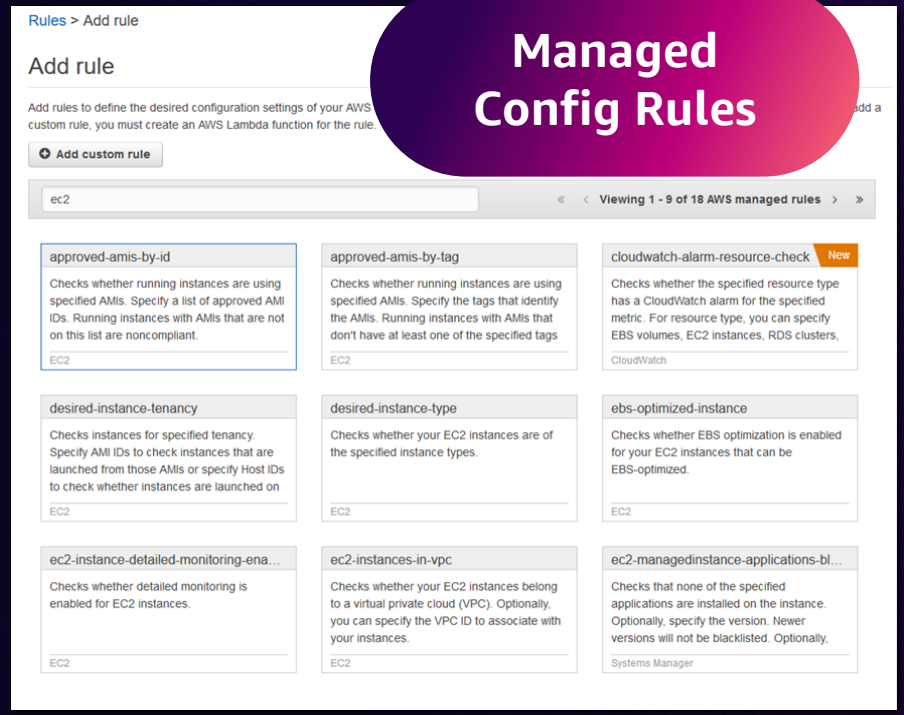
What *is* automated reasoning?

Let’s look at some examples

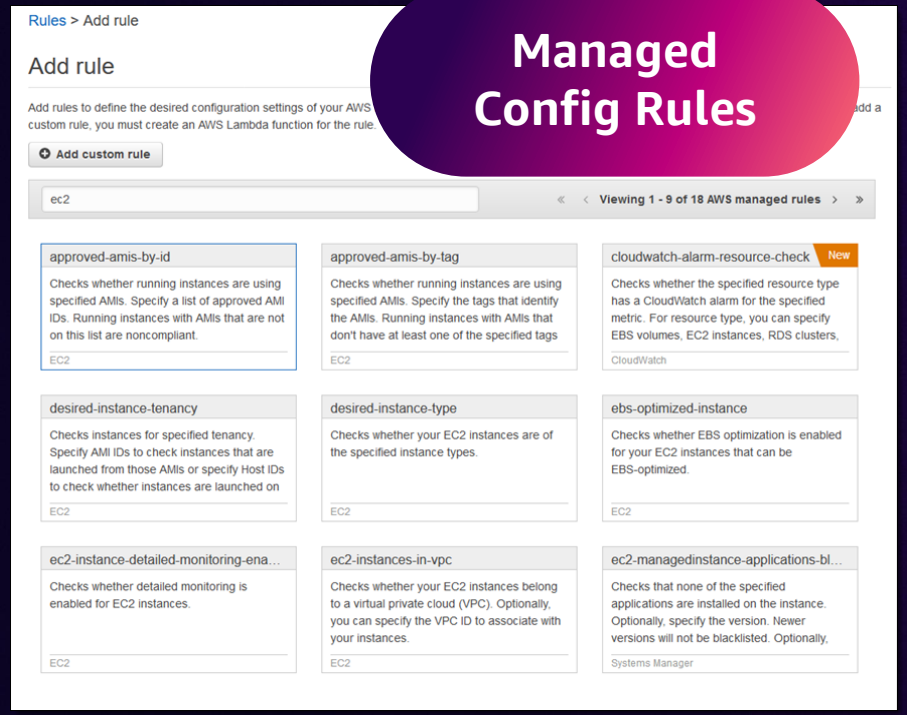
AWS has been heavily invested in both Automated Reasoning and Machine Learning for 10+ years



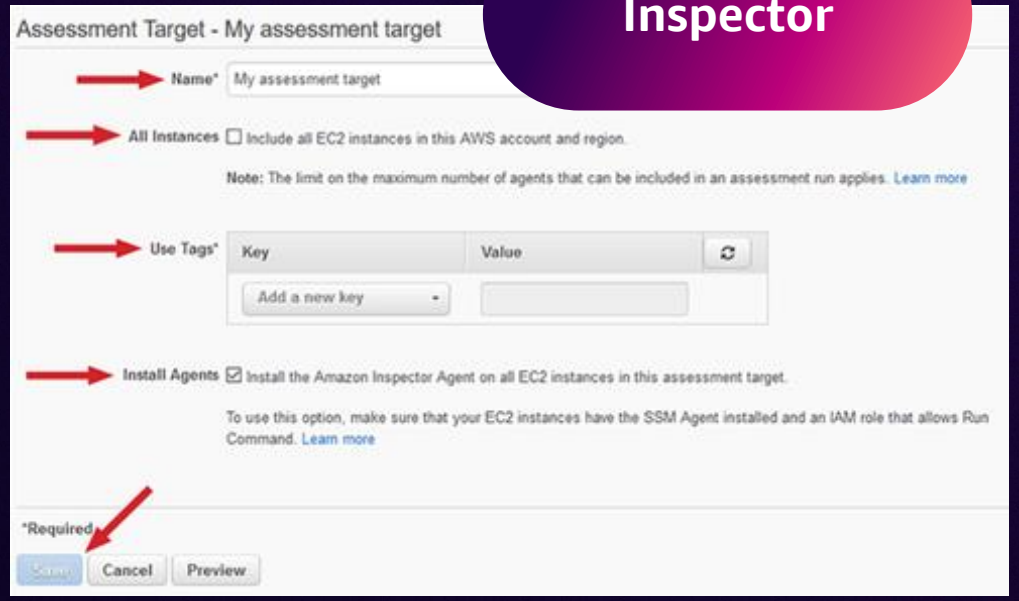
Managed Config Rules

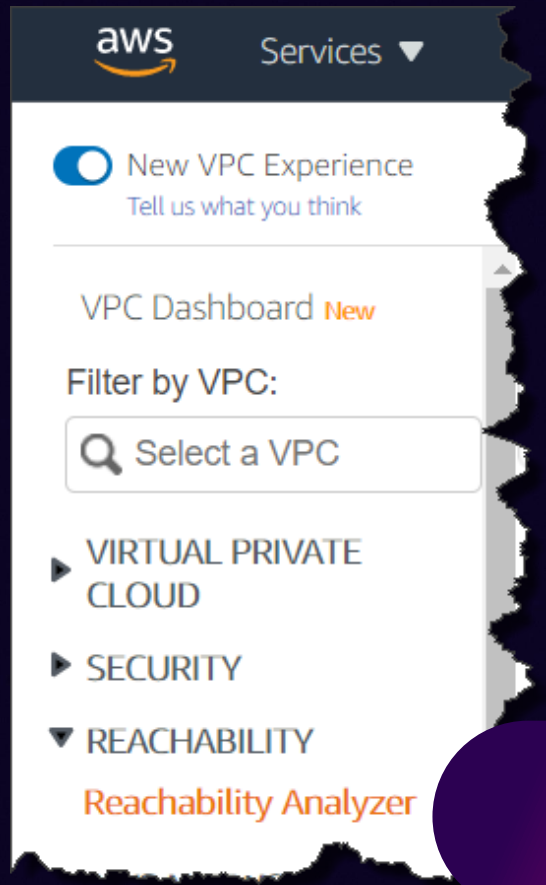


Managed Config Rules

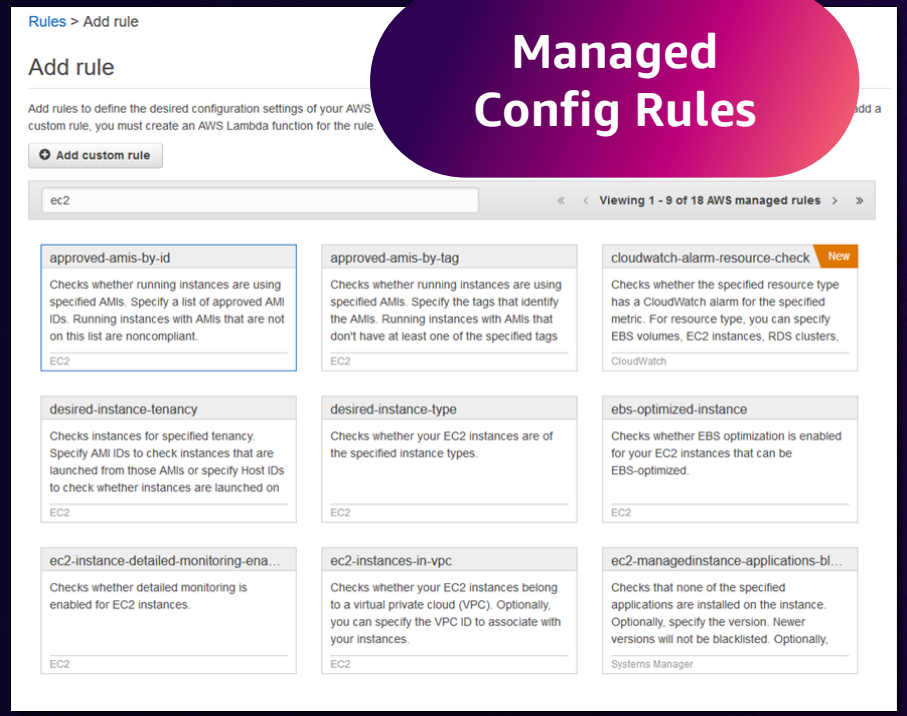


Inspector

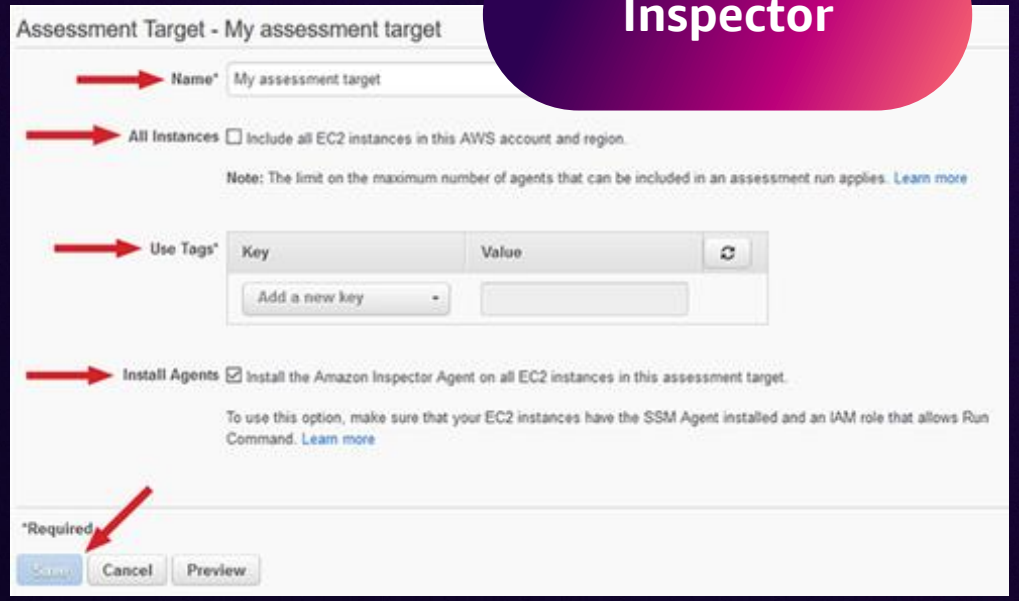




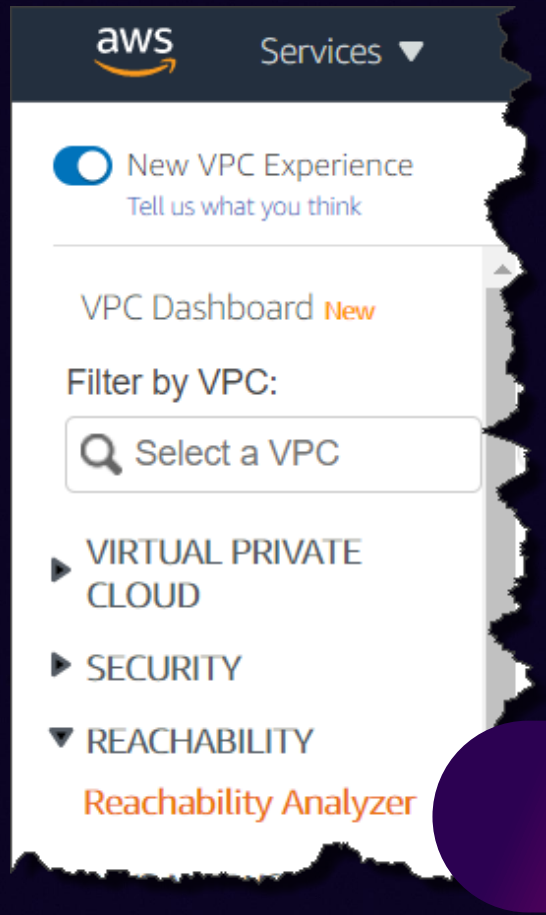
VPC Reachability Analyzer



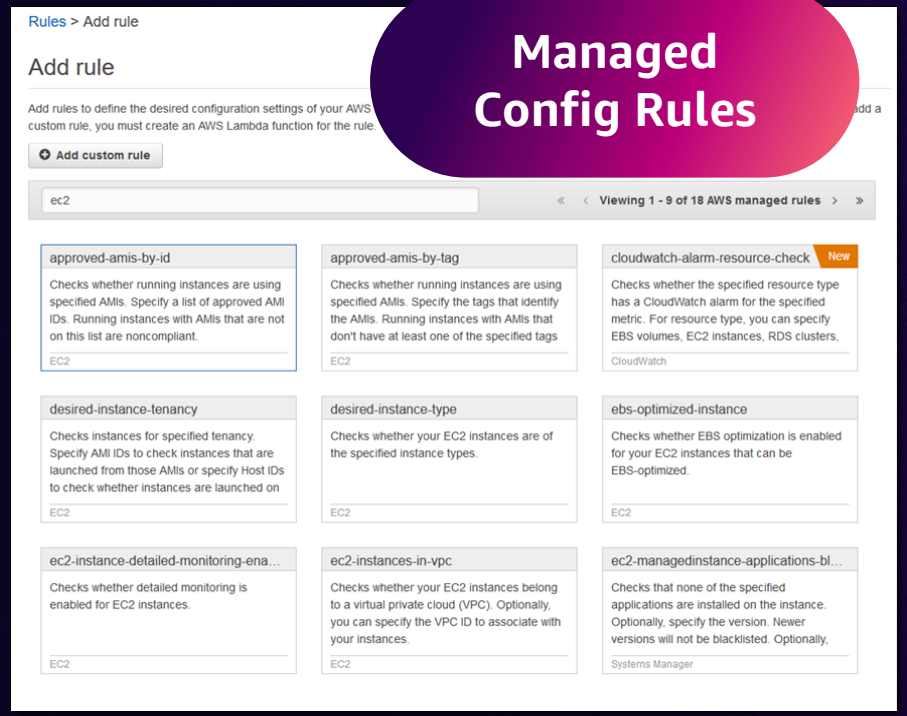
Managed Config Rules



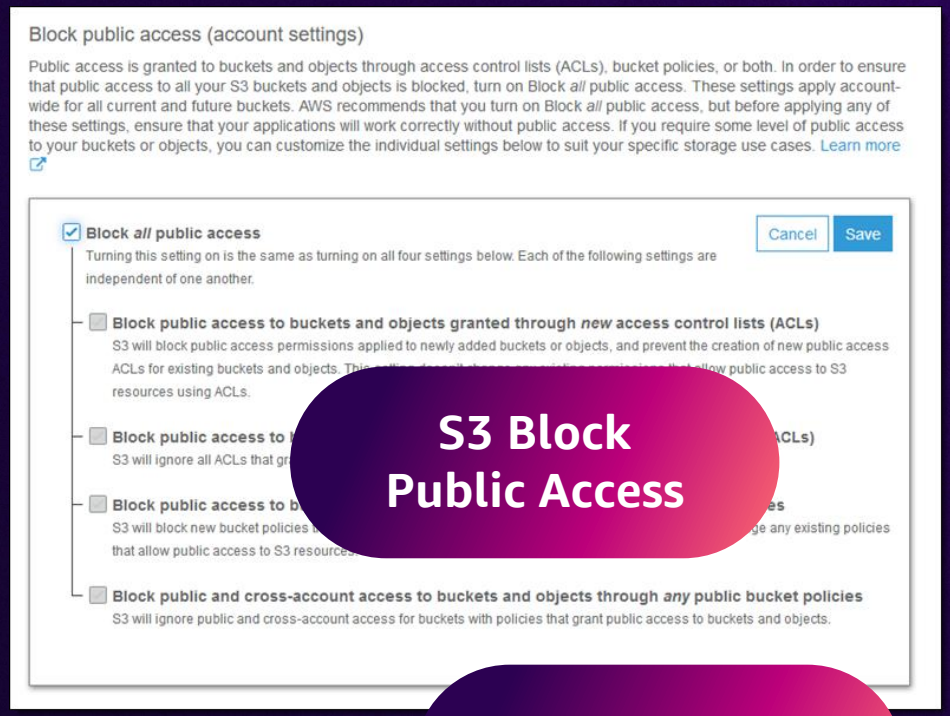
Inspector



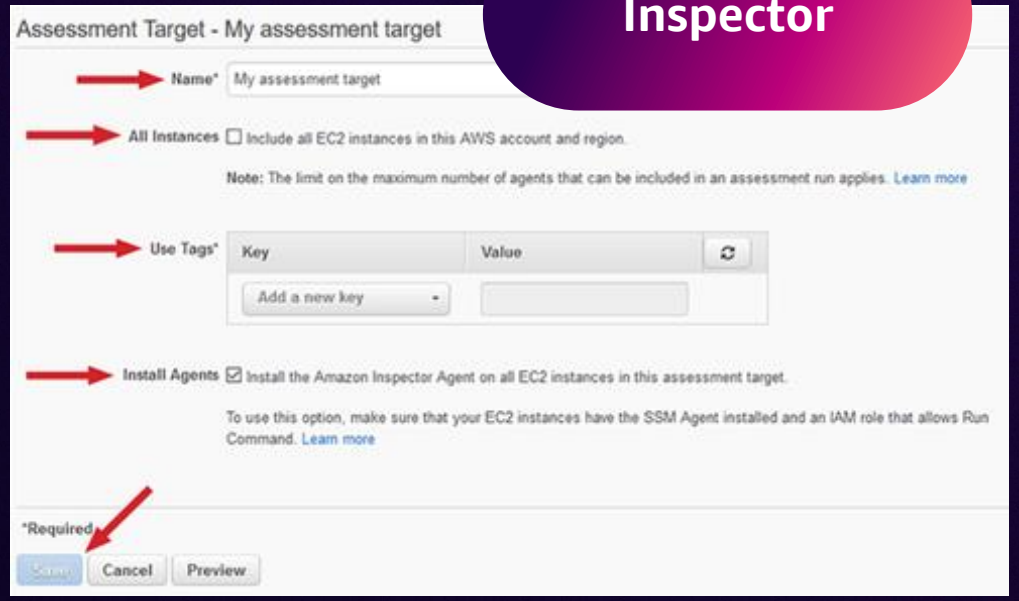
VPC Reachability Analyzer



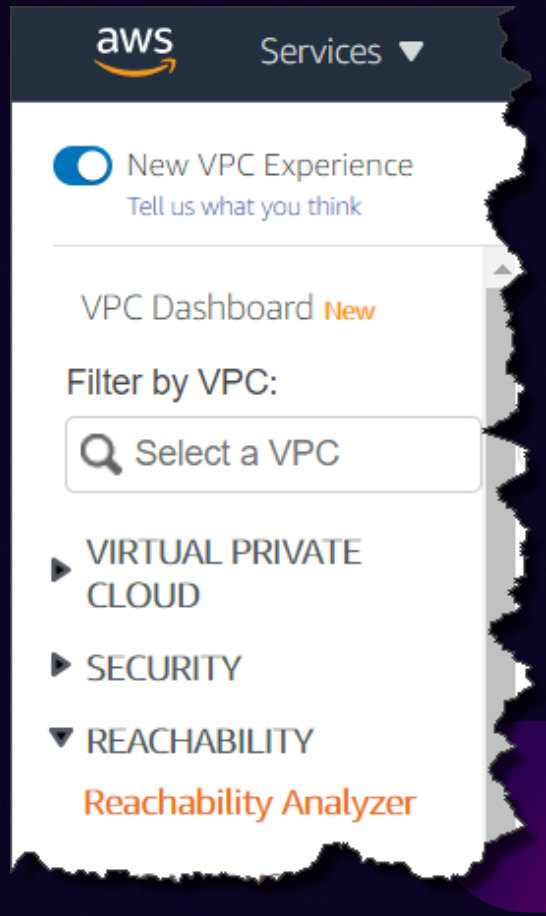
Managed Config Rules



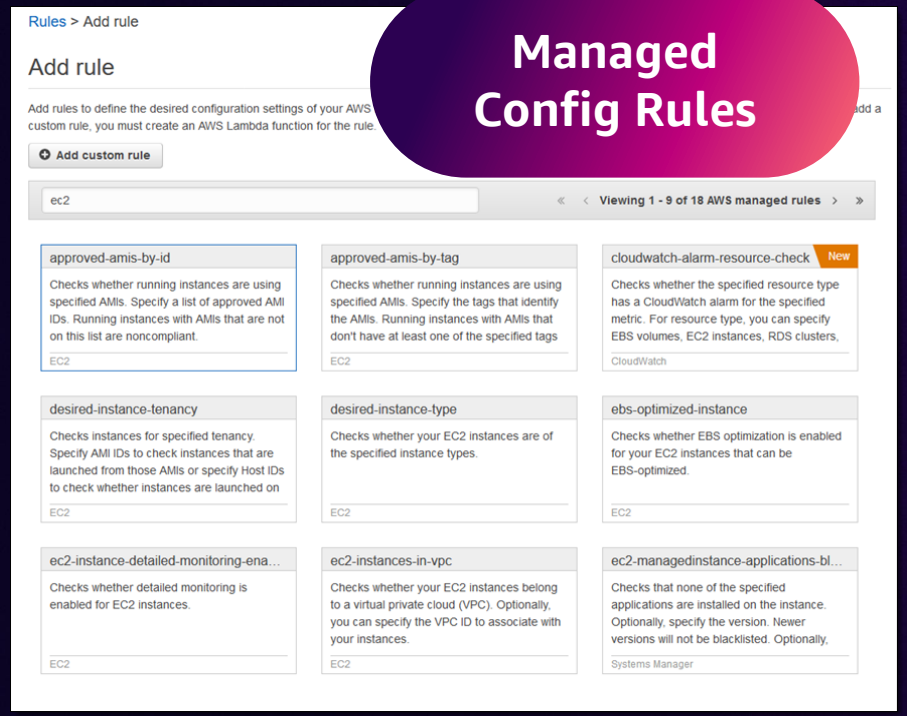
S3 Block Public Access



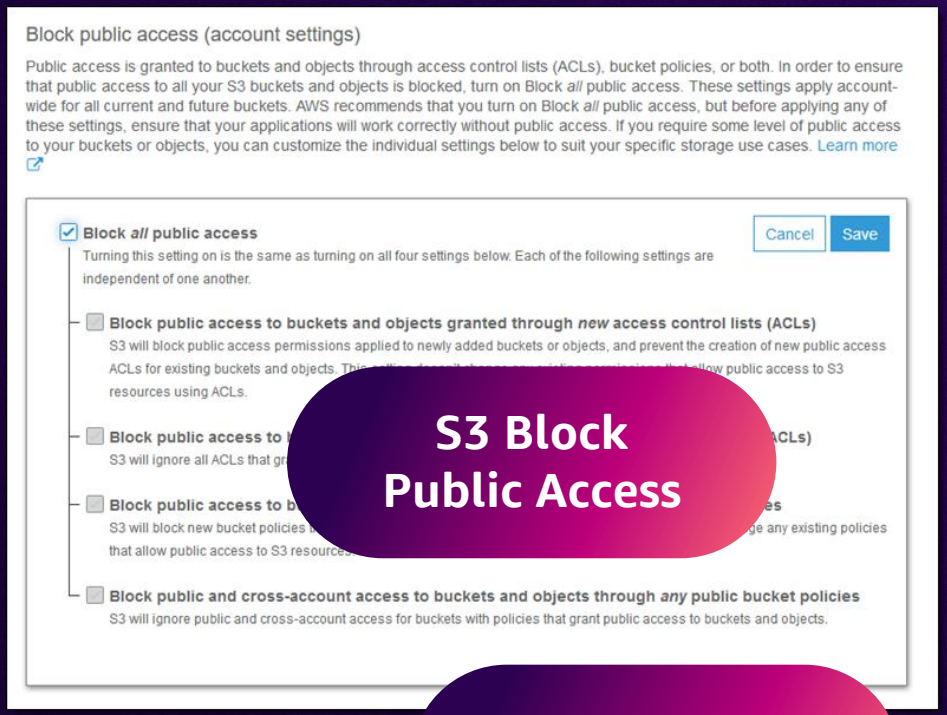
Inspector



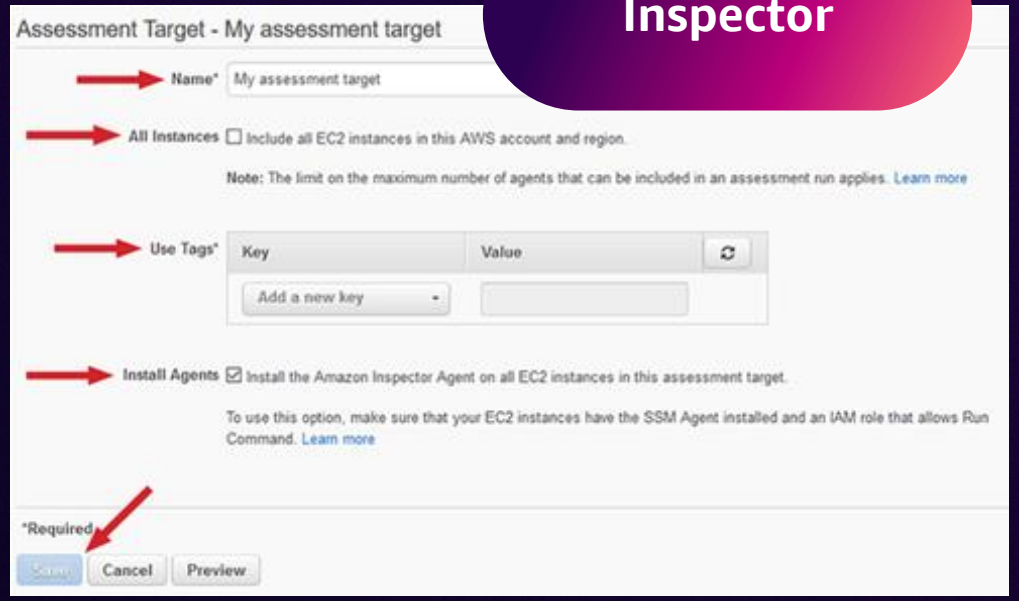
VPC Reachability Analyzer



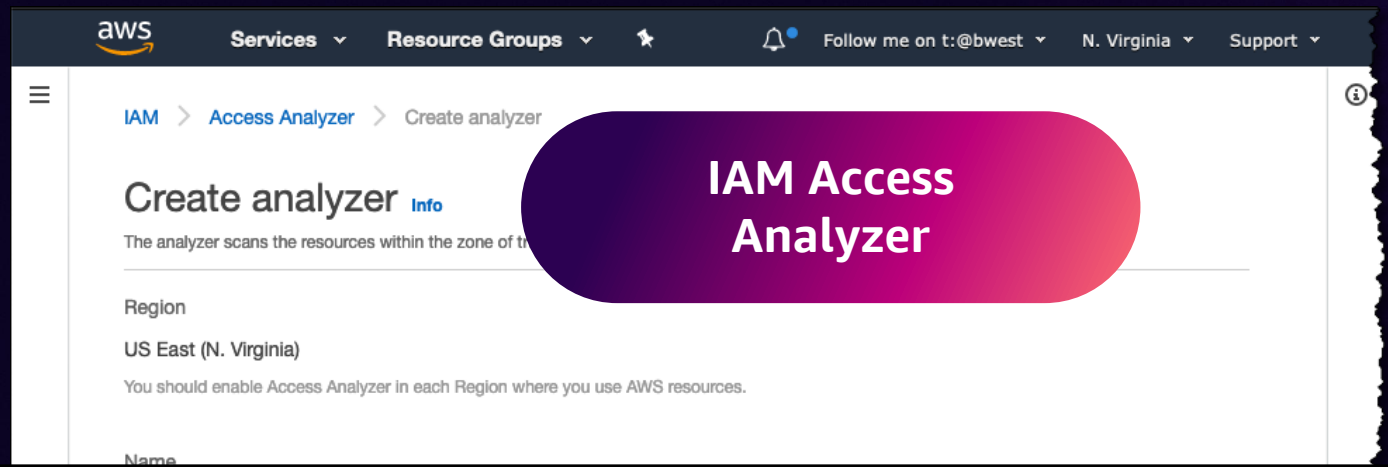
Managed Config Rules



S3 Block Public Access

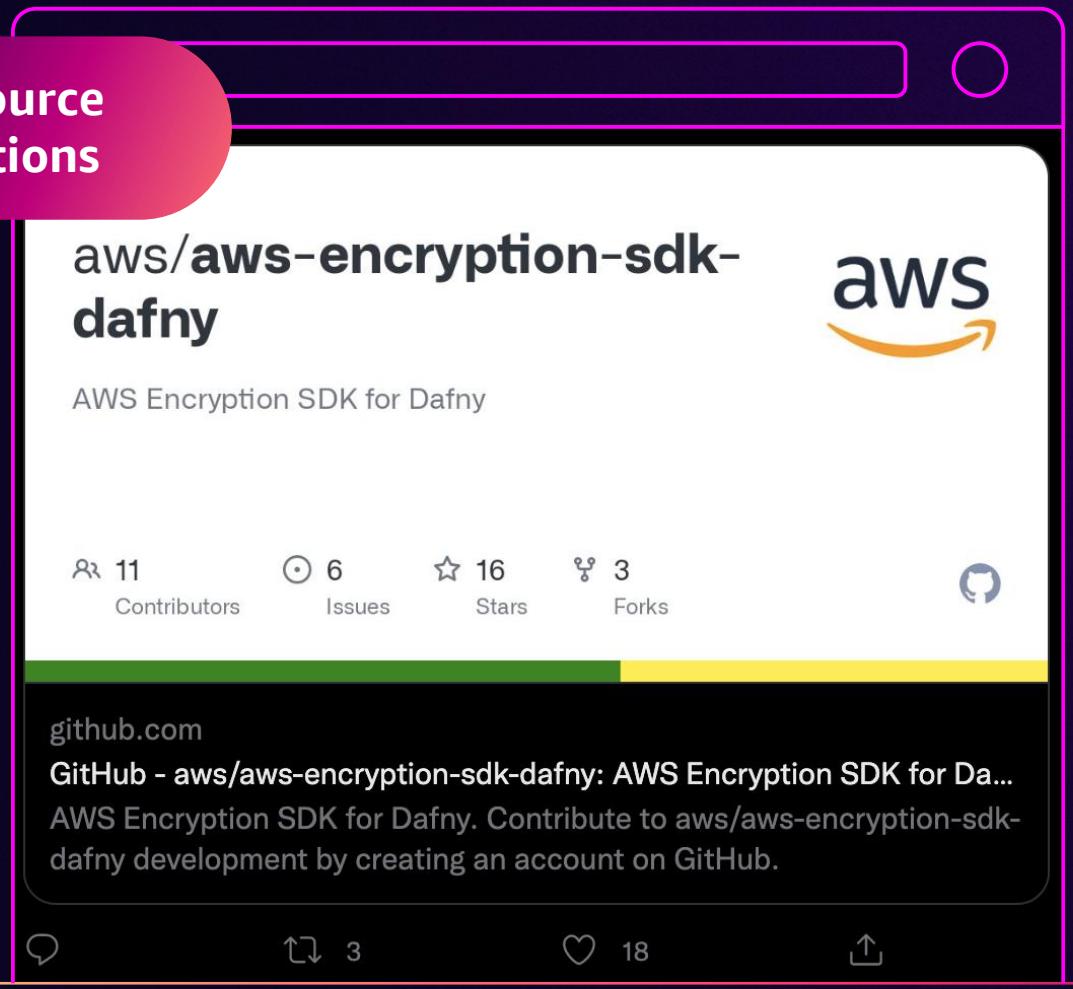


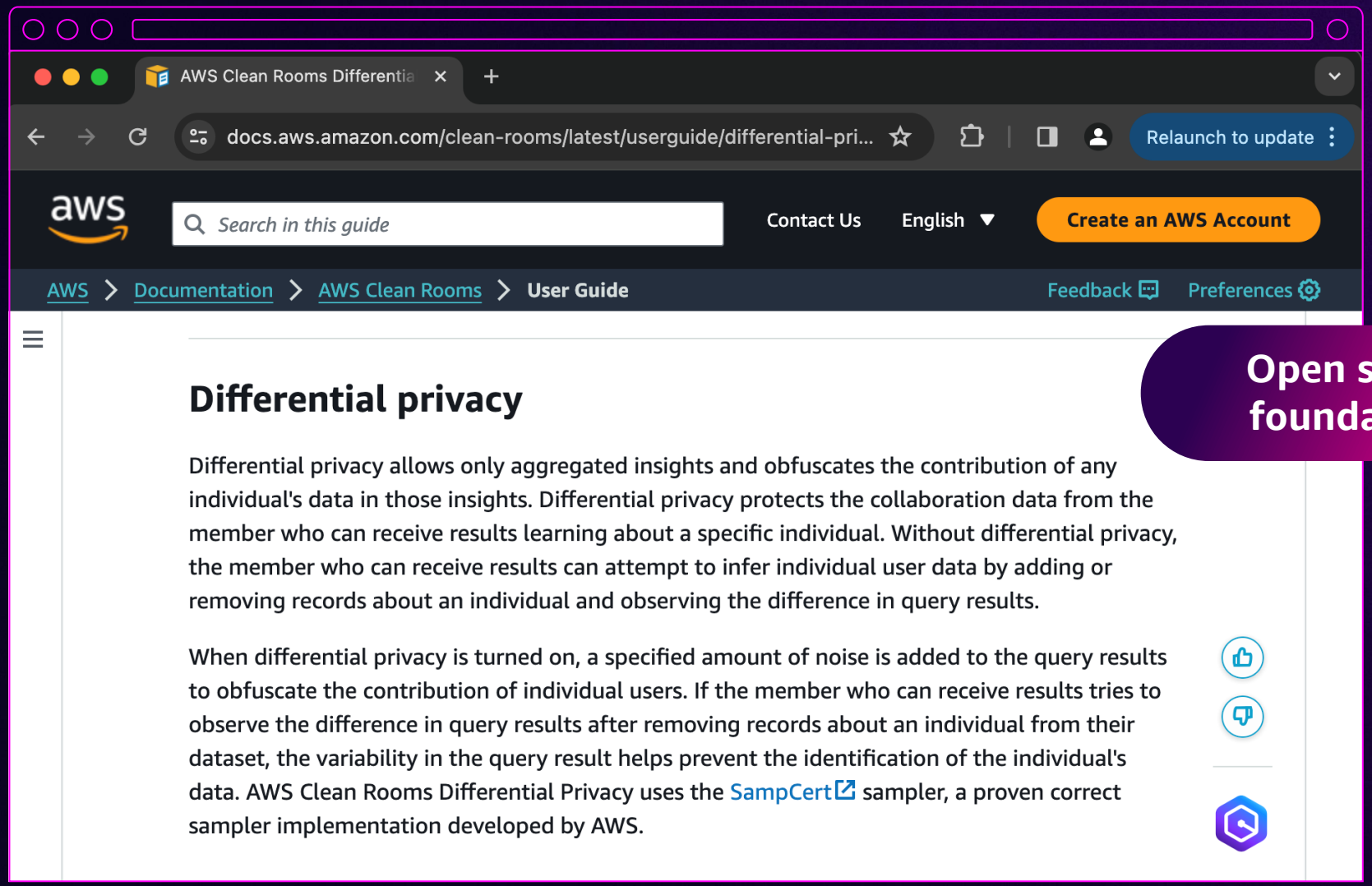
Inspector



IAM Access Analyzer

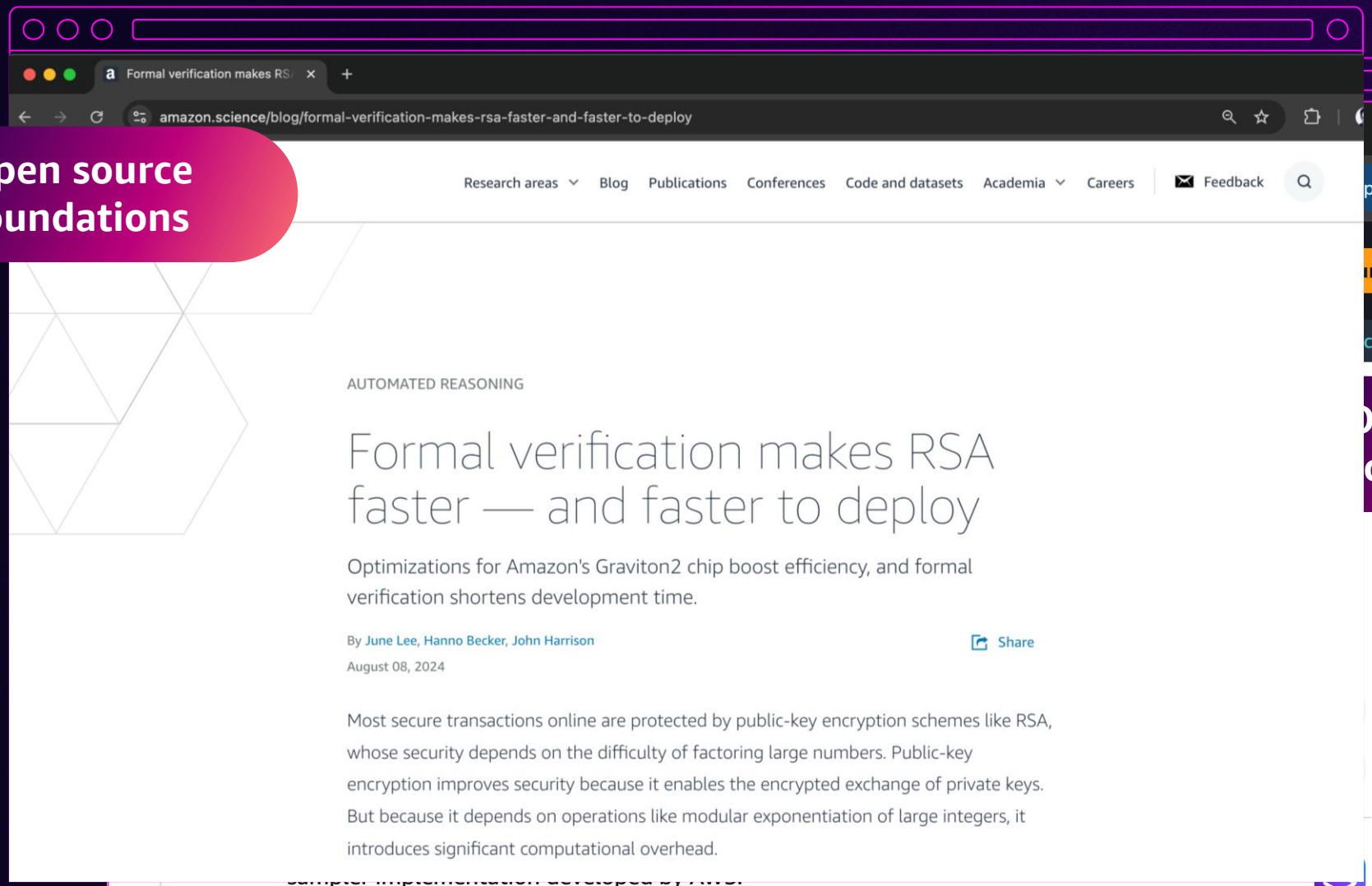
Open source foundations





Open source foundations

Open source foundations



Open source foundations

AWS product categories

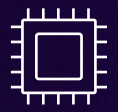
Analytic

Application Integration

Blockchain

Business Applications

Cloud Financial Management



Compute

Containers

Customer Engagement

Database

Developer Tools

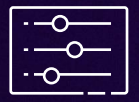
End User Computing

Front-End Web & Mobile

Game Tech

Internet of Things

Machine Learning



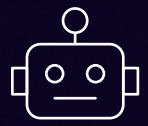
Management & Governance

Media Services

Migration & Transfer

Networking & Content Delivery

Quantum Technologies



Robotics

Satellite

Security, Identity & Compliance

Serverless

Storage

VR & AR

AWS product categories

Analytic | Application Integration | Blockchain | Business Applications | Cloud Financial Management | Compute | Containers | Customer Engagement | Database

Developer Tools | End User Computing | Front-End Web & Mobile | Game Tech | Internet of Things | Machine Learning | Mana Gov

Networking & Content Delivery | Quantum Technologies | Robotics | Satellite | Security, Identity & Compliance | Serverless | S

Practically every area touched by automated reasoning in some way

AWS product categories

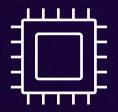
Analytic

Application Integration

Blockchain

Business Applications

Cloud Financial Management



Compute

Containers

Customer Engagement

Database

Developer Tools

End User Computing

Front-End Web & Mobile

Game Tech

Internet of Things

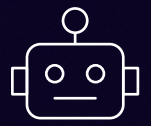
Example

Machine Learning

Mana Gov

Networking & Content Delivery

Quantum Technologies



Robotics

Satellite

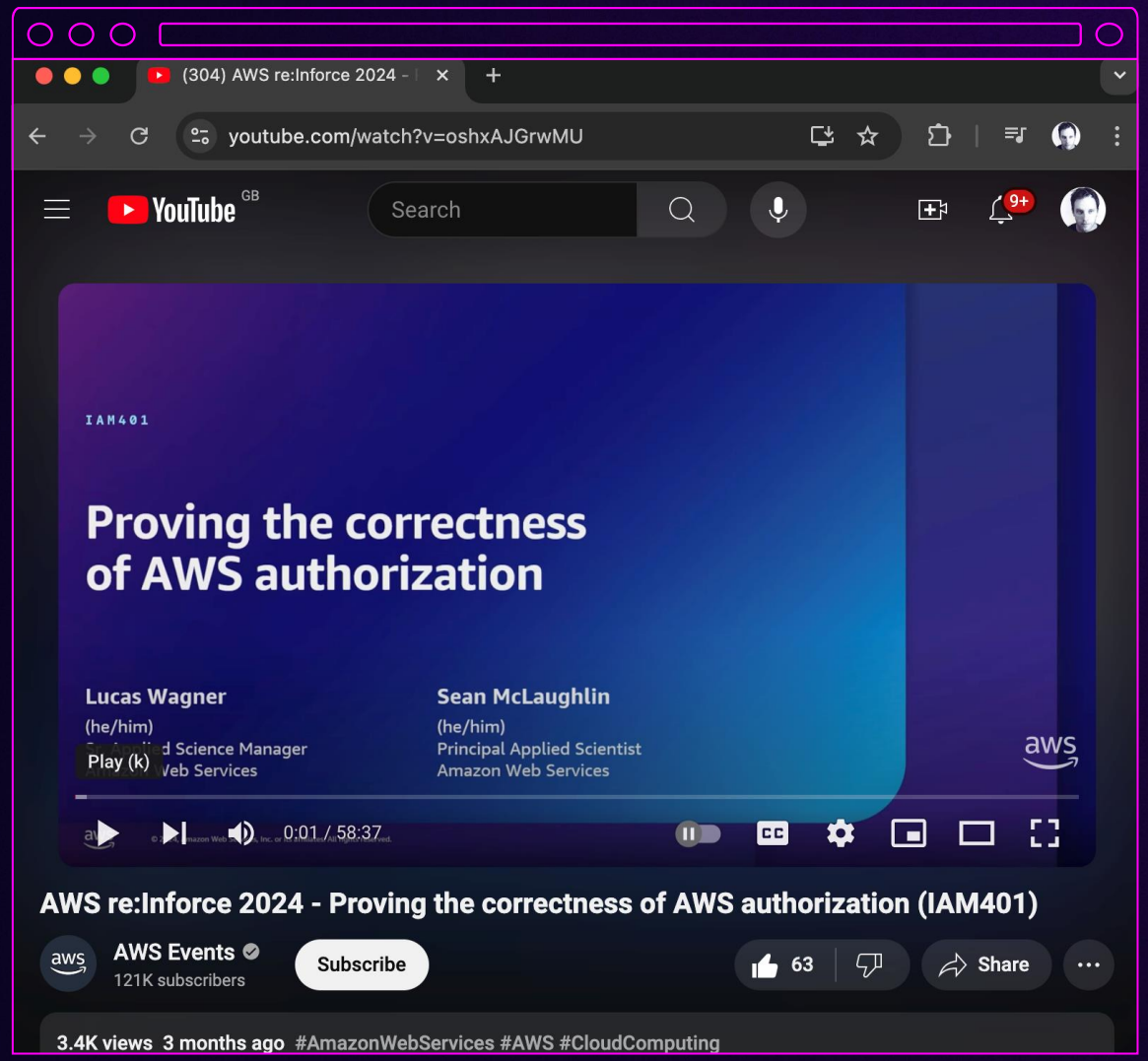
Security, Identity & Compliance

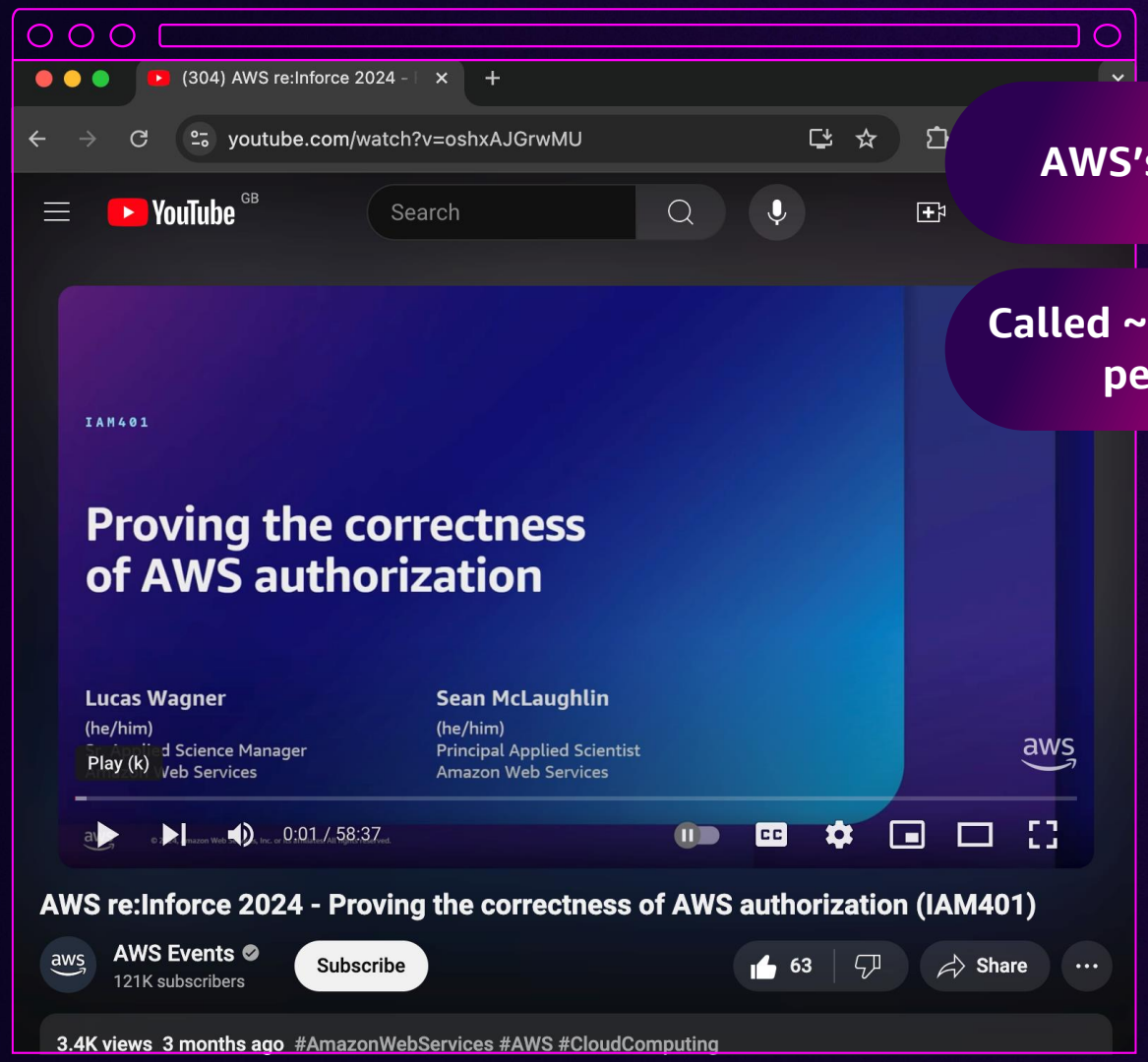
Serverless

S

Practically every area touched by automated reasoning in some way

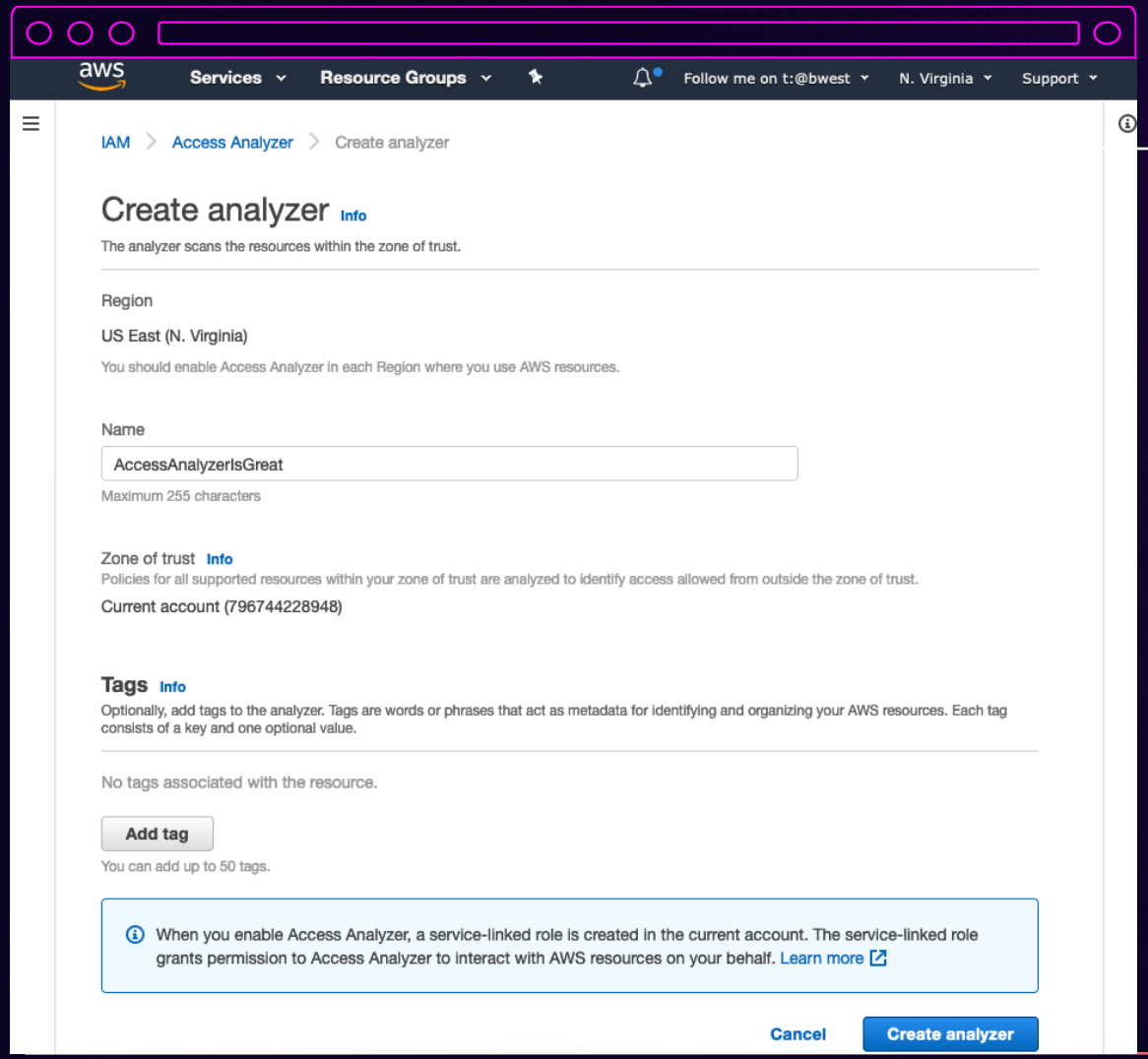
aws



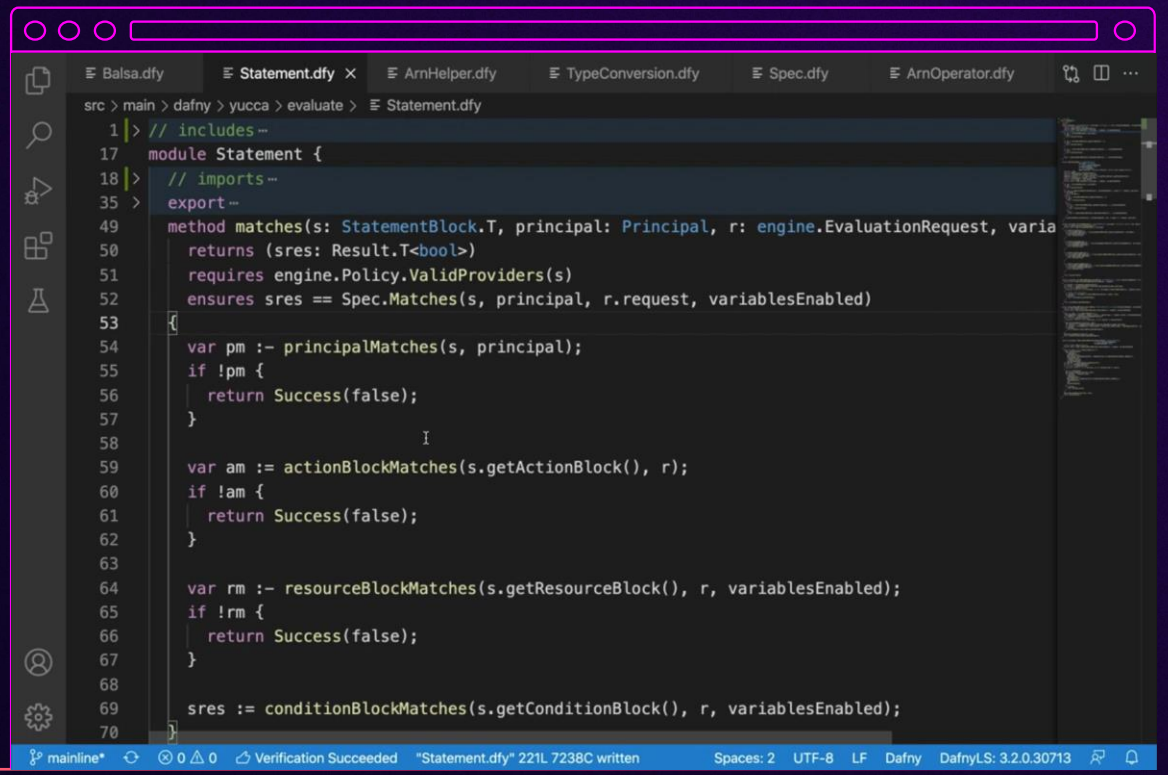


AWS's front door

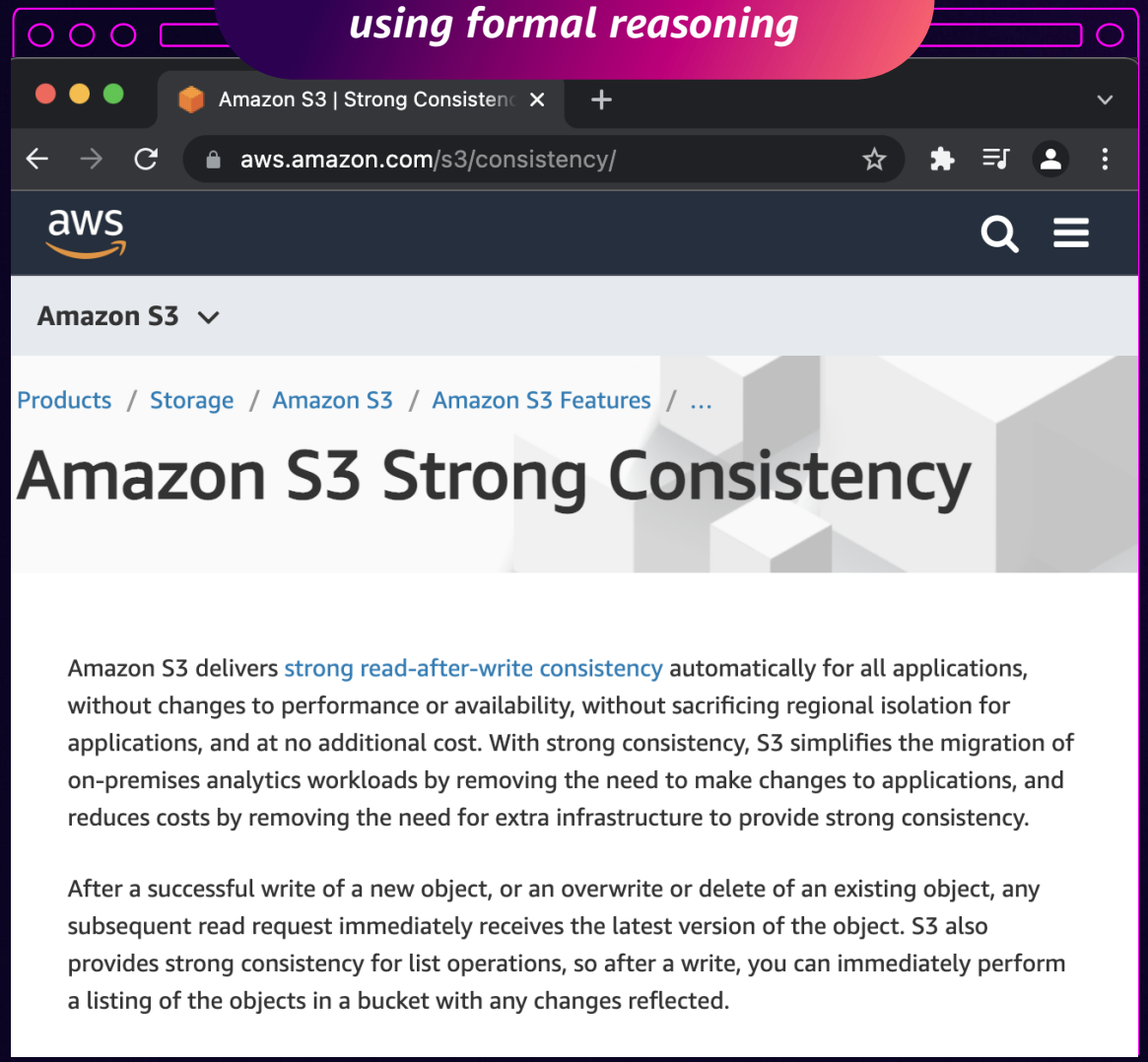
Called ~2 billion times per second

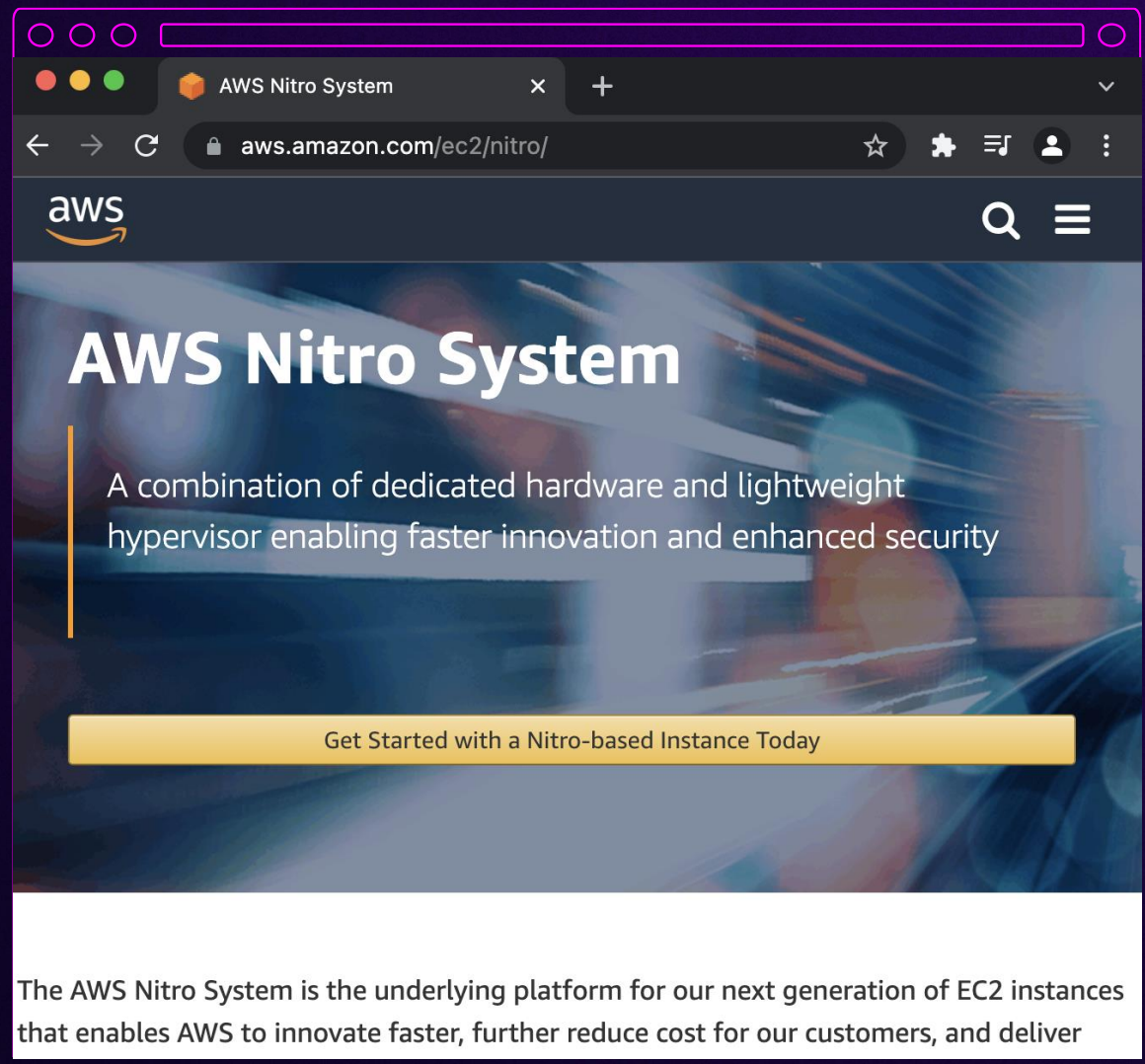


"For all possible authorization requests, deny always take precedence over allow"



Additional AWS systems rebuilt using formal reasoning





AWS product categories

All services use Storage

All services use Virtualization

All services use Networking

All services use Cryptography

a.k.a. *symbolic* AI

What *is* automated reasoning?

AIM393

Introduction to Automated Reasoning checks in Amazon Bedrock Guardrails

Stefano Buliani
(he, him)
Product Manager
Amazon Web Services

Byron Cook
(he, him)
VP, Distinguished Scientist
Amazon Web Services

Getting started

Let’s pick one of our use cases

They will reduce the cost of **onboarding new employees**

They will improve **customer support** experience

Automate **complex decisions**

Onboarding employees is expensive

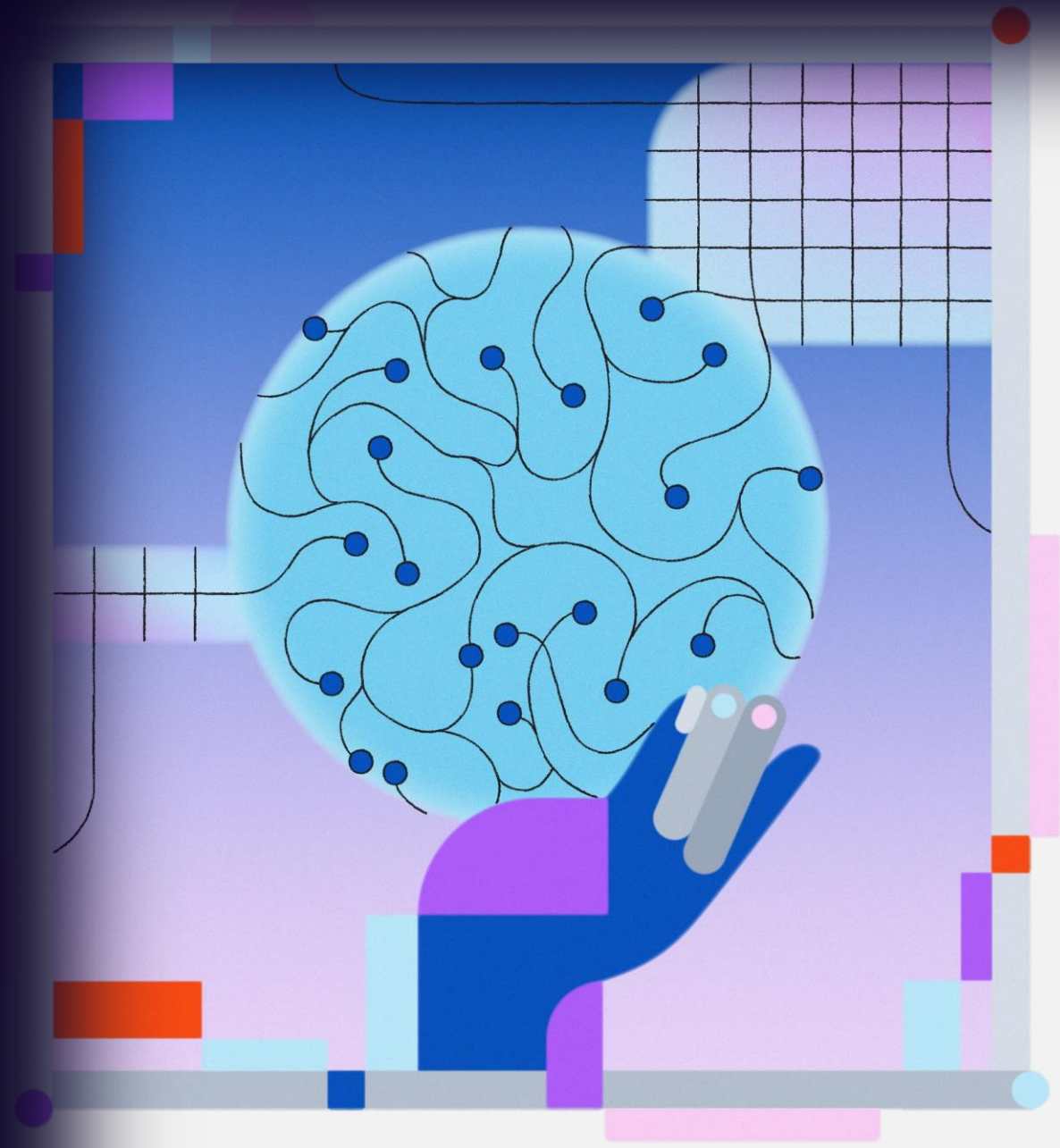
- Internal workflows
- HR policies
- You must train them on their actual job . . .

Improve productivity

Knows your workflows and policies

Can quote them **accurately**

Saves an **auditable explanation** of why an answer is correct



It’s a 3-step process

01

Create an **Automated Reasoning (AR) policy** of your rules

02

Configure **Automated Reasoning checks** in Amazon Bedrock Guardrails to use the AR policy

03

Validate and correct LLM answers

1. Create an AR policy

Leave of Absence (LoA)

Employees with more than 10 years of tenure at Senior level or higher, or at Vice President (VP) level or higher, are allowed up to one year of paid leave of absence (LoA)*

Upload your policy documents using the Amazon Bedrock console

1. Create an AR policy – Schema

Leave of Absence (LoA)

Employees with more than 10 years of **tenure** at senior **level** or higher, or at vice president (VP) level or higher, are **allowed** up to one year of paid leave of absence (LoA)*

Identify a schema of important concepts

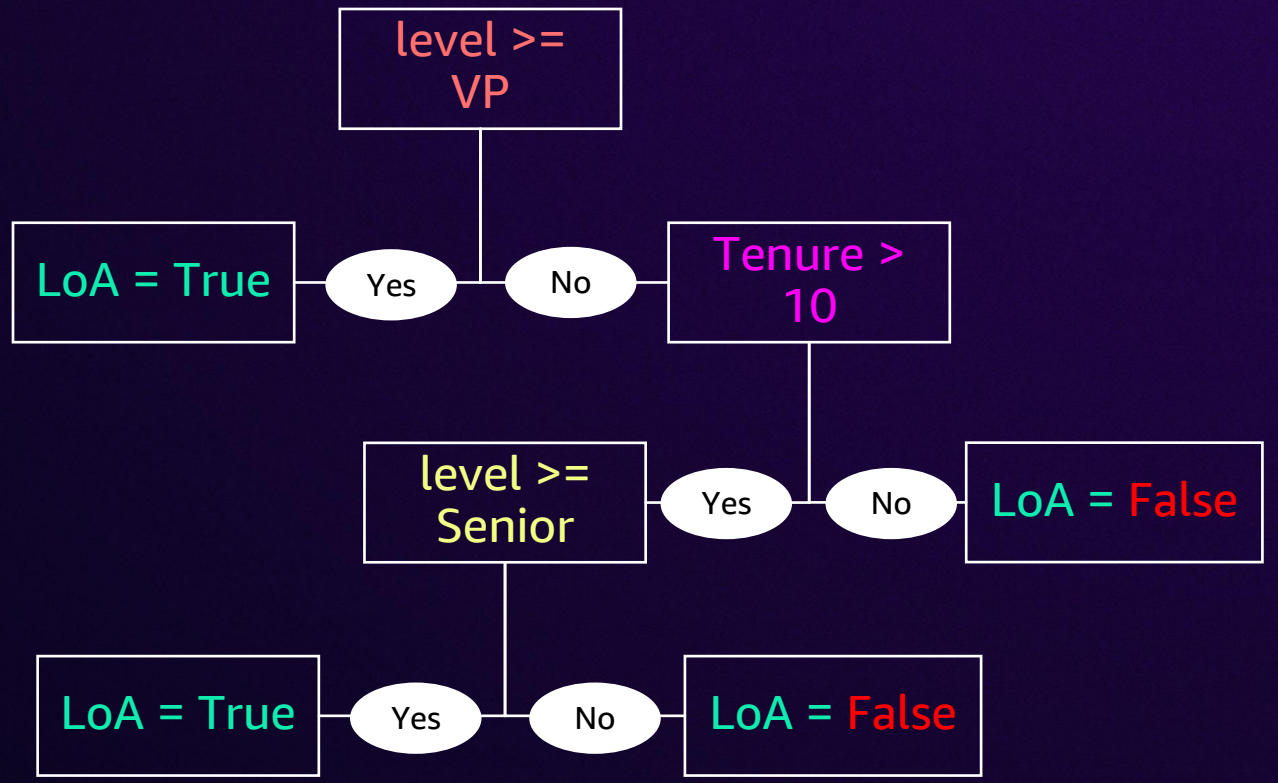
Name	Type	Description
Tenure	Int	Time at company
Level	Int	Employee experience
Allowed	Bool	Factual conclusion

1. Create an AR policy – Rules

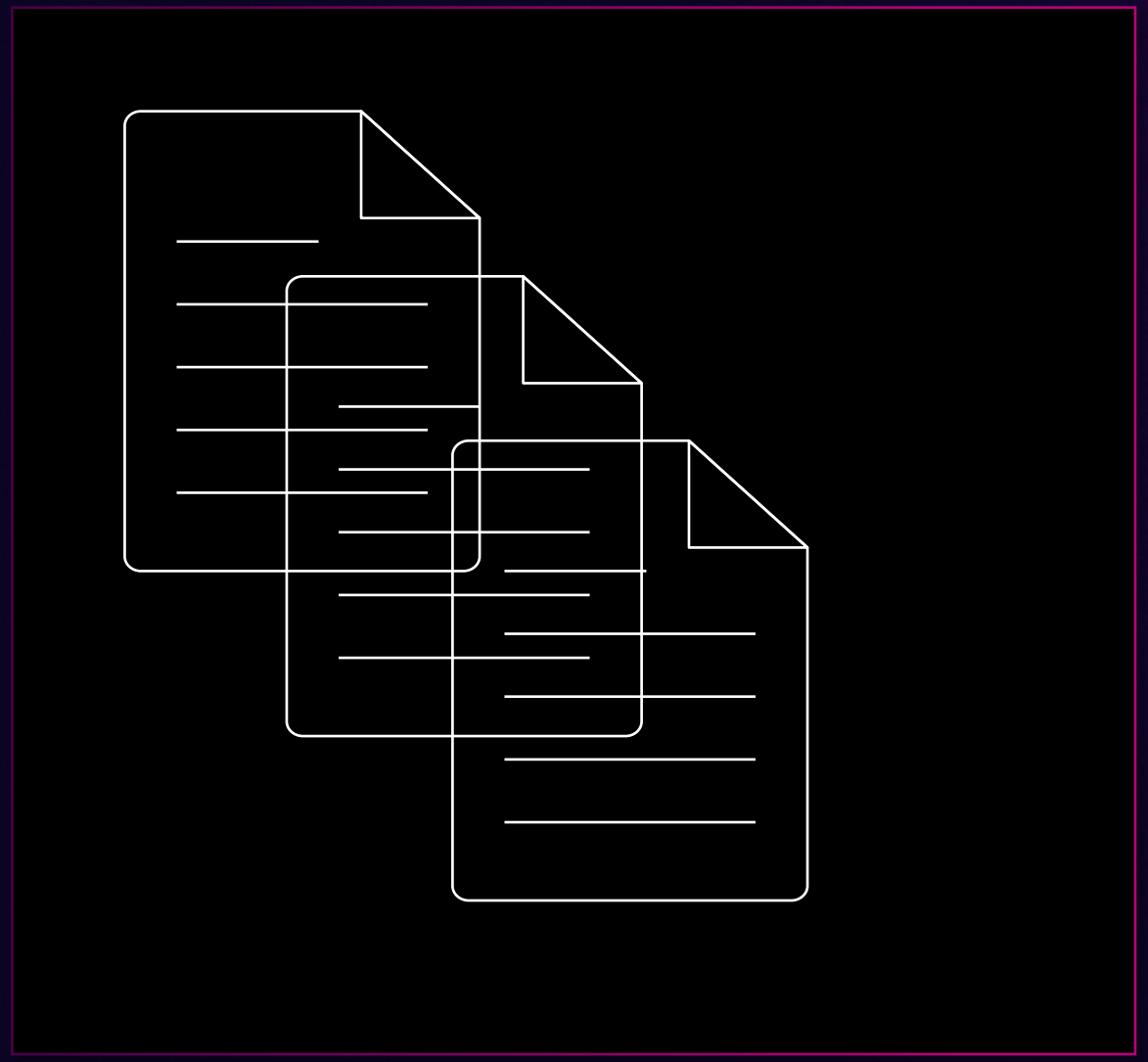
Leave of Absence (LoA)

Employees with **more than 10 years of tenure** at **senior level or higher,** or at **vice president (VP) level or higher, are allowed** up to one year of paid leave of absence (LoA)*

Identify rules



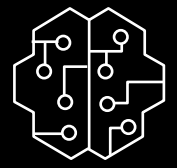
1. Create an AR policy – Resource



AR policies are **versioned**

Each version has a **unique ARN**

2. Configure guardrails



Configure the Automated Reasoning checks in Amazon Bedrock Guardrails to use the new AR policy

```
Type: AWS::Bedrock::Guardrail
Properties:
AutomatedReasoningPolicyConfig:
    - PolicyIdentifier: "abcd1234qwer"
    - PolicyVersion: "12"
```

Demo time!

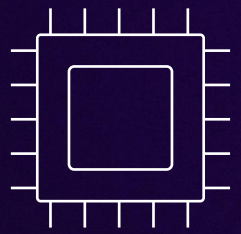
Using the output

3. Validate and correct LLM answers

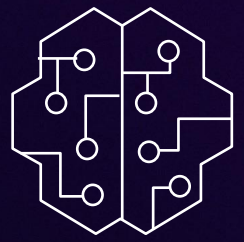
JD

Can I take 1 year of paid leave of absence?

Yes. Employees are allowed to take up to one year of paid leave of absence (LoA)!



ApplyGuardrail

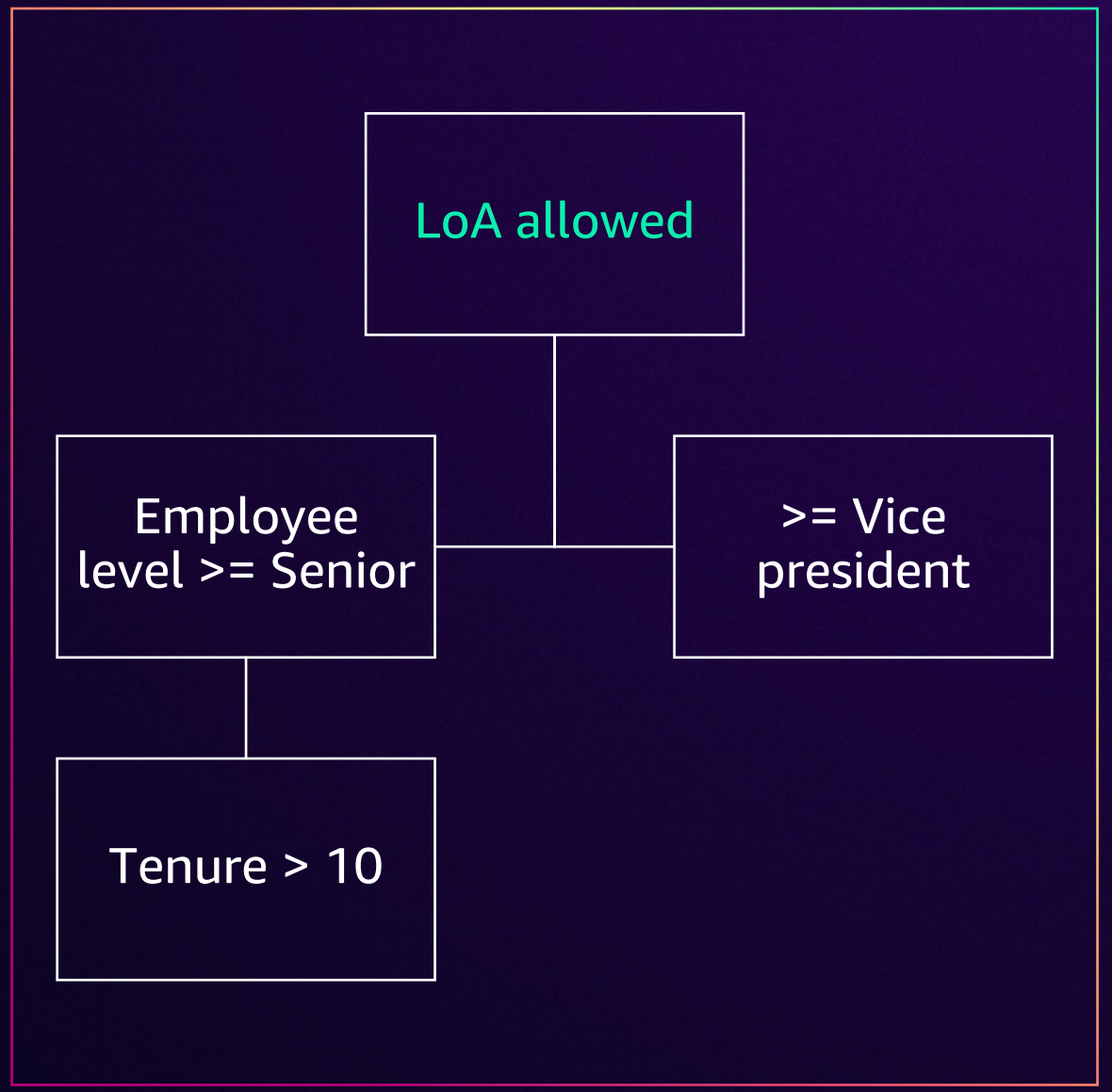


3. Validate and correct LLM answers

JD

Can I take 1 year of paid leave of absence?

Yes. Employees are allowed to take up to one year of paid leave of absence (LoA)!

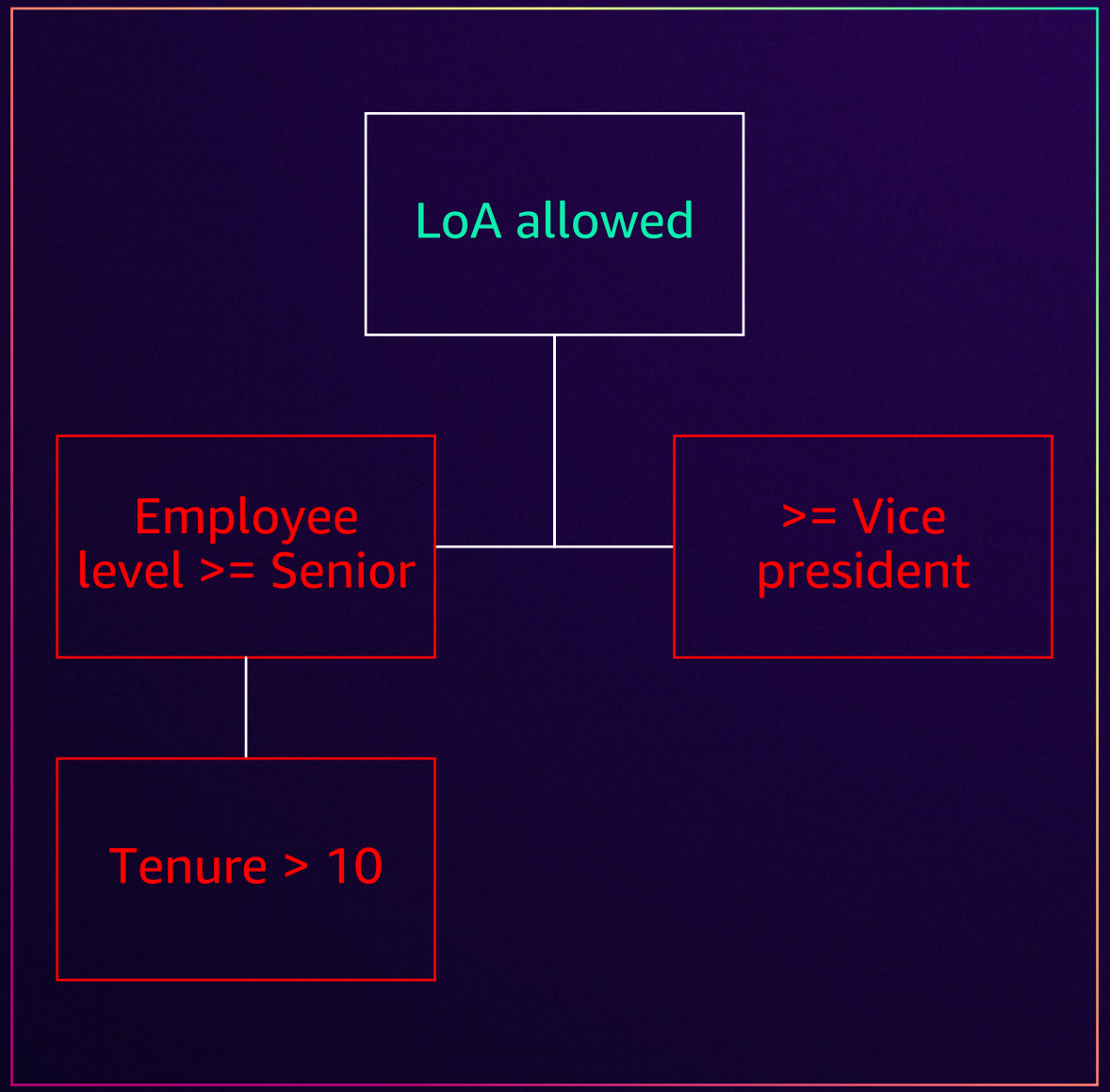


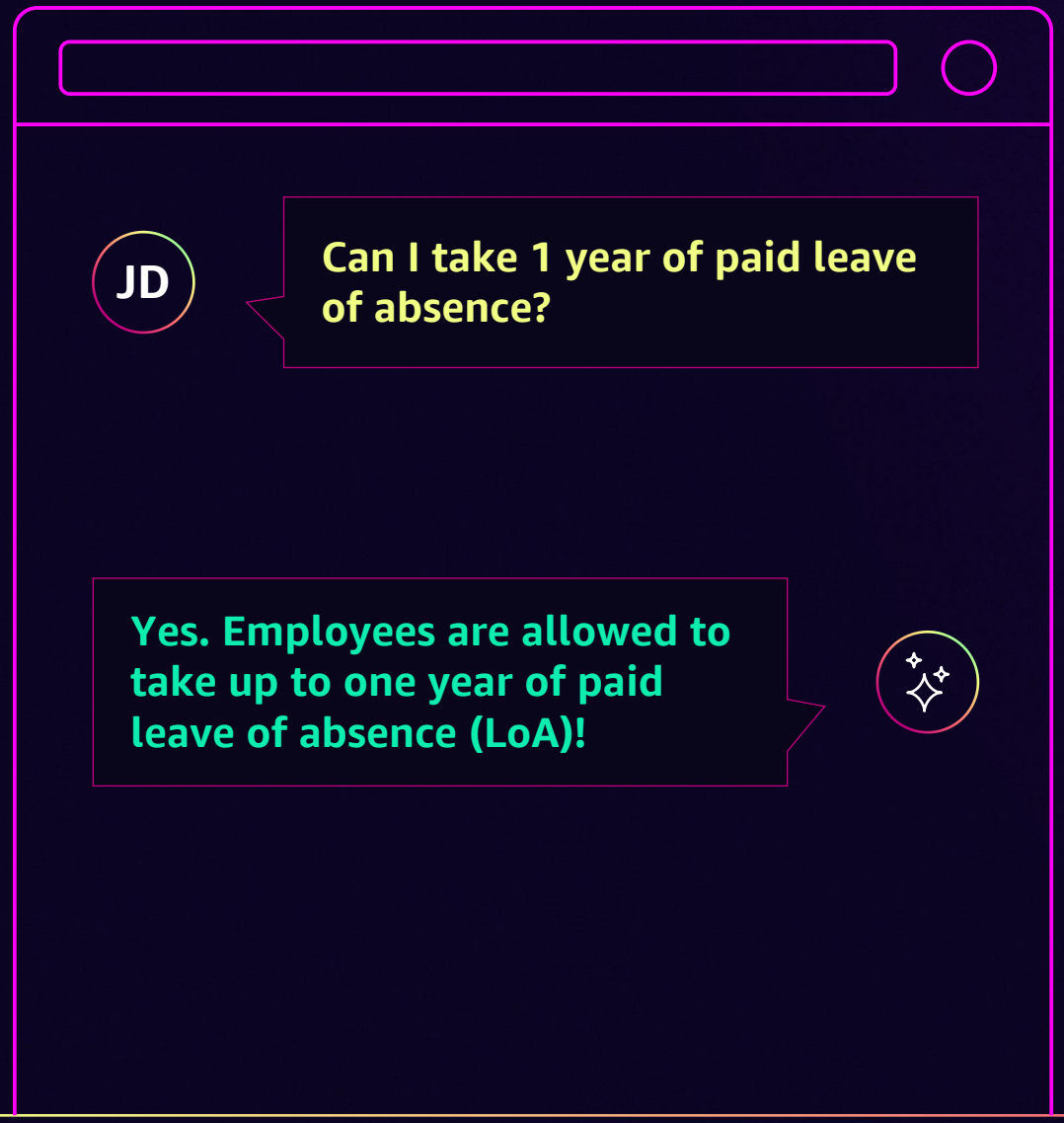
3. Validate and correct LLM answers

JD

Can I take 1 year of paid leave of absence?

Yes. Employees are allowed to take up to one year of paid leave of absence (LoA)!





3. Validate and correct LLM answers

`is_paid_loa_allowed: true`

- Validation result: `valid`
- Suggestions
  - Assumption: `tenure_years > 10`
  - Assumption: `employee_level > 6`
- Explanation: Employees must have more than 10 years of tenure. Employees must be at Senior level or higher.

Let’s dig deeper in the feedback

Yes. Employees are allowed to take up to one year of paid leave of absence (LoA)!

01 The answer is valid

```
is_paid_loa_allowed: true
```

- Validation result: valid
- Suggestions
  - Assumption: tenure_years > 10
  - Assumption: employee_level > 6
- Explanation: Employees must have more than 10 years of tenure. Employees must be at Senior level or higher.

LoA policy

Employees with more than 10 years of tenure at senior level or higher, or at vice president (VP) level or higher, **are allowed up to one year** of paid leave of absence (LoA)*

Let’s dig deeper in the feedback

Yes. Employees are allowed to take up to one year of paid leave of absence (LoA)!

```
is_paid_loa_allowed: true
```

- Validation result: valid
- Suggestions
  - Assumption: tenure_years > 10
  - Assumption: employee_level > 6
- Explanation: Employees must have more than 10 years of tenure. Employees must be at Senior level or higher.

02 Unstated assumptions

LoA policy

Employees with more than **10 years of tenure** at **senior level or higher**, or at vice president (VP) level or higher, are allowed up to one year of paid leave of absence (LoA)*

Let’s dig deeper in the feedback

Yes. Employees are allowed to take up to one year of paid leave of absence (LoA)!

03 Rewriting feedback

```
is_paid_loa_allowed: true
```

- Validation result: valid
- Suggestions
  - Assumption: tenure_years > 10
  - Assumption: employee_level > 6
- Explanation: Employees must have more than 10 years of tenure. Employees must be at Senior level or higher.

3. Correct LLM answers

`is_paid_loa_allowed: true`

- `Validation result: valid`
- `Suggestions`
  - `Assumption: tenure_years > 10`
  - `Assumption: employee_level > 9`
- `Explanation: Employees must have more than 10 years of tenure. Employees must be at Vice President (VP) level or higher.`

01 Ask your LLM to rewrite

02 Annotate the answer

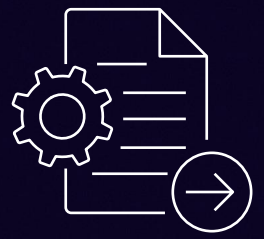
03 Ask clarifying questions

Rewrite the answer

You stated X. You conclusion is **valid** only under these circumstances:

Employees must have more than 10 years of tenure. Employees must be at vice president (VP) level or higher.

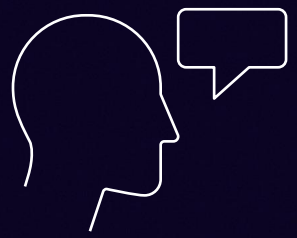
Please rewrite your answer considering this input . . .



Annotate the answer

Yes. Employees are allowed to take up to one year of paid leave of absence (LoA)[1]!

[1] Employees must have more than 10 years of tenure. Employees must be at vice president (VP) level or higher.



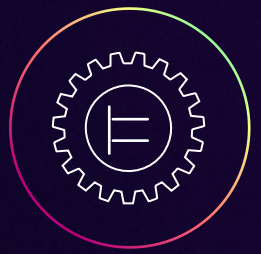
Clarifying questions

Depends, what is your level?

Automated Reasoning checks

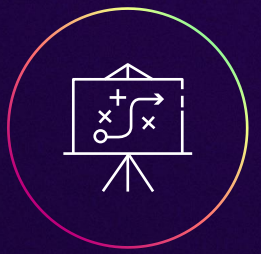
Accurate

Helps you build factually accurate conversational experiences



Sound

Helps you decide when clarifications are necessary to arrive at a definitive answer



Transparent

The validation is explainable and deterministic

Next steps

Resources

What is Automated Reasoning?

Intro to Automated Reasoning for developers

Amazon Bedrock Guardrails

Intro to Automated Reasoning checks

Thank you!

Please complete the session survey in the mobile app

Stefano Buliani

@sapessi

linkedin.com/in/sbuliani/

Byron Cook