Mechanisation of the AKS Algorithm (Visual)

Hing Lun Chan

College of Engineering and Computer Science
Australian National University

PhD Thesis, November 2019

Outline

Hing-Lun Chan

Mechanisation of AKS Algorithm

PhD final year

College of Engineering and Computer Science, The Australian National University.

ORCID iD: orcid.org/0000-0003-1811-1684

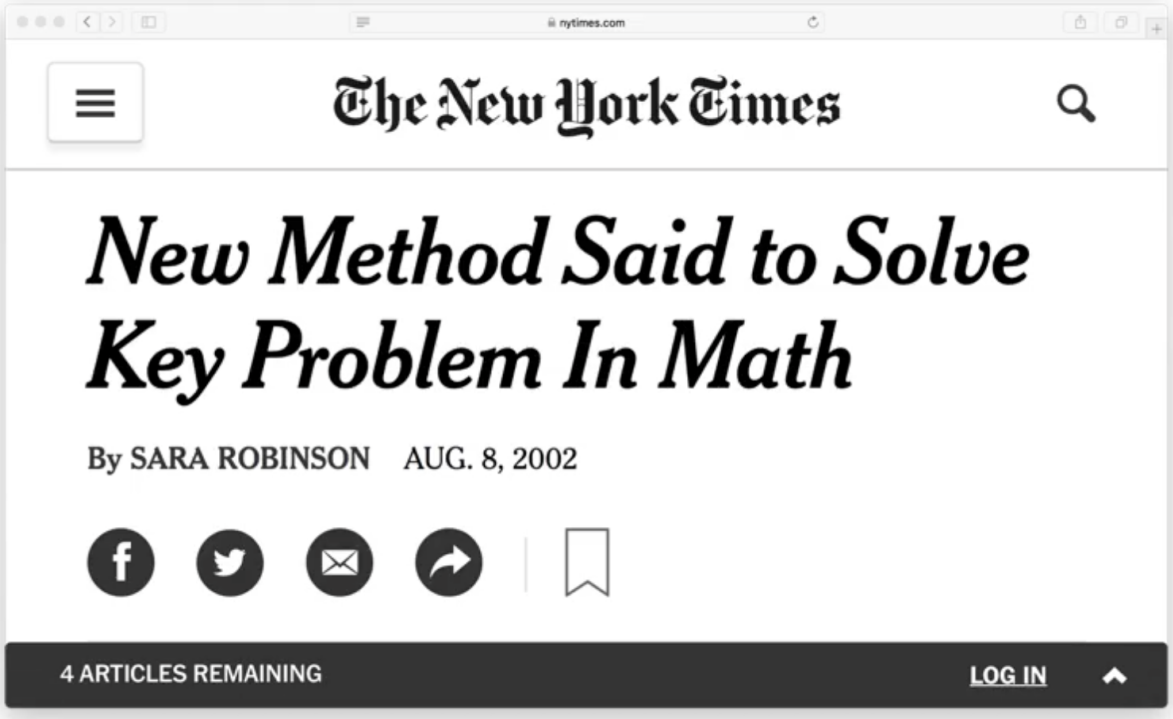
@jhlchan

Australian National University

Visualise *your* thesis

presented by THE UNIVERSITY OF MELBOURNE

Math in the News



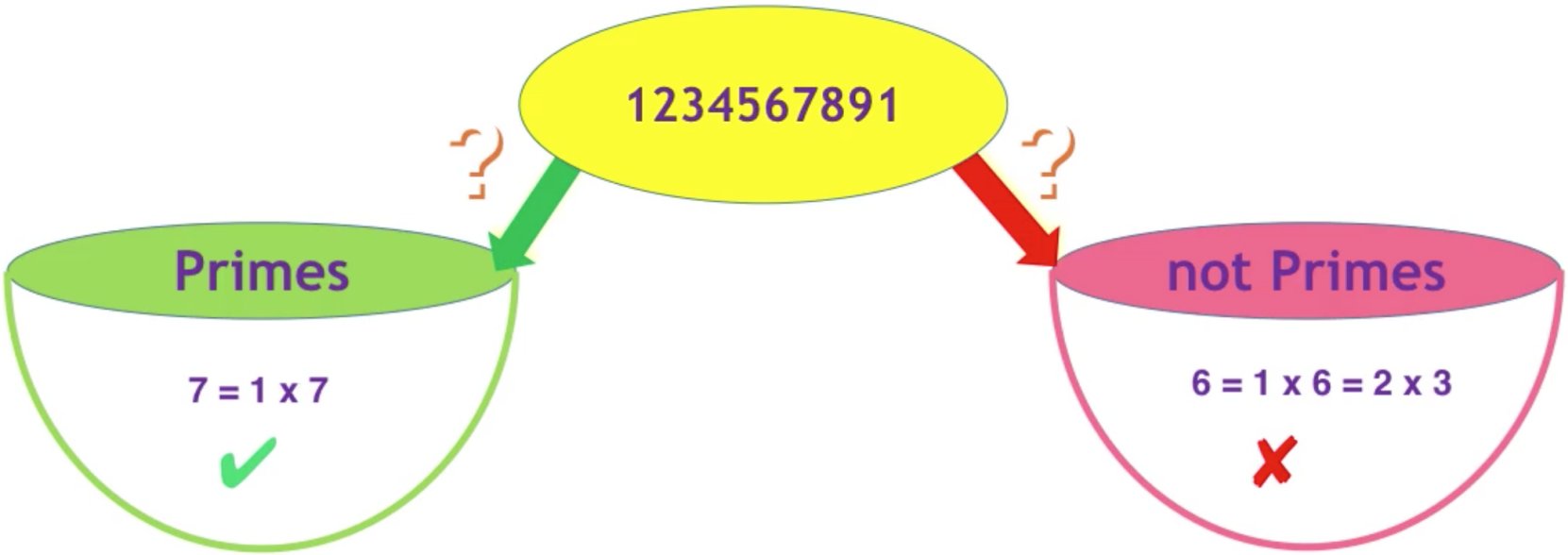
Breakthrough concerns cyber-security

Modern Cyber-security: https

Keys are generated by prime numbers

longer primes = stronger keys

Sorting out primes: those with trivial factors



Is there a "fast" way to tell primes?

technically: "Is PRIMES in P" ?

The AKS breakthrough

Annals of Mathematics, **160** (2004), 781–793

PRIMES is in P

By Manindra Agrawal, Neeraj Kayal, and Nitin Saxena*

Abstract

We present an unconditional deterministic polynomial-time algorithm that determines whether an input number is prime or composite.

The AKS breakthrough

Annals of Mathematics, **160** (2004), 781–793

PRIMES is in P

There is a "fast" way to tell primes!

By Manindra Agrawal, Neeraj Kayal, and Nitin Saxena*

Math foolproof?

Algorithm correct?

Performance "fast"?

Abstract

We present an unconditional deterministic polynomial-time algorithm that determines whether an input number is prime or composite.

PRIMES Is in P: A Breakthrough for "Everyman"

Folkmar Bornemann

As reported in Notices of the AMS (American Mathematical Society)

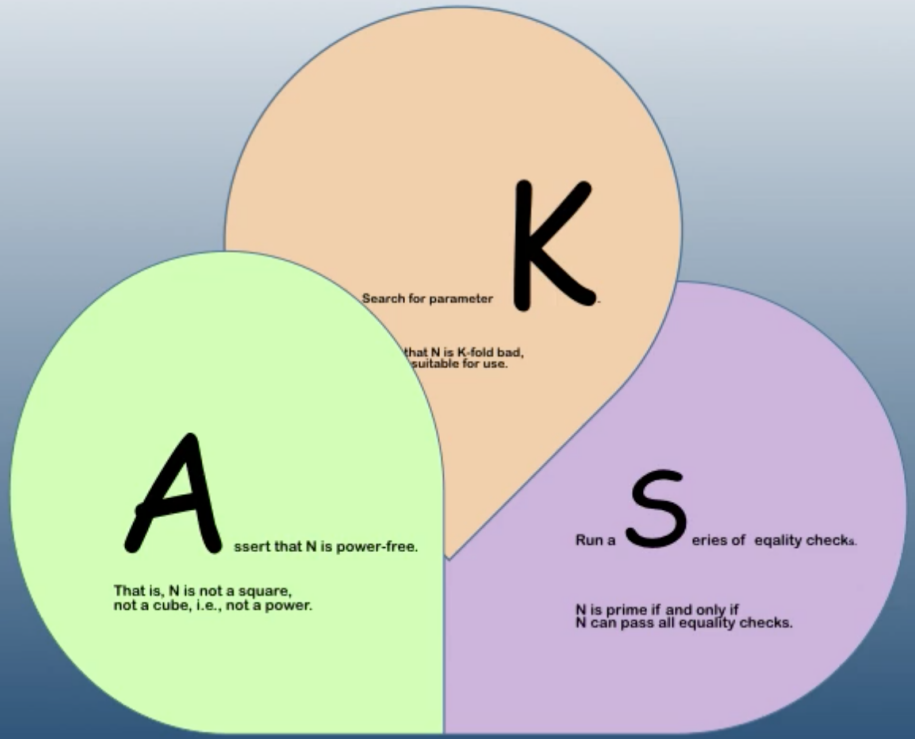
"New Method Said to Solve Key Problem in Math" was the headline of a story in the *New York Times* on August 8, 2002, meaning the proof of the statement PRIMES $\in \mathcal{P}$, hitherto a big open problem in algorithmic number theory and theoretical com-

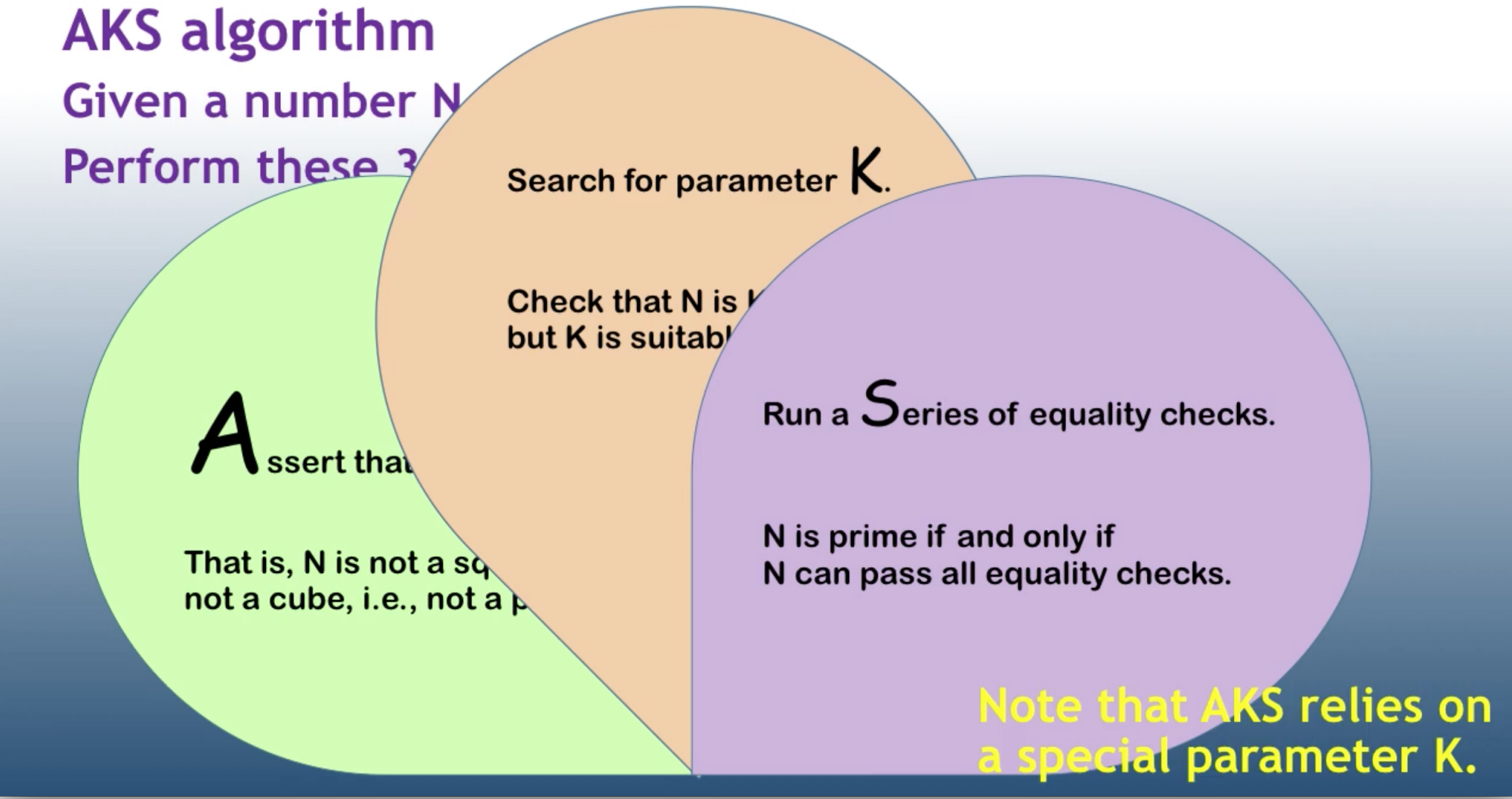
The remarks ... are unfounded and/or inconsequential. ... The proofs in the paper do NOT have too many additional problems to mention. The only true mistake is ..., but that is quite easy to

AKS algorithm

Given a number N, is it a prime?

Perform these 3 stages:




AKS algorithm
Given a number N
Perform these 3
Search for parameter K.
Check that N is
but K is suitab
Assert that
That is, N is not a sq
not a cube, i.e., not a
Run a Series of equality checks.
N is prime if and only if
N can pass all equality checks.
Note that AKS relies on
a special parameter K.

Math behind AKS

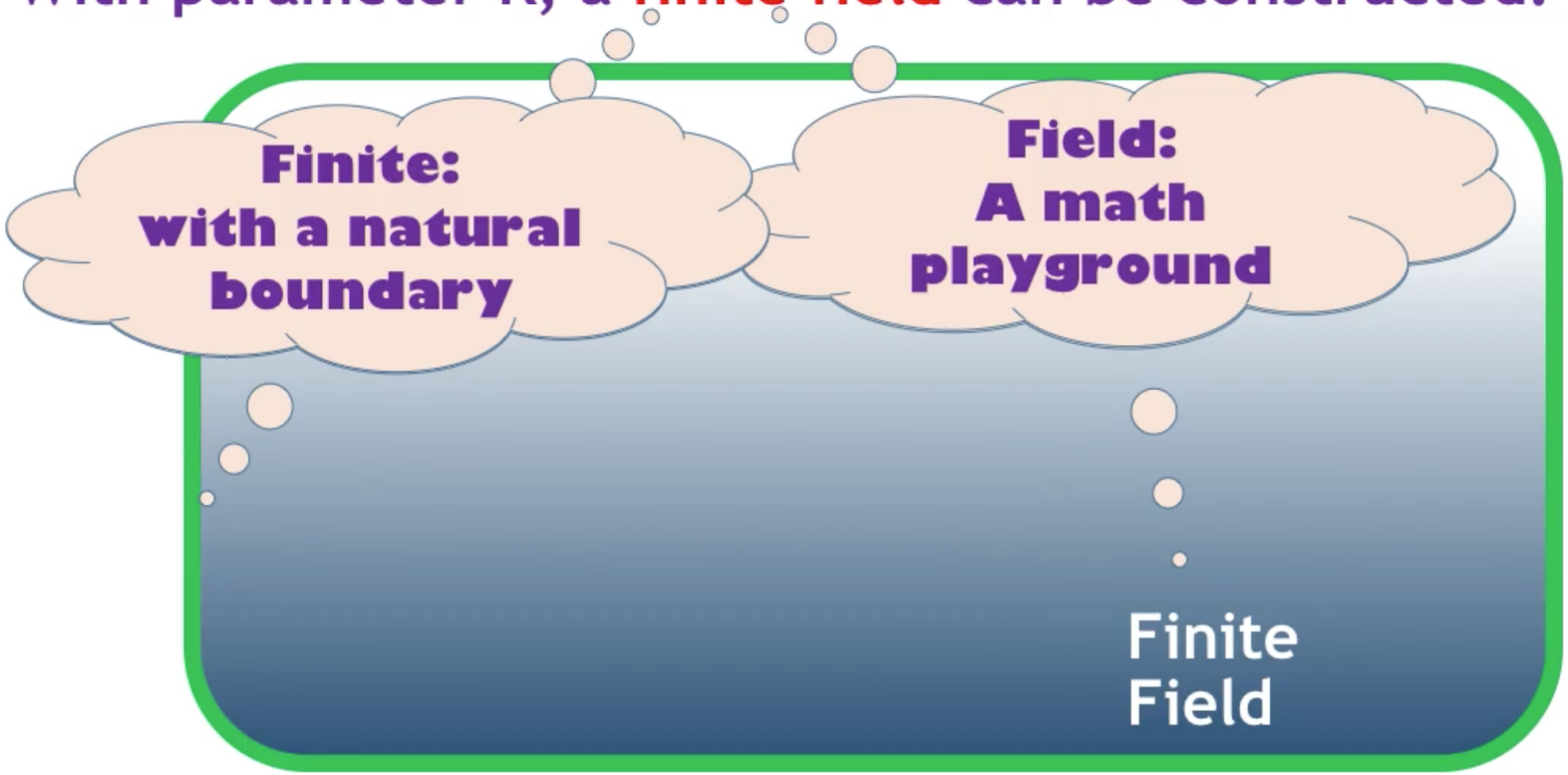
Let N = p q, with a prime factor p.

With parameter K, a finite field can be constructed.

Math behind AKS

Let N = p q, with a prime factor p.

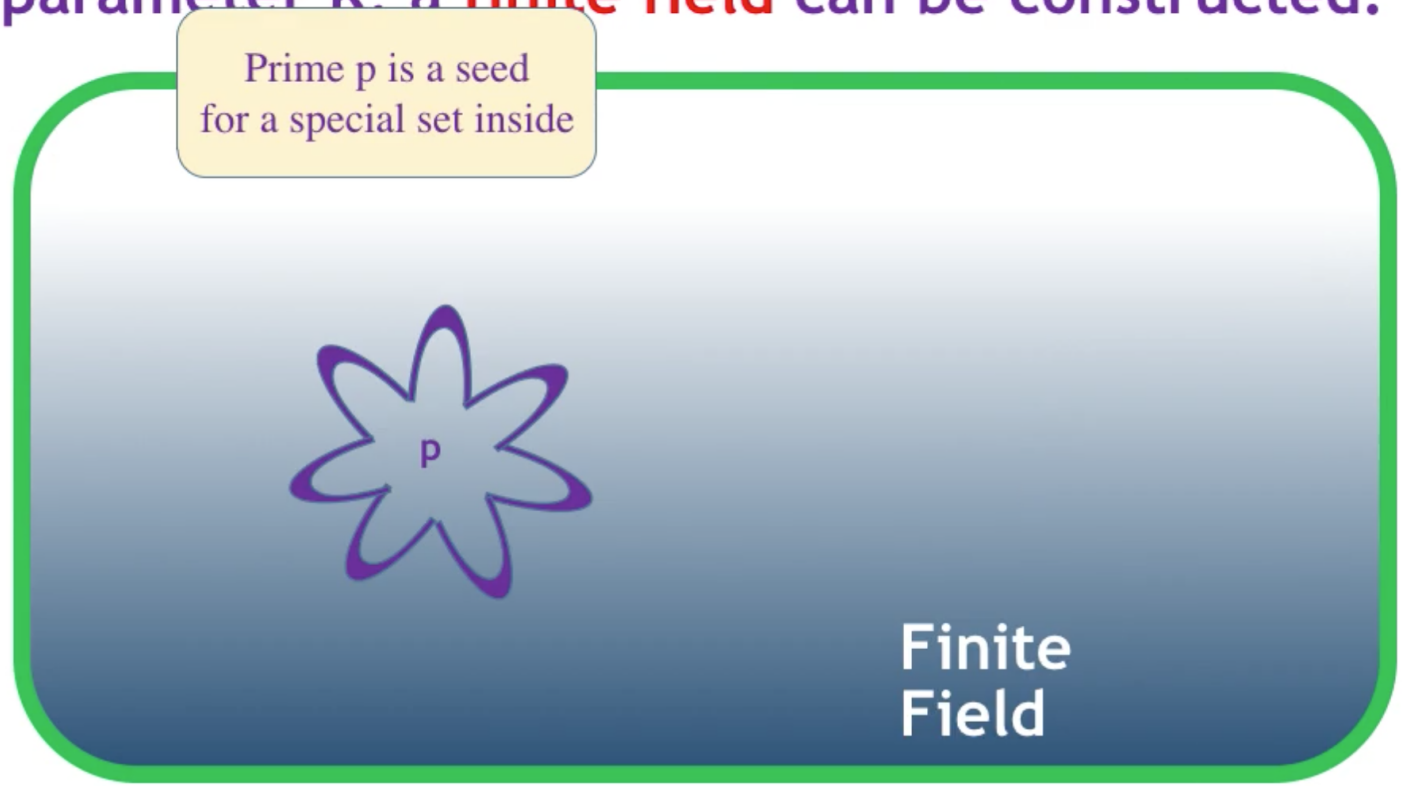
With parameter K, a finite field can be constructed.



Math behind AKS

Let N = p q, with a prime factor p.

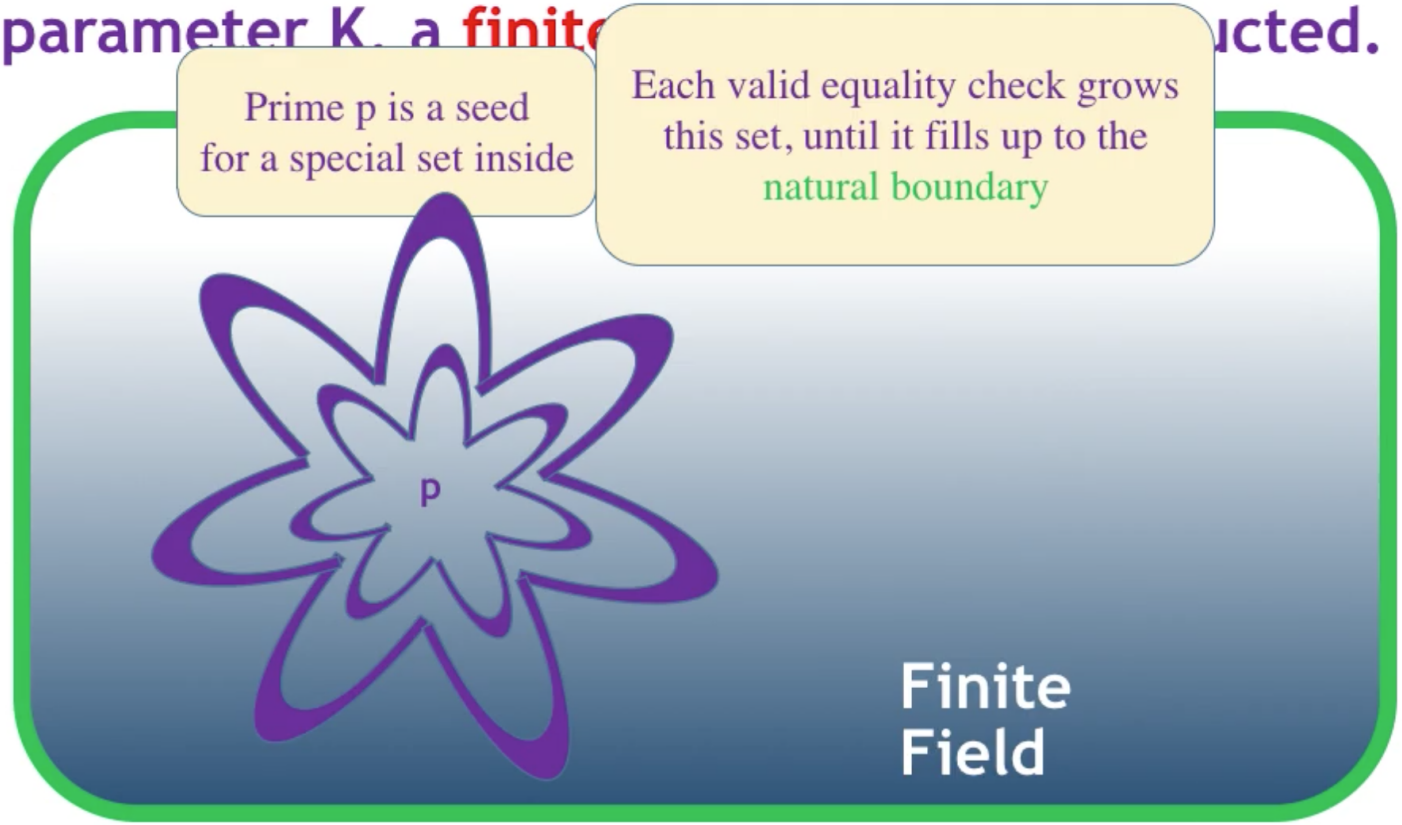
With parameter K, a finite field can be constructed.



Math behind AKS

Let N = p q, with a prime factor p.

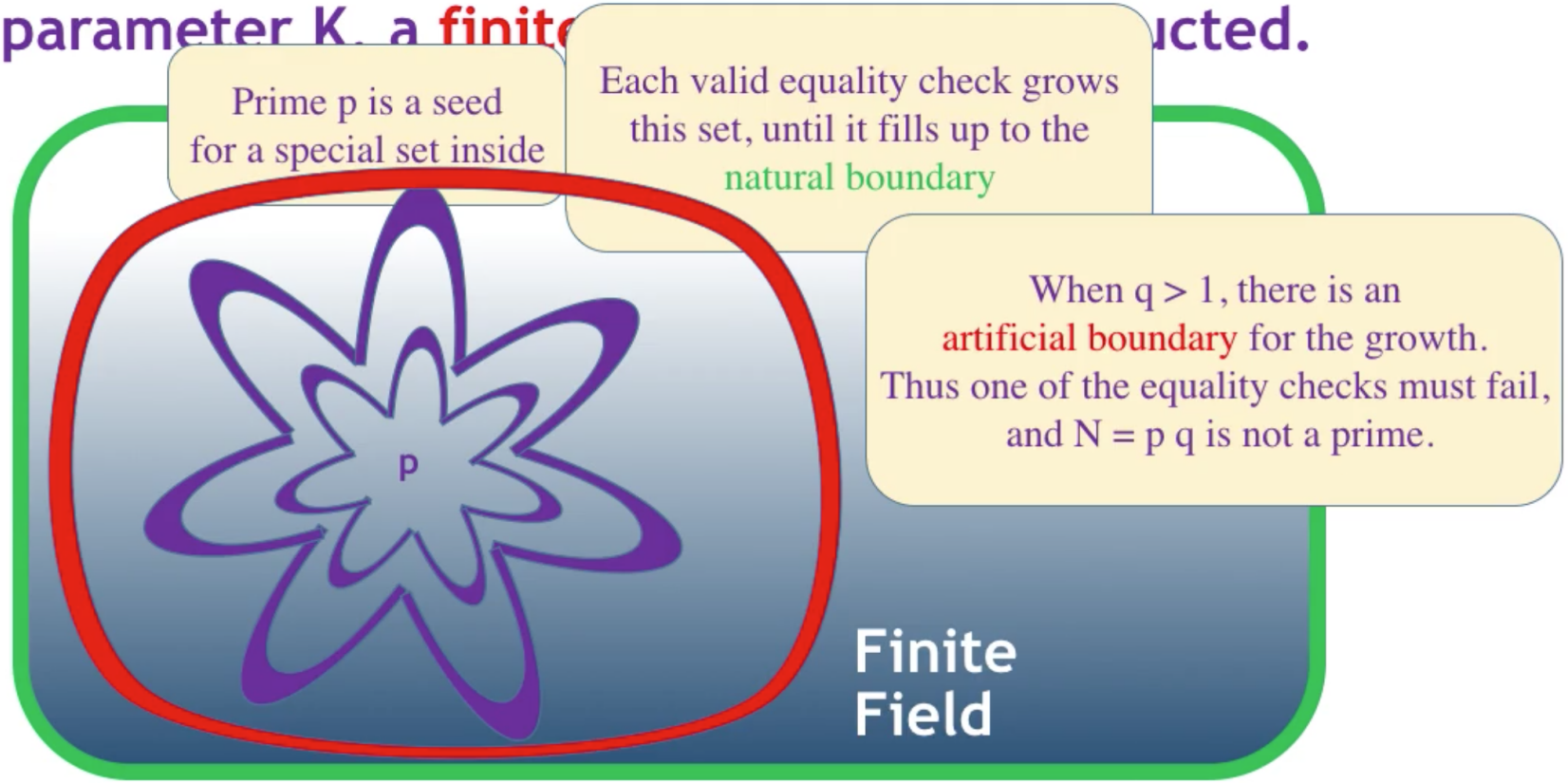
With parameter K, a finite ucted.



Math behind AKS

Let N = p q, with a prime factor p.

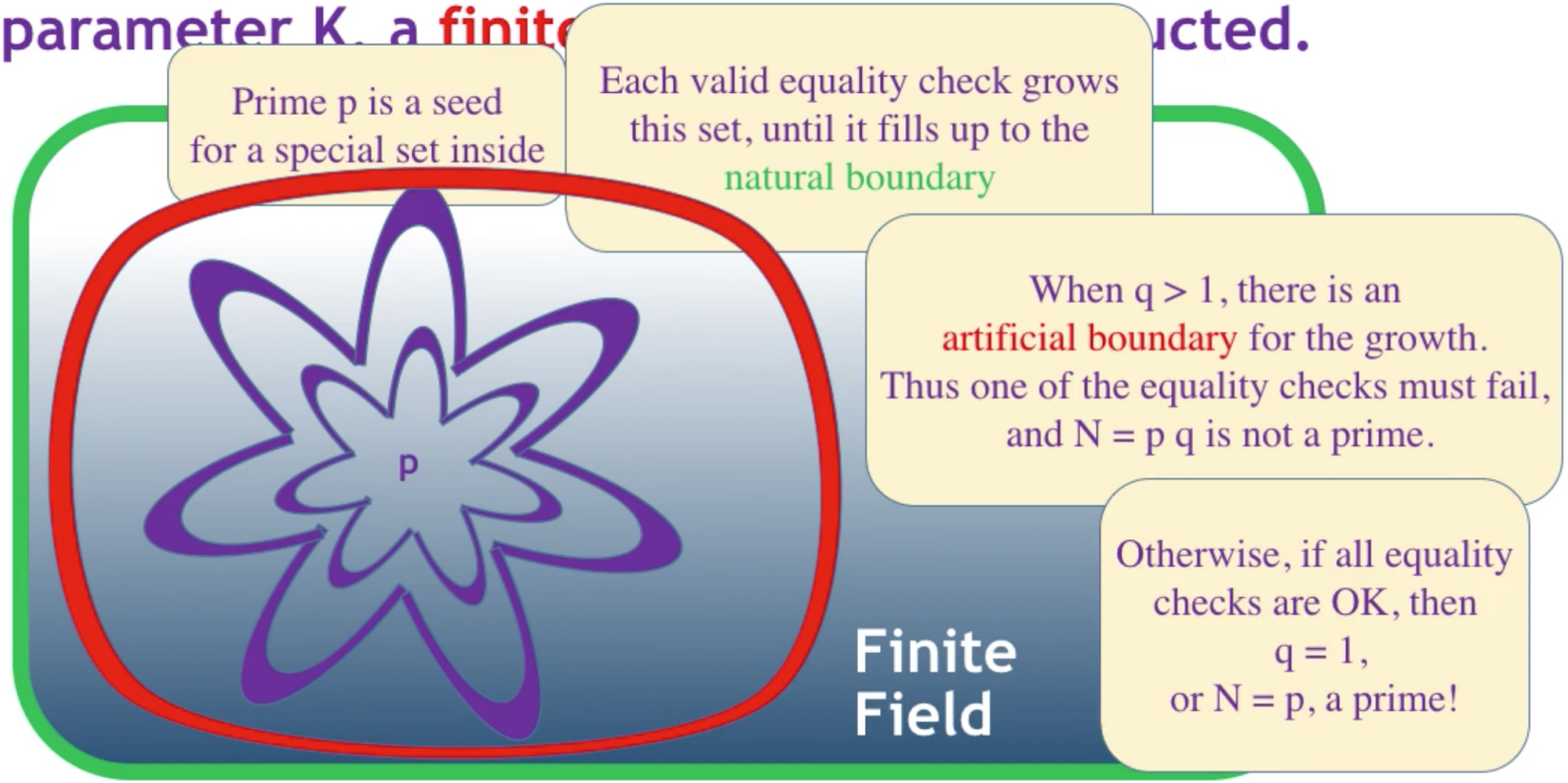
With parameter K, a finite ... ucted.



Math behind AKS

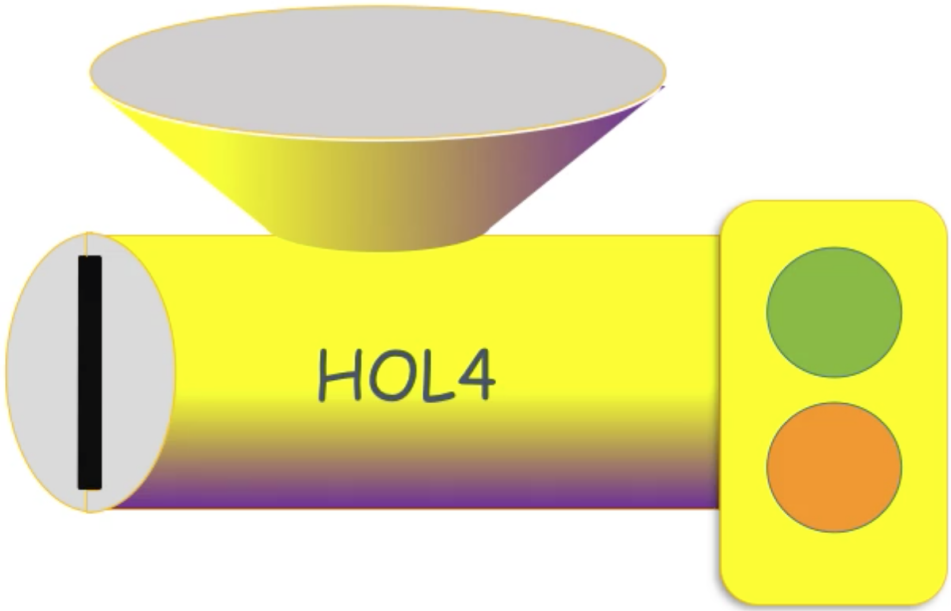
Let N = p q, with a prime factor p.

With parameter K, a finite ... ucted.



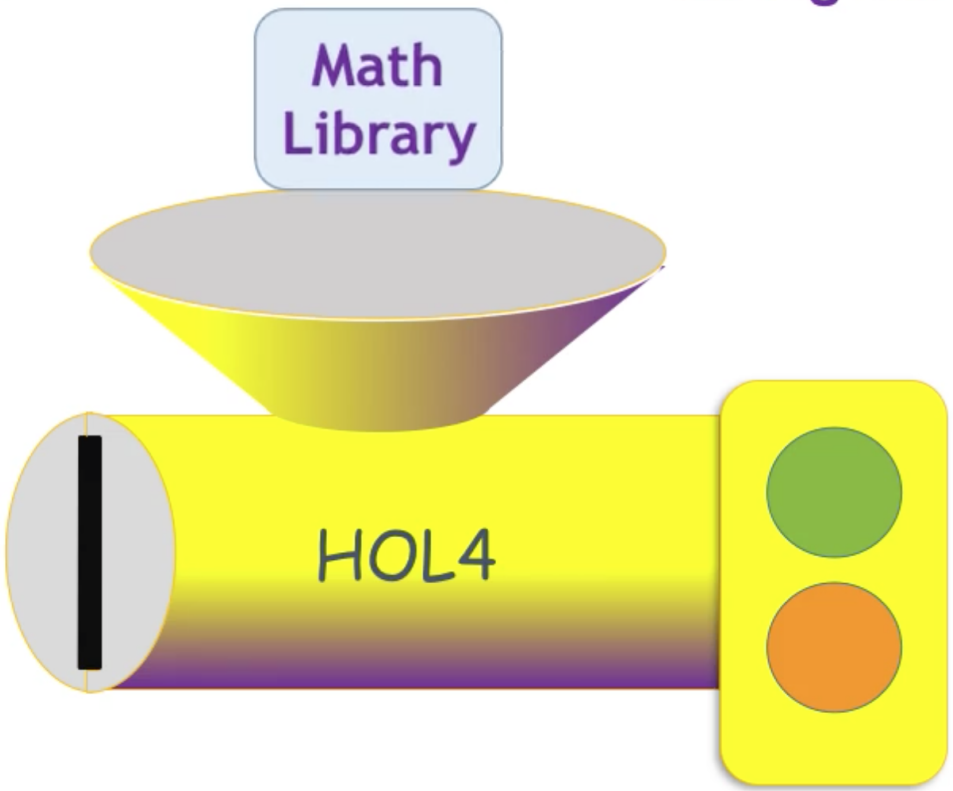
Verify AKS in HOL4: a theorem prover

A program to check all logical deductions



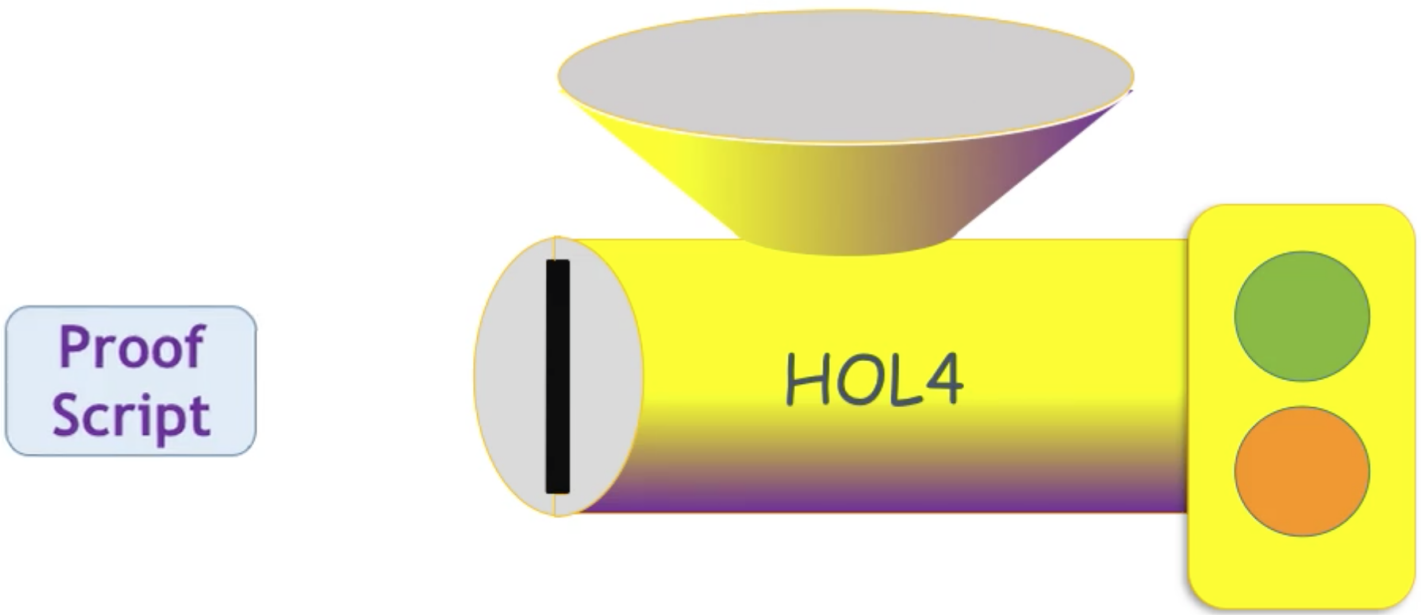
Verify AKS in HOL4: a theorem prover

A program to check all logical deductions



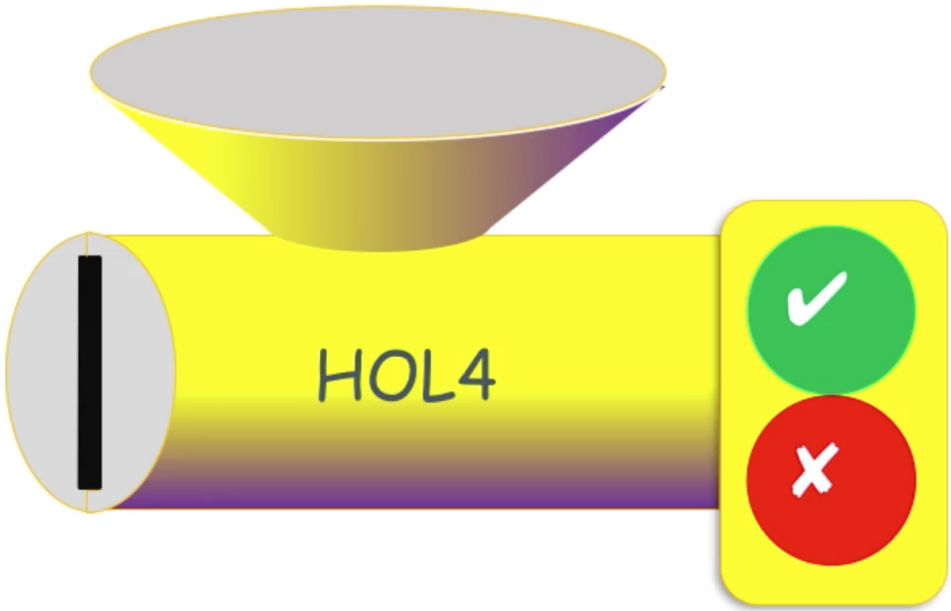
Verify AKS in HOL4: a theorem prover

A program to check all logical deductions



Verify AKS in HOL4: a theorem prover

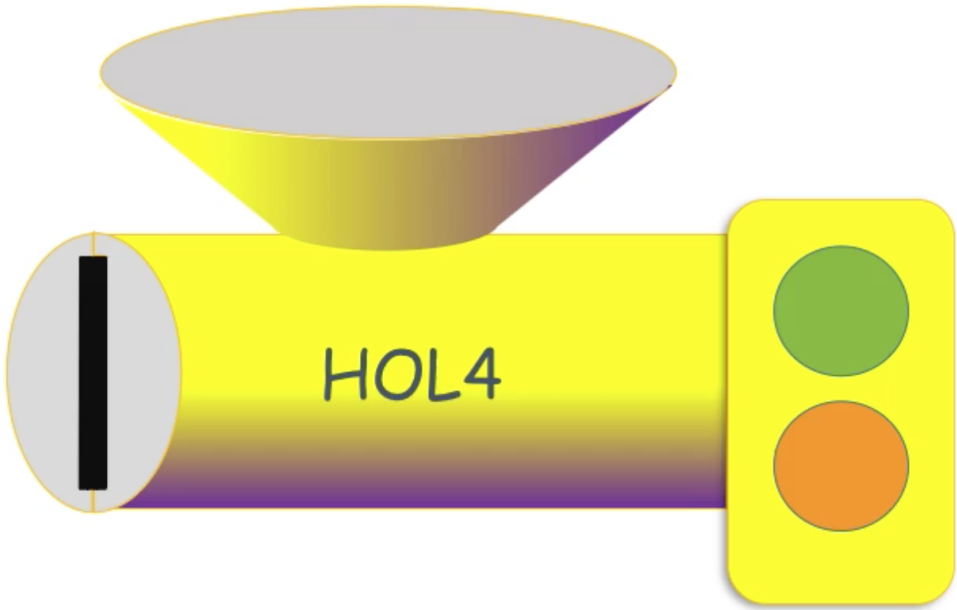
A program to check all logical deductions



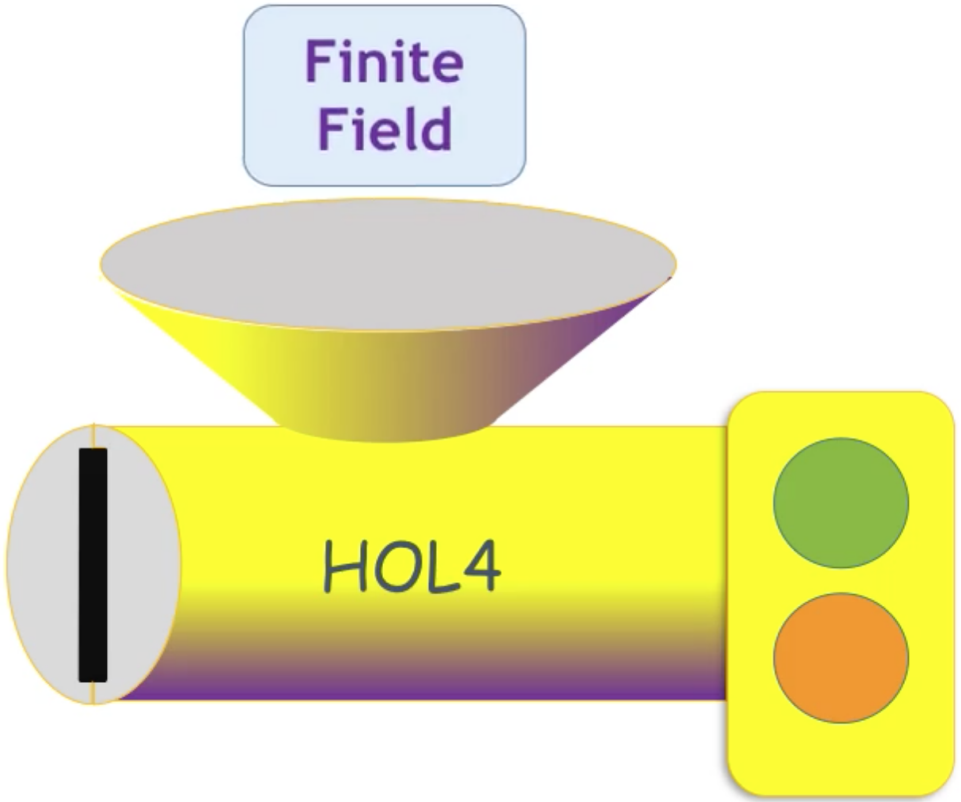
Formally decide a theorem

PhD Part 1: AKS math

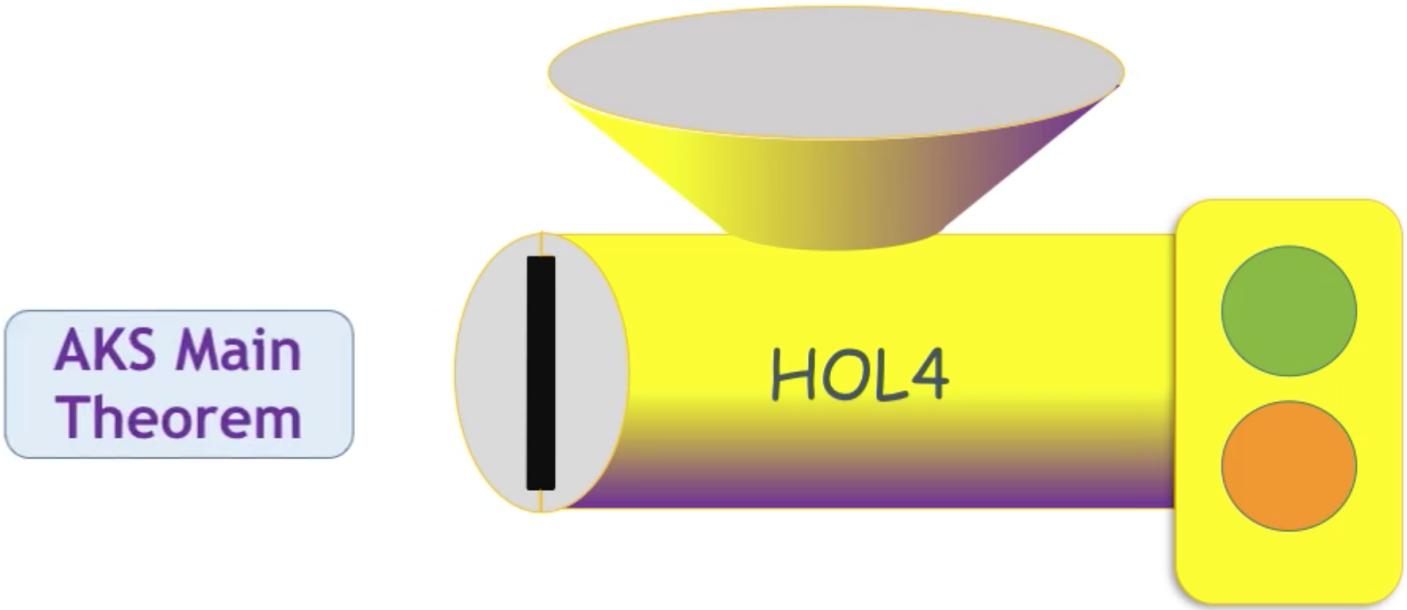
Algebra



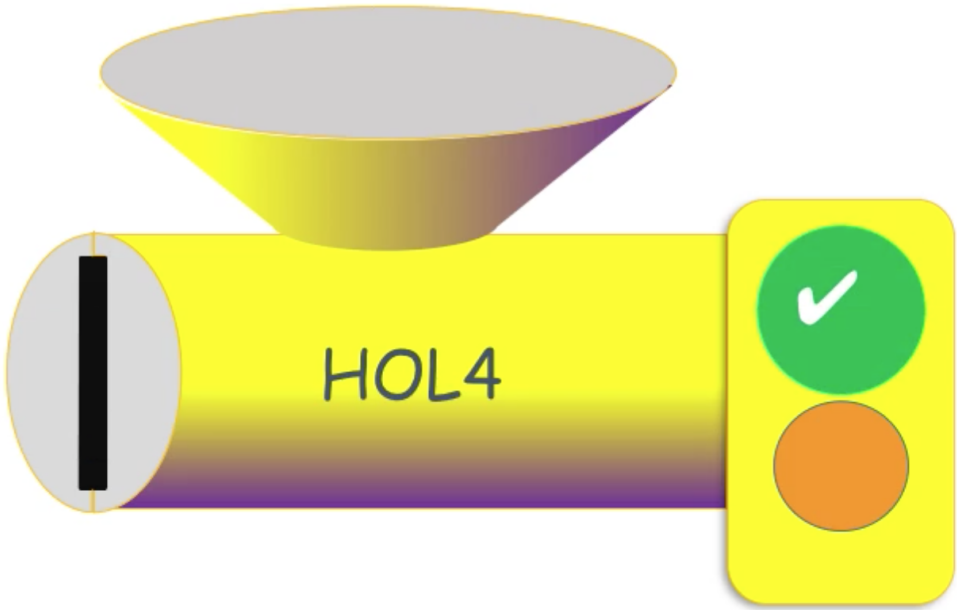
PhD Part 1: AKS math



PhD Part 1: AKS math

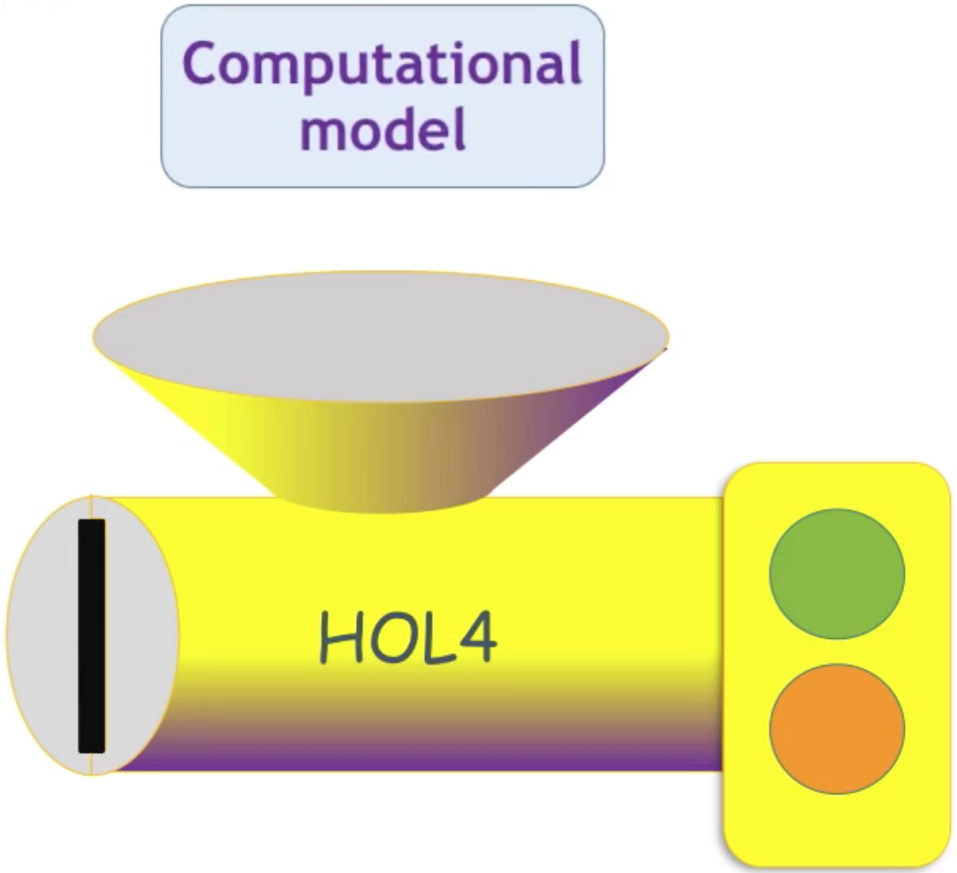


PhD Part 1: AKS math

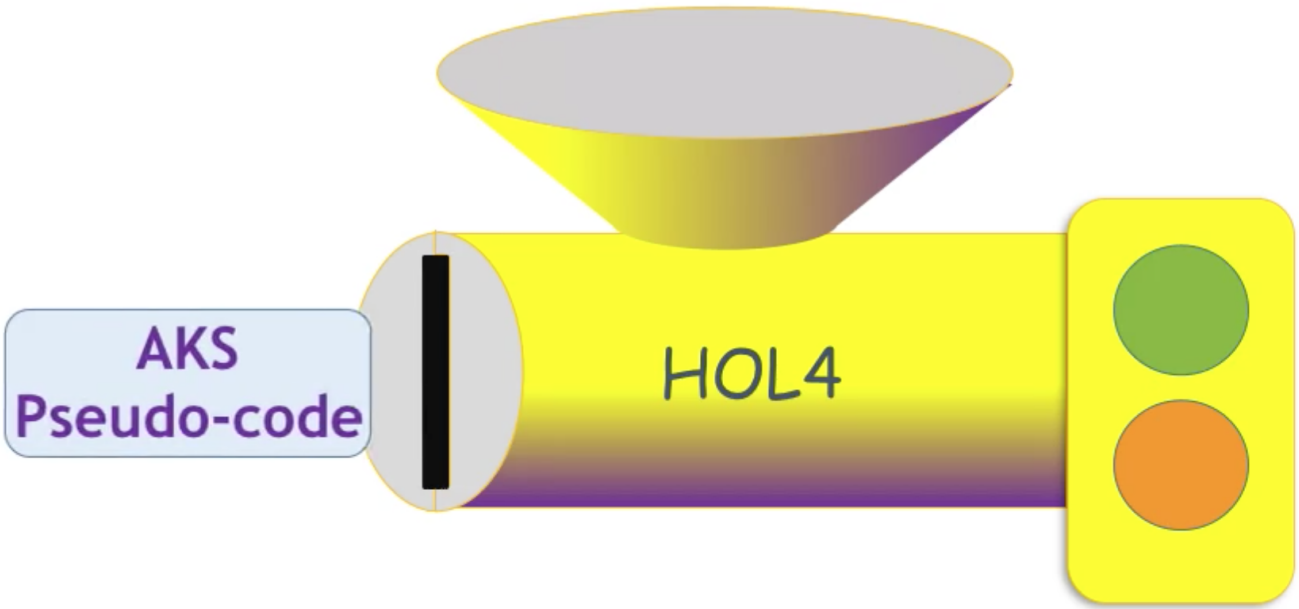


Math is valid!

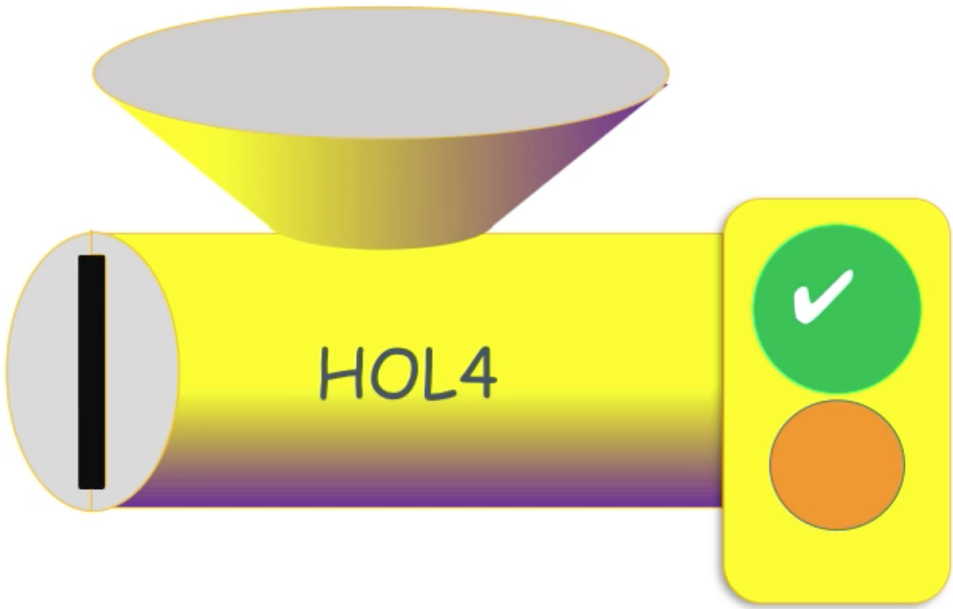
PhD Part 2: AKS algorithm



PhD Part 2: AKS algorithm

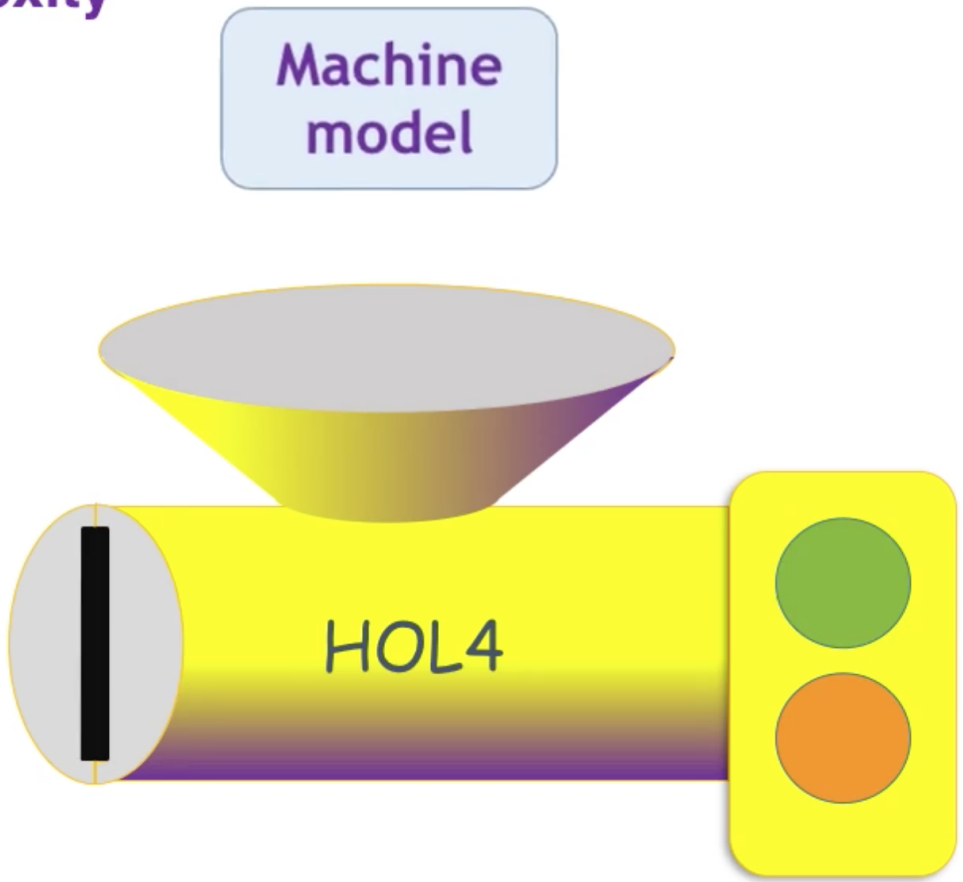


PhD Part 2: AKS algorithm



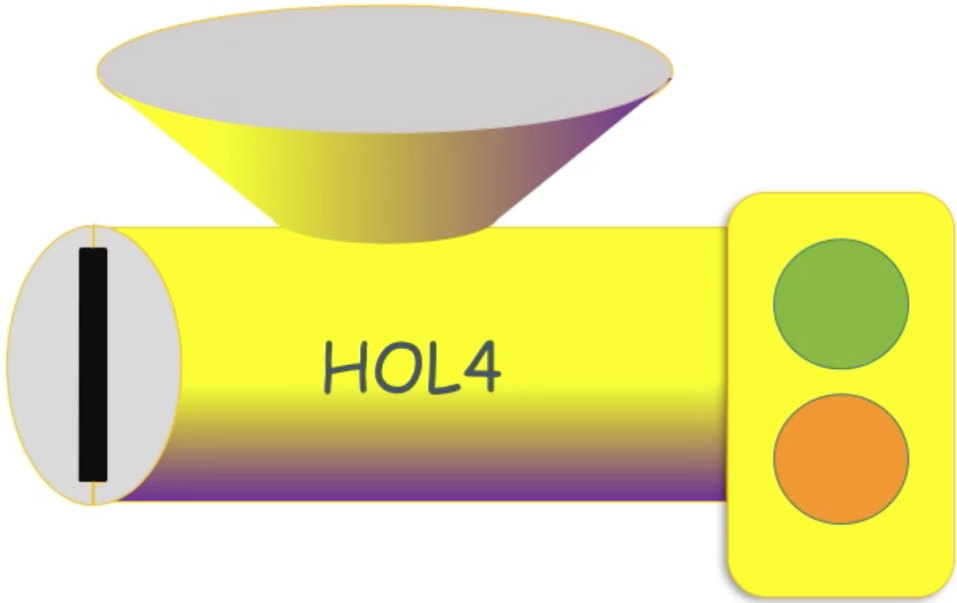
Method is correct!

PhD Part 3: AKS complexity

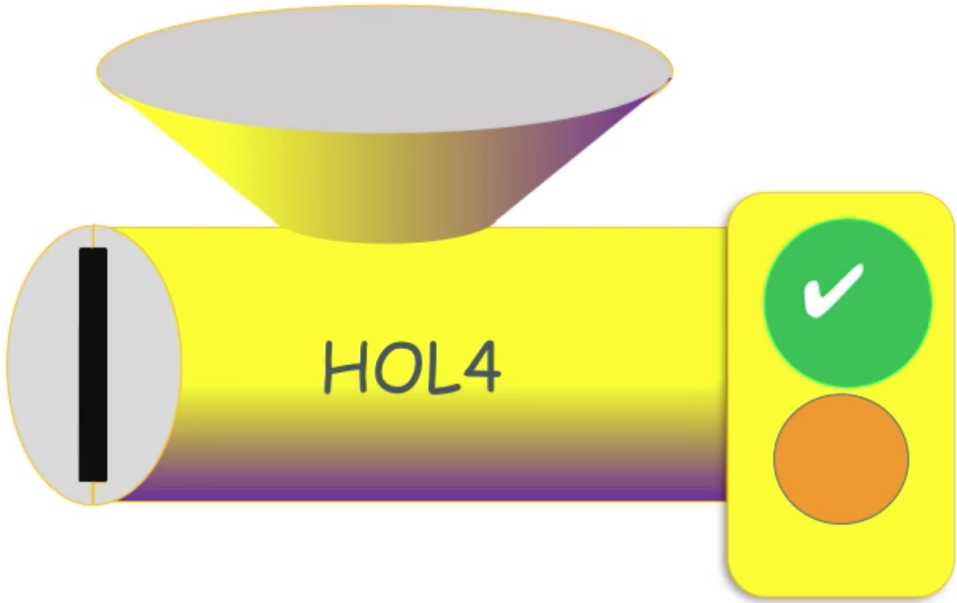


PhD Part 3: AKS complexity

AKS
Machine-code

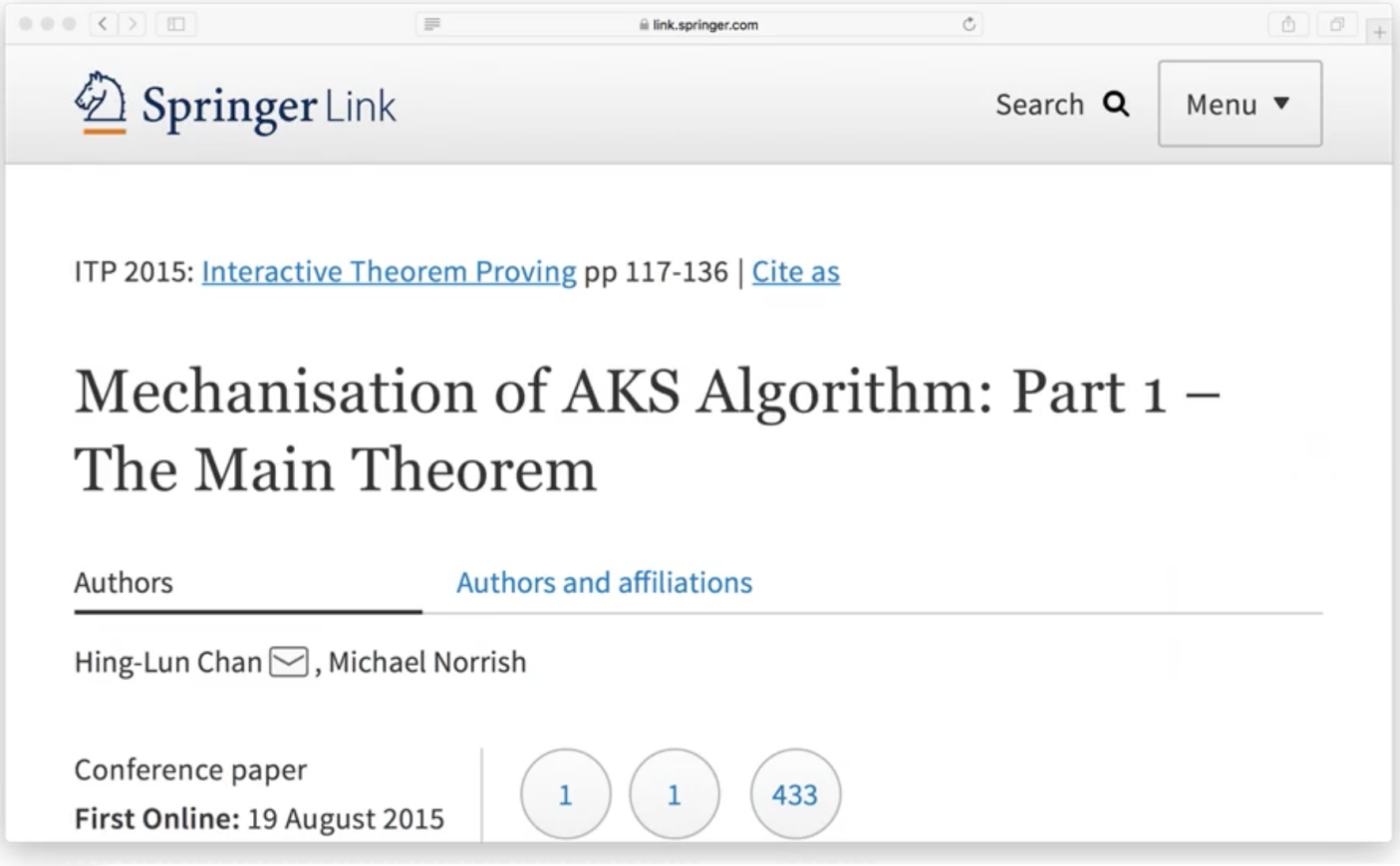


PhD Part 3: AKS complexity

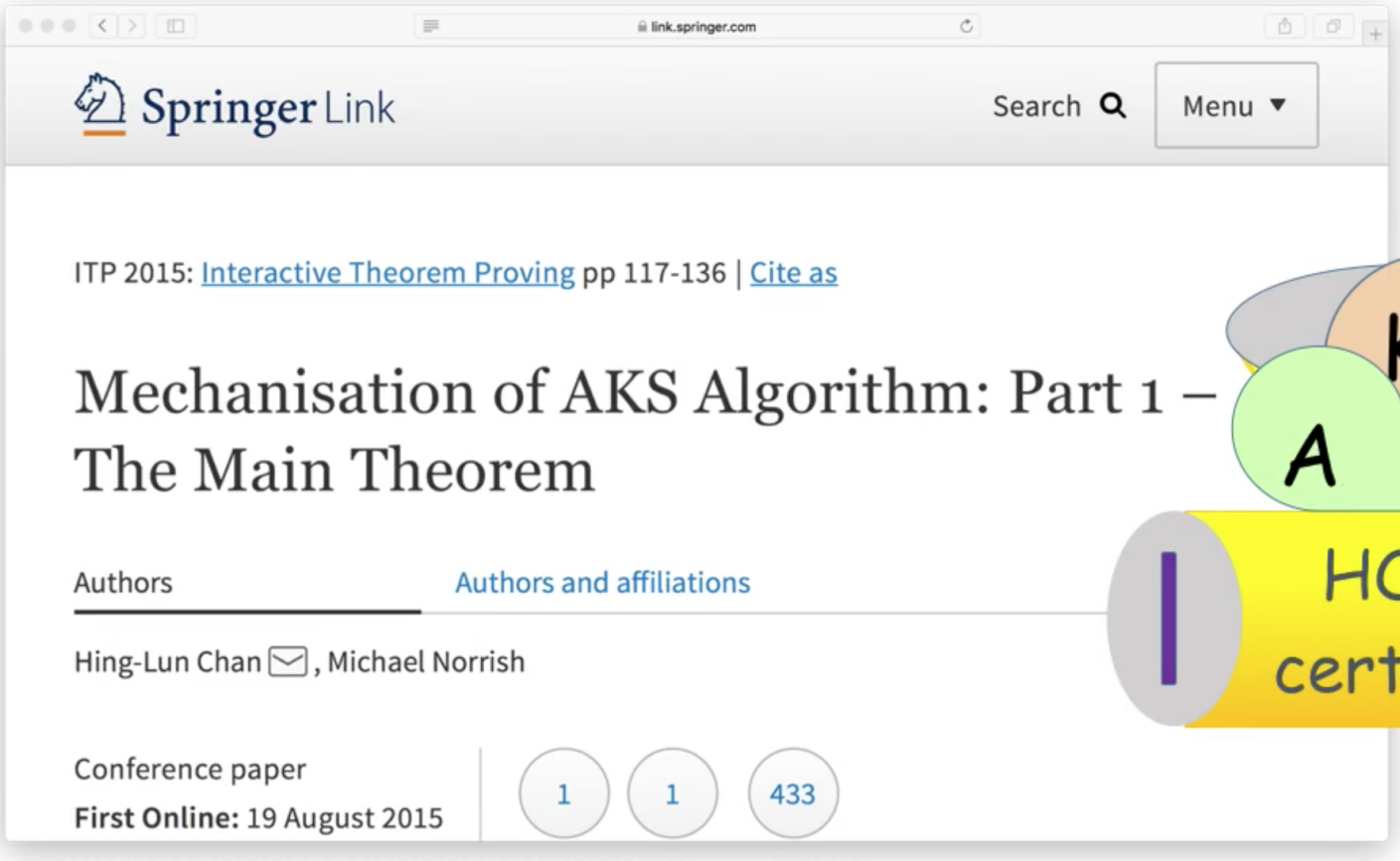


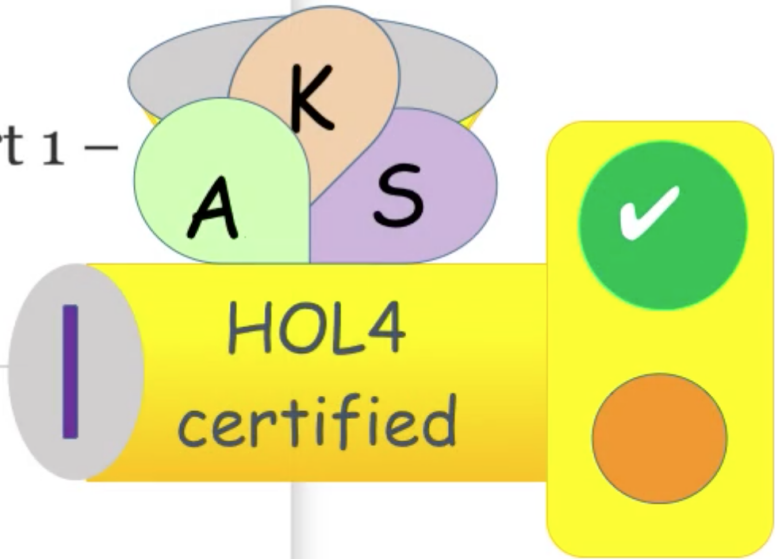
AKS is “fast”!

Part 1 published in 2015



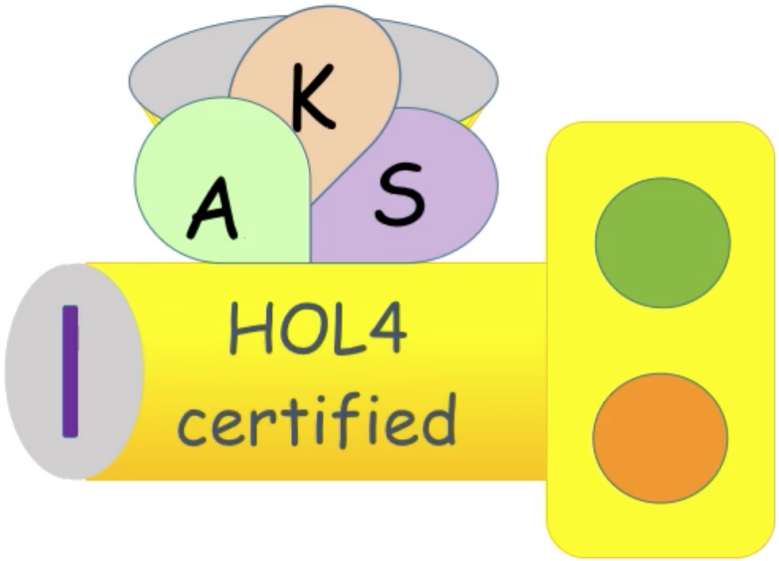
Part 1 published in 2015



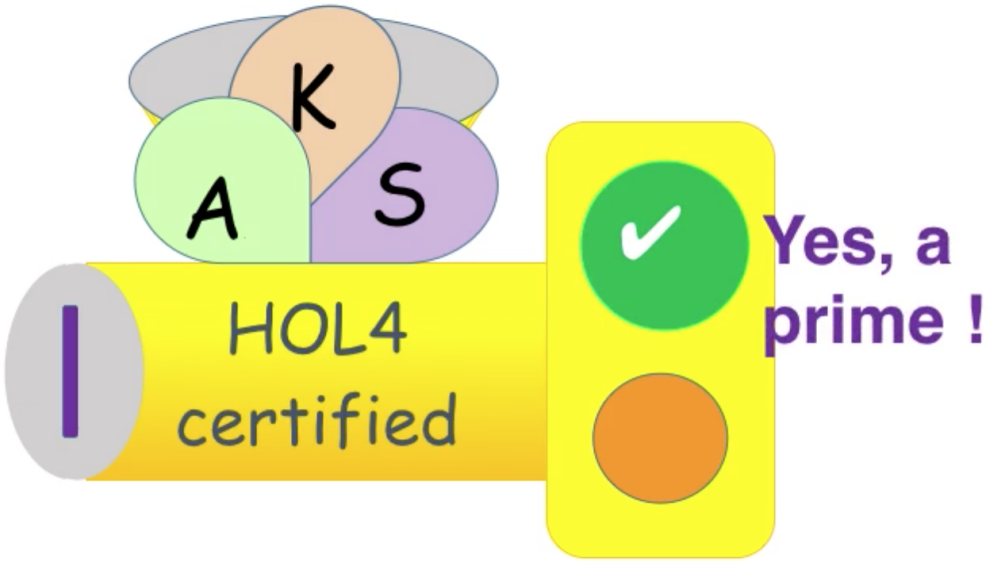


Is 1234567891 a prime?

1234567891



Is 1234567891 a prime?



100% sure!

REFERENCES

[1] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. **PRIMES is in P.** *Annals of Mathematics*, 160(2):781–793, September 2004.

Available from http://annals.math.princeton.edu/2004/160-2/p12

[2] Hing-Lun Chan and Michael Norrish. **Mechanisation of AKS Algorithm: Part 1 — the Main Theorem.**

In Christian Urban and Xingyuan Zhang, editors, *Interactive Theorem Proving, ITP 2015*, number 9236 in LNCS, pages 117–136.

Springer, August 2015. Available from http://link.springer.com/chapter/10.1007/978-3-319-22102-1_8

Media Citations

Slide 2: Image of article from https://www.nytimes.com/2002/08/08/us/new-method-said-to-solve-key-problem-in-math.html

Slide 3: Images in public domain, from https://cdn.pixabay.com/photo/

Slide 5: Image of paper from [1]. Slide 10: Image of paper from [2].

The ANU Logo is provided by https://services.anu.edu.au/marketing-outreach/marketing-materials/anu-logo

Background guitar instrumental “Romance d’Amour” by Anis Haifa, from https://soundcloud.com/anis-haifa/autumn-in-my-heart-romance

Acknowledgments

Thanks to my supervisors: Michael Norrish, Peter Baumgartner, and Jeremy Dawson.

Thanks also to the Logic and Computation Group of the Research School of Computer Science at ANU, especially Rajeev Goré and Dirk Pattinson.

Thanks to all the staff from Research Training, in particular Professor Inger Mewburn, and University Librarian Candida Spence.

Visualise *your* thesis

Australian National University

presented by THE UNIVERSITY OF MELBOURNE