Mechanisation of the AKS Algorithm (Thesis)

Hing Lun Chan

College of Engineering and Computer Science
Australian National University

PhD Thesis, November 2019

Outline

Focus

A Milestone

Beauty is truth,
truth beauty.
— John Keats (1819)[15]

Beauty is in the eye of the beholder, but the following are definitely true:

$$\vdash \mathsf{prime}\ n \iff \mathsf{aks}\ n$$
$$\vdash \mathsf{valueOf}\ (\mathsf{aksM}\ n) \iff \mathsf{aks}\ n$$
$$\vdash \mathsf{stepsOf} \circ \mathsf{aksM} \in \mathcal{O}(\lceil \log n \rceil^{21})$$

Focus

A Milestone

Beauty is truth,
truth beauty.
— John Keats (1819)[15]

Beauty is in the eye of the beholder, but the following ar

$\vdash$ prime $n \iff$ aks n
$\vdash$ valueOf (aksM n) $\iff$ aks
$\vdash$ stepsOf $\circ$ aksM $\in \mathcal{O}(\lceil \log n$

A thing of beauty is a joy forever.
At odds with Lord Byron,
both English Romantic poets.

Chapter 1: Introduction

If you can't explain your mathematics to a machine,
it is an illusion to think you can explain it to a student.
— Nicolaas Govert de Bruijn (2003)[1]

1.1 Formalisation

To formalise is to understand, in detail: explain the logic to a machine, as de Bruijn proclaims.

Chapter 1: Introduction

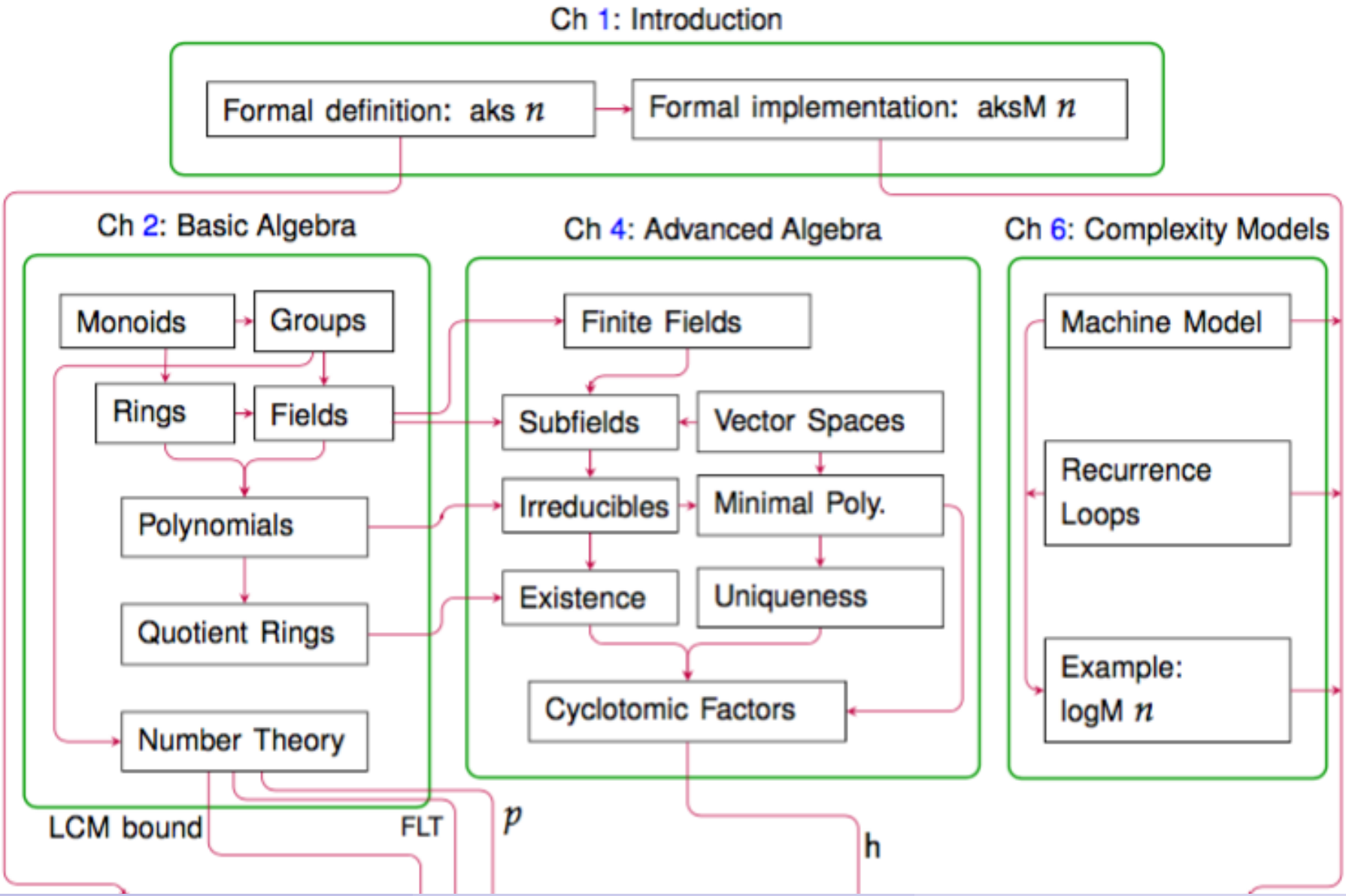
If you can't explain your mathematics to a machine,
it is an illusion to think you can explain it to a student.
— Nicolaas Govert de Bruijn (2003)[1]

1.1 Formalisation

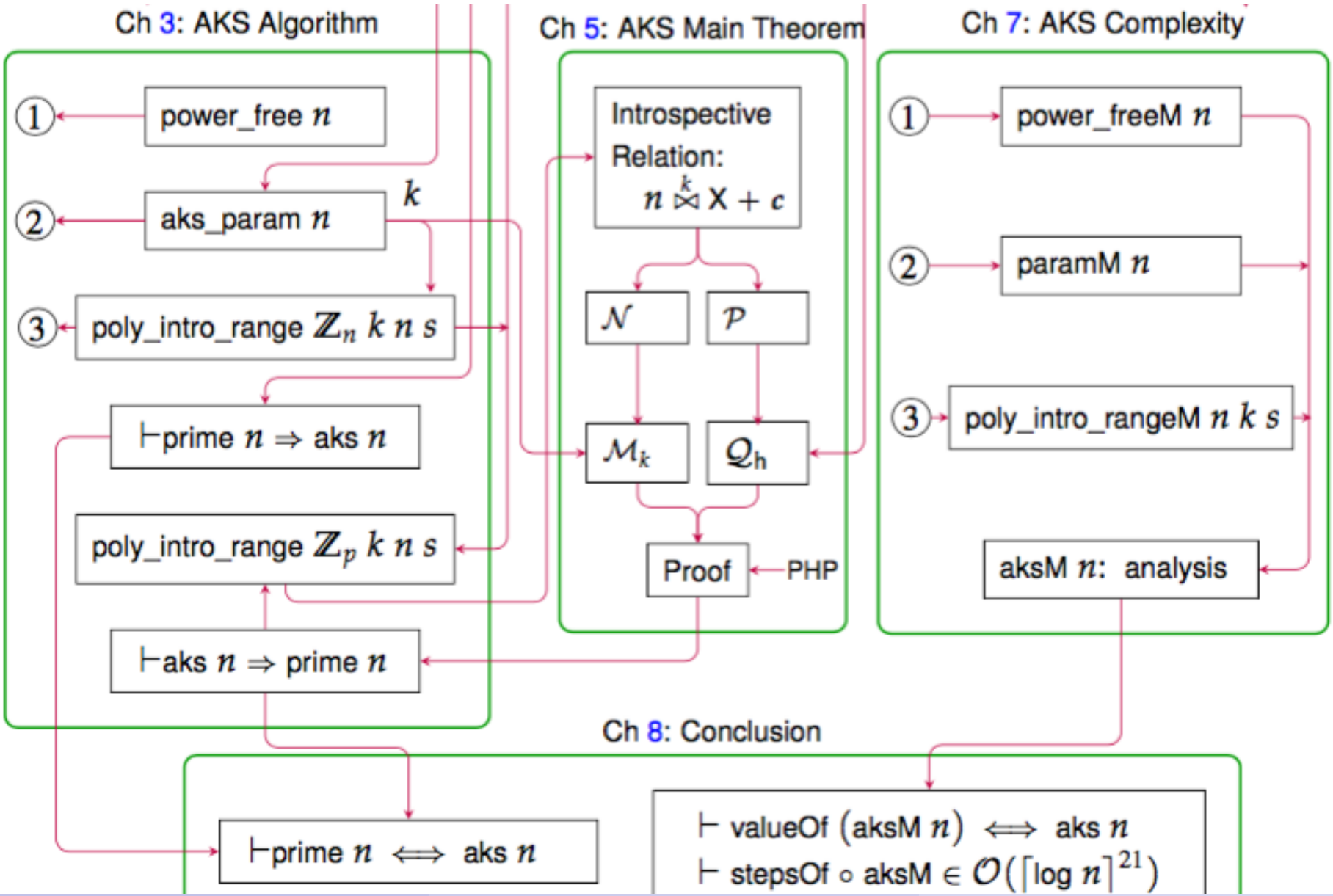
To formalise is to understand, in detail: explain the logic to a

Pioneer of *Automath*

Dependency


Ch 1: Introduction
Formal definition: aks n
Formal implementation: aksM n
Ch 2: Basic Algebra
Monoids
Groups
Rings
Fields
Polynomials
Quotient Rings
Number Theory
Ch 4: Advanced Algebra
Finite Fields
Subfields
Vector Spaces
Irreducibles
Minimal Poly.
Existence
Uniqueness
Cyclotomic Factors
Ch 6: Complexity Models
Machine Model
Recurrence Loops
Example: logM n
LCM bound
FLT
p
h

Dependency (continued)



Chapter 2: Basic Algebra

> Mathematics is the work of the human mind,
> which is destined to study rather than to know,
> to seek the truth rather than to find it.
> — Évariste Galois (1832)[1]

2.1 Algebraic Structures

It was the work of Galois' mind where the concept of a group was first conceived and studied. This transformed the study of algebra: from concrete numbers to abstract structures. Moreover, a short paper by Galois [1830] laid the foundation for the study of finite fields — they are also called Galois fields in his honour.

Chapter 2: Basic Algebra

Mathematics is the work of the human mind,
which is destined to study rather than to know,
to seek the truth rather than to find it.
— Évariste Galois (1832)[1]

2.1 Algebraic Structures

It was the work of Galois' mind where the concept of a g
This transformed the study of algebra: from concrete num
a short paper by Galois [1830] laid the foundation for the
called Galois fields in his honour.

"Don't cry. I need all my courage to die at twenty."

Chapter 3: AKS Algorithm

The journey of a thousand miles
begins with a single step.
— Lao Tzu (老子) (*circa* 600 BC)[1]

3.1 AKS Pseudocode

Our journey to formalise the AKS algorithm begins with its pseudocode, see Algorithm 1. The pseudocode shows the details of each phase, discussed briefly in Section 1.3. We make use of

Chapter 3: AKS Algorithm

The journey of a thousand miles
begins with a single step.
— Lao Tzu (老子) (*circa* 600 BC)[1]

3.1 AKS Pseudocode

Our journey to formalise the AKS algorithm begins with its pseud
pseudocode shows the details of each phase, discussed briefly in

道德經：「千里之行，始於足下。」

Chapter 4: Advanced Algebra

Algebra is nothing more than geometry, in words;
geometry is nothing more than algebra, in pictures.
— Sophie Germain (1831)

4.1 Finite Field Classification

The AKS Main Theorem, as formulate in the proof of Theorem 73, is:

$$\vdash \mathsf{FiniteField}\ \mathcal{F} \wedge |\mathsf{F}| = \mathsf{char}(\mathcal{F}) \Rightarrow \forall n\ k.\ \mathsf{aks\_criteria}\ \mathcal{F}\ n\ k \Rightarrow n\ \mathsf{power\_of}\ \mathsf{char}(\mathcal{F})$$

Toward this goal, we shall take a field/subfield pair, treating the field as an extension of the subfield. These ideas involve the vector spaces, a geometric picture for finite fields.

Chapter 4: Advanced Algebra

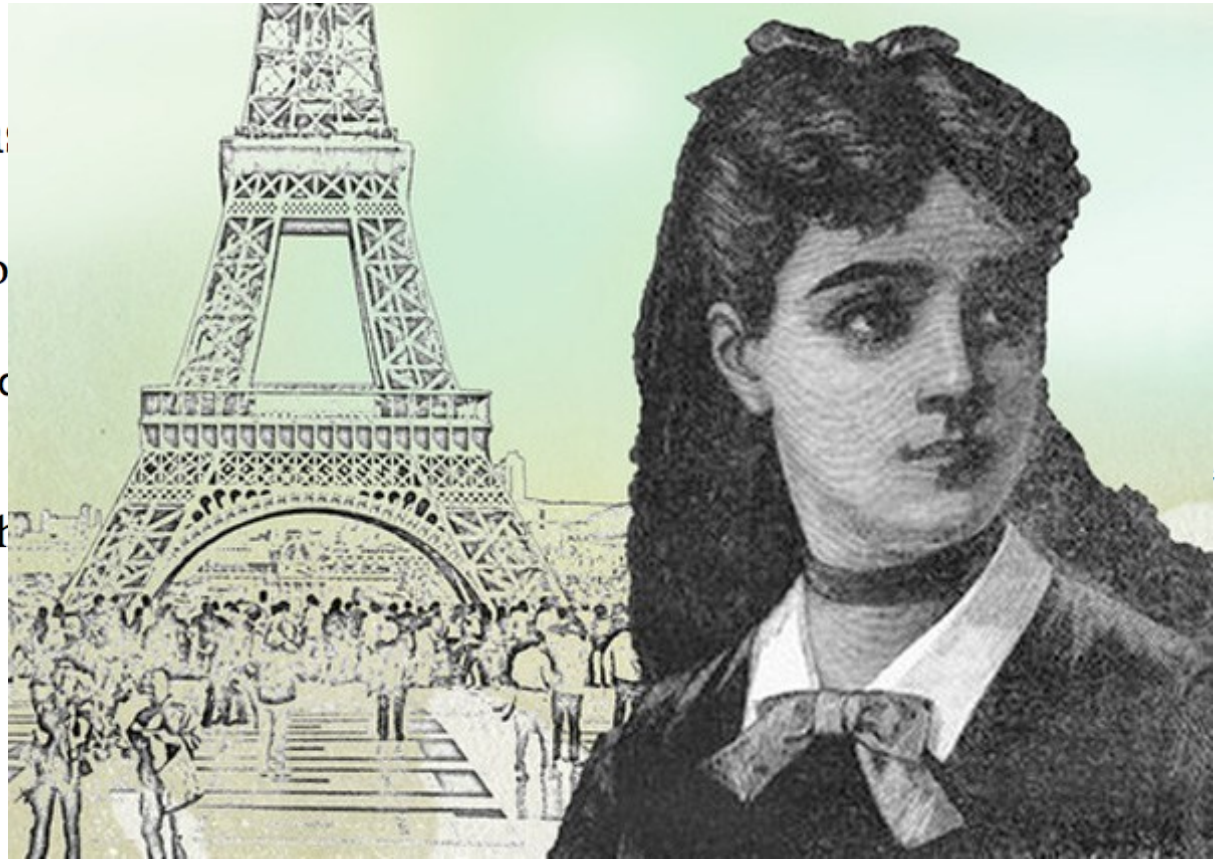
Algebra is nothing more than geometry, in words;
geometry is nothing more than algebra, in pictures.
— Sophie Germain (1831)

4.1 Finite Field Cla

The AKS Main Theorem, as fo

$\vdash$ FiniteField $\mathcal{F} \wedge |\mathsf{F}| =$ c

Toward this goal, we shall
subfield. These ideas involve th



Marie-Sophie Germain

Chapter 5: AKS Main Theorem

Reductio ad absurdum, which Euclid loved so much,
is one of a mathematician's favourite weapons.
It is a far finer gambit than any chess gambit:
a chess player may offer the sacrifice of a pawn
or even a piece, but a mathematician offers the game.
— Godfrey Harold Hardy (1940)[1]

5.1 Main Theorem

We shall finish the proof that a number n passing the AKS tests must be prime (Theorem 73):

$$\vdash \mathsf{aks}\ n \Rightarrow \mathsf{prime}\ n$$

by establishing this AKS Main Theorem:

Otherwise, the **Pigeonhole principle** will be violated.

Chapter 5: AKS Main Theorem

Reductio ad absurdum, which Euclid loved so much,
is one of a mathematician's favourite weapons.
It is a far finer gambit than any chess gambit:
a chess player may offer the sacrifice of a pawn
or even a piece, but a mathematician offers the game.
— Godfrey Harold Hardy (1940)[1]

5.1 Main Theorem

We shall finish the proof that a number n passing the AKS

$$\vdash \mathsf{aks}\ n \Rightarrow \mathsf{prime}\ n$$

by establishing this AKS Main Theorem:

Otherwise, the **Pigeonhole principle** will be violated.

Beauty is the first test: there is no permanent place in the world for ugly mathematics.

Chapter 6: Complexity Models

A Writer monad value is a pair: (computation, log).
Binding replaces the computation value
with the result of applying the bound function
to the previous value and appends any log data
from the computation to the existing log data.
— All About Monads, HaskellWiki[1]

6.1 Monadic Computation

Chapter 6: Complexity Models

A Writer monad value is a pair: (computation, log).
Binding replaces the computation value
with the result of applying the bound function
to the previous value and appends any log data
from the computation to the existing log data.
— All About Monads, HaskellWiki[1]

6.1 Monadic Computation

Logician: Haskell Brooks Curry

Chapter 7: AKS Complexity

We may say most aptly that
the Analytical Engine weaves algebraic patterns,
just as the Jacquard loom weaves flowers and leaves.
— Ada Lovelace (1843)[1]

7.1 AKS Implementation

We shall weave the 3 phases of the AKS algorithm in monadic style (see Definition 3) for an implementation (compare with the pseudocode in Algorithm 1):

Chapter 7: AKS Complexity

We may say most aptly that
the Analytical Engine weaves algebraic patterns,
just as the Jacquard loom weaves flowers and leaves.
— Ada Lovelace (1843)[1]

7.1 AKS Implementation

We shall weave the 3 phases of the AKS algor
implementation (compare with the pseudocode

Daughter of poet Lord Byron, and
programmer of the *Analytical Engine*.

Chapter 8: Conclusion

We shall not cease from exploration,
and the end of all our exploring
will be to arrive where we started
and know the place for the first time.
— Thomas Stearns Eliot (1942)[1]

8.1 Overall Summary

We shall return to the starting dependency diagram (reproduced in Figure 8.1) to see how far we have explored the wonders of the AKS algorithm.

Chapter 8: Conclusion

We shall not cease from exploration,
and the end of all our exploring
will be to arrive where we started
and know the place for the first time.
— Thomas Stearns Eliot (1942)[1]

8.1 Overall Summary

We shall return to the starting dependency diagram (rep
have explored the wonders of the AKS algorithm.

Nobel Prize in Literature (1948)

Acknowledgment

Lastly, I would like to thank the world of mathematics, populated by many highly gifted mathematicians. I read broadly, and learn many excellent ideas and techniques through their work. That world is a world of dreams, with wonderful colors one cannot see, and delightful music one cannot hear. The experience is aptly expressed in the following quote:

In the broad light of day
mathematicians check their equations and their proofs,
leaving no stone unturned in their search for rigour.
But, at night, under the full moon, they dream,
they float among the stars
and wonder at the miracle of the heavens.
They are inspired.
Without dreams there is no art,
no mathematics, no life.
— Michael Atiyah[1]

Acknowledgment

Lastly, I would like to thank the world of mathematics, populated by many highly gifted mathematicians. I read broadly, and learn many excellent ideas and techniques through their work. That world is a world of dreams, with wonderful colors one cannot see, and delightful music one cannot hear. The experience is aptly expressed in the following quote:

Fields Medal (1966), Abel Prize (2004).

In the broad light of day
mathematicians check their equations and their proofs,
leaving no stone unturned in their search for rigour.
But, at night, under the full moon, they dream,
they float among the stars
and wonder at the miracle of the heavens.
They are inspired.
Without dreams there is no art,
no mathematics, no life.
— Michael Atiyah[1]

Examiner #1

[...] The dissertation has been written with great care, and although the candidate is apparently not a native speaker of English, this isn't obvious at a casual reading. The candidate has also demonstrated an impressive familiarity with related work.

Examiner #1

[...] The dissertation has been written with great care, and although the candidate is apparently not a native speaker of English, this isn't obvious at a casual reading. The candidate has also demonstrated an impressive familiarity with related work.

[...] the title of the dissertation should be something better, like "Primality Testing is Polynomial: A Mechanised Verification of the AKS Algorithm".

Examiner #2

Something that stood out for me was that the candidate has been creative in finding new proofs and new approaches. This to me is a good advertisement for the process of formalization: it's not just a matter of dotting i's and crossing t's, but can stimulate the development of new ideas.

Examiner #2

Something that stood out for me was that the candidate has been creative in finding new proofs and new approaches. This to me is a good advertisement for the process of formalization: it's not just a matter of dotting i's and crossing t's, but can stimulate the development of new ideas.

[...] The only criticism of the thesis generally is that the English is often a bit unidiomatic and sometimes technically wrong. This seldom obscures the intended meaning, but this can be a distraction. Given the exceptional quality of this work in other areas, [...]

Examiner #3

[...] I really enjoy reading the manuscript, it reads like a crime novel. We know the culprit (PRIMES is in P) and the chapters progressively introduce the different characters and how they participate to the story.

Examiner #3

[...] I really enjoy reading the manuscript, it reads like a crime novel. We know the culprit (PRIMES is in P) and the chapters progressively introduce the different characters and how they participate to the story.

[In the theorem-proving community, there is a term called] the "Mexican hat". The idea is the following. When someone wants to formalise a difficult mathematical theorem, he/she first needs to formalise a large corpus of mathematics. This is the base of the hat. From this corpus, it is then possible to reach high to the difficult theorem.

Examiner #3

[...] I really enjoy reading the manuscript, it reads like a crime novel. We know the culprit (PRIMES is in P) and the chapters progressively introduce the different characters and how they participate to the story.

[In the theorem-proving community, there is a term called] the "Mexican hat". The idea is the following. When someone wants to formalise a difficult mathematical theorem, he/she first needs to formalise a large corpus of mathematics. This is the base of the hat. From this corpus, it is then possible to reach high to the difficult theorem.

This work presented here clearly follows the Mexican hat shape but the owner of the hat has a really impressive large head!

Salute