Utrecht University

EINDHOVEN UNIVERSITY OF TECHNOLOGY

25 April, 2025

Introducing formalization of mathematics with Tutte's theorem

Pim Otte
PhD Candidate

Outline

Outline

About me

- Pim Otte
- PhD candidate at Utrecht University & Technical University of Eindhoven
- Topic “Type Theory for Education”
- Webpage: `https://pim.otte.dev`

Topic

- Formalization of mathematics: What and Why?
- Demo: Formalizing Tutte's theorem

Outline

Formalization

- What: Encoding mathematics in a formal system

Formalization

- What: Encoding mathematics in a formal system
- Why: To teach mathematics to computers

Formalization

- What: Encoding mathematics in a formal system
- Why: To teach mathematics to computers
- Why: To create proof assistants (Interactive Theorem Provers)

Why do we want proof assistants?

- Verification

Why do we want proof assistants?

- Verification
- To build tools to help mathematicians

Why do we want proof assistants?

- Verification
- To build tools to help mathematicians
- To scale mathematical collaboration

Verification

- Computer assisted proofs: The four colour theorem [G$^+$08]

Verification

- Computer assisted proofs: The four colour theorem [G+08]
- Mathematical doubt: The Liquid Tensor Experiment [Buz22] [Com21]

Tools for mathematicians

- Proof *assistant*

Tools for mathematicians

- Proof *assistant*
  - Interactive theorem proving

Tools for mathematicians

- Proof *assistant*
    - Interactive theorem proving
    - Theorem search

Tools for mathematicians

- Proof *assistant*
  - Interactive theorem proving
  - Theorem search
  - Automated theorem proving

Tools for mathematicians

- Proof *assistant*
  - Interactive theorem proving
  - Theorem search
  - Automated theorem proving
- Teaching tools

Scaling mathematical collaboration

- What's the biggest mathematical collaboration in the room?

Scaling mathematical collaboration

- What's the biggest mathematical collaboration in the room?
- Liquid Tensor Experiment (29 contributors)

Scaling mathematical collaboration

- What’s the biggest mathematical collaboration in the room?
- Liquid Tensor Experiment (29 contributors)
- Busy Beaver 5 (28 contributors)

Scaling mathematical collaboration

- What’s the biggest mathematical collaboration in the room?
- Liquid Tensor Experiment (29 contributors)
- Busy Beaver 5 (28 contributors)
- Fermat’s Last Theorem (ongoing) (44 contributors)

Scaling mathematical collaboration

- What’s the biggest mathematical collaboration in the room?
- Liquid Tensor Experiment (29 contributors)
- Busy Beaver 5 (28 contributors)
- Fermat’s Last Theorem (ongoing) (44 contributors)
- Equational Theories (56 contributors)

Scaling mathematical collaboration

- What's the biggest mathematical collaboration in the room?
- Liquid Tensor Experiment (29 contributors)
- Busy Beaver 5 (28 contributors)
- Fermat's Last Theorem (ongoing) (44 contributors)
- Equational Theories (56 contributors)
- Mathlib (413 contributors)

Bonus: Interaction with Generative AI

- Problem: Generative AI is hit or miss

Bonus: Interaction with Generative AI

- Problem: Generative AI is hit or miss
- A formal (intermediate) language allows verification

Bonus: Interaction with Generative AI

- Problem: Generative AI is hit or miss
- A formal (intermediate) language allows verification
- Positive feedback loop (during training and at runtime)

Bonus: Interaction with Generative AI

- Problem: Generative AI is hit or miss
- A formal (intermediate) language allows verification
- Positive feedback loop (during training and at runtime)
- Examples: AlphaProof [AA24], Deepseek Prover [XGS$^+$24]

Outline

Curry-Howard correspondence

- Core idea: Encode mathematical statements as types in a programming language

Curry-Howard correspondence

- Core idea: Encode mathematical statements as types in a programming language
- With A, B propositions, A implies B: $A \implies B$

Curry-Howard correspondence

- Core idea: Encode mathematical statements as types in a programming language
- With A, B propositions, A implies B: $A \implies B$
- A function $f : \mathbb{R} \to \mathbb{Z}$ turns a real number into an integer

Curry-Howard correspondence

- Core idea: Encode mathematical statements as types in a programming language
- With A, B propositions, A implies B: $A \implies B$
- A function $f : \mathbb{R} \to \mathbb{Z}$ turns a real number into an integer
- A function $f : A \to B$ turns a proof of A into a proof of B.

Curry-Howard correspondence

- Core idea: Encode mathematical statements as types in a programming language
- With A, B propositions, A implies B: $A \implies B$
- A function $f : \mathbb{R} \to \mathbb{Z}$ turns a real number into an integer
- A function $f : A \to B$ turns a proof of A into a proof of B.
- Similarly: for $P : \mathbb{R} \to \mathrm{Prop}$, $\forall x : \mathbb{R}, P(x)$ corresponds to a function that provides a proof of $P(x)$ on an input x.

Curry-Howard correspondence

```
theorem example1 {A : Prop} : A → A := fun (a : A) => a

theorem example2 {P : ℕ → Prop} :
    (∀ (n : ℕ), P n) → P 37 := fun Pforall => Pforall 37
```

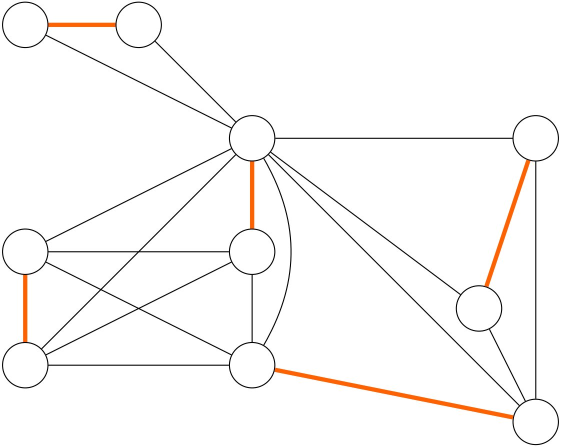
Tactics Demo

Tactics Demo

```lean
import Mathlib

theorem rearranging (x y z : ℝ) :
    (5*x + y) * z + (3*z)*y = 5*x*z + 4*y*z := by
  ring

theorem integer_inequalities (n m : ℤ)
    (h : n < 5 * m) (h2 : 5 + n > -m) : m > -1 := by
  omega

theorem linear_inequalities (a b : ℝ) (h : 5*a + b < 10) (h2
    : 9*a - 5*b > -20) :  b < 6 := by
  linarith
```

Outline

Perfect Matching



Perfect Matching

Definition (Perfect matching).

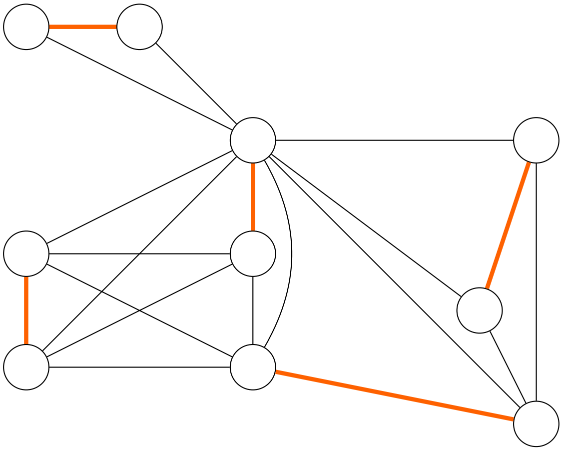
A perfect matching of G is a subgraph M, such that every vertex in G is connected in M to exactly one other vertex.

Tutte's theorem

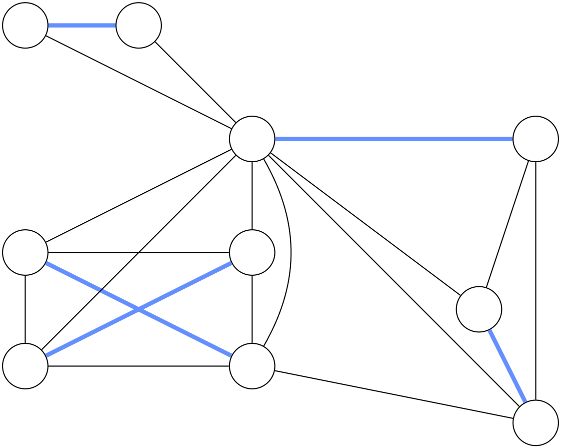
Theorem (Tutte, 1947).

A graph G has a perfect matching if and only if for any subset $U \subseteq V$ the graph $G - U$ has at most $|U|$ components of odd size.

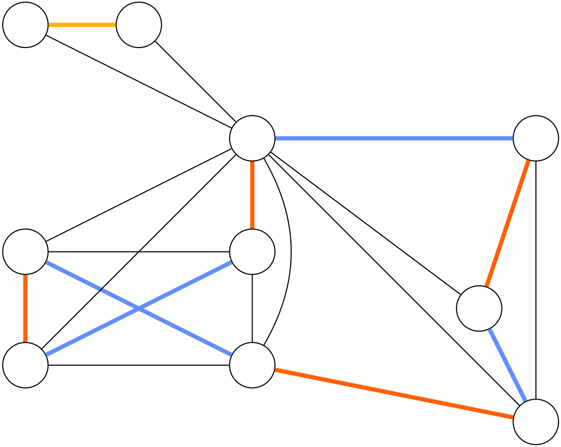
Alternating cycles



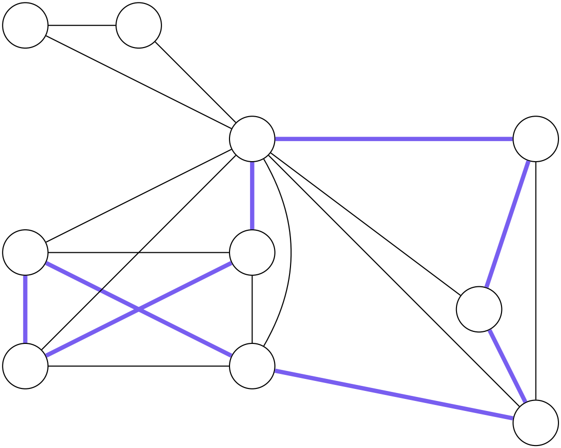
Alternating cycles



Alternating cycles



Alternating cycles



Alternating graph

Definition (Alternating).

A graph G is alternating with respect to some other graph G' if exactly every other edge in G is in G'.

Symmetric difference

Definition (Symmetric difference).

The symmetric difference of G and G' (denoted by $G \Delta G'$) is the graph consisting of edges that are in exactly one of G and G'.

Symmetric difference of perfect matchings is alternating

Lemma.

Let M, M' be perfect matchings of a graph G, then the symmetric difference $M \Delta M'$ is alternating with respect to M.

Symmetric difference of perfect matchings is alternating

Lemma.

Let M, M' be perfect matchings of a graph G, then the symmetric difference $M \Delta M'$ is alternating with respect to M.

Proof.

It suffices to show that for any vertex v in $M \Delta M'$ and two edges including v, exactly of these edges is in M. By definition of $M \Delta M'$, both of these edges must be in M or M'. Since M and M' are perfect matchings, each edge must be in exactly one of the two. So in particular, exactly one of these edges is in M. □

Outline

Introduction

Motivation

Concepts

Tutte’s theorem

Demo

Conclusion

Demo

Demo

```
lemma
  Subgraph.IsPerfectMatching.isAlternating_symmDiff_left
    {M' : Subgraph G'} (hM : M.IsPerfectMatching)
    (hM' : M'.IsPerfectMatching) :
    (M.spanningCoe △ M'.spanningCoe).IsAlternating
  M.spanningCoe := by
  sorry
```

Outline

Conclusion

- Teaching computers mathematics: verification, tools and collaboration

Conclusion

- Teaching computers mathematics: verification, tools and collaboration
- How to get started?
  - Lean, Rocq, Isabelle, Agda

Conclusion

- Teaching computers mathematics: verification, tools and collaboration
- How to get started?
  - Lean, Rocq, Isabelle, Agda
  - Natural number game: https://adam.math.hhu.de/

Conclusion

- Teaching computers mathematics: verification, tools and collaboration
- How to get started?
  - Lean, Rocq, Isabelle, Agda
  - Natural number game: https://adam.math.hhu.de/
  - Do/join/supervise a project

Conclusion

- Teaching computers mathematics: verification, tools and collaboration
- How to get started?
  - Lean, Rocq, Isabelle, Agda
  - Natural number game: https://adam.math.hhu.de/
  - Do/join/supervise a project
  - Utrecht Summer School

References

- AlphaProof and AlphaGeometry, *Ai achieves silver-medal standard solving international mathematical olympiad problems*, 2024.
- Kevin Buzzard, *Beyond the liquid tensor experiment*, 2022.
- Johan Commelin, *Liquid tensor experiment*, Nieuw Archief voor Wiskunde **22** (2021), no. 4, 231–234.
- Georges Gonthier et al., *Formal proof–the four-color theorem*, Notices of the AMS **55** (2008), no. 11, 1382–1393.
- Huajian Xin, Daya Guo, Zhihong Shao, Zhizhou Ren, Qihao Zhu, Bo Liu, Chong Ruan, Wenda Li, and Xiaodan Liang, *Deepseek-prover: Advancing theorem proving in llms through large-scale synthetic data*, 2024.

Utrecht University

Sharing science,
shaping tomorrow

Thanks to Yaël Dillies, Bhavik Mehta, Kyle Miller and other mathlib reviewers.

TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY

pim.otte.dev

Utrecht University

Sharing science,
shaping tomorrow

Thanks to Yaël Dillies, Bhavik Mehta, Kyle Miller and other mathlib reviewers.

TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY

TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY

pim.otte.dev