T.R.

GEBZE TECHNICAL UNIVERSITY

FACULTY OF ENGINEERING

DEPARTMENT OF COMPUTER ENGINEERING

LOGIC - THEOREM FORMALIZATION WITH LEAN PROOF ASSISTANT

FATIH DOĞAÇ

SUPERVISOR
ASSIST. PROF. TÜLAY AYYILDIZ AKOĞLU

GEBZE
2024

T.R.
GEBZE TECHNICAL UNIVERSITY
FACULTY OF ENGINEERING
COMPUTER ENGINEERING DEPARTMENT

LOGIC - THEOREM FORMALIZATION WITH LEAN PROOF ASSISTANT

FATIH DOĞAÇ

SUPERVISOR
ASSIST. PROF. TÜLAY AYYILDIZ AKOĞLU

2024
GEBZE

GEBZE TECHNICAL UNIVERSITY	GRADUATION PROJECT JURY APPROVAL FORM

This study has been accepted as an Undergraduate Graduation Project in the Department of Computer Engineering on 25/01/2024 by the following jury.

JURY

Member
(Supervisor) : Assist. Prof. Tülay Ayyıldız Akoğlu

Member : Prof. Dr. Didem Gözüpek

ABSTRACT

Proof assistant softwares are fairly new concept in computer science. LEAN is one of the most user friendly one. Like all others, it helps you manipulate the computer to check if the logic you follow make sense.

Keywords: keyword1, keyword2.

ÖZET

I used Lean Theorem Prover to prove Pick's Theorem. I did it by using Euler's polyhedron formula. I used deduction to prove that theorem and in the end it proves itself because of the reflexivity.

Anahtar Kelimeler: lean, Pick's theorem, deduction, theorem prover.

ACKNOWLEDGEMENT

I would like to thank my teacher, Tülay Ayyıldız, for the help she provided to me in this project throughout the semester, for her interest and relevance, who carried this project much further than I could.

Fatih Doğaç

LIST OF SYMBOLS AND ABBREVIATIONS

Symbol or Abbreviation		**Explanation**
R	:	Stands for real numbers.
rw	:	In lean, it rewrites the formula according to the given hypothesis.
ring	:	ring tactic in lean. It simplifies the formula
A	:	Area.
f	:	Number of faces of the graph.
e	:	Edges in graph.
e_i	:	Interior edges in graph.
e_b	:	Boundary edges in graph.
i	:	Stands for interior vertices.
b	:	Stands for boundary vertices.
v	:	Total vertices number in graph.

CONTENTS

1. INTRODUCTION

In the realm of mathematical exploration, theorem provers serve as powerful tools that aid in the formal verification of mathematical conjectures. These computational systems are designed to assist mathematicians and researchers in constructing and verifying proofs with a high degree of certainty. One such notable theorem prover is Lean, a modern and efficient tool that leverages formal logic to establish the correctness of mathematical statements.

The study of geometric properties and their mathematical formulation has yielded numerous theorems, each contributing to the foundational understanding of spatial relationships. Among these, Pick's theorem, conceived by the German mathematician Georg Alexander Pick in 1899, occupies a noteworthy position. This theorem elucidates a systematic approach to determining the area of lattice polygons, specifically those whose vertices are lattice points within a two-dimensional grid.

2. PROOF METHODS

A theorem is a mathematical statement that is true and can be (and has been) verified as true. A proof of a theorem is a written verification that shows that the theorem is definitely and unequivocally true. A proof should be understandable and convincing to anyone who has the requisite background and knowledge. In this chapter, we will look into some of the proof methods.

2.1. Induction proof

Induction proof has two steps:

- **Basis Step**
  The first step is to prove that the statement is true for the smallest natural number in the set you are interested in.

- **Induction Step**
  Assume true for k (an arbitrary number),

$$n = k$$

Then prove for the next natural number which is k+1,

$$n = k + 1$$

2.1.1. Induction Proof Example

Prove that;

$$4 + 9 + 14 + 19 + ... + (5n - 1) = \frac{n}{2}(3 + 5n)$$

$$n \in \mathbf{N}$$

Basis Step:
Smallest natural number for this case is 1, so solve for n=1

$$4 + 9 + 14 + 19 + ... + (5n - 1) = \frac{n}{2}(3 + 5n)$$

$$(5 * 1 - 1) = \frac{1}{2}(3 + 5 * 1)$$
$$4 = \frac{8}{2}$$
$$4 = 4$$

Because of the reflexivity, it suffices.
Induction Step:
Assume: n = k,

$$4 + 9 + 14 + 19 + ... + (5k - 1) = \frac{k}{2}(3 + 5k)$$

Show: n = k+1,

$$4 + 9 + 14 + 19 + ... + (5k - 1) + (5(k + 1) - 1) = \frac{k + 1}{2}(3 + 5(k + 1))$$

$$\frac{k}{2}(3 + 5k) + (5k + 4) = \frac{(k + 1)(5k + 8)}{2}$$
$$\frac{13k}{2} + \frac{5k^2}{2} + 4 = \frac{13k}{2} + \frac{5k^2}{2} + 4$$

Left-hand side and right-hand sides of the equation are same. And basis step is correct too. So this formula has proven by induction.

2.2. Direct proofs

Direct proof basically says: Assume p is true, prove q is true

$$p \to q$$

2.2.1. Direct Proof Example

If x is odd, then x^2 is odd. $x \in \mathbf{R}$

Any odd number can be written in the form:

$$x = 2n + 1$$

So, x^2 would be

$$x^2 = (2n + 1)^2$$

$$x^2 = 4n^2 + 4n + 1$$

So, when we change the shape of the equation:

$$x^2 = 2(\underbrace{2n^2 + 2n}_{\text{n}}) + 1$$

This has been proven because it fits the above situation

2.3. Indirect Proof

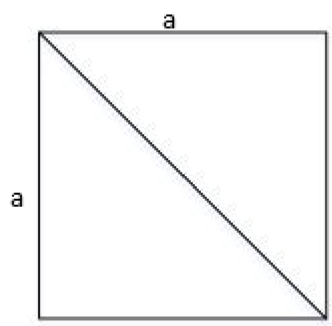
Indirect Proof has three steps:

We want to prove Y

- Assume ¬Y
- Find some contradiction
- Claim ¬¬Y which is Y

2.3.1. Indirect Proof Example

Prove if a square with side length a cut diagonally, there will be two triangles



with the area of $\frac{a^2}{2}$

For this example we will use the lemma: A square's area with side length a is a^2

- Assume that if a square with side length a is cut diagonally, it does not result in two triangles with an area of $\frac{a^2}{2}$
- We assume that when a square cut diagonally, it results in two triangles with an area different from $\frac{a^2}{2}$. Let's call this area **A**. So, $\mathbf{A} \neq \frac{a^2}{2}$
- According to lemma, the total area of the square (before cut) is a^2.
- Total area of the triangles will be 2**A**
- But $a^2 \neq 2\mathbf{A}$ (Contradiction)
- Therefore, initial assumption is false, and it must be the case that when a square with side length a is cut diagonally, it indeed results in two triangles, each with an area of $\frac{a^2}{2}$

2.4. Proof by Deduction

Proof by deduction is like connecting the dots logically. If we have some basic facts (premises) and we use clear rules to link them together, we can be sure that our final answer (conclusion) makes sense and is true too.

2.4.1. Proof by Deduction Example

Say;

$$a = b + 1 ①$$

$$b = c - 1 ②$$

$$a, b, c \in \mathbf{N}$$

Prove that $a = c$

If we write $b + 1$ wherever we see a a in the formula wanted to be proven, it will give us this:

$$b + 1 = c$$

So, if we move $+1$ to the right-hand side of the equation.

$$b = c - 1$$

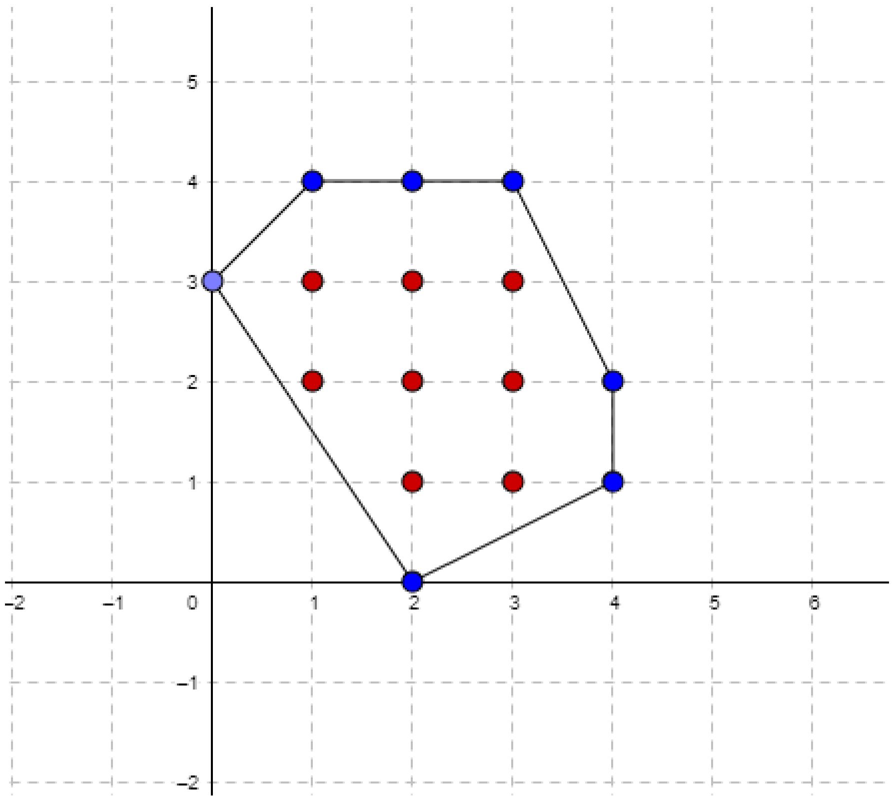
We will get ②. So its proven.

3. PICK'S THEOREM (1899)

Pick's Theorem provides a method to calculate the area of simple polygons whose vertices lie on lattice points—points with integer coordinates in the x-y plane. The word "simple" in "simple polygon" only means that the polygon has no holes.

Pick claims that area of a simple lattice polygon is

$$A = i + \frac{b}{2} - 1$$



In the above polygon, boundary vertices colored blue and interior vertices colored red. If we use the formula, area of that polygon would be:

$$A = 8 + \frac{7}{2} - 1 = 10.5$$

It seems true. But, is the formula really true? To check that, we are going to use Euler's characteristic formula: *Euler's Polyhedron Formula*

3.1. Euler's Polyhedron Formula (1758)

Euler's polyhedron theorem states for a polyhedron p, that

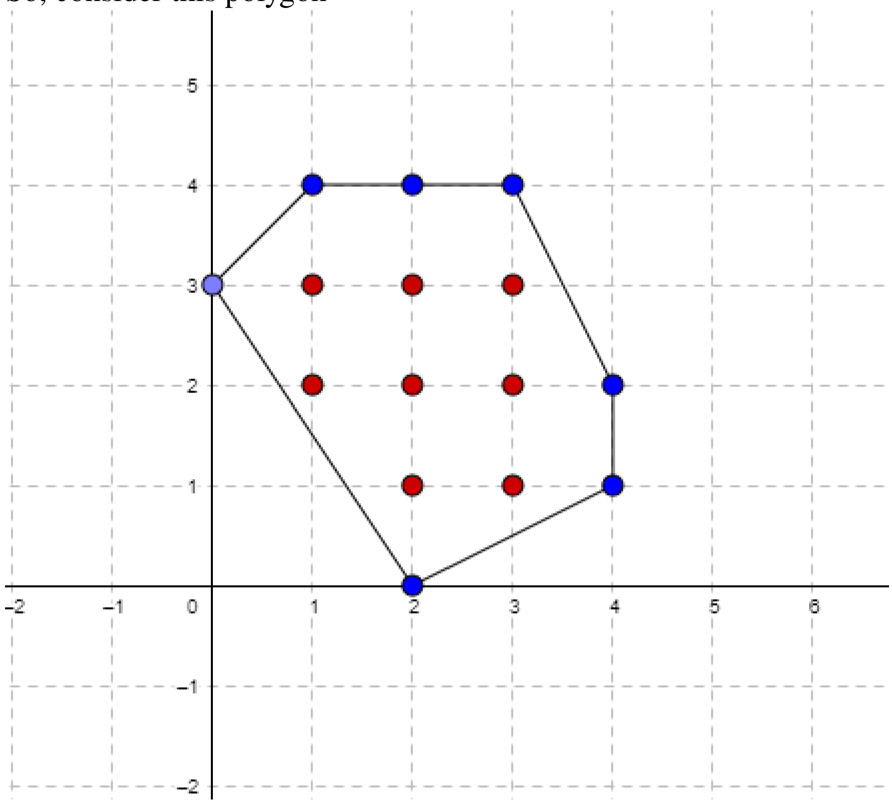
$$V - E + F = 2$$

where V , E, and F are, respectively, the number of vertices, edges, and faces of p. I considered it as a lemma and did my proof according to that.

3.2. Proof of Pick's Theorem

There is indeed another theorem I used which states that all lattice polygons could be divided into primitive triangles –primitive triangle means a triangle which has a area of $\frac{1}{2}$.

So, consider this polygon



If we divide this polygon into primitive triangles. The number of triangles will be $f - 1$. And each triangle has an area of $\frac{1}{2}$, the polygons area would be

$$A = \frac{(f-1)}{2}$$

The number of edges in a triangulated polygon is,

$$e = 3(f - 1)$$

But if we take it like that, we would be counted the interior edges twice. So the actual formula would be

$$3(f - 1) = 2e_{interior} + e_{boundary}$$

From now on, i am going to use some algebraic operations.
Adding $e_{boundary}$ and subtract $e_{boundary}$ So the equation won't be broken. And

$$e = e_{interior} + e_{boundary}$$

$$3(f - 1) = 2(e_{interior} + e_{boundary}) - e_{boundary}$$

$$3(f - 1) = 2e - e_{boundary}$$

$$f = 2(e - f) - e_{boundary} + 3$$

In a lattice polygon, every boundary edge follows a boundary vertice. So i am going to change $e_{boundary}$ to a more useful thing: b which is the number of the boundary vertices.

$$f = 2(e - f) - b + 3$$

Let's remember the Euler's formula

$$V - E + F = 2$$

So, my formula will become:

$$f = 2(v - 2) - b + 3$$

And v stands for the vertices. So, v equals the total number of the interior and the boundary vertices

$$v = i + b$$

Let's rewrite the formula according to that.

$$f = 2(i + b) - b + 3 - 4$$

$$f = 2i + b - 1$$

Remember,

$$A = \frac{(f-1)}{2}$$

So,

$$2A + 1 = 2i + b - 1$$
$$A = i + \frac{b}{2} - 1$$

That's it! We started from the Euler's planar graphs and polyhedral formula and in the conclusion, we reached the Pick's formula.

4. PROVING PICK'S THEOREM WITH LEAN

In the previous chapter, we proved the Pick's theorem by using Euler's polyhedral formula. So we are going to do it in Lean Theorem Prover.

But, let me warn you. Because of the computational difficulties, we might use the formulas at a different order.

4.1. Lean Code

Lines with starting "h" indicates hypotheses we accepted.

```
theorem Pick_s_Theorem (A f e e_b i b v : R  )
    (h_equal: e_b = b)
    (h_area: A = (f-1) / 2)
    (h_edge1 : (f-1)/2 = (2*(e-f) - e_b + 2)/2 )
    (euler : e-f = v - 2)
    (node_num : v = i + b)
 : A = i + (b/2) - 1 := by

rw [h_area , h_edge1, euler, h_equal, node_num]
ring
```

What happens here is, it is a proof by deduction proof. So we consider the $A = i + \frac{b}{2} - 1$ and then we will rewrite the formula according to our hypotheses. First rewriting h_area, Lean tells you where you are at the proving process at the last line.

```
1 goal
 A f e e_b i b v : ℝ
 h_equal : e_b = b
 h_area : A = (f - 1) / 2
 h_edge1 : (f - 1) / 2 = (2 * (e - f) - e_b + 2) / 2
 euler : e - f = v - 2
 node_num : v = i + b
 ⊢ (f - 1) / 2 = i + b / 2 - 1
```

Then let's go so on with rewriting.

```
A f e e_b i b v : ℝ
h_equal : e_b = b
h_area : A = (f - 1) / 2
h_edge1 : (f - 1) / 2 = (2 * (e - f) - e_b + 2) / 2
euler : e - f = v - 2
node_num : v = i + b
⊢ (2 * (e - f) - e_b + 2) / 2 = i + b / 2 - 1
```

```
A f e e_b i b v : ℝ
h_equal : e_b = b
h_area : A = (f - 1) / 2
h_edge1 : (f - 1) / 2 = (2 * (e - f) - e_b + 2) / 2
euler : e - f = v - 2
node_num : v = i + b
⊢ (2 * (v - 2) - e_b + 2) / 2 = i + b / 2 - 1
```

```
A f e e_b i b v : ℝ
h_equal : e_b = b
h_area : A = (f - 1) / 2
h_edge1 : (f - 1) / 2 = (2 * (e - f) - e_b + 2) / 2
euler : e - f = v - 2
node_num : v = i + b
⊢ (2 * (v - 2) - b + 2) / 2 = i + b / 2 - 1
```

```
A f e e_b i b v : ℝ
h_equal : e_b = b
h_area : A = (f - 1) / 2
h_edge1 : (f - 1) / 2 = (2 * (e - f) - e_b + 2) / 2
euler : e - f = v - 2
node_num : v = i + b
⊢ (2 * (i + b - 2) - b + 2) / 2 = i + b / 2 - 1
```

When we look at the last state of the proof, we see that

$$\frac{2(i+b-2)-b+2}{2} = i + \frac{b}{2} - 1$$

So what *ring* does is it does the mathematical simplification. And the equation will be transformed to this:

$$i + b - b + 2 - 4 = i + \frac{b}{2} - 1$$

$$i + \frac{b}{2} - 1 = i + \frac{b}{2} - 1$$

Because of the reflexivity. It is proven and Lean says it is okay too.

REFERENCES

Euler's Polyhedron Formula by Jesse Alama (2008)

Book of Proof by Richard Hammack (2018)