Computer Assisted Proofs and Their Effects on Pure Mathematics:

A case study of the four colour theorem

Juste Brikaite

Naud Megens

Olga Somova

Saim Kerem Ünal

Tyge Sørensen Felby

Supervisor: Martin Niss.

Roskilde University.

3rd Semester Project, Basic Studies in the Natural Sciences

Abstract

This project presents a discussion of what it means to prove something in mathematics. It outlines the history of proofs and their definitions, as a point of departure, for a case study of whether the proof, of the four colour theorem, by Appel and Haken, is valid and a part of mathematical knowledge. The doubt arises from the fact that the proof, due to being exhaustive with 1476 cases, is assisted by a computer for the critical part of reducing and discharging configurations and is, because of its enormity, uncheckable by human beings. It therefore forms a basis for a controversial subject; do computers deserve a role in pure mathematics? Some of the initial discussion fuelled by the proof is included. To elaborate on this discussion, the project contains the entirely handmade proof of the five colour theorem. These two proofs will form a comparison study of what is lost, on a philosophical level, by having a computer be the formalizer and surveyor. It is concluded that computer-aided proving does not challenge the "infallibility" of mathematical knowledge, but the lack of elegance that this kind of approach is prone to, constitutes a problem for the dissemination within mathematical knowledge.

Preface

This report is a third semester project from the Basic Studies in Natural Science at Roskilde University. It is the collective effort of five people spread out over the disciplines of natural sciences with common interest, though not experience, in the philosophy of science. The project is written so that it should be understandable by an undergraduate student without specific knowledge of mathematics or philosophy.

The proof of the four colour problem is the first computer generated proof. When the proof was published it was the centre of the discussion of computers in mathematics, and so to meet the requirements for the third semester: *Reflection on natural science and the dissemination of knowledge in the field of natural science,* the project presents a case study of the four colour problem as the core in a discussion on the role of computers in pure mathematics, and shows how a conjecture can evolve from being just a thought in the mind of an individual to being a controversial theorem, while on its path, helping to give birth to new areas within mathematics, thereby indirectly expanding mathematical knowledge.

With this project we aim at giving a valid conclusion on when a computer should be allowed a role in pure mathematics, and what obstacles and consequences this implementation entails for the dissemination and understanding of mathematical knowledge.

The project is organized as followed: Introduction, Problem Formulation, What is a Mathematical Proof, the Five and Four Colour Theorems, Discussion on Computers in Mathematics, Discussion, Conclusion and an Appendix containing an introduction to logic, Definitions and an introduction to graph theory. If you are unfamiliar with these concepts read the appendices before starting to read the section What is a Mathematical Proof, which will contain details on the different methods of proving with explanations and examples. The Five and Four Colour Theorems include the history of the theorem and its proof, leading up to the section Discussion on Computers in Mathematics, which is a discussion of the response from the mathematical community originally fuelled by the proof. If you are familiar with the four colour theorem and the methods used by Appel and Haken, and only interested in the philosophical complications surrounding it, simply go to this section and read on from there.

By including the history and the original discussion, we will be able to conclude on what has changed, with respect to computer use within pure mathematics, since the first proof was posted, this will then be discussed along with the acceptance of the four colour theorem within the mathematical community.

We would like to thank our supervisor Martin Niss for his input and patience during our discussions. We would also like to extend our gratitude towards Peter Frederiksen our opponent group's supervisor for his help on structuring the project towards readers outside the mathematical community.

Contents

Introduction

The science of mathematics is an ancient one. From the beginning of civilization mankind had a need for mathematics in everyday life: for trading goods, agriculture, counting seasons, taxation and so on. This kind of mathematics was mostly based on empirical experiences and there was no need for proof, the concept was simply unknown. Euclid (325 B.C.E.–265 B.C.E.) was the first scholar to bring the concept of proof to mathematics: by use of deductive logic and self-evident truths, axioms, Euclid was able to demonstrate the truth of a conclusion as an indisputable consequence of a hypothesis, yielding a theorem. Thereby introducing not just the notion of a proof but a rigorous perception of truth, a priori. This paradigm shift within mathematics; the concept of mathematical knowledge shifting from the empirical- to deductive derived truths, is one we still practice today. With the proof of the four colour problem as a basis we try to give an overview of the problems revolving Appel and Hakens solution in relation to this notion of mathematical knowledge.

Some conjectures are harder to prove than others, some of the ones that are extremely hard to prove become the life of interested mathematicians, whom go through tremendous amount of trouble and sometimes end up in no better place than before. At other times new connections are made between the conjecture and a theory or new insight discovered about the conjecture.

The four colour conjecture is one of those tantalizing problems that had been floating around in the mathematical community for 125 odd years. The reason for the continuing interest in the mathematical community probably comes from the simplicity of the conjecture; that four colours suffice to colour any planar map, so that no adjacent countries are of the same colour. The originator was a graduate of the University College London, Francis Guthrie. He showed that three colours are not enough, and so in the beginning of the 1850's the four colour conjecture was born. The first claimed proof came from Alfred Bray Kempe in 1879, but it was refuted a decade after by Heawood, who presented a counter example. Kempe's efforts were not completely in vain; he was able to show that a map has to contain a country with fewer than six neighbouring countries, and the work on the four colour conjecture carried on from there [Mackenzie, 1999].

When the four colour conjecture was finally proven, the year was 1976. Over a century had passed since the conjecture was formulated, and Kenneth Apple and Wolfgang Haken started their collaboration to solve it. They had been trying to elaborate on Kempe's successful efforts, (to put restrictions on the cases needed to be considered), with an idea by Heinrich Heesch; constructing an unavoidable set of configurations, making the cases finite. Through this, a proof by exhaustion would be possible.

There was only one problem with this procedure. The unavoidable set was likely to be big, turning out to contain 1476 configurations, a set so big that it would take a human being more than a lifetime to go through it. The procedure therefore became dependent on a computer for the reducibility check (removing a country while keeping the colouring intact). A theorem dependent this much on computer analysis was until then unheard of [MacKenzie, 1999]. To make matters worse, because of the extension of the computer analysis, the proof could not be checked by humans. The four colour theorem became a controversial entity which, for some, the very concept of proof depended on. It was felt that the proof imposed the empirical evidence of natural science on the world of pure mathematics, making mathematical knowledge fallible. Mackenzie (1999) concludes that the four colour theorem holds some philosophical problems as to what constitutes mathematical knowledge and makes the concept of proof negotiable. We present a discussion of this negotiability with the different views of some mathematicians and philosophers, demonstrating the discussions invoked by computer assisted theorem proving. The contribution of this project is to discuss the pros and cons of computer assisted theorem proving and provide a conclusion on its place in pure mathematics.

Problem formulation

Does the proof of the four colour theorem, being computer-assisted proof, violate the mathematical norms for what constitutes a proof?

What effects does it, if accepted, have on the perception of mathematical knowledge.

What is a Mathematical Proof?

The concept of proof plays a central role in mathematics, but how do we define a proof? What rules do we use when constructing proofs? These questions can be perceived in different ways; for a practising mathematician proof is the 'scientific' method, which provides certainty to his or her work. Philosopher examines the concept of proof and nature of the knowledge within it.

The Euclidian way of proof, following deductive logic is the way mathematicians define proof. We start with axioms [Appendix 2], which are basic, self-evident assumptions; one does not need to prove an axiom. Definitions explain the meaning of a concept or a piece of terminology, the relationships and properties of these concepts are defined by theorems. In order for a theorem to be valid it has to follow the inference rule or *modus ponens* (derivation of conclusions from given information or premises by any acceptable form of reasoning) [Appendix 1]. Using this deductive logic we construct proofs. Therefore we define proofs as deductively valid arguments demonstrating the truth of mathematical or logical statements, based on axioms and theorems derived from those axioms, hence providing a *priori* knowledge [Appendix 2]. However, it is not always easy to construct proofs by following these rules, sometimes even impossible, and logic here is as central as proofs are in mathematics. Mathematicians therefore have to find different ways to go about it.

Three general characteristics of proofs are expected in mathematics. A proof needs to be surveyable, formalizable and convincing. A surveyable proof is one that can be read through and checked by a mathematician by hand. After surveying the proof a mathematician should be able to come to its conclusion. A formalizable proof must be written in a way that it follows from axioms and the rules of logic and the conclusion can be deducted from these. Convincibility argument can be a bit vague, different from the previous two descriptions. In the mathematical sense, it needs to be convincing when read and we can take the actual dictionary definition about this. A proof needs to be convincing to rational agents, meaning that any mathematician with sufficient understanding of the field, which the proof is a part of, will be convinced of its correctness. In a more philosophical sense, a convincing proof need to have some characteristics, some of which are formalizability and surveyability.

Thousands of years of growing mathematical knowledge brought us many different kinds of proofs and many ways to use logic. Even though we are talking about traditional proofs there is really no single way or universal method for constructing a proof. It depends on degree of difficulty, properties of elements and other conditions. It can become very tedious and inefficient if one have to use all the axioms and definitions. Mathematicians can use short cuts, already proven theorems, omit "obvious" proofs, use multiple inference rules without explicitly explaining every step etc. Different techniques and combination of them allow mathematicians to use smallest possible set of axioms and logic rules, thereby minimizing possibility of error and making it easier to find the sources of the ideas [Appendix 2 – Occam's Razor], [Krantz, 2007]. For the proof to be valid, however, assumptions have to be clear and there should be no doubt of the truth of secondary arguments (other theorems). In this section we will discuss different kind of techniques used in mathematical proofs.

Proving Techniques Used by mathematicians:

Direct Proof:

Direct proof in mathematics is a most straightforward, it relays on combination of facts in terms of already existing lemmas [Appendix 2] and theorems and do not make further assumptions. Logic in this type of proof is almost always first-order logic using quantifiers *for all* ($\forall$) and *there exists* ($\exists$) [Appendix 1].

To illustrate this kind of proof in a simple way we choose the set of integers. Before starting to prove we assume that the following properties of integers are known:

- The sum (or difference) of any two integers is an integer.
- The product of two integers is an integer.
- The negative of an integer is an integer.

Theorem: The sum of two even integers is an even integer.

Proof: Let's take integers x and y, since they are even we can rewrite them as: $x=2a$ and $y=2b$. $x+y = 2a+2b = 2(a+b)$, and from here it's clear that the sum of x and y has a factor 2 and therefore it is even.

Trivial and vacuous proof:

Consider $P \Rightarrow Q$ [Appendix 1], for the trivial proof we have to show that Q is true and by definition of implication [Appendix 1] P is also true. We are showing that the conclusion is true. In the case of vacuous proof we have to show that P is always false and therefore the implication is true.

Proof by contrapositive:

This kind of proof establishes validity of the statement by showing the truth of the negated statement and since they are logically equivalent the statement therefore is also true.

If $P \Rightarrow Q$ is true, then $\neg P \Rightarrow \neg Q$ is true as well.

Proof by contradiction:

Reductio ad absurdum [Appendix 1]

In this kind of proof we assume that statement we want to prove is false and from there we show that this assumption leads to contradiction, in other words it is just nonsense. Since the statement can only be true or false and we proved that it couldn't be false therefore the statement is true. One of the examples is Euclid's proof of prime numbers. He assumes that there is finite number of primes and demonstrates that this statement is false, so there must be infinite amount of prime numbers.

Proof by exhaustion:

This kind of proof can be called brute force method simply because it exhausts all the possibilities. Firstly, the statement is split to a finite number of cases and then each case is checked/proved separately. This kind of proof has 3 stages:

1. Splitting the statement up into finite number of cases – e.g. unavoidable set [Appendix 2].

2. Proving that each instance of the statement has a condition of at least one of the chosen finite cases.

3. Proving the validity of each case in the unavoidable set.

This kind of proof at heart is traditional, however maybe lacking the simplicity and beauty of deductive proofs. It can also be controversial because of use of unavoidable set – the finite set [Appendix 2], which really has no upper limit for how many cases there should be. In the case of four colour problem computer has to be used, because of 1476 separate cases exists in the unavoidable set, consequently it is just impossible to compute so much data without help of a computer.

Proof by Mathematical Induction:

This kind of proof is usually used to prove some property of natural numbers. Let's say that we want to prove some property P is possessed by all the natural numbers: $\forall n \in NP(n)$[Appendix 1]. The idea behind this kind of proof is to show that the first natural number P(0) (base case) possesses this property and then by repeatedly adding 1 you can actually list all the natural numbers. So the induction step is to prove $\forall n \in N(P(n) \Rightarrow P(n + 1)$ [Appendix 1] valid and has the same property. From here by induction logic we have a valid proof for all the natural numbers [Book 1].

Proof from philosophical point of view:

The Euclidian way of doing mathematical proofs has been around for 2300 years and as society progressed new challenges in mathematical thinking emerged. Traditional school of thought or Platonic mathematics employs the following amongst working principles:

1. The belief that there exists ideal mathematical entities, which are abstract.

2. The belief in certain modes of deduction.

3. The belief that statements can be proven true or false.

4. Mathematics itself has no spatiotemporal or causal properties, is eternal and unchanging, fundamentally exists apart from the human beings and physical world altogether [Davis, 1972].

Nowadays proofs can consist of computer calculations (e.g. proof by exhaustion), physical models, computer algebra (MatLab or Maple), simulations or combination of various techniques. Proofs involving these kinds of techniques are called non-traditional. As a result, Platonic mathematics has been questioned and different schools of philosophy in mathematics emerged such as formalism, intuitionism, logicism and etc. [Appendix 2], consequently altering the concept of proof in philosophy. Even though some authorities believe that Euclidian way of constructing proofs is the hallmark of mathematics [Davis, 1972], we cannot deny that in the "new-age" mathematical thinking there is a place for a *posteriori* knowledge [Appendix 2], experimental mathematics and empiricism. The questions "What is a proof?" and "What are the rules for constructing proof?" requires a rather philosophical approach and it can all become a question of epistemic status [Appendix 2] of these new mathematical concepts. Many philosophers have put forward these questions, for that reason conflicting ideas surrounds this issue, which we will discuss in a later chapters.

Most of mathematical methods mentioned before, exercises deductive logic and are in sync with Platonic ways of practising mathematics, however computer aided proofs creates discussion in philosophy whether they submit to the traditional/deductive proof category, and whether they have *ceteris paribus reliability* [appendix 2], even though they are useful in mathematical practice [Peressini, 2003]. This computational aid by computer in some of the methods opened a new niche in philosophy of mathematics, which we wish to explore further in this project by the case study of the four colour theorem.

The Five and Four Colour Theorems

The four colour conjecture was initiated by Francis Guthrie in 1850s. It was his brother, Frederick Guthrie, who passed the problem on to the mathematical community in 1852. It was submitted to Augustus de Morgan and the problem started its long journey that would last around 125 years before the conjecture was finally solved [Fritsch & Fritsch, 1998].

The first problem that arises for anyone who sets out to prove the four colour conjecture is that it refers to all maps [Devlin, 1988]. This includes all maps we may create in the future of places we may not even have discovered yet in addition to all maps that we know. A proof would have to cover all possible cases that can be experienced. The four colour problem is concerned with the colouring of the geographical regions of a map in such a way that no two regions which share a common boundary are coloured the same [Devlin, 1988]. It is easy to realize from the above description that the actual sizes and shapes of the regions is not an issue, the only important thing is their relative positions to each other [Devlin, 1988]. More precisely this can be expressed as the topological structure of the map [Devlin, 1988].

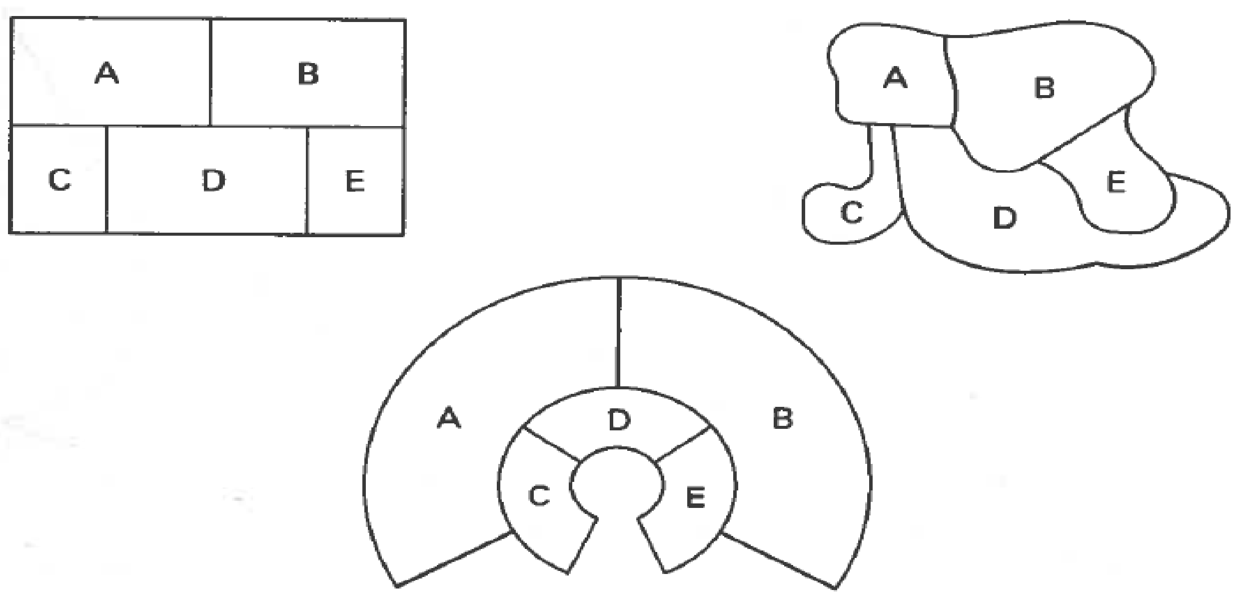


Figure 1: Topological Equivalence. Each of these shapes is equivalent as far as the four colour problem is concerned [Devlin, 1988].

The first announced proof of four colour theorem goes back to 1879. The attempt to prove the four colour problem was made by Alfred Kempe and for eleven years the four colour theorem was considered proven. In 1880 Heawood found an error in Kempe's proof. Heawood couldn't come up with an example of a map that will need more than four colours but showed flaws in Kempe’s proof. In mathematics if somebody claims that something is true like “four colours suffice”, to prove that the statement is wrong, one needs to come up with a counterexample e.g. a map that needs at least five colours. What Heawood showed was that Kempe’s proof was wrong without refuting the conjecture i.e. the result could be still true.

Kempe suggested a method to construct a dual of any given map by marking the capital city of each country in a map and then if two countries have a common border, join the capitals by a road across the common border that does not go through any other country [MacKenzie, 1999]. After this step if one deletes the original borders, what is left is a *graph* [MacKenzie, 1999]. The capital cities are the vertices of the graph, the roads joining them are its edges and the number of edges that a vertex has is its degree. Together they form the graph corresponding to the original map. If one can colour the capitals in a way that no 2 of them that are connected by a line share the same colour, so can the original map be coloured in the same manner [MacKenzie, 1999]. Kempe used a method that would later be called Kempe chains and reduced maps to graphs with help from Cauchy’s work on graph theory [MacKenzie, 1999]. Despite the failure of four colour problem proof, Kempe’s work lead Heawood to work on easier problem and prove that every planar map can be coloured with at most five colours.

After the refute, one of the strategies to produce a new proof was to reformulate Kempe’s strategy [MacKenzie, 1999]. It was this approach that Appel and Haken followed which solved the 125 year old problem.

There are a few notions that we need, to be able to understand their approach. The proofs of the following statements in this chapter can be found in [Fritsch & Fritsch, 1998].

An admissible colouring of a map means that whenever we have two bordering countries they will have different colours. By map, it should be understood a partition of an infinite plane in which there exists finitely many countries that are divided from one another by borders and of which, only one country is unbounded. A set of points in the plane is unbounded if no rectangle completely encompasses it [Fritsch & Fritsch, 1998]. Vice versa, a set is bounded if it is entirely contained within some rectangle. A map on a globe can be successfully transformed into a planar map by use of stereographic projection. One definition of the four colour theorem can be given as:

For every map there exists an admissible 4-colouring.

The basic approach to the difficult proof can be explained quite simply. It is the investigation of minimal counterexamples. The following idea form a basis for the approach: If there exists maps that cannot be coloured with four colours, then there must be one such map having the fewest number f of countries [Fritsch & Fritsch, 1998]. It follows from the definition that any map with fewer than f countries in it can be 4-coloured. Any map with less than 5 countries can be easily 4-coloured which implies f > 4. The entire proof consists in showing that there cannot exist such a minimal counterexample [Fritsch & Fritsch, 1998].

A search for this minimal counterexample put restrictions on it and shaped it over the years. A few of these can be listed as follows [Fritsch & Fritsch, 1998]:

- It will be a regular map (Connected, two distinct countries have at most one common border line, each vertex has at least degree 3.)
- If a country has more than three neighbors, then it has two that have no common borders.
- There is no country that has fewer than five distinct neighbors (each vertex has at least degree 5).
- Has at least six countries (this number grew over time up to 96 before the announcement of the proof).

NB. Appel and Haken did not use the latter restriction for their proof, since their approach was different.

The transformation from a map to a graph, as mentioned before, is known as a dual. There is one important definition concerning graphs: saturation. A plane graph is said to be saturated if it is not a proper sub graph (Appendix 3) of another plane graph having the same vertex set. This is also known as a maximally plane or a triangulated graph [Fritsch & Fritsch, 1998]. In practice, a plane graph is maximal if no new edges can be added to the graph without enlarging the vertex set.

As the solution of the four colour problem starts with the five colour theorem, let us now mention the basic ideas of how the five colour theorem is proved and which concepts are used for its proof.

There are several material resources based on which we completed five colour theorem proof for the report. We do not include references in "five colour theorem proof" as we are going through the proof itself, not analysis of it; and the proof is fully based on used materials. For the five colour theorem proof we are looking at some graph theory concepts. It is done in order to understand how from a planar map we can draw corresponding planar graph. The materials for a "graph theory" can be found in [Appendix 3].

Next, we look at Euler's formula proof which states that number of vertices minus number of edges plus number of faces equals to two (v-e+f=2), and at one of Euler's formula corollary. The corollary states that $e \leq 3v-6$; by proving this inequality we are able to prove that every planar graph contains a vertex of degree five at most. The five vertex theorem is very important for the five colour theorem prove. The theorems mentioned above are explained and proved in the report by using materials from course notes written by M. Sofia Massa [internet resource 1] and book [Fleck, 2012] pages 210-215.

Finally, after the five vertex theorem is proved we are able to proceed to the five colour theorem proof itself, which we prove by induction on the number of vertices. The proof materials for the five colour theorem are obtained from [Keinen, 1974] and [internet resource 2].

The five colour theorem states that any planar map can be coloured with at most five colours. What is a planar graph and how we can draw it from the given map? We can determine a planar graph as a collection of *vertices* (points) and *edges* (lines). Bellow in Figure 2 is shown an example of a planar graph.

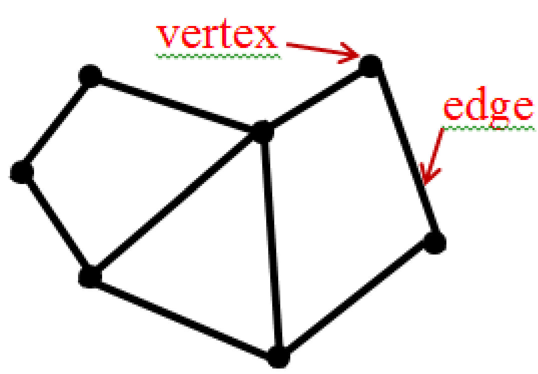


Figure 2 A planar graph

Any planar map can be represented as a planar graph and by proving that planar graph can be at most five colourable we will prove that any planar map can be five colourable as well. The example of planar map and corresponding planar graph is shown in Figure 3 below.

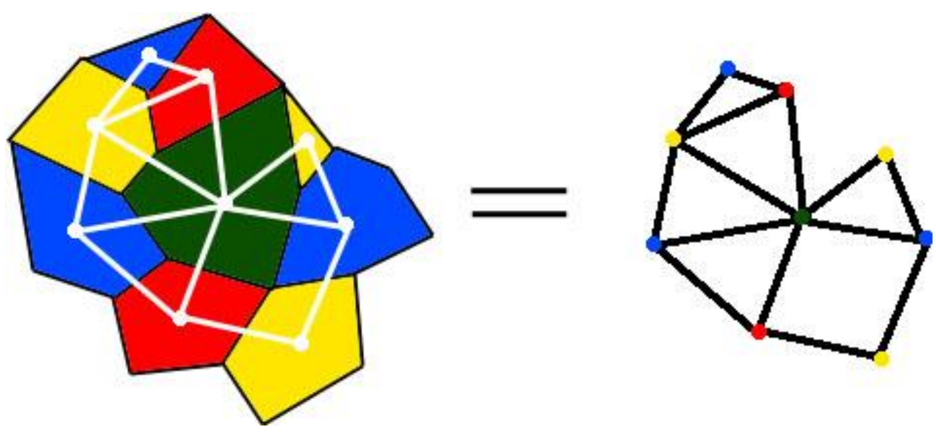


Figure 3: From planar map to a planar graph.

Before starting with a five colour theorem proof we have to go through number of other theorems on which the proof is based.

Euler's formula

Given a connected planar graph with e – edges, v – vertices and f – faces the Euler's formula states that $\boldsymbol{v - e + f = 2}$. We should mention that when graph is drawn on a plane with no crossing edges it divides the plane to different regions – *faces*. The unbounded area of a graph is also counted as a *face*.

The *degree* of a *face* is the minimum length of a boundary walk of a given *face*.

For the first step in a proof we are looking at specific type of planar graphs which are called free trees. The free tree is a connected graph with no cycles. As free tree graph does not have any cycles it consists of only one face. In case of free tree graph Euler's formula reduces to

$$\boldsymbol{v - e = 1} \; (v - e + 1 = 2 \Rightarrow v - e = 1).$$

Free tree Euler's formula proof

Let us say that we are given a free tree graph with n vertices. We will proof the formula by induction on n.

1. If graph contains no edges and only one vertex, the formula will be $1 - 0 = 1$ which is true.
2. We suppose that formula works for all free tree graphs with vertices $v \leq n$
3. Let G be a free tree graph with vertices number $n + 1$.

In order to prove the Euler's formula for free tree graphs we need to show that G consists of n edges ($v - e = 1 \Rightarrow n + 1 - e = 1 \Rightarrow e = n$)

In any free tree graph we can find a vertex with degree one. As the graph does not have cycles then by starting from any vertex and taking any direction we will come to the *"end point"*. The *"end point"* vertex g will have degree 1. The next step is to remove the vertex g from our graph G and the edge which goes into it. By removing them we get a new free tree G' which consists of n vertices ($n + 1 - 1$). *By* our inductive hypothesis G' has $n-1$ edges ($v - e = 1 \Rightarrow e = n - 1$). As G has one more edge then G' we get that G has n edges ($n - 1 + 1$). This is what we needed to prove and therefore the formula is true.

Euler's formula proof

After proving Euler's formula for free trees we can prove it for any connected planar graph.

We will prove by induction on the number of edges in the planar graph.

1. If the number of edges $e = 0$ we have a graph consisting of a single vertex with one face surrounded it. Then we get $1 - 0 + 1 = 2$ which is true.
2. Let suppose that formula is true for all graphs with edges $e \leq n$
3. Let K be a graph with $n + 1$ edges.

We get two cases – the first one when K does not contain a cycle which means it is a free tree graph and we have already proved that Euler's formula is true for free tree graphs. The second case contains at least one cycle. Let choose any edge on a cycle and call it k. By removing edge k from the cycle we get a new graph K'. The cycle from which we have removed k was separating graph K to two different *faces*. After removing edge k the faces merge. Which means that K' has one edge and one face less than K. As K has $n + 1$ edges it gives to us n edges for K'. As K' got n edges it means that formula works for it by our induction hypothesis.

For K' we have (corresponding to K):

$v' = v$ (the same number of vertices like in K)

$e' = e-1$ (one less edge than in K)

$f' = f-1$ (one less face than in K)

By inserting values to the Euler's formula $v - e + f = 2$ we get that:

$v - (e - 1) + (f - 1) = 2 \Rightarrow v - e + f = 2,$ what was needed to be proved.

Euler's formula corollary

For the five colour theorem proof we will need to prove that every planar graph contains a vertex of degree 5 or less. To be able to prove it we need to look at a derivation from Euler's formula.

Let say we are given a connected planar graph J with v – vertices, e – edges and f – faces, where $v \geq 3$. We want to prove that for a given graph J the inequality $e \leq 3v - 6$ is true.

As an edge forms two faces (one from each side of it) the sum of the degrees of the faces equals to twice the number of edges. We are given the graph J which is connected planar graph and which means that each face must have degree greater or equals to 3; from where follows that $3f \leq 2e$.

Euler's formula says that $v - e + f = 2$, so $f = e - v + 2 \Rightarrow 3f = 3e - 3v + 6$

Now let us combine $3f \leq 2e$ and $3f = 3e - 3v + 6$, we get that:

$3e - 3v + 6 \leq 2e \Rightarrow e \leq 3v - 6$, which is what we needed to prove.

Five vertex proof

We will prove that every planar graph contains a vertex of degree 5 at most by contradiction. The first axiom we are using to prove it says that the sum of the degrees of all vertices of a graph equals to twice number of all edges.

For our proof we assume that G is a planar graph and all vertices of G have degree greater or equal to 6. As each vertex has a degree of 6 or more we get that:

$$6v \leq 2e \Rightarrow 3v \leq e \quad (A)$$

Where v *is the* number of vertices in a graph G and e *is the* number of edges.

From the corollary of Euler's Formula we have that:

$$e \leq 3v - 6 \quad (B)$$

So, from statements *(A)* and *(B)* we have that:

$$3v \leq e \leq 3v - 6$$

Which is impossible as $3v > 3v - 6$. So, we came to contradiction to our assumption and therefore if the graph G is planar it has at least one vertex of degree 5 or less.

The five colour theorem proof

Now we are able to return to the five colour theorem proof.

Let n be the order of the planar graph G, then it is obvious that the theorem is true for $1 \leq n \leq 5$.

We are going to prove the five colour theorem by induction on n.

Let assume that every planar graph of order n - 1 is five colourable, where $n \geq 6$

Every planar graph contains a vertex of degree 5 or less (see *"five vertex proof").* Therefore our graph G contains a vertex v such that $v \leq 5$.

By removing vertex v from the graph G we get a planar graph of order n - 1 which from our induction statement is five colourable. Let the graph G-v be coloured with five colours – 1, 2, 3, 4 and 5.

If one of these colours is not used to colour the neighbors of v, then we are using this colour to colour v and are getting a five colouring result for the graph G (see Figure 4)

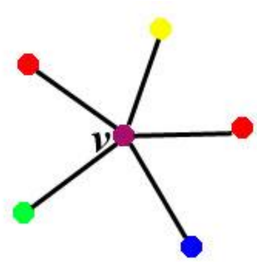


Figure 4: Five coloring when two neighbors can be assigned same color.

So, let us assume that all of five colours are used to colour neighbors of vertex v (see Figure 5).

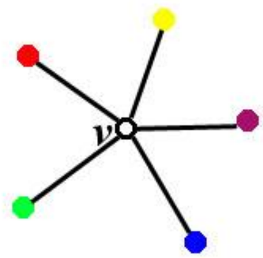


Figure 5: All 5 neighbours have different colours.

Let there be a planar embedding of a graph G and let say that v_1, v_2, v_3, v_4, and v_5 are neighbors of vertex v cyclically arranged around it (see Figure 5) where i is an assigned colour for v_i and $1 \leq i \leq 5$.

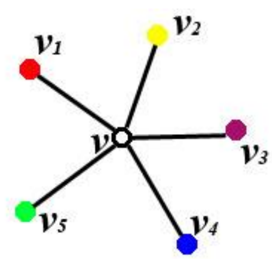


Figure 6: Planar embedding of v with five distinct coloured neighbors, where i is an assigned colour.

Let H be a sub graph of G - v induced by set of vertices coloured with colours 1 or 3. If vertices v_1 and v_3 belong to different components of H then we can interchange the colours of vertices in component including v_1. Afterwards we can assign colour 1 to v which will produce five colouring of G (see Figure 7).

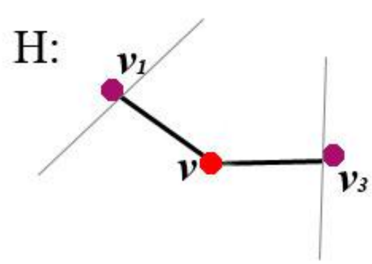


Figure 7: New colour assignment on the neighborhood of v after the operation.

If vertices v_1 and v_3 belong to the same component of H there exist a v_1 - v_3 path (P) in G - v. The path P and the path v_1, v, v_3 create a cycle in G (see Figure 8).

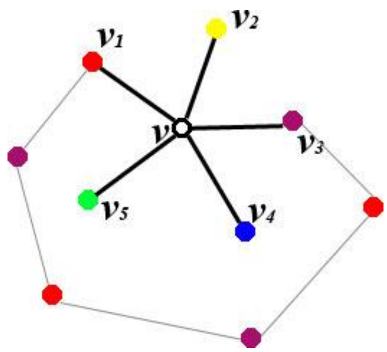


Figure 8: Two neighbors of v (v_4 & v_5) that are in the same component.

It will cause v_2 or both v_4 and v_5 to be enclosed which means there does not exist v_2 - v_4 nor a v_2 - v_5 path in G - v. Let us say that F is a sub graph of G - v induced by the set of vertices coloured by colour 2 or 4 (see Figure 9).

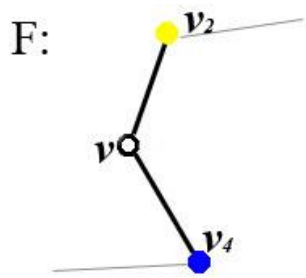


Figure 9: Two neighbors of v that are not in the same component.

As v_2 and v_4 belong to different components of sub graph F we can interchange colours of the vertices in component including v_2 and by assigning colour 2 to v we are getting five colouring of G (see Figure 10).

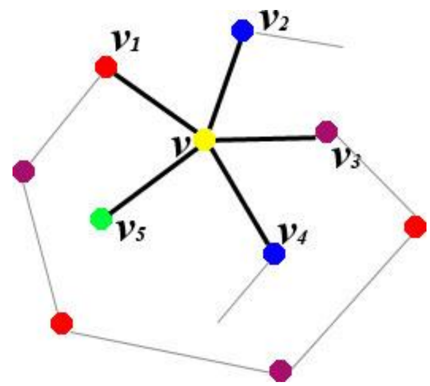


Figure 10: Five colouring of the original graph.

So, by looking at all possible variations it can be said that the five colours suffice.

There are a few more things worth to mention before we go further with the report. With the five colour theorem proof we were going through a number of other theorems and their proofs which was a great example of how mathematical proofs work. The types of proofs used here are proof by induction and proof by contradiction.

Let us now go back to the four colour theorem by continuing with even more definitions.

Normal Maps, An Unavoidable Set of Configurations and Reducibility

A normal map is defined as one in which no country is entirely surrounded by another, and in which no more than three countries meet at any one point [MacKenzie, 1999]. The idea is to simplify the problem by showing that any map can be modified into a normal map which requires as many colours [MacKenzie, 1999]. Recall that a minimal five chromatic map is the map containing the lowest number of countries for which there exist an admissible five colouring. Using normal maps and minimal counter example together, the idea is that if you can find a reduction operation which will reduce the size of your map by even one country, without altering the requirement for five colours, you will at once have a contradiction since the reduced map can be colourable with 4 colours while still being not colourable by less than 5 [Devlin, 1988].

Kempe had shown that any normal map must contain a country with fewer than six neighbors [MacKenzie, 1999]. So the following set of configurations is unavoidable, a country having: two, three, four or five neighbors [MacKenzie, 1999]. One of these configurations must appear in any normal map. A country having only one neighbor (when one country is covered completely by another) is already considered in the case of normal maps. Appel and Haken's work is to find an unavoidable set of configurations all of which are reducible, therefore completing the proof. The problem with this approach is the immense number of unavoidable configurations that needs to be checked. In 1948 Heinrich Heesch estimated the set of reducible configurations might have about 10.000 members [MacKenzie, 1999]. He would later develop a technique called D – reduction, which is highly algorithmic that it was possible to be implemented on a computer [Saaty & Kainen 1977].

One important concept that needs to be examined is the certain graphs that crop up primarily as sub graphs of normal graphs. These are called configurations and their exact definition requires some more definitions [Fritsch & Fritsch, 1998].

A combinatorial graph is a pair G = (E, L) consisting of finite sets of E (vertices) and L (edges) which is a two element subset of E. Let G = (E, L) be a combinatorial graph [Fritsch & Fritsch, 1998]. Then:

- Two vertices of G are said to be neighboring vertices if they are distinct from each other and are end points of the same edge in L.
- A sequence $(x_1, x_2, \dots, x_r)$ of vertices is called a chain if they are pairwise distinct and each successive pair consists of neighboring vertices. The length of the chain is r and the edges that join two successive vertices are called the links of the chain.
- A chain K in G with at least 3 vertices is said to be closed if the initial and the final vertices of the chain are neighbors. In this case, the edge that joins the two end vertices is also considered to be one of the links of the chain.
- A set R of vertices is called a ring if its elements can be arranged so that they form a simple closed chain. The number of elements in R is also the size of R.

A graph C is said to be a configuration if [Fritsch & Fritsch, 1998]:

- It is regular

- The outer vertices form a ring whose size >= 4
- Inner vertices exist
- The bounded faces have triangular borders
- Every triangle is the border of a face

The interior domain of C is the sub graph spanned by the vertices inside the ring and all edges that join them. In the graph C, we distinguish between three types of edges [Fritsch & Fritsch, 1998]:

- Inner edges, which join two inner vertices
- Outer edges, which join two outer vertices,
- Legs, which join one inner vertex to one outer vertex

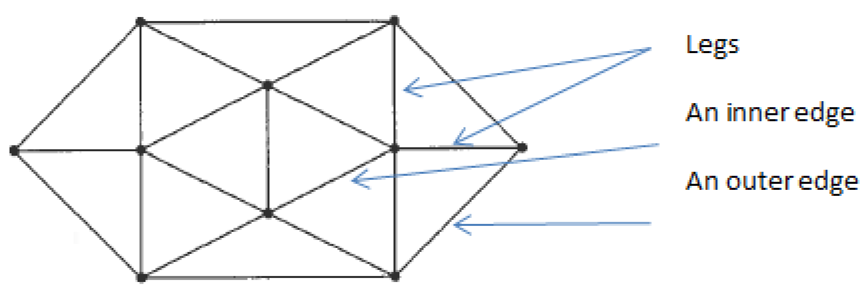


Figure 11: Birkhoff Diamond [Fritsch & Fritsch, 1998].

Inner vertices and inner edges form the core of the configuration [Fritsch & Fritsch, 1998].

A configuration is called a star if it contains only one inner vertex, called its hub. In particular it is said to be a k-star if it is a star with precisely k outer vertices and therefore k + 1 (k >= 4) vertices [Fritsch & Fritsch, 1998]. With this definition, we can add another requirement on the minimal counter example list:

A minimal triangulation cannot contain a 4-star but contains at least 12 5-stars [Fritsch & Fritsch, 1998].

A useful definition regarding rings is embedding. The graph G is said to embed the configuration C if there exists a closed chain K in G such that the sub graph C_k of G spanned by the vertices of K and the vertices lying in the interior domain of K forms a configuration that is equivalent to C. The configuration C is said to be properly embedded in G if K is a simple closed chain [Fritsch & Fritsch, 1998].

A configuration C is said to be reducible if a normal graph containing C as a configuration cannot be a minimal counter example. Otherwise, it is said to be irreducible [Fritsch & Fritsch, 1998]. A set U of configurations is said to be unavoidable if each normal graph contains an element of U.

The main method used by Appel and Haken for generating the unavoidable set of configurations was Heesch's discharging method [Devlin, 1988]. It was in fact way more complicated than this but let us start with discharging.

The idea behind discharging is to draw an analogy between the graph and a electrical circuit; assigning charges to the network so that each vertex has a charge. The charge is given by the $c = 6 - k$, where c is the charge and k is the degree of the vertex. Thus vertices of degree 5 have $c=1$, vertices of degree 6 have $c=0$, vertices of degree 7 have $c = -1$ etc. From Kempe's work we know that summing up the charges of all the vertices for any network yields a positive charge of 12. The fact that the total charge is positive implies that there will be at least one vertex with positive charge (q-positive). The discharging procedure consist of moving the charges around the network, (for the analogy of the graph this means to move the edges around), so that some vertices with positive charge may end up with a negative, vice versa, notice that this will not affect the overall charge of the network. The final configuration will then depend on the specific discharging procedure, but with any discharging procedure applicable to any map it is possible to generate a finite list of configurations, all of which also has a positive charge. The finite list will then contain configurations where all possible receivers of positive charges are included. Any network will contain at least one of these configurations i.e. the finite list of configurations is unavoidable.

At this point one might wonder how we get from infinite possibilities to finite numbers for the unavoidable set. The answer lies in the probability argument of the proof. To begin with, the qualitative behavior of the probability that a configuration is reducible is examined.

m and n rule: for given ring size n, the likelihood of reducibility increases rapidly with the number m of the vertices inside the ring. In particular, if any configuration satisfies:

$$m > \frac{3n}{2} - 6$$

Then it contains an obstacle free sub-configuration that also satisfies the above inequality, and is almost certainly reducible (no counter examples are known) [Appel & Haken, 1986].

For a configuration R of fixed ring size n, as the number of m of the vertices in R exceeds some critical value, R becomes very likely to reduce. The argument in the original proof estimates the critical value of n is certainly <= 17 and probably <=14. Rather than using 17, they actually insisted on using ring size not exceeding 14. If the discharging procedure produced a configuration of size 15, the procedure is modified to yield only configurations of smaller ring size. Incidentally, using 14 instead of 17 had the benefit of decreasing the time required to run the final experiment from four years to six months [Saaty & Kainen, 1977].

Appel and Haken's computer program for discharge and reducibility was built as follows. They first obtained reasonable criteria for the likely reducibility of configurations and then modified Heesch's original discharging algorithm so that the unavoidable sets produced contained only configurations which were likely to reduce [Saaty & Kainen, 1977]. In 1971 Heesch contributed another key observation: he noted three reduction obstacles whose presence inhibits the reducibility of a configuration. A configuration R is called geographically good if it does not contain either of these obstacles [Saaty & Kainen, 1977]:

- A four-legger vertex – a vertex R connected with four or more vertices in the ring Q surrounding R.
- A three-legger articulation vertex – a vertex whose removal separates R and which is connected to three or more vertices in Q.

- A hanging 5-5 pair – a pair of adjacent five-vertices connected by edges to only one other vertex of the configuration.

Configurations which avoid these three reduction obstacles are termed likely to reduce. Appel and Haken saw that they could use these ideas to develop a systematic method for trying to prove the four colour conjecture. Begin with Heesch discharging algorithm or some variant. Try and manipulate the procedure so that all the configurations in the unavoidable set are likely to be reducible. When such an unavoidable set is found, test each of its elements to show either directly that it is reducible or that it contains a configuration which was previously proved reducible. If some configuration cannot be shown reducible go back to discharging algorithm and change it to replace the offending configuration with other likely-to-reduce configurations [Saaty & Kainen, 1977]. An algorithm schema of this process would look like below:

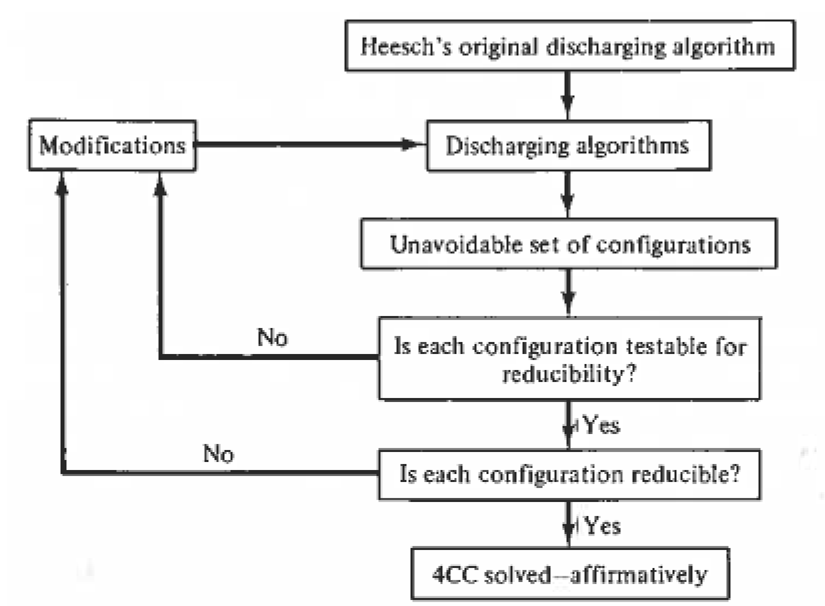


Figure 12: Appel Haken 4CC Proof Algorithm [Saaty & Kainen, 1977].

The final count for the set of unavoidable configurations was 1478 and all of these configuration were proved to be reducible thus four colour conjecture was proved. However it should be noted that their discharging rules in the end topped over 300 and as shown later were not the most efficient ones, but of course they were efficient enough to do the job [Appel & Haken, 1986].

Appel and Haken later wrote that some mistakes were found in their proof and all of them were corrected. Due to the way the proof is built it is almost certain that any mistake that can be found within the computer parts of the proof can be corrected. They distinguish several degrees of seriousness [Appel & Haken, 1986]:

1. The least serious possibility is that the q-positive (charge distribution after a discharge procedure) situation does contain some reducible configuration in U but a wrong entry was made in the bookkeeping lists. Such an error can be corrected in a few minutes.

2. The q-positive situation may contain a reducible configuration but one that is not a member of U and whose reducibility may not have been proved. One way to correct such an error is to perform another computation to verify the reducibility of the configuration and add it to U.

3. The q-positive situation may not contain any reducible configuration (or at least no configuration whose reducibility is easily proven by the programs). In this case they treat the situation exactly as they treated the thousands of bad situations that arouse in construction of the discharge procedures and modify some of the procedures. In this case the repair can take up to a few days.

By 1993, different discharging procedures (32 in total), more powerful proofs of reducibility lead to the unavoidable set of only 633 members (This proof is by Neil Robertson, Daniel P.Sander, Paul Seymour and Robin Thomas).

In 2005, Dr. Georges Gonthier of the Microsoft Research in England used a new computer technology to verify a proof of the four colour theorem [internet resource 3]. According to Keith Devlin, this new result is particularly significant due to the use of Coq, a widely used general purpose utility, which can be verified experimentally [internet resource 4]. He believes this will put to rest any doubts about the proof [internet resource 4].

Discussion on Philosophy of Computers in Mathematics

As mentioned in the introduction a discussion was raised over whether computers, and to some an empirical approach to mathematics, change the way of how a proof could be acquired. The theorem was entirely rejected as a theorem by some, e.g. Bonsall (1982) considers computer-aided proofs “pseudo mathematics”, to others its acceptance meant that the definition of what constitutes a proof needed to be changed. As a result, a debate started and many articles were published in the areas of mathematics and philosophy. It was the proof of four colour theorem that fueled this controversial discussion of computers in pure mathematics. We will now present excerpts from a selection of those articles, showing the different approaches scientists had towards this new tool being used in mathematics, and in our case study pointed towards the four colour theorem.

When Tymoczko's article “The four-colour problem and its philosophical significance” got published in the Journal of Philosophy in 1979, it invoked a lot of response from the mathematical and philosophical society, discussing Tymoczko's reasoning and assumptions on how computers are being used within mathematics, discussing whether computer-aided proofs are viable. The viability of a proof as stated by Tymoczko is dependent on whether it's surveyable, convincing and formalizable. Tymoczko ,like Bonsall, seems to question the acceptance of the computer as a mathematical aid, “They can contain “bugs,” or flaws that go unnoticed for a long time”[Tymoczko, 1979, p.74] For certain this can easily be debunked by the thought that it would be the same for a pen and paper proof written by hand without the aid of computers, but still leaving possibilities to make mistakes.

Tymoczko advocates the believe that one should distinguish between the old four colour problem and the new. Where the old problem is the purely mathematical four colour theorem, and the new four colour problem is the philosophical question of whether a computer aided proof constitutes a theorem or not. What should be pointed out is that he evidently sees the the four colour problem as solved, “the mathematical question can be regarded as definitively solved.” [Tymoczko, 1979, p. 57] but goes on to say that it is questionable whether it has been proven. The point, he makes, is that the use of computers is experimental and is beneath the eminence of rigorous mathematical arguments. “The most natural interpretation of this work, I will argue, is that computer-assisted proofs introduce experimental methods into pure mathematics. This fact has serious implications not only for the philosophy of mathematics...” [Tymoczko, 1979, p. 58]. The implications on philosophy includes the fallibility of theorems and therefore the fallibility of mathematical knowledge, an otherwise rigorous entity in which only a priori knowledge is contained, “we must admit that the current proof is no traditional proof, nor a priori deduction of a statement from premises. It is a traditional proof with a lacuna, or gap, which is filled by the results of a well-thought-out experiment. This makes the four colour theorem the first mathematical proposition to be known a posteriori.” [Tymoczko, 1979, p. 58]. That an a posteriori truth has found its way into mathematical knowledge and that all theorems “should” be known a priori is, as Swart points out the main thesis of the article [Swart, 1980 p. 697]. Swart on the other hand notes that “there are many mathematical truths that cannot be verified “in our heads” and can only be accessed by recourse to our physical senses – to the carrying out of a type of experiment” [Swart, 1980 p. 699] here he refers to the method of writing down, with pencil and paper, and goes as far as to draw an analogy between this method and the use of a computer. In doing so he states that the four colour theorem is a priori knowledge and is so no matter how you categorize it in terms of offloading the task at hand. Davis (1972) uses the terminology “offloading” with which is meant the act of out-sourcing cognitivity to other people and or machines. Though Swart mostly argues against Tymoczko's refrain from calling it the four colour theorem, and directly calls it a theorem, he also advocates the use of a new proposition, between conjecture and theorem; agnogram, and that these are what is believed to be true, “It should thus be clear that agnograms are neither a priori truths nor a posteriori truths, but conjectures to which we can attach a high degree of credence.” [Swart, 1980 p. 706]. He goes on to say that the four colour theorem might be put in this category because of the uncertainty argument used for the creation of the unavoidable set and not because of the use of computers “Most surprisingly, Tymoczko fails to recognize the fact that in so far as there is any weakness in the Haken/Appel proof of the four colour theorem it lies not so much in the reducibility testing-which is almost certainly correct and has been independently corroborated to a large extent-but in the discharging procedure, which gives rise to the unavoidable set of configurations.” [Swart, 1980 p. 697]

“We've noted three features of proofs: that they are convincing, surveyable, and formalizable. The first is a feature centered in the anthropology of mathematics, the second in the epistemology of mathematics, and the third in the logic of mathematics. The latter two are the deep features. It is because proofs are surveyable and formalizable that they are convincing to rational agents.”[Tymoczko, 1979, p. 61]

Although surveyability, convincibility and formalizability are purely characteristics a proof needs to have to be able to check their validity, that doesn't mean a proof without such characteristics cannot be right, but whether it constitutes a proof or not can be discussed.

As Teller mentions about surveyability “It is a characteristic which some proofs have, and which we want our proofs to have so that we may reasonably assure ourselves that what we take to be a correct proof is so.”[Teller, 1980 p.798] Convincibility hangs on tight to that, as something will seem convincing when one can overview the proof, which in turn depends on how formalized the proof is, since this will help with surveying the proof.

If you can't see every step that is being made, e.g. a computer was used for intermediate calculations, it cannot be said that the proof is surveyable. This would merely confer that the theorem is true, but remains void of the “how is it true?” question, while the “if it's true?” is answered. Without being able to tell why something is true, you'll have a hard time convincing anyone of truth thus controversy might arise.

Since making mistakes is but human, and computers are made by humans, they're expected to make mistakes, and thus human beings' work and computer generated work, both have to be surveyed. As stated by Swart (1980, p703) “... flaws in the computer implementation of algorithms are nothing more than *errors of logic,* no different in essence from errors that crop up in proofs that have nothing do with computers.” There is also consideration that a proof and a program are more alike than one might think at first glance. They're both based on logic statements that are convincible, and axiomatic in their nature; A proof can be compared with a program. The axioms are analogous to the input. The theorem is analogous to the output while the proof is the program. To find a proof consists of finding a program. To verify a giving proof we need only rerun the program.” [Davis, 1972 p.256].

Davis (1972) states interesting ideas about the probabilities concerning the amount of errors made by man and machine, and how a computer gets to its errors. Interesting is the idea that indeed a computer might make errors, but it computes at a very high speed compared to humans. So the amount of errors might be higher than the amount of errors a human would make within the same time frame. What should be taken into account is that there's a lot more work done within that same time frame.

“Proofs cannot be too long, else their probabilities...” to be correct “... go down and they baffle the checking process. To put it in another way: all really deep theorems are false (or at best unproved or unprovable). All true theorems are trivial.”[Davis, 1972 p.260] A bold statement by Davis after he discusses the probabilistics of symbols used in mathematics, which, when written down, can never be the same on microscopic level. So this introduces the probability of misinterpretation. An example is given by him with written one's and/or sevens to illustrate the simplicity with which certain errors could occur. Below the figure Davis (1972) used to illustrate this, also notable is that Davis wrote this article as a general discussion about this subject, and was written long before Appel & Haken came with their proof and started this controversy.

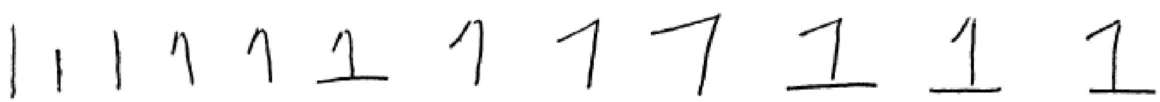


Figure 13: 1s or 7s ? [Davis 1972 p.256]

Although this example fixates on handwriting, nowadays we have the possibilities to scan printed pages, or handwritten pages, and use text-recognition, which could introduce these handwritten problems into machines. Davis considers a future in which we will adapt to the increased amount of calculations needed to solve a problem and take the probabilistics that come with this into account; “It is possible that a new type of mathematics might develop in which the “derivations” or the “processes” are so enormously long that the probabilistic nature of the result will be an integral feature of the subject” [Davis, 1972 p.263]. Davis reasons that the order of magnitude of mistakes made by computers compared to the amount of work they deliver, is roughly equal to that of humans and concludes with “A derivation of a theorem or a verification of a proof has only probabilistic validity. It makes no difference whether the instrument of derivation or verification is a man or a machine."

Rufener (2011) considers computers as an extended mind in which we can offload our computations on a computer. Our brains have always tried to find ways to offload work on our surroundings, may it be a leader in a group of people that delegates others to work out problems, to come to a communal solution with the group or a calculation worked out with pen and paper, because it has to many factors to remember at the same time. Rufener (2011 p.155) suggests a world X which "... is identical to ours in every way except that everyone has knowledge on the rudiments of first order logic. In this world, they too are concerned with the surveyability of a proof, so, when confronted with a proof similar to the four colour theorem (in terms of length) they divide the proof so that each person surveys and checks a segment. With everyone in the world surveying, the task now went from taking a few lifetimes to survey by hand to taking as long as a computer to survey and check the entire proof." Thus increasing the amount of work that can be done on one person's idea by spreading the workload, or on the other hand using knowledge databases to quickly recall information that has previously been offloaded by others. This all helps in increasing our cognitive capabilities since one doesn't have to remember everything by heart, but can be recalled from outside sources. "So it seems fair to say that when we are confronted with mathematical problems or proofs that are too tedious and we are not able to solve them with our inherent on-board cognitive capacities, we then adapt and use tools to solve them." [Rufener, 2011 p.219].

There are many opinions, views and statements from many people on this subject, of which some have been represented here. From people that have funny, bold and interesting ideas about how to tackle the computer-aided proof discussion, and whether computers are a valid tool or an easy way to extend our minds, or have no place in the pure mathematics.

Discussion

A decade after their proof, Appel and Haken were forced to respond to the negative rumors that surrounded the proof. The response was ten pages, published in the Mathematical Intellingencer, explaining the methods they had used, from reaching the unavoidable set to the error-correction. One reason that rumors sprouted is likely to be that, in 1981, Ulrich Schmidt, while completing his Diploma Thesis, found errors in the proof, one of which was of degree three. An error of degree three is as mentioned earlier when a q-positive situation, arrived at by the discharging procedure, does not contain a configuration, which is reducible. This may have seemed like Ulrich Schmidt had found a counterexample to the proof, just as Heawood did for Kempe's proof. However this was not the case. The situation had been missed in the bookkeeping and was because of this, not taken care of by the right discharging rules. Appel and Haken describes the rumors in the response:

> "A combinatorialist friend of ours, when told in 1975 that we thought we could prove the theorem by a method involving computer proof of reducibility exclaimed in horror, " God would never permit the best proof of such a beautiful theorem to be so ugly." When faced with such a proof even the fairest minded mathematician can be forgiven for wishing that it would just go away rather than being forced to think about the fact that en "elegant" proof may never appear and thus our Eden is defiled. Such a person greets news that the proof is incorrect with a sense of relief, providing fertile ground for rumors"
>
> [Appel & Haken, 1986, p. 12]

This lack of elegance brings us to Tymoczko's argument; that a proof needs to be formalized, convincing and surveyable. Which means a proof should be convincing about the accurate results, formalized in theoretic part (from axioms till conclusion) and it should be possible to follow the proof. Clearly the proof of the four colour theorem is formalized, going from proving lemmas to the induction hypothesis of the unavoidable set to the proof that each configuration is reducible, the latter in a way so that even a computer can understand it (which needs a very formal language), but is it surveyable? We agree with Tymoczko that computer-assisted proofs cannot be fully surveyed in the sense he demands. No one has surveyed the proof entirely and it cannot be checked step by step. The last part of the proof is exhaustive and can, for the maximum ring size (14-ring), involve approximately 265720 different colouring considerations [Appel & Haken, 1986, p. 12]. Due to this it is impossible for a human to reproduce or check the proof in its entirety by hand, which can be done by a computer simply by running it again. However the program is written in a highly formal language and *can* be checked by humans. Since a computer is not an intelligent partner, it has to perform the operations given to it, thus to check the code is to verify that the methods should be carried out correctly. The surveyability of a computer aided proof is therefore twofold, and the question is not whether the proof is surveyable, but how it can be surveyed. It is obvious that if a computer is required for validating statements in an exhaustive proof, then a computer must also have a part to play in the verification of the proof.

There is one very important aspect of computers in mathematics that we have yet to discuss, that is the random change of the stored data. During a program run some of the data may unintentionally be altered due to hardware errors or software bugs. We already mentioned the surveyability of the software i.e. the algorithm and the program, so any software bugs can be eliminated. One solution to deal with hardware error is to run the program several times and on different systems, which will dramatically reduce the chance of getting the same error at the same instance of the program run. This process will make the probability of error infinitesimal, but it will never eliminate the chance of encountering this situation. We have already mentioned that Tymoczko links traditional proofs with surveyability. This along with the random change of a bit may be the key to why some, like Tymoczko, have a problem with computer-assisted proofs, since one mathematician cannot check the proof and the only method with which it can be checked is fallible, thus making mathematics fallible. Software related bugs are also a possible but basically they do not differ from mistakes which could be made by humans which is very similar to what Swart stated in his article. Humans misuse notations and make syntactical mistakes as well. Actually, calculations made by humans are more error-prone than those of computer. People are using calculators or applying computer help to make complex calculations as computers are more reliable; so, can computer assistance in four colour theorem proof be seen in the same role? If we take Rufener's point of view that computers are an extended mind which we can offload our computations on, above mentioned assistance must be seen in the same way.

Conclusion

The discussions surrounding the four colour theorem have been going on for over 30 years and it is likely that they will continue to be a part of philosophy and mathematics for many years to come. However we would suggest that the matter should be put to rest and that computer assisted proofs should be accepted as part of mathematical knowledge.

Swart suggests the use of the term agnogram for a conjecture that is very likely to be true. However as the point of mathematical knowledge is universal truth and complete conviction, the adding of such a mathematical concept would bend the concept of proofs so that one can no longer trust in the correctness of the assertion and make mathematical knowledge a feeble entity. Tymoczko points out the dangers that comes with unsurveyable proofs but seems to rejects the use of a computer to do the surveying as he makes mathematics out to be a human activity. A computer result can never be trusted to be completely accurate, due to the possibility of hardware related bugs, but it should be acknowledge that there are methods to reduce the chance of this happening to infinitesimal.

We already accept that when a proof is published, it can have some errors in it. What is important is if these errors can be corrected when found. The same approach should be considered in computer assisted work as well. As we have stated in the discussion, a computer's assistance in a proof is doing the long and complex calculations that will take for a human mind such a long time that it may not be possible to finish in a lifetime. However, these calculations follow an algorithm, or the logic of the program, which does not differ from a formalized proof. We agree that there is a certain lack of elegance when it comes to computer assisted work. This constitutes a problem for the dissemination within mathematical knowledge as mathematician that follow the proof will most likely be unable to construct the same mental process as the originators, and is therefore left with the question of why the theorem is true.

We believe the mathematical community must let go of some of its strict views on proofs and accept the use of computers in this area. The end result may not be considered as beautiful as if done without computer assistance, but the likelihood of an error occurring in such a proof is infinitesimal. As the logic of the program in a computer assisted proof can be checked, it is our belief that such proofs does not challenge the infallibility of mathematical knowledge.

Literature

1. Appel, K. and Haken W. (1986), "The Four Color Proof Suffices" *The Mathematical Intelligencer,* Vol. 8, No 1, pp. 10-20

2. Chartrand, G., Polimeni, Albert D., Ping Zhang "Mathematical Proofs A Transition to Advanced Mathematics" (2nd edition) *Addison Wesley* 2007

3. Davis, P.J. (1972), "Fidelity in Mathematical Discourse: Is One and One Really Two?" *The American Mathematical Monthly,* Vol. 79, No 3, pp. 252-263

4. Devlin, K. "Mathematics: The New Golden Age" (1st Edition) *Penguin Books*, London, 1988

5. Fallis, D. (Apr 1997), "The Epistemic Status of Probabilistic Proof" *The Journal of Philosophy*, Vol. 94, No. 4 pp. 165-186

6. Fleck, M.M. "Building Blocks for Theoretical Computer Science" (1st edition) 2012

7. Fritsch, R., Fritsch, G. "The Four-Color Theorem" *Springer* 1998

8. Jacquette, D., "Philosophy of Mathematics – An Anthology" (1st edition) *Wiley, John & Sons, Incorporated* 2001

9. Jaffe, A., Quinn, F. (Jul 1993), "Theoretical Mathematics: Toward a cultural synthesis of Mathematics and theoretical Physics." *Bulletin of the American Mathematical Society*, Vol. 29, No. 1 pp. 1-13

10. Kainen, P.C. (Sep 1974), "A Generalization of the 5-color Theorem" *Proceedings of the American Methematical Society*, Vol. 45, No. 3 pp 450-453

11. Krantz, S.G. (Feb 2007), "The History and Concept of Mathematical Proof"

12. MacKenzie, D. (Feb 1999), Slaying the Kraken: The Sociohistory of a Mathematical Proof. *Social Studies of Science*, Vol. 29, No. 1 pp. 7-60

13. Peressini, A. (Feb 2003), Proof, Reliability and Mathematical Knowledge. Theoria Vol. 69, No. 3, pp. 211–232

14. Rufener, C.M. (2011) "The Four-Color Theorem Solved, Again: Extending the Extended Mind to the Philosophy of Mathematics," *Res Cogitans*, Vol.2, No. 1, Article 23.

15. Saaty, T.L., Kainen, P.G. "The Four-Color Problem: Assaults and Conquests" (1st edition), *McGraw Hill*, 1977

16. Swart, E. R. (Nov 1980), "The Philosophical Implications of the Four-Colour Problem." *Experimental Mathematics,* Vol. 14, No.3, pp. 285-298

17. Teller, P. (Dec 1980), "Computer Proof" *The Journal of Philosophy,* Vol. 77, No. 12, pp. 797-803

18. Tymoczko, T. (Feb 1979), "The Four-Color Problem and Its Philosophical Significance." *The Journal of Philosophy*, Vol. 76, No. 2, pp. 57-83

19. Velleman, D.J. "HOW TO PROVE IT A Structured Approach" (2nd edition) *Cambridge University Press 1994* 2006

Webpages:

1. Devlin, K., (2005) "Last doubts removed about the proof of the Four Color Theorem" http://www.maa.org/devlin/devlin_01_05.html

   (accessed 04/01/2013)

2. Massa, S., (2012) "Graph Theory"

   http://www.stats.ox.ac.uk/~massa/GraphTheory_2012/notes_massa.pdf

   (accessed 04/01/2013)

3. "The five colour theorem proof" http://math.byu.edu/~forcader/FiveColor.pdf (accessed 04/01/2013)

4. Gonthier, G. “Microsoft research: A computer-checked proof of the Four Colour Theorem” http://research.microsoft.com/en-us/um/people/gonthier/4colproof.pdf (accessed 04/01/2013)

5. “Enciclopedia Britannica, Academic Edition: Epistemology” http://www.britannica.com/EBchecked/topic/190219/epistemology (accessed 10/12/2012)

6. “Enciclopedia Britannica, Academic Edition: Inference” http://www.britannica.com/EBchecked/topic/287533/inference (accessed 10/12/2012)

7. Reutlinger, A., Schurz, G., Hüttemann, A. (2011) “Ceteris Paribus Laws”, *The Stanford Encyclopedia of Philosphy* Edward N. Zalta (ed.), http://plato.stanford.edu/archives/spr2011/entries/ceteris-paribus/ (accessed 10/12/2012)

8. Spade, P.V., Panaccio, C., "William of Ockham", *The Stanford Encyclopedia of Philosophy (Fall 2011 Edition)*, Edward N. Zalta (ed.), http://plato.stanford.edu/archives/fall2011/entries/ockham/ (accessed 10/12/2012)

Appendix 1: LOGIC

The content of this appendix is taken from [Chartrand et. Al, 2007] and [Vellerman, 2006].

Encyclo paedia Britannica defines logic as “the study of correct reasoning, especially as it involves the drawing of inferences”. These rules of inference or in other words deductive reasoning is this kind of reasoning one arrives at a conclusion from some other statements, called premises, which are known or said to be true. Deduction is essential for constructing proofs is mathematics. Few simple example of deductive reasoning:

Modus Ponendo Ponens or Modus Ponens - (Latin: "The way that affirms by affirming"):

Premises:

Plants that are green have chlorophyll.

Tomato plant is green.

Conclusion: Therefore, tomato plant has chlorophyll.

Modus Tollendo Tollens or Modus Tollens - (Latin: "The way that denies by denying"):

Premises:

If hands are washed with soap, they are clean.

My hands are not clean.

Conclusion:

Therefore, my hands have not been washed with soap.

If the premises are true, the conclusion inevitably is true, and the argument is valid. Argument can only be invalid if one or more of the premises are false.

In logic, in mathematics the set of symbols is often used to express logical representations. Some of these symbols are illustrated in table 1 below.

Table 1: Some symbols in logic.

Symbol	Meaning
$\wedge$	And (conjunction)
$\vee$	Or (disjunction)
$\neg$	Not (negation)
$\forall$	For all (universal quantification)
$\exists$	There exists (existential quantification)
$\Rightarrow$	Implies that (implication)
$\Leftrightarrow$	If and only if, iff (equivalence)
$\veebar$	Either Or (exclusive disjunction)

In mathematics we are usually dealing with statements - declarative sentences or assertions. Every statement can be true or false, meaning it has a *truth-value*. We denote T for *True* and F for *False*. These statements are usually represented by various letters e.g. P, Q, R. When we assign truth-value to one or more statements we can derive other statements and by the rules of logic find out the validity of these new statements. These new statements are called compound statements. For this purpose it is appropriate to use truth tables. For example we choose 2 statements P and Q, and since for the purpose of illustrating the rules of logic the statements themselves do not matter we will not assign the meaning for them just yet. We can construct the truth table:

P	**Q**	**$P \wedge Q$**	**$\neg P \vee Q$**	**$P \Leftrightarrow Q$**	**$Q \Rightarrow \neg P$**
T	T	T	T	T	F
T	F	F	F	F	T
F	T	F	T	F	T
F	F	F	T	T	T

So from the truth table above we can see that we can always deduce the validity of any new statement if we know the rules of logic and validity of the original statement.

To illustrate this better we can assign statements to the letters, for example:

P: It is going to rain tomorrow

Q: Tyge is going to write an introduction tomorrow

From the truth table we can see that statement **P∧Q** is: It is going to rain tomorrow and Tyge is going to write an introduction. And again from the table we see that this statement is only true if both P and Q are true. Let us consider **¬P∨Q:** It is not going to rain tomorrow or Tyge is going to write an introduction. We can again see that in this occasion the truth of the compound statement depends on only one of the statements (disjunction), either P has to be false, because of the negation in compound statement or Q has to be true. Furthermore we can make sentences for all of these statements of our truth table.

This kind of inference allow us to create infinite amount of compound statements and it all can be followed back to the original statements, therefore the validity of these statements are the only variable in this equation of deduction.

Reductio ad absurdum - (Latin: "Reduction to absurdity")"is a mode of argumentation that seeks to establish a contention by deriving an absurdity from its denial, thus arguing that a thesis must be accepted because its rejection would be untenable. It is a style of reasoning that has been employed throughout the history of mathematics and philosophy from classical antiquity onwards." [http://www.iep.utm.edu/prop-log/- 07 Dec. 2012]

Appendix 2: Definitions

An axiom (or postulate)

Latin *axioma* meaning “what is thought fitting” or *axios* meaning “worthy” it is a starting point or first principle for inference in logic, it does not need to be proven, it is self-evident. The basic axiom in algebra is e.g. commutative property of addition: x + y = y + x [Encyclopaedia Britannica].

***A posteriori* knowledge**

“A posteriori knowledge is knowledge that is known by experience (that is, it is empirical, or arrived at afterward)” [Rufener & Casey, 2011].

***A priori* knowledge**

“A priori knowledge is knowledge that is known independently of experience (that is, it is non-empirical, or arrived at beforehand, usually by reason). It will henceforth be acquired through anything that is independent from experience.” [Rufener & Casey, 2011].

***Ceteris paribus* reliability**

Latin: "all other things being equal or held constant." Statement *ceteris paribus* is a qualification that the possibility of any factors overturning original logic relationship between statements in question is ruled out [Reutlinger et al., 2011].

Conceptualism

“Take on several forms, but can be summarized as the theory that mathematics is ultimately an investigation of the formal properties of the ideas or concepts as the content of thought.” Meaning that to construct a mathematical object is to conceptually define it as a mental picture of the constructing process [Jacquette, 2001].

Epistemology

From Greek *episteme* meaning knowledge + *logos* meaning reason, it is one of four main branches of philosophy (other three being: metaphysics, logic and ethics) also known as the theory of knowledge. “It is a study of nature, origins and limits of human knowledge”

[Encyclopaedia Britannica].

Formalism

No more, no less than mathematical language based on axiomatic set theory and formal logic. The truth of a proposition is characterized by "formal matters of mathematical notation" and can be derived from axiomatic set theory via rules governed by formal logic. Formalism thereby states that truths have no meaning unless given interpreting context, advocating rigorous syntax in theorems. Thus formalism emphasize abstraction, not origin, as to oppose a more general understanding of proofs; a theorem on the subject of a certain object is said to be demonstrated, when the construction of its type of object is displayed as objects with its asserted properties [Jacquette, 2001].

Intuitionism

There is a fundamental idea in intuitionism that mathematics is created by the mind. A proof is therefore a mental construction of a mathematical proposition that shows the statement is true. The existence of proofs is then a tool of communication that "serves as a means to create the same mental process in different minds", hence a proof must be surveyable and any discussion of the nature of a mathematical proposition, its truth and conditions can only take place after a rigorous proof, within a strong mathematical system, has been created. Intuitionism does not accept the law of the excluded middle hence neither proof by contradiction [Jacquette, 2001].

Lemma

From greek lemma – thing taken, assumption. A subsidiary or intermediate theorem in an argument or proof [Merriam-Webster].

Logical inference (*modus ponens*)

"Inference, in logic, is derivation of conclusions from given information or premises by any acceptable form of reasoning. Inferences are commonly drawn by deduction, which, by analyzing valid argument forms, draws out the conclusions implicit in their premises, by induction, which argues from many instances to a general statement, by probability, which passes from frequencies within a known domain to conclusions of stated likelihood, and by statistical reasoning, which concludes that, on the average, a certain percentage of a set of entities will satisfy the stated conditions." [Encyclopaedia Britannica].

Occam's (or Ockham's) Razor

Can be expressed as: "Don't multiply entities beyond necessity" basically it says that you should exclude all the unnecessary parts in you theories or proofs and promotes simplicity as the "right" way. If there are few competing theories around the subject the one, which offers the simplest explanation, is the right one. [Spade et al., 2011]

Realism

The truth is out there in the sense that the world of mathematics is immutable with an unconditional validity, thus to do mathematics is to discover the existence of real abstract entities and the properties asserted to them. This proclamation means that no matter how we define objects through theorems it is the objects that validate the theorem and the theorem that allows us to perceive the object. The implications of such an understanding of mathematics are that, like other sciences, such as physics, the truth of a proposition is autonomous to the method of verification. It is therefore open to a variety of verification techniques [Jacquette, 2001].

Appendix 3 – Graph Theory Concepts

This appendix and the figures included are taken from the book Graph Theory by J.A.Bondy and U.S.R. Murty, published by Springer in 2008, a part of the Graduate Texts in Mathematics series. We will try to summarize the chapters 1, 2, 3 and 10 to explain some of the concepts that pass in our project and also give a short background introduction for the readers.

Some situations experienced in life can be described by a diagram with a set of points and lines joining these points that show relations between them. This gives rise to the concept of graphs.

A *graph G* is an ordered pair (V(G), E(G)) which includes V(G), a set of vertices and E(G), a set of edges disjoint (disjoint here means the intersection of these two sets is the empty set) from V(G) . There is also the incidence function ψ_G that associates with each edge of G, an unordered pair of vertices of G. The associated edges need not be distinct. If *e* is an edge and *u* and *v* are vertices such that $\psi_G = \{u,v\}$ then e is the edge joining the vertices u and v which are called the *ends* of e. The number of vertices and edges in G are denoted by *v(G)* and *e(G)* and these are also called the *order* and *size* of G, respectively.

Example:

$$G = (V(G), E(G))$$

where;

$$V(G) = \{u,v,w,x,y\}$$

$$E(G) = \{a,b,c,d,e,f,g,h\}$$

$$\psi_G(a) = uv \qquad \psi_G(b) = uu \qquad \psi_G(c) = vw \qquad \psi_G(\mathrm{d}) = \mathrm{wx}$$

$$\psi_G(\mathrm{e}) = \mathrm{vx} \qquad \psi_G(\mathrm{f}) = \mathrm{wx} \qquad \psi_G(\mathrm{g}) = \mathrm{ux} \qquad \psi_G(\mathrm{h}) = \mathrm{xy}$$

One possible graphical representation of the diagram associated with the above graph can be seen in figure 1, where each vertex is represented by a point and edges with a line.

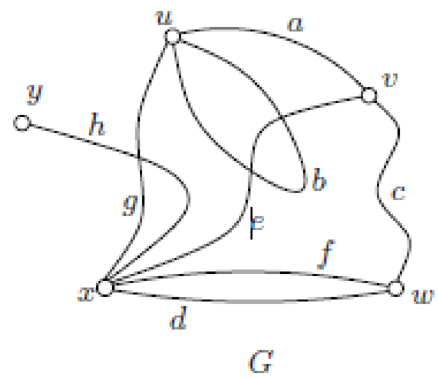


Figure 1: Diagram of Graph G

It should be noted that there is no unique way to draw a graph. The relative positions of vertices and the shapes of the edges have no significance. A diagram of a graph only shows the incidence relation (ψ_G) between vertices and edges. In practice, a diagram of a graph is often drawn and referred to as the graph itself.

With this graphical representation, we can come up with some concepts and definitions. The ends of an edge are *incident with* the edge and vice versa. Two vertices which are incident with a common edge are *adjacent*, as well as two edges which are incident with a common vertex. Two distinct adjacent vertices are *neighbors*. The set of neighbors of a vertex v in a graph G is denoted by $N_G(v)$.

An edge with identical ends is called a *loop*, whereas an edge with distinct ends is called a *link*. Two or more links with the same pair of ends are *parallel edges*. In figure 1, edge b is a loop and all other edges are links. d and f are parallel edges.

A graph is *finite* if both its vertex set and edge set are finite. The graph with no vertices is the *null graph*. Any graph with only one vertex is a *trivial graph*. All other graphs are *nontrivials*. A graph is *simple* if it has no loops or parallel edges.

A set V, together with a set E of two-element subsets of V, defines a simple graph (V,E), where the ends of an edge uv are exactly the vertices u and v. In any simple graph, the incidence function ψ can be dispensed by renaming each edge as the unordered pair of its ends. In a diagram of such a graph, the labels of the edges can be omitted to simplify the drawing.

Special Families of Graphs

A *complete graph* is a simple graph in which any two vertices are adjacent, an *empty graph* is one in which no two vertices are adjacent (i.e. edge set is empty set). A graph is *bipartite* if its vertex set can be partitioned into two subsets X and Y so that every edge has one end in X and one end in Y. This kind of partitioning is called a *bipartition* of the graph and X and Y are its parts. A bipartite graph G with bipartition (X, Y) is denoted as *G[X, Y]*. If G[X, Y] is simple and every vertex in X is joined to every vertex in Y, then G is called a *complete bipartite graph*. A *star* is a complete bipartite graph G[X, Y] with either one of X or Y having only one vertex.

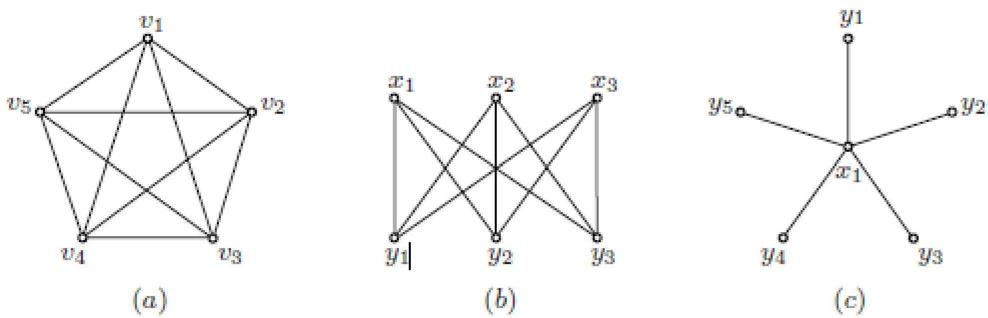


Figure 2: (a) A complete graph, (b) a complete bipartite graph, (c) a star

A *path* is a simple graph whose vertices can be arranged in a linear sequence in such a way that two vertices are adjacent if they are consecutive in the sequence, and are nonadjacent otherwise. A *cycle* on three or more vertices is a simple graph whose vertices can be arranged in a cyclic sequence and is a path. The length of a path or a cycle is the number of its edges. A path or cycle of length k is called a *k-path* or *k-cycle*. A 3-cycle is often called a triangle, a 4-cycle a quadrilateral, a 5-cycle a pentagon, and a 6-cycle a hexagon.

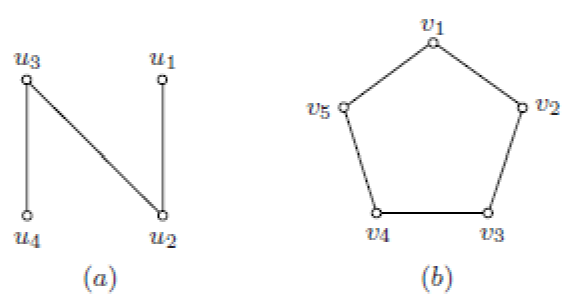


Figure 314: (a) A path of length three, (b) a cycle of length five

A graph is *connected* if, for every partition of its vertex set into two nonempty sets X and Y, there is an edge with one end in X and one end in Y. Otherwise the graph is *disconnected*. In other words, a graph is disconnected if its vertex set can be partitioned into two nonempty subsets X and Y so that no edge has one end in X and one end in Y.

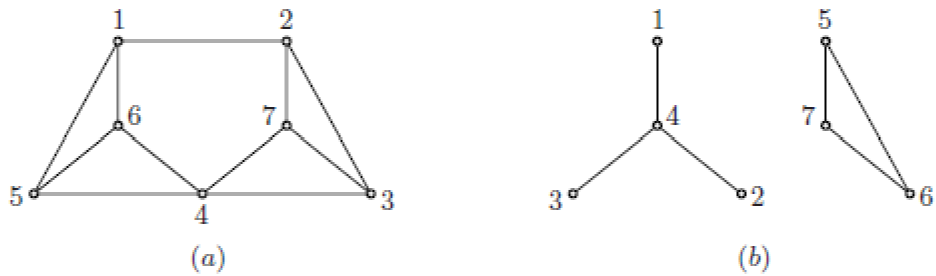


Figure 4: (a) A Connected graph, (b) a disconnected graph

For the sake of clarity, certain conventions are observed in representing graphs by diagrams. An edge cannot intersect itself and no edge can pass through a vertex that is not an end of the edge. A graph which can be drawn in the plane in such a way that edges only meet at points corresponding to their common ends is called a *planar graph* and such a drawing is called a *planar embedding* of the graph. For example the first to graphs in figure 2 are not planar.

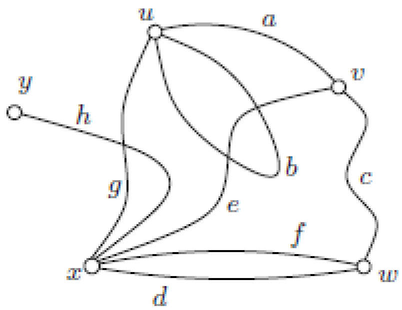
Incidence and Adjacency Matrices

Drawings are convenient means of specifying graphs, however they are not suitable for storing graphs in computers or for applying mathematical methods on them. For these purposes, two matrices can be considered that are associated with a graph.

If G is a graph with vertex set V and edge set E, the *incidence matrix* of G is the *n x m* matrix such that:

M_G : = (m_{ve}), where m_{ve} is the number of times (0, 1 or 2) that vertex v and edge e are incident.

The *adjacency matrix* of G is the *n x n* matrix A_G := (a_{uv}), where a_{uv} is the number of edges joining vertices u and v, each loop counting as 2 edges.



G

	a	b	c	d	e	f	g	h
u	1	2	0	0	0	0	1	0
v	1	0	1	0	1	0	0	0
w	0	0	1	1	0	1	0	0
x	0	0	0	1	1	1	1	1
y	0	0	0	0	0	0	0	1

M

	u	v	w	x	y
u	2	1	0	1	0
v	1	0	1	1	0
w	0	1	0	2	0
x	1	1	2	0	1
y	0	0	0	1	0

A

Figure 5: Incidence and adjacency matrices of a graph

Vertex Degrees

The degree of a vertex v in a graph G is denoted by $d_G(v)$. It is the number of edges of G incident with v, for which each loop counts as two edges. If G is a simple graph, $d_G(v)$ is the number of neighbors of v in G. A vertex of degree zero is called an *isolated vertex*. δ(G) and Δ(G) denote the *minimum* and *maximum* degrees of vertices of G, and d(G) denotes the *average degree* of the graph. For any graph, the sum of degrees of all vertices in the graph is 2 times the number of edges.

A graph G is *k-regular* if d(v) = k for all vertices in the graph. A regular graph is one that is k-regular for some k. K-regular graphs have very simple structures for k = 0, 1 and 2. 3 – regular graphs can be very complex and these are also referred to as cubic graphs.

Isomorphism

Two graphs are identical only when they have identical vertex and edge sets and an identical incidence functions. However it is possible for two different graphs to have essentially the same diagram. In this case the sole difference lies in the labels of their vertices and edges. This relation is called isomorphism.

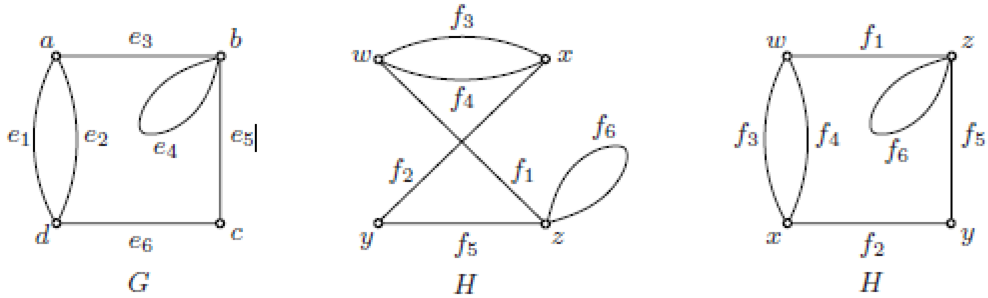


Figure 6: Isomorphic Graphs

Subgraphs and Supergraphs

Edge and Vertex Deletion

Given a graph G (with vertex set of n elements and edge set of m elements), there are two ways of deriving smaller graphs from it. If *e* is an edge of G, we may obtain a graph on m – 1 edges by deleting e from G but leaving the vertices and the remaining edges intact. The resulting graph is G \e. Similarly, if v is a vertex of G, we may obtain a graph on n – 1 vertices by deleting from G the vertex v together with all the edges incident with v. The resulting graph is G – v.

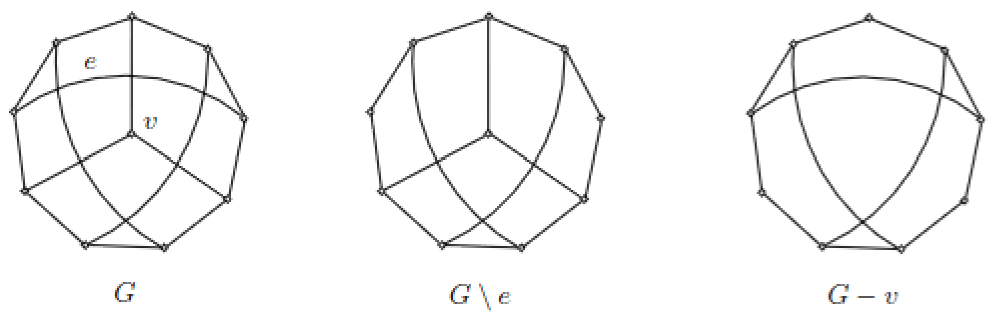


Figure 15: Edge deleted and vertex deleted subgraphs of G

The graphs G \ e and G – v are examples of subgraphs of G. G \ e is called an edge-deleted subgraph and G – v is called a vertex-deleted subgraph. A *supergraph* of a graph G is a graph H which contains G as a subgraph. Any graph is both a subgraph and a supergraph of itself. All other subgraphs and supergraphs are referred to as *proper*.