

Hilbert's Problems

G13PJS

Mathematics 3rd Year Project
Spring 2007

*School of Mathematical Sciences
University of Nottingham*

Matthew M Buck

Supervisor: Dr JP Zacharias

Division: Pure

Project code: JPZ P2

Assessment type: Review

May 2007

I have read and understood the School and University guidelines on plagiarism.

I confirm that this work is my own, apart from the acknowledged references.

Abstract

This report is an investigation into Hilbert's Problems, a set of twenty-three questions posed by David Hilbert in 1900. In particular, the report focuses on the first and third problems - those of the Continuum Hypothesis, following Cohen's original proof of its independence; and the Equidecomposability of Polyhedra, following Hadwiger's proof. It also looks at sets of problems for the twenty-first century.

Contents

1	Introduction	4
2	A Brief Introduction to Hilbert's Problems	5
3	Problem 1 - Cantor's Problem of the Cardinal Number of the Continuum	11
3.1	An Introduction to Set Theory	13
3.1.1	Axioms of Set Theory	13
3.1.2	Ordered Pairs and Binary Relations	15
3.1.3	Cardinality	16
3.1.4	The Cardinality of \mathbb{R}	18
3.2	Foundations in Logic - Gödel's Theorems	20
3.3	Proving the consistency of the Continuum Hypothesis	21
3.3.1	Proof that A_L is provable in ZF	22
3.3.2	Proof that $(V = L)_L$ is provable in ZF	23
3.3.3	Proof that $(V = L) \Rightarrow$ AC and GCH	23
3.4	Independence of the Continuum Hypothesis	24
3.5	Conclusion	28
4	Problem 3 - The equality of two volumes of two tetrahedra of equal bases and equal altitudes	30
4.1	Properties of Volume	31
4.2	The 2-Dimensional Case	32
4.3	The 3-Dimensional Case	34
4.4	Conclusion	38
5	Conclusion - Hilbert's Legacy	39

1 Introduction

In 1900, at the International Congress of Mathematicians in Paris, David Hilbert delivered what has become one of the most important speeches in the history of mathematics. In it, he outlined twenty-three problems which he predicted would shape the next century of mathematics. Many have been resolved, some are the topic of intense research, and some are the subject of debate over precisely what the question means. However, they have indeed guided much of modern mathematics.

My aim in this report is to give a general overview of the problems, while looking at two in more detail. Thus I will first present an outline of each problem and whether or not it has been resolved (section 2). I will then go into detail about problems one and three: that of the Continuum Hypothesis (section 3), following Cohen's proof as given in [5]; and also the equidecomposability of polyhedra (section 4), following Hadwiger's proof as presented by Boltianskii in [3]. I will finally present a summary of Hilbert's legacy (section 5) - the 1974 symposium on the problems, and the efforts to create a new list of problems for the twenty-first century.

2 A Brief Introduction to Hilbert's Problems

I present here a brief list of the 23 original problems set by Hilbert. Not all of these were included in his original speech, but were published in full some time after. There was also a 24th problem, which was omitted by Hilbert but rediscovered a century later.

The first problem is one of Set Theory. I will discuss this in section 3. It deals with the Continuum Hypothesis - whether there exists a set whose size is between that of the integers and the real numbers, or, alternately, whether $\aleph_0 < \aleph_1 < 2^{\aleph_0}$. It was shown by Paul Cohen in 1963 that the Continuum Hypothesis is independent of Zermelo-Frankel set theory, and thus can be neither proved nor disproved.

The second problem was to prove that the axioms of arithmetic are consistent - ie that they cannot, in a finite number of steps, lead to a contradiction. Gödel showed in his incompleteness theorem that it is impossible to prove this within the axioms themselves. There is no consensus on whether or not this is a solution to the problem.

The third problem was a fairly simple one - to prove or disprove the theory that it is possible to cut any two polyhedra of equal volume into finite pieces and reassemble them into each other. It was in fact disproved within a year by Max Dehn, who provided the counterexample of a regular tetrahedron and a cube of equal volume. I shall discuss this in greater depth in section 4.

Problem number four is the first of the “vague” problems, in that Hilbert's speech does not contain a question. It instead suggests a general investigation in

Minkowski's geometry (constructed in *Geometrie der Zahlen*) into the theorem that a straight line is the shortest path between two points, as well as other elementary constructs. Other interpretations suggest that it is a request to find all geometries close to Euclidean geometry subject to various restrictions of which axioms may be weakened or removed. However, it is generally considered too vague to be answered properly.

The fifth problem concerned the characterisation of certain Lie Groups. Lie's geometrical transformations were required to be differentiable, and Hilbert believed that the transformations could be described in such a way that they had to be differentiable. The problem was solved in the affirmative by Andrew Gleason in 1952, and separately by Montgomery and Zippin. However, some mathematicians argue that, with a slightly different interpretation of the problem, it becomes the Hilbert-Smith conjecture, which remains thus far unsolved.

Problem six can be described in two words - "axiomatise physics". Whether this has been achieved or not is debatable as in many cases physics is an example of moving goalposts. That being said, classical mechanics was axiomatised by 1903, Thermodynamics by 1909, and Special Relativity by 1914. As each section of physics is fully explored, another appears, and thus the problem is not unlike Achilles and the tortoise - you can get infinitely close, but never quite catch it.

Problem seven was the first involving number theory. It asks whether a^b (where $a \neq 0, 1$ and b is algebraic and irrational) is necessarily transcendental (that it is not the root of any finite polynomial with integer coefficients). Proving that a number is transcendental is notoriously difficult - the proofs that e and π have this property are considered some of the most important in number theory.

Hilbert later noted in a lecture that he did not believe anyone in the room would live to see a proof that $2^{\sqrt{2}}$ was irrational. He was proved spectacularly wrong in 1929 by A.O. Gelfond, who five years later proved the general case by use of complex functions.

The eighth problem is probably the most important unsolved problem in mathematics. In general terms, it asks about prime numbers - it asks to prove the *Riemann Hypothesis* (that all non-trivial zeros of the Riemann Zeta Function (ζ) lie on the line $Re(z) = \frac{1}{2}$), and from that, attempt proof of the *Goldbach Conjecture* (that there are infinitely many pairs of primes $p, p + 2$). So far, no one has solved the Riemann Hypothesis and the problem remains open. It is in fact one of the Millennium Prize Problems (see section 5).

Problem nine tasked the community to generalise quadratic reciprocity for arbitrary powers in an algebraic number field. This problem was partially resolved in 1927 by Emil Artin, but the case of a non-abelian number field is still open.

The tenth problem is one of algorithmic nature. It asks that an algorithm be found which can either prove or disprove the statement that a certain diophantine equation with integer coefficients and any number of unknowns has integer solutions. In 1970, Yuri Matiyasevich, working on foundations provided by Julia Robinson, proved that no such algorithm existed.

Problem eleven was phrased as a furthering of the field of quadratic forms and solving a given quadratic equation in any number of variables. Credit for the solution to this is generally given to Helmut Hasse in 1923, a result extended by Siegel in the 1930s.

Problem number twelve proposed an extension of Kronecker's theorem on Abelian extensions of the rational numbers to any base number field. Although the problem has received much attention, and indeed some specific fields have been solved, the general case remains open.

The thirteenth problem appears fairly simple at the outset, it asks, generally, if it is possible to construct a solution to the equation $x^7 + ax^3 + bx^2 + cx + 1 = 0$ using a finite number of two-variable functions. This was proven possible in 1957 by Vladimir Arnold.

Problem fourteen asked whether certain rings are finitely generated. In 1959, Masayoshi Nagata found a counterexample, thus disproving the conjecture.

The fifteenth problem asked for a rigorous foundation of the so-called *Schubert calculus*. This is generally considered to have been achieved through work by van der Waerden, developing algebraic topology in the process. Others argue that the problem encompasses enumerative geometry as well, and it is less clear whether such a foundation has been achieved in this field.

Number sixteen is generally considered to be a two-part problem. The first part, an investigation into the relative positions of the branches of algebraic curves of order n , and then to extend this analysis to algebraic surfaces, was derived from work by Harnack and Hilbert. The second part concerned limit cycles of polynomial vector fields - a closed solution curve that all other solution curves converge to. This part was thought to have been partly solved by Henri Dulac, but his proof was flawed, and replaced by those of Ilyashenko and Écalle. The problem

is still considered unsolved, as is Hilbert's suggestion that the number of limit cycles depended only on the degree of the polynomials.

The seventeenth problem, that of expressing definite rational functions (functions which take value strictly greater than 0 over all values of variables) as quotients of sums of squares, has been solved several times. It was solved in 1927 by Emil Artin for closed fields such that -1 was not a sum of squares. Further work was devoted by finding other methods to solve the problem. Dubois showed that the conjecture is not true for all fields, and that some restrictions must be applied. However, Pfister showed that for fields where it did hold, the necessary number of squares was dependant only on the number of variables, not on the equation itself.

The eighteenth problem is commonly split into three parts. The first asks whether Euclidean n -dimensional space admits only finitely many patterns - ie how many different sorts of tiles there are that completely fill the space. This was confirmed in 1910 by Bierbach - there are 17 for the 2D plane, 219 for 3D space. Part two asked whether there are regions which can tile a plane but are not fundamental domains (an object or pattern that is a part of the pattern, as small as possible, which, based on the symmetry, determines the whole object or pattern) of a group. The answer again is yes, the first example being found in 1932 by Heesch. The third part asked what the densest unit-radius sphere-packing arrangement for 3D space was. The general consensus is that the face-centred-cubic, with slightly more than 74% filled, is the densest arrangement, but no proof has been forthcoming.

The nineteenth problem asked whether the solutions to Lagrangians are al-

ways analytic. Ennio de Giorgi proved this was true in his 1904 doctoral thesis.

Problem number twenty asked whether all boundary value problems have solutions. This has been proved true for the non-linear case.

The twenty-first problem, commonly called the *Riemann-Hilbert problem*, asks for a proof of the conjecture that there always exists a linear differential equation having prescribed singular points and monodromic group. However, there is no consensus on quite what the question means, and thus whether or not it has been solved.

Problem twenty-two is considered by some to be a special case of the twenty-first. It entails the uniformisation of analytic relations by means of automorphic functions. It was resolved by Paul Koebe in the early 20th century.

The final problem asks for the further development of calculus of variations, and was detailed by Hilbert in extreme length. This has been worked on extensively by any number of mathematicians, and is considered to be resolved.

In 2000, Rüdiger Thiele, a German historian, discovered a 24th problem in notes on Hilbert's original manuscript. It describes a quest in Proof Theory for a criterion for simplicity. However, this question was omitted by Hilbert for unknown reasons.

3 Problem 1 - Cantor's Problem of the Cardinal Number of the Continuum

The Continuum Hypothesis was first investigated by Georg Cantor as part of his study of the transfinite, and was considered so important that Hilbert made it the first problem. It asks, in simple terms, whether there exist any sets whose size is between that of the set of natural (counting) numbers, and the set of real numbers. I will first give a basic introduction to set theory, allowing us to see from where the Continuum Hypothesis arises, then will attempt to follow Paul Cohen's method to show that it is neither provable nor disprovable (thus proving its independence).

Hilbert phrased the problem thus:

Two systems, ie, two assemblages of ordinary real numbers or points, are said to be (according to Cantor) equivalent or of equal cardinal number, if they can be brought into a relation to one another such that to every number of the one assemblage corresponds one and only one definite number of the other. The investigations of Cantor on such assemblages of points suggest a very plausible theorem, which nevertheless, in spite of the most strenuous efforts, no one has succeeded in proving. This is the theorem:

Every system of infinitely many real numbers, ie, every assemblage of numbers (or points), is either equivalent to the assemblage of natural integers, 1, 2, 3,... or to the assemblage of all real numbers and therefore to the continuum, that is, to the points of a line; as regards equivalence there are, therefore, only two assemblages of numbers, the countable assemblage and the continuum.

From this theorem it would follow at once that the continuum has the next cardinal number beyond that of the countable assemblage; the proof of this theorem

would, therefore, form a new bridge between the countable assemblage and the continuum.

Let me mention another very remarkable statement of Cantor's which stands in the closest connection with the theorem mentioned and which, perhaps, offers the key to its proof. Any system of real numbers is said to be ordered, if for every two numbers of the system it is determined which one is the earlier and which the later, and if at the same time this determination is of such a kind that, if a is before b and b is before c , then a always comes before c . The natural arrangement of numbers of a system is defined to be that in which the smaller precedes the larger. But there are, as is easily seen, infinitely many other ways in which the numbers of a system may be arranged.

If we think of a definite arrangement of numbers and select from them a particular system of these numbers, a so-called partial system or assemblage, this partial system will also prove to be ordered. Now Cantor considers a particular kind of ordered assemblage which he designates as a well ordered assemblage and which is characterized in this way, that not only in the assemblage itself but also in every partial assemblage there exists a first number. The system of integers $1, 2, 3, \dots$ in their natural order is evidently a well ordered assemblage. On the other hand the system of all real numbers, ie, the continuum in its natural order, is evidently not well ordered. For, if we think of the points of a segment of a straight line, with its initial point excluded, as our partial assemblage, it will have no first element.

The question now arises whether the totality of all numbers may not be arranged in another manner so that every partial assemblage may have a first element, ie, whether the continuum cannot be considered as a well ordered assemblage - a question which Cantor thinks must be answered in the affirmative. It appears to me most desirable to obtain a direct proof of this remarkable statement

of Cantor's, perhaps by actually giving an arrangement of numbers such that in every partial system a first number can be pointed out.

3.1 An Introduction to Set Theory

The basic idea of a set is fairly simple - it is a collection of objects. For instance, we could have the set of all CDs owned by Richard Madeley, the set of all square numbers, the set of all equations with a root at $x = 0$, the set of all cats with purple fur. However, sets are not physical - if we took all Richard Madeley's CDs, we would not have a set of them. Sets are abstract, intangible, collections of objects bound together by some property - even if that property is solely that we choose to visualise them as bound together. We call each object (a) in the set (S) an element, and say that that a is a member of S ($a \in S$). If an object b is not in S , then we say b is not an element of S ($b \notin S$).

When mathematicians talk of sets, they generally mean a set of numbers, or, recursively, a set of sets. However, we have to be careful as it is easy to create a contradiction - for example, let X be the set of all sets which do not contain themselves. If $X \in X$, then clearly X contains itself and thus $X \notin X$.

3.1.1 Axioms of Set Theory

We can now discuss axiomatic set theory, in this case, Zermelo-Frankel Set Theory (ZF). By repeated application of these axioms, we may formulate our theories of sets.

- **The Axiom of Existence** - there exists a set which has no elements. We call this set the empty set, and denote it by \emptyset , or, alternatively, $\{\}$.
- **The Axiom of Extensionality** - If $\forall x \in X, x \in Y$ and $\forall y \in Y, y \in X$ then $X = Y$. This further implies that \emptyset is the only set with no elements,

and that each set is determined by its elements.

- **The Axiom of Comprehension** - Let $\mathbf{P}(x)$ be a property of x . For any set S , there exists a set T such that $x \in T$ if and only if $x \in S$ and $\mathbf{P}(x)$. Technically this is not one axiom, but an infinity of them since there is one for each property $\mathbf{P}(x)$.

At this point, it is sensible to define the standard syntax for a set:

$\{x \in S \mid \mathbf{P}(x)\}$ is the set of all $x \in S$ such that $\mathbf{P}(x)$ is true.

- **The Axiom of Pair** - For any sets S, T , $\exists U$ such that $x \in U$ if and only if $x = S$ or $x = T$. Thus $C = \{S, T\}$, and is unique. We call this an *unordered pair*.
- **The Axiom of Union** - For any set S , $\exists U$ such that $x \in U$ if and only if $x \in T$ for some $T \in S$. U is called the *union* of S ($\bigcup S$).

We now define the notion of a subset. A subset T of S ($T \subseteq S$) is a set such that $\forall x \in T, x \in S$. A proper subset T of S ($T \subset S$) is a subset such that $T \neq S$.

- **The Axiom of Power Set** - For any set S , there exists a set P which contains all subsets of S as elements (if $T \subseteq S$, then $T \in P$). We call this set the *Power Set* of S , and denote it $\mathcal{P}(S)$.
- **The Axiom of Choice** - If $a \rightarrow S_a \neq \emptyset$ is a function defined for all $a \in T$, then $\exists f(a)$ such that $\forall a \in T, f(a) \in S_a$. ie, given any sets, we can “choose” elements from them to create new sets, even if we have no explicit property to choose them with. This axiom is fairly controversial, and is excluded from normal ZF. If we include the Axiom of Choice (AC), then we call the system ZFC - Zermelo-Frankel with Choice.

3.1.2 Ordered Pairs and Binary Relations

Now we can introduce the idea of an ordered pair. We have seen that an unordered pair is a set $\{a, b\}$. We define an *ordered pair*, (a, b) as $\{\{a\}, \{a, b\}\}$. Unlike an unordered pair, $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$. We can use ordered pairs to define the notion of the *cross product* of two sets S and T . $S \times T = \{(s, t) \mid s \in S, t \in T\}$.

From this, we can define a *binary relation*. A set R is a binary relation if all elements of R are ordered pairs. We write xRy instead of $(x, y) \in R$. From this we can also define ordered triples $((a, b), c) = (a, b, c)$, and thus ordered n-tuples. There are various types of binary relations. Let R be a relation in some set S :

- **Reflexivity** - R is *reflexive* in S if $\forall x \in S, xRx$
- **Symmetry** - R is *symmetric* in S if $\forall(x, y) \in S$ such that xRy, yRx
- **Antisymmetry** - R is *antisymmetric* in S if $\forall(x, y) \in S$ such that xRy and yRx , then $x = y$.
- **Asymmetry** - R is *asymmetric* in S if $\forall(x, y) \in S$ such that xRy then yRx does not hold.
- **Transitivity** - R is *transitive* in S if $\forall(x, y), (y, z) \in S$ such that xRy and yRz , then xRz .

We are now in a position to discuss orderings of sets. A binary relation R in S which is reflexive, antisymmetric and transitive is called a *partial ordering*. For instance, \leq is a partial ordering in \mathbb{R} . We say the pair (S, R) is an *ordered set*. A binary relation which is both transitive and asymmetric, but not reflexive is called a *strict ordering* (for instance, $<$ in \mathbb{R}). A *well-ordering* of a set is an ordering such that all non-empty subsets have a least element. We say an ordering is *linear* or *total* if we can compare the position in the ordering of any two

elements of the set.

We also need to briefly discuss ordinals - ordinals can be seen as generalisations of the natural numbers, but more specifically are sets ordered by \in and which are transitive. We write $On(a)$ to mean that a is an ordinal. We further define *rank* as the smallest ordinal greater than the rank of all members of the set, with the rank of \emptyset defined as 0. We also define ω as the first infinite ordinal.

3.1.3 Cardinality

At this point, it makes sense to introduce the concept of the size of a set. For this, we define the *cardinality* of a set, $|S|$, as the number of elements the set contains. For instance, if we take the set $A = \{a < 5 \mid a \in \mathbb{N}\}$, where $\mathbb{N} = \{1, 2, 3, \dots\}$ denotes the set of all natural numbers, it is obvious that $|A| = 4$. This set is obviously finite. Indeed, we define a set S as finite if $|S| \in \mathbb{N}$. If a set is not finite, then it is said to be *infinite*. We say that two sets A and B are *equipotent* (have equal cardinality, $|A| = |B|$) if there exists some one-to-one function f with domain A and range B . A has cardinality less than or equal to that of B ($|A| \leq |B|$) if there exists some one-to-one mapping of A into B .

From this, we can deduce that for a finite set S , there is no one-to-one mapping from S onto any proper subset of S .

We can do arithmetic with cardinal numbers. If two sets are disjoint (they have no common elements - any two sets S and T are disjoint if $S \cap T = \emptyset$, where \cap means the intersection between two sets), then the cardinality of their union is equal to the sum of their individual cardinalities. Generally, for any two sets S and T , $|S \cup T| = |S| + |T| - |S \cap T|$. We can also define the cardinality of the cross product of two sets: $|S \times T| = |S||T|$, and hence see that $|S|^n = |S^n|$.

It is of vital importance that we look at the cardinality of the power set. As stated before, the power set of a set is the set of all subsets of that set. Say we look at the power set $\mathcal{P}(S)$ where $|S| = n$. The number of subsets of S with cardinality $r \leq n$ is $\binom{n}{r} = \frac{n!}{(n-r)!r!}$. Since $\sum_{r=0}^n \binom{n}{r} = 2^n$, it is clear that $|\mathcal{P}(S)| = 2^{|S|}$. This is obviously true for finite sets, but there is no real meaning for infinite sets since 2^∞ has no value. However, it is still used as notation for the cardinality of the power set of an infinite set.

We noted earlier a finite set as being a set for which there is no one-to-one mapping of that set onto a proper subset of that set. Thus, we can obviously define an infinite set as being a set where a one-to-one mapping of itself onto a proper subset of itself does exist. For example, the mapping in \mathbb{N} of $n \mapsto n + 1$ shows that \mathbb{N} is infinite. In fact, we say this set is *countably infinite*, since we can order the set in a way that we can count it (obviously $1, 2, 3, \dots$). We define $|\mathbb{N}| = \aleph_0$, and further state that a set is countable if there exists a bijection between it and \mathbb{N} .

\aleph_0 is an interesting number - since it is infinite, for any $n \in \mathbb{N}$, $\aleph_0 + n = \aleph_0$, $n \times \aleph_0 = \aleph_0$, and $(\aleph_0)^n = \aleph_0$. We define \aleph_1 as the next highest cardinal number after \aleph_0 , \aleph_2 as the one after that, etc.

We have shown that \mathbb{N} is countable, now let us turn our attention to \mathbb{Z} , the integer set. It is obviously infinite, and we can create a bijection between \mathbb{Z} and \mathbb{N} using the sequence $0, 1, -1, 2, -2$, etc. Thus $|\mathbb{Z}| = |\mathbb{N}| = \aleph_0$.

The next obvious candidate is the set of rational numbers, $\mathbb{Q} = \{\frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{N}\}$. However, let us start with the set $\mathbb{Q}_+ = \{\frac{a}{b} \mid a, b \in \mathbb{N}\}$. We cannot numerate these using $>$, as given any two numbers $\frac{a}{b} < \frac{c}{d}$, we can define $\frac{e}{f}$ such that $\frac{a}{b} < \frac{e}{f} < \frac{c}{d}$. Between any two rational numbers lies a further infinity of rational numbers. Thus we must find another way. Cantor used the sequence $\frac{1}{1}, \frac{2}{1}, \frac{1}{2}, \frac{1}{3}, \frac{2}{2}, \frac{3}{1}, \frac{1}{4}, \frac{2}{3}, \frac{3}{2}, \dots$. This sequence can be used to generate every rational

number greater than zero. By this argument, we can say that $|\mathbb{Q}_+| = \aleph_0$, and from the argument for $|\mathbb{Z}|$, state further that $|\mathbb{Q}| = \aleph_0$.

So, we come to the real numbers. Following Cantor's proof, we first assume that \mathbb{R} is the range of some infinite sequence $\langle r^n \rangle_{n=1}^\infty$, and further let $r^n = x_0^n . x_1^n x_2^n x_3^n \dots$ (note this defines that \mathbb{R} is countable. We assume that all r^n are unique, so \nexists any m such that r^m has only 9s after a certain point). We now create another number, y such that $y_m = x_m^n + 1$ (modulo 10). Thus by construction, $y \neq r^n \forall n \in \mathbb{N}$, thus this number (which is obviously real) is not in our list of real numbers - a contradiction. Thus we have shown that \mathbb{R} is uncountable.

3.1.4 The Cardinality of \mathbb{R}

Now, we wish to find the cardinality \mathbb{R} . However, we must first work out how to define \mathbb{R} in terms of sets we already know about - \mathbb{Q} for instance. We first need to know more about *orderings*.

It is clear that \mathbb{N} , \mathbb{Z} and \mathbb{Q} are different, even though they have the same cardinality. In order to distinguish between them properly, we need to look at how they are ordered. For instance \mathbb{N} and \mathbb{Z} differ in that \mathbb{N} has a least element: 1, while \mathbb{Z} does not. Similarly, \mathbb{Q} and \mathbb{Z} differ in that between any two numbers $x, y \in \mathbb{Z}$, there are only finitely many integers, but infinitely many rationals. We defined ordering before (3.1.2). Now, we define a set $(S, <)$ as *dense* if it has at least two elements and $\forall a, b \in S, a < b \Rightarrow \exists s \in S$ such that $a < s < b$. By our previous notes about \mathbb{Q} , it is clear that \mathbb{Q} is dense.

For any dense, linearly ordered set $(S, <)$ without endpoints, there exists a complete linearly ordered set.

We define a *gap* in a linearly ordered set $(S, <)$ as a pair (A, B) of sets such that A and B are non-empty disjoint subsets of S with $A \cup B = S$; and $\forall a \in A, b \in B; a < b$, and A does not have a greatest element, nor B a least element.

A dense, linearly ordered set with no gaps is said to be *complete*.

We can now see that we could have shown that \mathbb{R} was uncountable by noting that $(\mathbb{R}, <)$ is a dense linear ordering without endpoints. If it were countable, it would be isomorphic to \mathbb{Q} , but this is impossible since \mathbb{R} is complete but \mathbb{Q} is not.

We now define a *cut* of a set S as a pair of sets (A, B) such that A and B are disjoint non-empty subsets of S with $S = A \cup B$ and $\forall a \in A, b \in B; a < b$. A gap is a special form of a cut, which is only applicable to incomplete sets. If S is dense, then it is impossible for A to have a greatest element and B to simultaneously have a least element.

For any dense, linearly ordered set $(S, <)$ without endpoints, there exists a complete linearly ordered set without endpoints (T, \prec) such that $S \subseteq T$; if $a, b \in S$, then $a < b \Leftrightarrow a \prec b$; S is dense in T ($\forall a, b \in S, \exists c \in T$ such that $a \prec c \prec b$). (Proof: [9], pp87-89). If we set $(S, <) = (\mathbb{Q}, <)$, then $(T, \prec) = (\mathbb{R}, <)$. Thus, we have defined the real numbers from \mathbb{Q} .

We can now see that the set of all sets of natural numbers is uncountable. Obviously the function $f(n) : \mathbb{N} \rightarrow \mathcal{P}(\mathbb{N}) = \{n\}$ is one-to-one, hence $|\mathbb{N}| \leq |\mathcal{P}(\mathbb{N})|$. For every sequence $\langle S_n | n \in \mathbb{N} \rangle$ of subsets of \mathbb{N} , $\exists S \neq S_n \forall n \in \mathbb{N}$. We define $S = \{n \in \mathbb{N} | n \notin S_n\}$. Hence, if $n \in S_n$, then $n \notin S \Rightarrow S \neq S_n$; and if $n \notin S_n$, then $n \in S \Rightarrow S \neq S_n$. Thus, there is no mapping of \mathbb{N} onto $\mathcal{P}(\mathbb{N})$, hence $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$.

So, back to the cardinality of \mathbb{R} . We defined the real numbers as cuts in \mathbb{Q} . The function that assigns to each $r = (A, B) \in \mathbb{R}$ the set $A \subseteq \mathbb{Q}$ is a one-to-one mapping from \mathbb{R} into $\mathcal{P}(\mathbb{Q})$. Thus, $|\mathbb{R}| \leq |\mathcal{P}(\mathbb{Q})| = |\mathcal{P}(\mathbb{N})|$. Introducing the *characteristic function* of a set, $\chi_S(n)$, which takes value 0 if $n \in S$, and 1 otherwise. Obviously, for each subset of \mathbb{N} , there are \aleph_0 values in the domain of the characteristic function, hence there are $|\{0, 1\}^{\aleph_0}|$ values which the characteristic

function can take - one for each subset of \mathbb{N} , hence there is a one-to-one mapping of $\mathcal{P}(\mathbb{N})$ onto $2^{\aleph_0} \Rightarrow |\mathcal{P}(\mathbb{N})| = |2^{\aleph_0}|$.

We also see that each unique infinite sequence of 0s and 1s is a unique decimal expansion of some real number, thus $2^{\aleph_0} \leq |\mathbb{R}|$. Therefore we have $|\mathcal{P}(\mathbb{N})| = 2^{\aleph_0} \leq |\mathbb{R}| \leq |\mathcal{P}(\mathbb{N})| \Rightarrow |\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$.

2^{\aleph_0} has similar properties to \aleph_0 : any finite or countable number multiplied by 2^{\aleph_0} is 2^{\aleph_0} , and $(2^{\aleph_0})^n = 2^{\aleph_0} (n \in \mathbb{N})$. Also by this property, $2^{\aleph_0} - \aleph_0 = 2^{\aleph_0}$.

We now understand the properties of \aleph_0 and 2^{\aleph_0} . However, we must ask - how much bigger than \aleph_0 is 2^{\aleph_0} ? However, as noted above, $2^{\aleph_0} - z$ where z is at most finite is still 2^{\aleph_0} , so that isn't much help. Instead, we ask *does there exist a smaller uncountable number than 2^{\aleph_0}* ?. Or, put another way, does $2^{\aleph_0} = \aleph_1$?. This is the basic question of the Continuum Hypothesis (CH). The more general version *Generalised Continuum Hypothesis*, (GCH) asks if $\aleph_{n+1} = 2^{\aleph_n} \forall n \in \mathbb{N}$.

3.2 Foundations in Logic - Gödel's Theorems

Mathematics is based on logic, and thus must follow its rules. Already in this text, we have used logic without really thinking about it. A founding principle of logic is that of *consistency*. A set of statements, S , is consistent if they cannot be used in any combination to form the contradiction that both A and *not* A are simultaneously true for any A . For instance, the set of statements $x = 1$, $x = y$, $y = 2$ is inconsistent because it leads to the contradiction $1 = 2$.

Let us consider a set of statements S containing statements c_1, c_2, \dots, c_n , and M be another set of statements containing d_1, d_2, \dots, d_m , and there exists some map $c_i \rightarrow d_j$, then M is a *model* for S if all the statements of S are true in M . If A is a valid statement, it is true in every model, and if a S has a model then it is consistent.

Kurt Gödel proved in 1929 the important result that for any consistent set of

statements S , there exists a model, M , for S such that $|M| \leq |S|$ if S is infinite, and $|M|$ is countable if S is finite. I omit the proof here, but it can be found in [5] pp13-17. This is known as the *Gödel Completeness Theorem*. However, Gödel is also known for his *Incompleteness Theorem*, which is of critical importance to us. It states, in general terms, that in any axiom scheme Z whose axioms are given by some recursive rule, the consistency of Z cannot be proven in Z . Again, the proof can be found in [5].

We also introduce at this point the *Löwenheim-Skolem Theorem*. It states that for some formula A in ZF, it can be proven that for any set S , there is a set $S' \supseteq S$ with $|S'| = \max(\aleph_0, |S|)$ and $\forall x \in S, A(x) \Leftrightarrow A_{S'}(x)$. $A_{S'}$ is the formula A with all variables restricted to S' .

3.3 Proving the consistency of the Continuum Hypothesis

Throughout this section, we will be using ZF, ie excluding the Axiom of Choice. Our goal is to give Gödel's argument that if ZF is consistent, then so is ZFC+CH (Zermelo-Frankel with the Continuum Hypothesis and the Axiom of Choice).

We first define a certain sequence of sets, M_α by $M_0 = \emptyset$ and $M_\alpha = \bigcup_{\beta < \alpha} M_\beta$, given that α is an ordinal ($On(\alpha)$). We then define a set S as *constructible* if $\exists \alpha$ such that $On(\alpha)$, and $S \in M_\alpha$. We now denote the "class" of constructible sets by L , but note that $S \in L$ means that S is constructible, not that L is a set. For any formula A , A_L denotes the same formula with the restriction that all variables are constructible. We further define the universal class as V . From this, we define the *Axiom of Constructability* as the statement that every set is constructible, $V = L$. Since our definition of M_α can be defined by simple induction, it can be formalised in ZF, thus $V = L$ is a single statement in ZF. The result is thus:

- If A is an axiom of ZF, then A_L is provable in ZF.

- $(V = L)_L$ is provable in ZF.
- $(V = L) \Rightarrow$ AC and GCH is provable in ZF.

However, we must still prove these. So...

3.3.1 Proof that A_L is provable in ZF

We must prove that each of our axioms of ZF, when restricted to the class of constructible sets, is still true. We note that if $x \in S$ and $S \in M_\alpha$, then $x \in M_{\alpha-1} \subseteq M_\alpha$.

- **Axiom of Existence** - This is obviously true since $M_0 = \emptyset$, and thus $\emptyset \in L$.
- **Axiom of Extensionality** - $x \in X_L \rightarrow x \in L$. Hence, $\forall x \in X_L, x \in Y$ and $\forall y \in Y, y \in X_L \rightarrow y \in L \rightarrow Y \in L$.
- **Axiom of Comprehension** - Let $\mathbf{P}_L(x)$ be the property $\mathbf{P}(x)$ relativised to L , such that it defines a bijection in L , with some range v on some set $u \in L$. $\exists \alpha$ such that $v \subseteq M_\alpha$. Let us now define $M'_\alpha \supseteq M_\alpha$ such that $\forall x \in M'_\alpha, \mathbf{P}(x) \Leftrightarrow \mathbf{P}_{M'_\alpha}(x)$. $M'_\alpha \in M_\beta$ for some β , so since $\forall y \in v, y \in M'_\beta$, $v \in L$.
- **Axiom of Pair** - Let $S \in M_\beta, T \in M_\alpha, \beta \leq \alpha$. Then $S, T \in M_\alpha$. $\{S, T\} = \{x | x \in M_\alpha, (x = S \text{ or } x = T)\}$, and so $\{S, T\} \in M_{\alpha+1}$, and thus $\{S, T\} \in L$.
- **Axiom of Union** - If $S \in M_\alpha$, then $\bigcup S = \{x | x \in M_\alpha \text{ and } \exists T \in S \text{ such that } x \in T\} \subseteq M_{\alpha+1}$. Hence, $\bigcup S \in L$.
- **Axiom of Power Set** - Let $S \in L$ and $\mathcal{P}_L(S) = \{x | x \in \mathcal{P}(S) \text{ and } x \in L\}$. For each $x \in \mathcal{P}_L(S)$, let $\theta(x)$ be the least α for which $x \in M_\alpha$. Then, let

$\beta = \max(\theta(x))$. Thus, $x \in M_\beta$. Now consider $\{x \mid x \in M_\beta \text{ and } \forall t, t \in M_\beta \rightarrow t \in x \rightarrow t \in S\}$. This set is clearly constructible, and is equal to $\mathcal{P}_L(S)$.

Thus, we have shown that the axioms of ZF are provable in ZF when limited to the constructible class.

3.3.2 Proof that $(V = L)_L$ is provable in ZF

This is fairly intuitive, since when restricted to the constructible case, the universal class is obviously constructible.

3.3.3 Proof that $(V = L) \Rightarrow \mathbf{AC}$ and \mathbf{GCH}

We first define the notion of a primed set, eg X' . If A is some function, then $X' = X \cup \{Y \mid \forall A, Y = \{z \in X \mid A_X(z)\}\}$.

It can be shown ([5], p95) that for any set X , there exists a well-ordering of that set which induces a well-ordering of X' . We can define a well-ordering on M_α - if we have defined the well-ordering for all $\beta < \alpha$, then we can well-order $M_\alpha = \bigcup_{\beta < \alpha} M_\beta$ in an obvious way. Thus we can define a well-ordering on M_α . Assuming $V = L$, define $\theta(x) =$ the least α such that $x \in M_\alpha$, and hence define $x < y$ if and only if $\theta(x) \leq \theta(y)$ and x precedes y in the well-ordering of M_α . Thus, we have a single formula which well orders **all** sets, and hence we have shown that $(V = L) \Rightarrow$ Axiom of Choice. We now must show that this leads us to the Generalised Continuum Hypothesis.

First, we note that if $S \in M_\alpha$, with infinite α and $T \subseteq S$, then $\exists \beta$ with $|\beta| = |\alpha|$ such that $T \in M_\beta$.

There is an extensional set T ($x, y \in T$ and $x \neq y \Rightarrow \exists z \in T$ such that z is in exactly one of x and y), with $|T| = |\alpha|$, such that $M_\alpha \subseteq T$ and $M_\beta, \beta \in T$, such that $(\beta \text{ constructs } M_\beta)_T$ is valid. To prove this, we note that the statement says that there is a function in ZF, defined for all $\gamma < \beta$ such that $\forall \gamma, f(\gamma) =$

$(\bigcup_{\delta < \gamma} f(\delta))'$ and $f(\beta) = M_\beta$. This then follows using the Löwenheim-Skolem Theorem.

For all infinite α , $|\alpha| = |M_\alpha|$ (proved by induction on α). If α is a cardinal number, then $\alpha \in M_{\alpha+1}$, and thus if β is the next cardinal number after α , then $\mathcal{P}(\alpha) \subseteq M_\beta \Rightarrow |\mathcal{P}(\alpha)| \leq |\beta|$. We know already that $|\mathcal{P}(\alpha)| > |\alpha|$, hence $|\mathcal{P}(\alpha)| = |\beta|$, ie $2^{\aleph_\alpha} = \aleph_{\alpha+1}$. Thus, we have shown that the Axiom of Choice and the Generalised Continuum Hypothesis are consistent with Zermelo-Frankel set theory, and indeed hold in the case that all sets are constructible. However, this does not mean we have proved that the CH is true.

3.4 Independence of the Continuum Hypothesis

Having shown that the GCH is compatible with ZF, we now need to show that it cannot be proven from ZF. The best way to do this is to show that we can create a model for ZF in which the GCH is false. I am following Cohen's proof from [5], however, I freely admit that there are parts of this proof that I do not fully understand, specifically the end of the passages on forcing, and the idea of generic sets. However, I hope that my presentation of the proof is nonetheless comprehensible.

First, we need to look into the basic ideas of model theory. The *Standard Model Axiom* (SM) states that there is a set M such that under some relation $R = \{\langle x, y \rangle | x \in y, x, y \in M\}$ is a model for ZF. (This is however unprovable, since it implies the consistency of ZF (Gödel Incompleteness Theorem)). However, let us consider M , for now, to be an uncountable model, with $\alpha_0 = \sup\{\alpha | \alpha \in M, \text{On}(\alpha)\}$, and assume the the Axiom of Choice holds. Then if α_0 is uncountable, M contains all countable ordinals. Otherwise, there must be some $\beta < \alpha$ such that the set of all elements of M with rank β is uncountable.

Thus, M contains a set which is uncountable but well-ordered (AC), and thus M contains an uncountable ordinal, which is a contradiction. Thus α is uncountable. From $V = L$, we know that every real number is constructible from a countable ordinal, thus every real number is constructible in M , ie $\mathbb{R} \in L$, with $|\mathbb{R}| = \aleph_1 \Rightarrow$ There is a map from the countable ordinals (relative to L) onto \mathbb{R} , and thus \exists a map from \aleph_1 onto \mathbb{R} . Hence, if our model is uncountable, we cannot create a model in which AC holds but the CH does not. Cohen thus uses a countable model for ZF.

We shall begin with model M , defined as $\bigcup\{M_\beta|\beta < \sup\{\alpha|\alpha \in M, On(\alpha)\}\}$. This is the *minimal model*, and we shall henceforth use N as our model as we add various sets to it. We must use the ordinals in M and therefore construct N by broadening M with extra sets of rank α where $\alpha < \alpha_0 = \sup\{\alpha|\alpha \in M, On(\alpha)\}$. We wish to add sets $a \subseteq \omega$ such that $a \in N, a \notin M$. If $a \in N$, then all sets constructible from it must also be in N . Let $M_0(a) = \omega \cup \{a\}$ and $M_\alpha(a) = \bigcup_{\beta < \alpha} M_\beta(a)$. Thus N is of the form $\bigcup\{M_\beta(a)|\beta < \alpha_0\}$.

Cohen's breakthrough in the analysis of the Continuum Hypothesis was to introduce the concept of *forcing*. Thus far, working solely from ZF, we only know that $2^{\aleph_0} > \aleph_0$, although we know that CH is consistent with ZF. It is therefore necessary to add "new" sets to obtain a model where $2^{\aleph_0} > \aleph_1$.

Let us consider a single set of natural numbers, X . It must be realised that we cannot expect to have complete information about X . If we knew a property which could completely define X , then we could simply state $X = \{n \in \mathbb{N}|\mathbf{P}(n)\}$, and would note that this set was already in our model, and thus disregard it. Cohen realised that partial descriptions are sufficient, describing X with a collection of approximations in much the same way we can approximate irrational numbers

by rationals. We create a finite sequence of 0s and 1s, and call these *conditions*, with the k^{th} entry giving information about the presence (or not) of the number k (counting from 0). A 0 indicates that $k \notin X$, a 1 that $k \in X$. For instance, $\langle 1, 0, 0, 0, 1 \rangle$ would tell us that $0, 4 \in X$ and $1, 2, 3 \notin X$.

Adding in our set X gives rise to further new sets created by interactions between X and other sets in our model. For instance, we would now have sets such as $X \times Y$ (for some $Y \in M$), $\mathcal{P}(X)$, etc. Each condition allows us to draw conclusions about other sets in our universe. We say p forces \mathbf{P} ($p \Vdash \mathbf{P}$). For instance, $\langle 1, 0, 0, 0, 1 \rangle \Vdash \{0, 4\} \in X \times \mathbb{N}$. This means that *if* $0, 4 \in X$ and $1, 2, 3 \notin X$, *then* $\{0, 4\} \in X \times \mathbb{N}$. Forcing conditions can clash, and we only know which of the results is correct if we know about X - ie which of the conditions is true. There are however some conditions which can be decided. First, it is necessary to note that anything that can be deduced from, say, a length three condition, can also be deduced from that same condition, followed by some arbitrary series of 1s and 0s. For instance whatever can be deduced from $\langle 1, 0, 0 \rangle$ can also be deduced from $\langle 1, 0, 0, 1, 0, 1, 0, \dots \rangle$. From this we know that X is infinite, since if we said that some condition p forces X to have n elements, then we could create a condition q , which contains p , but also forces X to have more than n elements. Similarly, we can conclude that X is different from any other set in our model.

It is helpful here to define a *subcondition*. This works much like a subset, and in fact we use the same notation. p is a subcondition of q ($p \subseteq q$) if q contains p . $\langle 1, 0 \rangle \subseteq \langle 1, 0, 0, 1 \rangle$.

Forcing has some interesting properties - for instance, p forces A is not the same as p forces *notnot* A . However, it is still true that one condition cannot force a statement and its negative. Also, for all conditions p and statements A , $\exists q \supseteq p$ such that $q \Vdash A$ or $q \Vdash \text{not}A$.

We need to introduce the idea of forcing to our model. We define a *complete sequence* of forcing conditions, $\{P_n\}$, as a sequence of conditions such that $\forall n, P_n \subseteq P_{n+1}$, and for any statement A , $\exists n$ such that P_n either forces A or *not* A . We can prove the existence of this sequence, since as M is countable, we can number all statements it contains, and define P_n as $Q \supseteq P_{n-1}$ such that Q forces either A_n or *not* A_n . Indeed, for each k , some P_n forces either $k \in a$ or $k \notin a$. From this, we define $\bar{a} = \{k \mid \exists n \text{ such that } P_n \text{ forces } k \in a\}$. We further say that in our model, N , a statement A is true if and only if $\exists n$ such that $P_n \Vdash A$.

So, having chosen a complete sequence $\{P_n\}$, with $N = \bigcup \{M_\beta(\bar{a}) \mid \beta < \alpha_0\}$, we now need to show that this is a model of ZF. Thus, we show that the axioms of ZF hold in N . However, this is fairly simple, being much like we showed in 3.3.1.

We now need to show that the GCH and AC hold in N . Since $M_0(\bar{a})$ is well-ordered, the same argument as in L (3.3.3) shows that there is a well-ordering of all N which has a single constant \bar{a} . We then follow the exact same argument as before, but replacing M_α with $M_\alpha(\bar{a})$.

Thus, we have now proved that in our model N , the GCH and AC hold, and that N is a model for ZF. Before continuing, we need to introduce the ideas of *labeling* and *the class of generic sets*. We first define a *labeling* as a mapping in ZF which assigns to each ordinal $0 < \alpha < \alpha_0$ a set S_α and function θ_α (defined in that set), such that the sets are disjoint, and if $c \in S_\alpha$, $\theta_\alpha(c)$ is a formula with all bound variables restricted to $X_\alpha = \bigcup_{\beta < \alpha} M_\beta(a)$, and which may have elements of S_β ($\beta < \alpha$) as constants. $S_0 = \omega \cup \{a\}$; $S = \bigcup_\alpha S_\alpha$. A certain subset G of S we call *generic sets*: if $c_\alpha \in S_\alpha - G$, the c is a formula which contains elements of X_α as constants, and has all bound variables restricted to that same set. We

can assume that for some $\alpha > \alpha_1$ (where α_1 is fixed), there is a bijection between these S_α and these formulae. This is all assumed to be in M .

Finally, we can move on to the proof of the independence of the Continuum Hypothesis. Let \aleph_τ be some cardinal in M , with $\tau \geq 2$. We define S as $\forall \alpha < \aleph_\tau, S_\alpha = \{c_\alpha\}$, and $\bar{c}_\alpha = \alpha$. $\forall \alpha, c_\alpha \in G$. For $\alpha = \aleph_\tau, S_\alpha$ has \aleph_τ elements, all in G , denoted by $a_\delta, \delta < \aleph_\tau$. Thus we have defined S_α . We can now define $S_{\alpha+1}$ and $S_{\alpha+2}$, though we are not really interested in these, so I omit it. $S_{\alpha+3} = \{W\}$, where $W \in G$ and $|S_{\alpha+3}| = 1$. $\bar{W} = \{\langle \delta, a_\delta \rangle | \delta < \aleph_\tau\}$.

In N , every set must be constructible from \bar{W} . Thus, if \bar{W} is the *transitive closure* of M_0 (smallest transitive relation on M_0 that contains the relation \in), and M_α is defined in the usual way, then $N = \bigcup \{M_\alpha | \alpha \in M\}$. We also note that the Axiom of Choice holds in N (M_0 is well ordered because of \bar{W} , hence so is N). We also require that if α, β are ordinals in M (and hence in N), and $|\alpha| < |\beta|$ in M , then the same holds true in N ([5], p132). From this, we know that all cardinals in M are also cardinals in N .

Here we come to the most important theorem: **in N , $|\mathbb{R}| \geq \aleph_\tau$, hence the Continuum Hypothesis is false in N .** This is because all our δ are distinct, hence $|\{\delta\}| \leq |\mathbb{R}|$. However, we know there are \aleph_τ δ s, thus $|\aleph_\tau| \leq |\mathbb{R}|$. Since $\tau \geq 2$, $|\aleph_2| \leq |\mathbb{R}|$, and hence the Continuum Hypothesis does not hold in N .

3.5 Conclusion

Thus, we have now shown that there exist models for Zermelo-Frankel set theory where the Continuum Hypothesis does hold, and also ones where it does not. At present, it appears that unless we can discover more axioms, the question will never be decided. Those newly discovered axioms would most likely be to restrict what sets we can use - for instance, $V = L$ as used in 3.3. Many

mathematicians, Cohen included, believe the Continuum Hypothesis is patently false, not to mention rather restricting. His personal view was that the way that the Continuum was generated - by use of the power set axiom - meant that $|\mathbb{R}|$ was larger than such cardinals such as $\aleph_{\aleph_0}, \aleph_{\aleph_{\aleph_0}}, \aleph_{\aleph_{\aleph_{\aleph_0}}}, \dots$. However, he did also mention one important idea - problems which cannot be solved in arithmetic, can be solved in set theory. It is quite possible that, if we call set theory a “higher” system than arithmetic, there exists some system higher than set theory, where such problems will be solvable. Of course, this system, by Gödel’s Incompleteness Theorem, will have further problems which would need to be solved in a yet higher system.

Another possibility is that set theory is akin to geometry. Geometry also has various axioms - for instance, in Euclidean geometry, we have the *Triangle Inequality*, that states that the distance between any two points A and B is equal to or less than the distance from A to some third point, C , to B . If we remove one of these axioms, we get a different sort of geometry, standing, as Hilbert put it, “next to” Euclidean geometry. In fact, this geometry is the *Minkowski Spacetime* in which Einstein’s theories of relativity are set. We could conceivably obtain new set theories, next to but incompatible with the standard Cantorian set theory. For instance, we could have a theory whereby the Continuum Hypothesis holds, or where $2^{\aleph_0} = \aleph_{42}$. Granted, these are not “nice” solutions to the problem, but could be avenues of further research.

4 Problem 3 - The equality of two volumes of two tetrahedra of equal bases and equal altitudes

We consider first an arbitrary shape on a piece of squared paper. A child, if asked how big the shape was, might count the number of squares that the shape encompassed totally. Another might count the number of squares that totally encompassed the shape. Doing so would yield an upper and lower bound for the area. By using smaller and smaller squares, we would refine our bounds for the area of the shape, until, if we could count infinitely small squares, we would know the exact area of the shape. We can apply the same concept to three dimensions - counting cubes for instance, and using smaller and smaller cubes until we were counting infinitely small cubes, thus finding the volume.

As we progress, we learn various tricks to avoid this counting. We develop formulae to tell us the volume of an object, for instance, the volume of a cube would be the length of one side taken to the third power. We unconsciously learn properties of volume - that it is conserved, for instance. If I take a model made of Lego, deconstruct it, and then rebuild it into a different shape, the volume of the model will be the same. We might even wonder whether, if we could break other things down into pieces, we could rebuild them into anything else that had the same volume. That is, in essence, the third problem. Hilbert phrased it thus:

In two letters to Gerling, Gauss expresses his regret that certain theorems of solid geometry depend upon the method of exhaustion, ie, in modern phraseology, upon the axiom of continuity (or upon the axiom of Archimedes). Gauss mentions in particular the theorem of Euclid, that triangular pyramids of equal altitudes are

to each other as their bases. Now the analogous problem in the plane has been solved. Gerling also succeeded in proving the equality of volume of symmetrical polyhedra by dividing them into congruent parts. Nevertheless, it seems to me probable that a general proof of this kind for the theorem of Euclid just mentioned is impossible, and it should be our task to give a rigorous proof of its impossibility. This would be obtained, as soon as we succeeded in specifying two tetrahedra of equal bases and equal altitudes which can in no way be split up into congruent tetrahedra, and which cannot be combined with congruent tetrahedra to form two polyhedra which themselves could be split up into congruent tetrahedra.

I will first give a general overview of the properties of volume, then look at two-dimensional case of this problem, and then present Hadwiger's proof that two solids of equal volume cannot necessarily be decomposed into each other.

I should note here that *congruence* means that given two shapes, one can be transformed into the other through a series of translations, reflections and rotations. However, from his formulation of the question, *volume of symmetrical polyhedra by dividing them into congruent parts*, it appears that Hilbert did not consider reflections to be allowable, which would after all be impossible working with real bodies. Thus, from here, I shall consider congruence as excluding reflections.

4.1 Properties of Volume

Throughout this chapter, I will be assuming that Euclidean geometry holds, as this is the one with which we are most familiar. As noted previously, we unconsciously learn the properties of volume through childhood play. However, we can formalise these properties thus:

- **Nonnegativity** - The volume function, V , is non-negative, ie, for any figure F , $V(F) \geq 0$.
- **Additivity** - If F and G are disjoint figures with measurable volume, then $V(F \cup G) = V(F) + V(G)$.
- **Invariance** - V is invariant under translations, reflections and rotations. If F is some figure, and F' is that figure after being translated, reflected or rotated, then $V(F) = V(F')$.
- **Normalisation** - The function V is normalised, ie, the unit cube (a cube with edges of length 1) has measurable volume equal to 1.

A *polyhedron* is defined as either a bounded, closed set in space, whose surface is the union of a finite number of planes; or as the union of a finite number of *tetrahedra* (the three-dimensional analog of triangles). It is relatively simple to show that all polyhedra are of measurable volume, since we just need to show that the volume of any tetrahedron is measurable. To do this, we use our idea of measuring the number of cubes contained in and containing the figure, and then let the length of the edge of the cubes tend to 0. We then find that the lower bound equals the upper bound, and thus we know that the tetrahedron is of measurable volume. We can also prove that a figure F is only measurable if for any arbitrary $\varepsilon > 0$, there exist figures G and H such that $G \subset F \subset H$ and $V(H) - V(G) < \varepsilon$. It is also intuitively obvious that given any two figures, any combination of them using the standard set operations \cup, \cap and \setminus is also measurable (or 0).

4.2 The 2-Dimensional Case

It is intuitively obvious to us that if two polygons are *equidecomposable* (one can be broken down into finite pieces and rearranged into the other. Some texts

call this *scissors congruence*), then they must have the same area. We use the notation $F \sim G$ to denote equidecomposability. We can then ask whether the reverse is true, ie does $F \sim G \Leftrightarrow A(F) = A(G)$ (using $A(F)$ to denote the area of F). We here define a *polygon* as a closed figure whose perimeter is composed of a finite number of straight lines.

First, we note the intuitive fact that if $F \sim G$ and $G \sim H$ then $F \sim H$. This is obvious since if we can decompose F and reform it into G , and separately decompose G and reform it into H , then we can simply go via G to decompose F and reform into H . We then show that any triangle is equidecomposable with some rectangle - if ab is the longest side of triangle abc , we draw a line perpendicular to ab down from c to a point d in ab . We draw a line through the midpoint of cd , parallel to ab , and drop lines from it at e and f , perpendicular to ab , at a and b . The two triangles above the new line can then be translated into the vacant spaces in rectangle $abfe$, completing the rectangle. It is obvious that any two rectangles of the same area are equidecomposable. Finally, we note that any polygon can be decomposed into a finite number of triangles.

From these, we reach the *Bolyai-Gerwein Theorem*, that any two polygons of the same area are equidecomposable. Every polygon F can be divided into a finite number (k) of triangles, each of which is equidecomposable with some rectangle R . Thus $F \sim \bigcup_k R_k$. We then choose an arbitrary line a_0b_0 , and erect perpendiculars a_0c and b_0d . We then cut this into rectangles with lines $a_i b_i$ and call these rectangles H_i so that $A(H_i) = A(R_i) \forall i$, and hence $H_i \sim R_i \forall i$. From this, any polygon is equidecomposable with some rectangle $a_0 b_0 b_k a_k$. If two polygons have the same area, then they are equidecomposable to rectangles of the same area, which are equidecomposable into each other, hence the theorem holds.

4.3 The 3-Dimensional Case

The third problem was solved almost before it was posed. Max Dehn showed in 1900 that a cube and a regular tetrahedron of the same volume are not equidecomposable (and indeed cannot be made equidecomposable by addition of congruent pieces). He also showed that there are tetrahedra with congruent bases and equal height which are not equidecomposable. In 1903, Veniamin Kagan published a more refined version of Dehn's argument, and it was further updated in the 1950s by Hugo Hadwiger. Here we follow the updated proof as presented in [3].

Given a set of real numbers, M , we say that the numbers $x_1, x_2, \dots, x_n \in M$ are *linearly dependent with integral coefficients* if $\exists c_1, c_2, \dots, c_n \in \mathbb{Z}$ (with $\exists i \in 1, \dots, n$ such that $c_i \neq 0$) such that $c_1x_1 + c_2x_2 + \dots + c_nx_n = 0$. This is called a *linear dependence*. A function $f : M \rightarrow \mathbb{R}$ is called *additive* if for every linear dependence in M , $c_1f(x_1) + c_2f(x_2) + \dots + c_nf(x_n) = 0$. For a polyhedron G , we let $c_i = l_i$, the length of edge i , and let $x_i = \alpha_i$, the *dihedral angle* at edge i . The dihedral angle of an edge is the angle between the two planes which meet at that edge, in the plane perpendicular to both those planes. We now define $D(G) = l_1f(\alpha_1) + l_2f(\alpha_2) + \dots + l_nf(\alpha_n) = \sum_i l_if(\alpha_i)$ as the *Dehn Invariant* of the polyhedron.

Let f be an additive function defined on M , and $\gamma \notin M$. Define $M^* = M \cup \{\gamma\}$, then we can extend f onto M^* . Then either there is no linear dependence in M^* where the coefficient of γ is non-zero (and thus we can choose $f(\gamma)$ freely), or there is a dependence. In this case, we take one dependence and hence define $f(\gamma) = \frac{-1}{c}(\sum_i c_if(x_i))$ from $\sum_i c_if(x_i) + cf(\gamma) = 0$. This leads to a linear dependence in M^* as follows:

We take $y \in M \forall j$ and $x_i \neq y_j \forall i, j$, and form the linear dependence $\sum_i d_i x_i + \sum_j e_j y_j + d\gamma = 0$. We now wish to prove that the function is still additive. Thus, we take $c \left(\sum_i d_i x_i + \sum_j e_j y_j + d\gamma \right) - d \left(\sum_i c_i x_i + c\gamma \right) = \sum_i (cd_i - dc_i) x_i + c \sum_j e_j y_j = 0$ which is a linear dependence on M , and hence $\sum_i (cd_i - dc_i) f(x_i) + c \sum_j e_j f(y_j) = 0$. We then add d times the equation from which we gained $f(\gamma)$, giving us $\sum_i cd_i f(x_i) + c \sum_j e_j f(y_j) + cd f(\gamma) = 0$, and divide through by c to obtain the desired result.

Now let G, P_1, P_2, \dots, P_n be polyhedra with $G = \sum_{i=1}^n P_i$, and let M be the set containing π and all dihedral angles of all the polyhedra. Also let f be an additive function defined on M with $f(\pi) = 0$. First consider all line segments that are edges of the polyhedra, and on those lines mark all vertices, together with points where edges intersect each other. We thus obtain a finite number of line segments, which we call *links*. In general, each edge will consist of several links. Given any edge of G , let m be the length of that link and $\alpha \in M$ the dihedral angle. Hence $f(\alpha)$ is defined, and we call $mf(\alpha)$ the weight of the link. It is easy to see that if an edge l is divided into links m_1, m_2, m_3 then, since they have the same dihedral angle, $lf(\alpha) = m_1 f(\alpha) + m_2 f(\alpha) + m_3 f(\alpha)$. We note that this is Dehn Invariant of the polyhedron.

Obviously, it suits our purposes if $G = \sum_i P_i \Leftrightarrow D(G) = \sum_i D(P_i)$. Given a link m adjoined by some number of polyhedra P_j , then the weight of that link is equal to the sum of the weights of that link in all adjoining polyhedra. Obviously, there are three types of link:

1. Links entirely inside G (discounting their endpoints). If m is such a link and polyhedra P_i, \dots, P_j adjoin it, then the sum of all adjoining dihedral angles γ is $2\pi = \gamma_i + \dots + \gamma_j$. We rearrange this into $\gamma_i + \dots + \gamma_j - 2\pi = 0$, which is a linear dependence on M . Hence, by additivity of f , we have

$f(\gamma_i) + \dots + f(\gamma_j) - 2f(\pi) = 0$. We defined f to have $f(\pi) = 0$, hence $f(\gamma_i) + \dots + f(\gamma_j) = 0$, and thus the weight of m vanishes in G .

2. Links which lie on the face of G , but not on its edges. Here $\gamma_i + \dots + \gamma_j = \pi$, and hence, again, the weight of m vanishes in G .
3. Links lying on the edges of G . Here we have $\gamma_i + \dots + \gamma_j = \alpha$ or $\gamma_i + \dots + \gamma_j = \alpha - \pi$, where α is the dihedral angle in G . Either way, $f(\gamma_i) + \dots + f(\gamma_j) = f(\alpha)$.

From this, we see that we do indeed have a function such that $G = \sum_i P_i \Leftrightarrow D(G) = \sum_i D(P_i)$. Now consider two equidecomposable polyhedra $G = \sum_i P_i, H = \sum_i Q_i$ such that $P_i \cong Q_i \forall i$ (P_i is congruent to Q_i), with an additive function D defined on M . We can, as shown earlier, add in the dihedral angles of P (and thus Q) to create M^* , and still have D defined on it. Since P_i is congruent to Q_i , $D(P_i) = D(Q_i)$. Hence, $D(G) = \sum_i D(P_i) = \sum_i D(Q_i) = D(H)$. Therefore, any two equidecomposable polyhedra have equal Dehn Invariant. It is also obvious from this that if two polyhedra are not equidecomposable, then they will have different Dehn Invariants.

Let us now move on to actually using our Dehn Invariants, and look at whether a cube is equidecomposable with a regular tetrahedron of the same volume. Obviously the dihedral angle of a cube is $\frac{\pi}{2}$, and it is fairly easy to show that the dihedral angle of the tetrahedron is $\varphi = \arccos\left(\frac{1}{3}\right)$. Hence, $M = \{\pi, \frac{\pi}{2}, \varphi\}$, and we define a real function f on M with $f(\pi) = 0, f\left(\frac{\pi}{2}\right) = 0, f(\varphi) = 1$. However, we must first prove that $\frac{1}{\pi} \arccos\frac{1}{n}$ is irrational $\forall 3 \leq n \in \mathbb{N}$.

First, suppose that $\frac{\varphi}{\pi} = \frac{\arccos\left(\frac{1}{n}\right)}{\pi} = \frac{a}{b} \in \mathbb{Q}$. Since $b\varphi = a\pi$, $\cos(b\varphi) = \cos\left(\frac{a}{b}\pi\right) = \pm 1$. This means that $\cos\left(\frac{a}{b}\pi\right) \in \mathbb{Z}$. We wish to obtain a contradiction

by showing that $\cos(b\varphi) = \frac{x}{y}$, with x coprime to y . We use the trig identity $\cos((b+1)\varphi) + \cos((b-1)\varphi) = 2\cos(b\varphi)\cos\varphi \Rightarrow \cos((b+1)\varphi) = \frac{2}{n}\cos(b\varphi) - \cos((b-1)\varphi)$.

We deal first with the case that n is odd. We use our trig identity to prove that $\cos(b\varphi)$ can be expressed as a fraction with denominator n^b and a numerator which is relatively prime (coprime) with n . $\cos\varphi = \frac{1}{n}$, $\cos(2\varphi) = 2\cos^2\varphi - 1 = \frac{2}{n^2} - 1 = \frac{2-n^2}{n^2}$. Since n is odd, $2 - n^2$ and n^2 are necessarily coprime. We now assume that the inductive hypothesis holds for all $b \leq k$ where $k \geq 2$. We can define $\cos(k\varphi) = \frac{p}{n^k}$ and $\cos((k-1)\varphi) = \frac{q}{n^{k-1}}$ where p and q are coprime to n . From our identity, $\cos((k+1)\varphi) = \frac{2}{n} \frac{p}{n^k} - \frac{q}{n^{k-1}} = \frac{2p-qn^2}{n^{k+1}}$. Since 2 and p are coprime to n , so is $2p$, and hence so is $2p - qn^2$. Hence for odd n , $\cos(b\varphi) \notin \mathbb{Z} \forall b \in \mathbb{Z}$.

If, however, n is even, then $n = 2m$ where $2 \leq m \in \mathbb{Z}$. Hence $\cos(b\varphi)$ can be expressed as a fraction with denominator $2m^k$, and a numerator which is coprime to m . The proof then proceeds in the same way as for odd n . Hence, for even n , $\cos(b\varphi) \notin \mathbb{Z} \forall b \in \mathbb{Z}$, and thus $\forall n \in \mathbb{N}, \cos(b\varphi) \notin \mathbb{Z} \forall b \in \mathbb{Z}$.

We now return to the cube and the tetrahedron. Let $c_1\pi + c_2\frac{\pi}{2} + c_3\varphi = 0$ be a linear dependence on M . If $c_3 \neq 0$, we deduce that $\frac{1}{\pi} \arccos \frac{1}{3} = \frac{\varphi}{\pi} = \frac{c_1 + \frac{c_2}{2}}{c_3} \in \mathbb{Q}$, which contradicts our earlier proof. Hence $c_3 = 0$. Thus, applying our function f , $c_1f(\pi) + c_2f(\frac{\pi}{2}) + c_3f(\varphi) = 0$, we find that f is additive. Finally, we calculate the Dehn Invariants of the two polyhedra. For the cube, Q , each edge length l , $D(Q) = 12lf(\frac{\pi}{2}) = 0$. If the tetrahedron, T , has edge length m , then $D(T) = 6mf(\varphi) = 6m \neq 0$. Thus a cube and regular tetrahedron of equal volume are not equidecomposable. This shows that the concepts of equidecomposability and volume are not equivalent as equidecomposability and area are in two dimensions.

All that remains now is to show the existence of two tetrahedra with non-equal Dehn Invariants. I will not show this directly, but instead note that the English mathematician M. J. M. Hill discovered several special tetrahedra, now known as *Hill's Tetrahedra*, which were equidecomposable with cubes. A diagram of one of these can be found in [3], p99. The tetrahedron in question has three mutually perpendicular edges of equal length, ab, bc, cd , and can be equidecomposed into a right-angled triangular prism, which it is clear can easily be equidecomposed into a cube.

4.4 Conclusion

As mentioned earlier, Dehn's work has been modernised several times. It is best written in modern formulation using tensor products of Abelian groups $\mathbb{R} \otimes_{\mathbb{Z}} (\mathbb{R}/\mathbb{Z})$. For a polyhedron P , $D(P) = \sum_i l_i \otimes \frac{\alpha_i}{\pi}$, where i represents the "number" of a given edge, l_i the length of that edge, and α_i the dihedral angle at that edge. The proof I followed is attributable to Hadwiger, and is generally thought to be the easiest to understand. It has been proved that in $\mathbb{R}^n \forall n \geq 3$, equality of the n -dimensional volume and equidecomposability are not equivalent as in \mathbb{R}^2 . The proof has also been extended to non-Euclidean geometries, and the conditions under which the n -dimensional volume and equidecomposability are equivalent have been studied extensively, although there are still some situations where their equivalence is disputed. However, Boltianskii wrote in [3] "*the theory of equidecomposability... of polyhedra has been solved in all its main aspects, and that resulting beautiful edifice is a worthy monument to the memory of David Hilbert.*"

5 Conclusion - Hilbert's Legacy

In 1974, at the Northern Illinois University, another mathematical gathering took place (a full account of proceedings can be found in [4]). Sponsored by the American Mathematical Society, the symposium discussed the effect that Hilbert's Problems had had on mathematics in the previous 74 years, in addition to presenting papers on all the problems except numbers three and sixteen. In addition, they published a further list of twenty-seven problems, emulating Hilbert. However, the 1974 problems, and indeed almost every other attempt (for there have been many) to set a similar list of problems, have had very little impact on the face of mathematics.

It must be asked why Hilbert's problems proved to be such a great motivator for the mathematical community. In 1900, mathematics was a lot less diverse than it is now, over a century later. It was in a state which somewhat paralleled science in the mid 1600s - when one man could be an innovator in many fields. Newton, for instance, in addition to great contributions to physics (the theory of gravity) and mathematics (calculus), also researched chemistry, optics, and did great work for the Royal Mint, making coins harder to counterfeit. Early 20th century mathematicians such as Hilbert and Poincaré were renowned in many fields. Of the twenty three Hilbert problems, most, if not all, were in some way connected to work Hilbert had done during the course of his career. Now, it is very difficult to be expert in anything but the smallest field of mathematics. Mathematics has become more diverse, but at the cost of cohesiveness. The 1974 problems were collated by committee.

The only set of problems which have generated any real attention are the so-called *Millennium Prize Problems*. Established in May 2000 by the Clay Mathematics Institute of Massachusetts, it is a list of seven conjecture, the solution

to any of which bring with it a million dollar prize. Only one of these has been solved.

- **The Birch and Swinnerton-Dyer Conjecture** - a more specific case of Hilbert's tenth problem.
- **The Hodge Conjecture**
- **Navier-Stokes Equations**
- **The $P = NP$ problem**
- **The Poincaré Conjecture** - solved in 2003 by Grigori Perelman.
- **The Riemann Hypothesis** - Hilbert's eighth problem.
- **Yang-Mills Theory**

The very fact that I am writing this, and indeed that you are reading this, tells us that Hilbert's problems are still important. The solution to problem eight, and correspondingly proof of the Riemann Hypothesis and Goldbach Conjecture would have startling implications in the modern world - not least in the science of cryptography. They have contributed greatly to mathematics generally - it's all very well researching for its own sake, but the problems set objectives and targets, even prizes, which gives people incentive. Simply stating a problem gives it an allure - take, for example, the efforts down the years to find the proof to Fermat's Last Theorem (finally completed by Andrew Wiles in 1995).

Hilbert hoped that his problems would inspire mathematicians and shape mathematics for years to come. In a way this was a self-fulfilling prophecy, and it is interesting to wonder how many of the problems would have been solved had Hilbert not stated them. It is unclear how much the Millennium Prize Problems

will shape the mathematics of the twenty-first century - there has been no other list akin to that of Hilbert, and seven problems, however important, surely miss out large areas of possible research. Mathematics will certainly not stall, but it is unlikely that this century will prove to be as much of a golden age for mathematics as the last was. That being said, perhaps we should listen to Hilbert's wisdom on the subject - the words he started his famous speech with:

Who of us would not be glad to lift the veil behind which the future lies hidden; to cast a glance at the next advances of our science and at the secrets of its development during future centuries? What particular goals will there be toward which the leading mathematical spirits of coming generations will strive? What new methods and new facts in the wide and rich field of mathematical thought will the new centuries disclose? ... Just as every human undertaking pursues certain objects, so also mathematical research requires its problems.

References

- [1] Website giving a translation of Hilbert's speech into English <http://aleph0.clarku.edu/~djoyce/hilbert/problems.html>, visited 12th March 2007.
- [2] Clay Mathematics Institute webpage <http://www.claymath.org/>, visited 29th April 2007.
- [3] V. G. Boltianskii (translated by R. A. Silverman), *Hilbert's Third Problem* (V. H. Winston and Sons, Washington, D.C., 1978).
- [4] F. E. Browder (ed.), *Proceedings of Symposia In Pure Mathematics, Volume XXVIII - Mathematical Developments Arising From Hilbert Problems*, (American Mathematical Society, Rhode Island, 1976).
- [5] P. J. Cohen, *Set Theory and the Continuum Hypothesis*, (W. A. Benjamin, New York, 1966).
- [6] J. L. Dupont, *Scissors Congruences, Group Homology and Characteristic Classes* (World Scientific, Singapore, 2001).
- [7] J. J. Gray, *The Hilbert Challenge* (Oxford University Press, New York, 2000).
- [8] S. Hawking (ed.), *God Created The Integers*, (Penguin, London, 2005).
- [9] T. Jech, K. Hrbacek, *Introduction to Set Theory*, Third Edition (Marcel Dekker, New York, 1999).
- [10] B. H. Yandell, *The Honors Class - Hilbert's Problems and Their Solvers*, (A. K. Peters, Massachusetts, 2002).