Cristian Calude and Hermann Maurer

Pocket mathematics

in Gh.Păun (ed.)

Mathematical Aspects of Natural and Formal Languages,

Scientific World, Singapore, 1995, 13-41.

POCKET MATHEMATICS *

Cristian Calude† and **Hermann Maurer**‡

Abstract

Mathematics is in a dramatic and massive process of changing, mainly due to the advent of computers and computer science. Our aim is to present a *pocket* image of this phenomenon; a "case study" will give us the opportunity to describe some of these new ideas, problems, and techniques. Particularly, we will be concerned with foreseeable mutations in the interaction between deductive and experimental trends.

1 Introduction

The experimental trend and the deductive trend are interacting in the history of Mathematics. Their importance and influence vary from historical periods, countries, and even authors. For instance, Euclid, Hilbert, and Bourbaki can be safely considered champions of the deductive method, while Fermat or Euler are more representative for the experimental way of thinking. It is worth noticing that the deductive method has changed fairly little, say from Euclid's time, while the experimental component has evolved significantly, both in meaning and philosophy: it has got a completely new face in view of the development of computers.

This paper is aimed to give a *pocket* image of some new ideas, problems, and techniques in mathematics, with emphasis on mutations in the interaction between the deductive and experimental trends. Our "case study" pertains propositional tautologies, a completeley axiomatizable theory. This "toy universe" is rich enough to permit a non-trivial discussion of problems concerning proofs (nature, organization, utility), theorems (structure, decidability, complexity), theoretical credibility and feasibility.

---

*The work of the first author has been supported by Auckland University Research Grant A18/XXXXX/62090/3414012.

†Computer Science Department, The University of Auckland, Private Bag 92109, Auckland, New Zealand; Email: cristian@cs.auckland.ac.nz.

‡IICM (Institute f. Information Processing and Computer Supported Media), Graz University of Technology A-8010 Graz, Austria and Computer Science Department, The University of Auckland, Private Bag 92109, Auckland, New Zealand; Email: hmaurer@iicm.tu-graz.ac.at.

2 From Empirical Observations to Formal Systems

The fundamental faith in mathematics comes from the fact that virtually everything is **rigorously proved**. But, what do we mean by a “proof”? K. Devlin, in the introduction to the month’s column *Computers and Mathematics* wrote [14]

> ...[we] mathematicians ... are somewhat schizophrenic when it comes to answering this question. ... we generally feel confident in our ability to tell a sound argument from an invalid one. Moreover, we tend to feel that it really is not an issue of judgement, and that for all their surface brevity, the proofs we construct and publish are, in an absolute sense, genuine *proofs*.

A good way to explain is *to do*. Our choice refers to the simplest way to analyse the mathematical thinking, i.e. by means of the model initiated more than a hundred of years ago by George Boole, currently referred as the *propositional calculus*. We are interested only in the “truth values” of propositions, and again our working hypothesis refers to the simplest case: propositions are only true or false, no other possibility is considered.[1]

We start with a (denumerable) set of *atomic propositions*. Denote by V this set. We add to V a new element, f, referring to it as the *universal false proposition*.

Using the usual propositional operations (disjunction, conjunction, negation, implication, etc.) we can form new propositions starting with the atomic ones. For the simplicity of the presentation we shall work with only one propositional operation – the *implication* (denoted by $\rightarrow$). Hence, we construct the “larger” set of propositions, call it P, defined by means of the following four rules:[2]

1. Every atomic proposition is a proposition, i.e. $V \subset P$.
2. The universal false proposition f belongs to P.
3. If x, y are arbitrary propositions, then $x \rightarrow y$ is a proposition.
4. Every proposition is obtained by rules 1-3.

Using only the implication and f doesn’t really make our approach less general; indeed, all propositional operations can be ”re-captured” as follows:

$$\text{negation: } \neg x = x \rightarrow f,$$

[1] It can be argued that even God is bound by logic. If God can lift any weight, then God is expressly prevented to create a weight so heavy that God cannot lift it. But God can do anything that does not involve a logical contradiction. (It seems that Einstein sympathised with this argument.) See also the discussion in Wiener [41], and Odifreddi [32, 33].

[2] *Note for algebraists*: P is the free universal algebra of type $(0, 2)$ generated by V.

$$\text{disjunction: } x \cup y = (\neg x) \to y,$$

$$\text{conjunction: } x \cap y = \neg((\neg(x) \cup \neg(y)).$$

How do we know that the above formulas actually work?

To this aim we introduce the notion of interpretation. The set of truth values will be denoted by $\{0, 1\}$ and we introduce on it the binary operation (called *truth implication*) which models the idea that an implication is false only in case the hypothesis is true but the conclusion is false:

$$\Longrightarrow : \{0, 1\} \times \{0, 1\} \to \{0, 1\},$$

$$m \Longrightarrow n = \max\{1 - m, n\}.$$

Here max stands for the usual maximum function. Clearly, $m \Longrightarrow n = 0$ iff $m = 1$ and $n = 0$.

An *interpretation* is a function

$$h : V \to \{0, 1\},$$

i.e. a way to assign truth values to atomic propositions. We can extend this interpretation to the set of all propositions imposing the following two conditions:[3]

a) $h(f) = 0$,

b) $h(x \to y) = h(x) \Longrightarrow h(y)$, for all $x, y \in P$.

If h is an interpretation and $x \in P$, then the proposition x is *true under* h if $h(x) = 1$.

We can now compute the interpretations of the negation, disjunction, conjunction, according to a fixed h:

$$h(\neg x) = h(x \to f) = h(x) \Longrightarrow h(f) = h(x) \Longrightarrow 0 = 0 \text{ iff } h(x) = 1,$$

i.e. $h(\neg x) = 1 - h(x)$. Similarly,

$$h(x \cup y) = h((\neg x) \to y) = h(\neg x) \Longrightarrow h(y)$$

$$= (1 - h(x)) \Longrightarrow h(y) = \max\{1 - (1 - h(x)), h(y)\} = \max\{h(x), h(y)\},$$

$$h(x \cap y) = h(\neg((\neg(x) \cup \neg(y))))$$

$$= 1 - h(\neg(x) \cup \neg(y)) = 1 - \max\{h(\neg x),$$

$$h(\neg(y)\} = 1 - \max\{1 - h(x), 1 - h(y)\} = \min\{h(x), h(y)\},$$

validating our claim.

[3] Algebraically, h is a morphism; as P is freely generated by V, h is uniquely determined by its values on generators, i.e. on V.

The next step is to model the idea of "semantic consequence": the proposition $a \in P$ can be semantically deduced from the set of premises $X \subset P$ (or X is a semantic model for a) if every interpretation which makes **all** premises in X true, makes true x as well. Formally,

$$X \models a$$

if for every interpretation h such that $h(x) = 1$, for all $x \in X$, one has $h(a) = 1$.[4] In case $X = \emptyset$ we simple write $\models a$.

Example 2.1. *The following relations are true:*

1. $\models a \to (b \to a)$, *for all* $a, b \in P$.
2. $\models (a \to (b \to c)) \to ((a \to b) \to (a \to c))$, *for all* $a, b, c \in P$.
3. $\models ((a \to f) \to f) \to a$, *for every* $a \in P$.
4. $\{a\} \models b \to a$, *for all* $a, b \in P$.

For instance, for the last relation we have to show that for every interpretation h such that $h(a) = 1$ one has $h(b \to a) = 1$. Indeed, $h(b \to a) = h(b) \Longrightarrow h(a) = h(b) \Longrightarrow 1 = 1$.

A special category of propositions is formed by "universal true propositions", i.e. propositions which are true with respect to all possible interpretations. We call them *tautologies*. The propositions $a \to (b \to a), (a \to (b \to c)) \to ((a \to b) \to (a \to c)), ((a \to f) \to f) \to a$ are all tautologies. Of course, not all propositions are tautologies; the extreme example is a proposition that is never true under any interpretation, for instance, $a \cap \neg a$.[5]

Example 2.2. *The following propositions are tautologies:*

1. $a \to a$, *(identity principle),*
2. $a \cup \neg a$, *(tertium non datur),*
3. $(a \cap (a \to b)) \to b$, *(modus ponens),*
4. $((a \to b) \cap (a \to \neg b)) \to \neg a$ *(negation principle),*
5. $a \to (a \cup b)$, *(disjunction principle).*

Several natural questions can be asked, for instance:

- Is there a compact way to "described" all and only all tautologies?

[4] It is interesting to note that in LaTeX the symbol $\models$ is written `\models`.

[5] From a strict formal point of view, $a \cap \neg a$ is *not* a proposition in P, as $\cap, \neg$ are not admissible operators. Howevere, we shall use the formula $a \cap \neg a$ as an abbreviation for the proposition

$$(((a \to f) \to f) \to ((a \to f) \to f)) \to f.$$

- What is the "structure" of the set of tautologies?
- Is it possible to "algorithmically" recognize a tautology? Is this a feasible task?

There are several possibilities to describe a set of propositions, specifically the set of tautologies. For our purpose the most interesting one is the deductive approach. The prototype of a deductive science is Euclid's geometry, developed around 300 B.C. Many of the facts about *geometry*[6] were collected by the Egyptians and Babylonians. The major step undertook by Euclid and his predecessors in Greece was to organise these facts into a deductive science or axiomatic-deductive geometry.

The truth or falsity of most propositions in geometry cannot be seen directly from their meanings. The *axioms*, however, are special propositions whose truths are immediately recognized from their meanings; in fact, for a long period, this was the major criterion to select axioms (we shall return to this problem later). Starting with axioms, by a series of logical steps that we accept as propagating truth forward, we construct a "proof" by which we can arrive at the truth of other propositions – called "theorems".[7]

Do we have a "solid" basis for recognizing the rules that allow us to propagate truth forward? This is a very delicate problem. For a long period Euclid's theory was considered the prototype of a perfect theory. However, in the nineteenth century people revealed flaws in Euclid's proofs, making essential use of "illustrated" figures.[8]

A fundamental change of view point has to be adopted: *deductions should be possible to carry out without reference to meanings.* In Euclid's case, proofs should read correctly with nonsense words substituted for "point", "line", "plane". The logical principles which mediate the steps in proofs should be stated in advance as *rules of inference.* So, the meanings of none of the words need to be considered in constructing proofs; the quality of being a valid proof depends then only on the form of the sentences. A valid proof has to be impersonal: whenever an alledged proof is submitted to a person who has previously been told the specifications of the system she/he should be able to *check* the proposed proof and decide whether it actually is a proof or not. No extra imagination or judgment is needed. In other terms, checking the validity of an alledged proof may be done by computer; this infinite class of yes-or-no questions is *algorithmically decidable.*[9]

In what follows we shall design an axiomatic system for tautologies. To this aim we "isolate" a few tautologies (called *axioms*) and a "deduction principle"

[6] Earth measurement.

[7] Whose truth we might not have been ready to accept directly from their meanings.

[8] False "theorems" were discovered: "proofs" read just Euclid's proofs, except that some figures were "fudged" a little bit.

[9] This explains why the working mathematicians may differ (and, indeed, they do) in their views of what constitutes a rigorous proof, in spite of the fact that all of them believe in rigorous proofs.

with the aim of "deriving" all and only all tautologies. The axioms will be the first three tautologies in Example 2.1:

A1. $a \to (b \to a)$, for all $a, b \in P$.

A2. $(a \to (b \to c)) \to ((a \to b) \to (a \to c))$, for all $a, b, c \in P$.

A3. $((a \to f) \to f) \to a$, for every $a \in P$.

As a deduction rule we make use of the most fundamental principle (called *Modus Ponens*), modeling the following inference: if one proves y from x, and x has a proof, then y has a proof.

Modus Ponens : *For all $x, y \in P$, if x and $x \to y$, then y.*

We have got a "formal system". Within it we can discuss about "(formal) **proofs**".[10] Informally, a **proof** is just a finite sequence of propositions such that every element in the sequence is an axiom or can be deduced from propositions already in the sequence by *Modus Ponens*. Sometimes our **proofs** make use of extra hypotheses X; they will be called X**-proofs**.

Let X be a set of propositions and $a \in P$. An X**-proof** for a (i.e. a **proof** (within the system) of a from the set X of premises) is a sequence

$$x_1, x_2, \ldots, x_n$$

of elements in P such that $x_n = a$ and for all $1 \leq i \leq n$ one has:

- $x_i \in X$ or,
- x_i is an axiom, or
- there exist $1 \leq k, l < i$ such that $x_j = x_k \to x_j$ (i.e. x_i can be deduced from x_k and x_j via *Modus Ponens*).

The proposition a is called an X**-theorem** in this case. Sometimes we write:

$$X \vdash a,$$

or simply

$$\vdash a,$$

in case $X = \emptyset$.

Example 2.3. *For all $a, b, c \in P$, the following relations are true:*

1. $\vdash a \to (b \to a)$,

[10] To distinguish between "proofs within our system" and "proofs outside the system", the first ones will be written in bold characters.

2. $\vdash a \to a$*,*

3. $\{b\} \vdash a \to b$*,*

4. $\{a \to (c \to b), a \to c\} \vdash a \to b$*.*

Proof. The first proposition, $a \to (b \to a)$, is an axiom. For $a \to a$ we can write the following **proof**:

1. $a \to ((b \to a) \to a)) \to ((\to (b \to a)) \to (a \to a))$ (by A2.)
2. $a \to ((b \to a) \to a)$ (by A1.)
3. $(a \to (b \to a)) \to (a \to a)$ (by *Modus Ponens* from 2. and 1.)
4. $a \to (b \to a)$ (by A1.)
5. $a \to a$ (by *Modus Ponens*, from 4. and 3.).

The following sequence represents an $\{b\}$**-proof**:

1. $b \to (a \to b)$
2. b
3. $a \to b$.

Finally, the following sequence represents an $\{a \to (c \to b), a \to c\}$**-proof**:

1. $(a \to (c \to b)) \to ((a \to c) \to (a \to b))$
2. $a \to (c \to b)$
3. $(a \to c) \to (a \to b)$.
4. $a \to c$
5. $a \to b$.

□

The following theorem, due to Herbrand [23], makes explicit the relation between the implication ($\to$), as an inner operator of the system, and the syntactical derivation ($\vdash$), the external deduction.

Theorem 2.4 (Deduction Theorem). *Let* $X \subset P$*, and* $a, b \in P$*. The following statements are equivalent:*

a) $X \vdash a \to b$*,*

b) $X \cup \{a\} \vdash b$*.*

Proof. For the direct implication let $x_1, x_2, \ldots, x_n$ be an X**-proof** for $a \to b$. Then $x_1, x_2, \ldots, x_n, a, b$ is an $X \cup \{a\}$**-proof** for b.

We are proving the converse implication. Let $x_1, x_2, \ldots, x_n$ be an $X \cup \{a\}$**-proof** for b. We prove, by induction on i, that

$$X \vdash a \to x_i.$$

For $i = n$ we get the desired conclusion:

$$X \vdash a \to b,$$

as $x_n = b$.

There are four possible cases to be discussed:

- $x_i \in X$: since $\{x_i\} \vdash a \to x_i$ one deduces $X \vdash a \to x_i$, as $x_i \in X$.
- $x_i = a$: since $\vdash a \to a$, by Example 2.3, $X \vdash a \to a$.
- x_i is an axiom: one has $\vdash x_i$, so $\{x_i\} \vdash a \to x_i$, i.e. $X \vdash a \to x_i$.
- $x_k = x_j \to x_i, j, k < i$: by hypothesis, $X \vdash a \to x_j$ and $X \vdash a \to x_k$. By virtue of Example 2.3,

  $$\{a \to x_j, a \to (x_j \to x_k)\} \vdash a \to x_i,$$

  so $X \vdash a \to x_i$.

□

Remark. There is a simpler, semantical analogue of the Deduction Theorem. It reads as following: *Let $X \subset P$, and $a, b \in P$. The following statements are equivalent:*

a) $X \models a \to b$,

b) $X \cup \{a\} \models b$.

Here are two more examples of X**-proofs**:

Example 2.5.

1. $\{f\} \vdash a$, *for all* $a \in P$,

2. $\{a, \neg a\} \vdash b$, *for all* $a, b \in P$.

Proof. Here is an $\{f\}$**-proof** for a:

1. f
2. $f \to ((a \to f) \to f)$
3. $(a \to f) \to f$
4. $((a \to f) \to f) \to a$
5. a.

Starting with the sequence

a. a

b. $a \to f$

c. f

and the above $\{f\}$**-proof**, i.e. steps 1.,2.,3.,4.,5. we get an arbitrary proposition b. □

3 Adequacy Problems

It's time to look critically at our system. Is it adequate? *Soundness* is the first required property, as we are interested to "describe" only tautologies. Specifically, the question reads: Is any **theorem** a tautology? A negative answer would ruin the whole construction.

We start proving that every X**-theorem** can be semantically deduced from X:

Proposition 3.1. *For all $X \subset P, a \in P$, if*

$$X \vdash a,$$

then

$$X \models a.$$

Proof. We use the definition of an X**-proof** inductively, noticing that all axioms are tautologies and *Modus Ponens* is an invariant rule. □

To be really successful we need to prove the completeness of our system, i.e. a converse of Proposition 3.1. The following proof will give some more insight on the nature of tautologies.

Definition 3.2. *A set $X \subset P$ is called* consistent *if it is free of contradictions; formally, if*

$$X \nvdash f.$$

Example 3.3. *The empty set is consistent. The set $\{a, \neg a\}$ is not consistent.*

Proof. Indeed, if $\vdash f$, then, by Proposition 3.1, $\models f$, which is absurd as for every interpretation h one has $h(f) = 0$. By Example 2.5, $\{a, \neg a\} \vdash f$. □

We shall prove now two technical results that are motivated by a typical algebraic construction: the embedding of a structure in a maximal structure of the same type.

Lemma 3.4. *The union of an increasing sequence (under set-theoretical inclusion) of consistent sets is still a consistent set.*

Proof. Let

$$B_1 \subset B_2 \subset \cdots \subset B_n \subset B_{n+1} \subset \cdots$$

be an increasing sequence of consistent sets and put

$$B = \bigcup_{n \geq 1} B_n.$$

If, by absurd, B is not consistent, then $B \vdash f$, i.e. there exists a finite set $X \subset B$ such that $X \vdash f$. So, $X \subset B_m$, for some natural $m \geq 1$ (as the sequence $(B_i)_{i \geq 1}$) is increasing). This contradicts the consistency of B_m. □

Definition 3.5. *A set $X \subset P$ is called* maximal consistent *if for every element $a \notin X$ the set $X \cup \{a\}$ is not consistent.*

Proposition 3.6. *Every consistent set can be embedded into a maximal consistent set.*

Proof. The usual way to prove such a result is to invoke Zorn's Lemma.[11] We proceed *constructively*, i.e. introducing an enumeration technique usually referred to as a *gödelization.* Assume that we have an one-one enumeration $v_i, i = 2, 3, \ldots$ of all atomic propositions. Then, we can construct an one-one function $g : P \to \mathbf{N}$ as follows:[12]

Put $v_1 = f$ and

$$g(v_i) = 2i + 1,$$
$$g(x \to y) = 2^{g(x)}.3^{g(y)}.$$

For instance, $g(f) = 0$,

$$g(v_1 \to (v_2 \to v_1)) = 2^{g(v_1)}.3^{g(v_2 \to v_1))}$$

$$= 2^1.3^{2^{g(v_2)}3^{g(v_1)}} = 2.3^{2^2.3^1} = 2.3^{12}.$$

Let $X \subset P$ be a fixed consistent set. Using the above function g we define the following sequence of sets of propositions:

$$B_0 = X,$$

$$\begin{array}{rcll} B_{n+1} & = & B_n \cup \{g(n)\}, & \text{if } B_n \cup \{g(n)\} \text{ is consistent,} \\ & = & B_n, & \text{otherwise.} \end{array}$$

Clearly, the sequence B_n is increasing and each B_n is consistent. So, by Lemma 3.4, $B = \bigcup_{n \geq 0} B_n$ is consistent as well. Since $B_0 = X \subset B$ the only fact it remains to be proven is the maximal consistency of B. Let $B \subset Y \subset P$ be such that $B \neq Y$, i.e. there exists a proposition

$$g(n) \in Y, g(n) \notin B.$$

[11] Let X be a consistent subset of P. The set $\Gamma = \{T \subset P | X \subset T, T \not\vdash f\}$ is non-empty ($X \in \Gamma$). More, Γ is inductively ordered: if $\{T_\alpha\}$ is a totally ordered family of elements of Γ and $T = \cup_\alpha T_\alpha$, then $X \subset T \subset P, T \not\vdash f$ (as, if f is provable from T means that f is provable from a finite subset of T). Use now Zorn's Lemma (*if S is a partially ordered set in which each chain has an upper bound, then S contains a maximal element*) to assert the *existence* of a maximal element in Γ. In general, no claim of constructivity can be made for such a reasoning; see, for instance, the treatment in Barnes and Mack [3].

[12] Assume that our enumeration $\{v_i\}$ was "computable", in the sense that there exists an *algorithm* computing v_i when presented i. Then, the function g is itself computable and given $i \in g(P)$ we can effectively discover the (unique) proposition $x \in P$ such that $g(x) = i$. We do not define the notion of algorithm; instead, we may think of an algorithm as a finite specification of a ste-by-step computation. A computer program is the most familiar instance of an algorithm.

From the relation $g(n) \notin B$ and the construction of B_{n+1} it follows that $g(n) \notin B_{n+1}$ – because $B_n \cup \{g(n)\}$ is not consistent, i.e.

$$B_n \cup \{g(n)\} \vdash f.$$

But, $B_n \subset Y$, $g(n) \in Y$, so $B_n \cup \{g(n)\} \subset Y$ and $Y \vdash f$, saying that Y is not consistent. □

Maximal consistent sets are "fixed-points" of the operator generating **theorems** and they obey the Bivalence Principle.

Proposition 3.7. *If $X \subset P$ is a maximal consistent set, then*

1. $\{a \in P | X \vdash a\} = X$,
2. *for every $a \in P$, one and only one of the following relations is true: $a \in X$ or $\neg a \in X$.*

Proof. 1) Clearly, $X \subset \{a \in P | X \vdash a\}$. But

$$f \notin \{a \in P | X \vdash a\} = \{a \in P | \{b \in P | X \vdash b\} \vdash a\},$$

so $\{a \in P | X \vdash a\}$ is consistent. In view of the inclusion $X \subset \{a \in P | X \vdash a\}$ we can make use of the maximality to derive the equality.
2) If $a \notin X$, then $X \cup \{a\}$ is not consistent, i.e.

$$X \cup \{a\} \vdash f.$$

We use now the Deduction Theorem to get

$$X \vdash a \to f = \neg a.$$

By virtue of 1), $\neg a \in X$. If $\neg a \notin X$, then $X \cup \{\neg a\}$ is not consistent,

$$X \cup \{\neg a\} \vdash f,$$

so by the Deduction Theorem

$$X \vdash \neg a \to f = (a \to f) \to f = \neg\neg a.$$

By the axiom A3.

$$\neg\neg a \to a,$$

so $X \vdash a$, i.e. $a \in X$ by virtue of maximality. Of course, it is not the case that both a and $\neg a$ are in X, as X is consistent (see Example 2.5). □

The next result shows that every maximal consistent set of propositions X has a model, i.e. there is an interpretation according to which all propositions in X are true.

Proposition 3.8. *Let X be a maximal consistent set. Then, c_X, the characteristic function of X (with respect to P) is an interpretation making true all propositions in X.*

Proof. Recall that $c_X : P \to \{0,1\}$, $c_X(a) = 1$ iff $x \in X$. As X is maximal consistent, $X \not\vdash f$, so $f \notin X$, i.e. $c_X(f) = 0$.

Take now $a, b \in P$. We shall prove that

$$c_X(a \to b) = c_X(a) \Longrightarrow c_X(b).$$

There are three cases to be analysed.

1. *If* $b \in X$, then $c_X(b) = 1$, so $c_X(a) \Longrightarrow c_X(b) = c_X(a) \Longrightarrow 1 = 1$. One has to prove that $c_X(a \to b) = 1$, i.e. $a \to b \in X$. We know that X is maximal consistent, so a fixed-point:

$$X = \{c \in P | X \vdash c\}.$$

   By axiom A1., $\vdash b \to (a \to b)$, so

$$X \vdash b \to (a \to b).$$

   By hypothesis, $b \in X$, so $X \vdash b$ and (by *Modus Ponens*) $X \vdash a \to b$. Again, by maximality, $a \to b \in X$.

2. *If* $a \notin X$, then $c_X(a) = 0$, so $c_X(a) \Longrightarrow c_X(b) = 0 \Longrightarrow c_X(b) = 1$. So, we have to prove again the relation $c_X(a \to b) = 1$. But $a \notin X$ implies, by Proposition 3.7, $\neg a \in X$. Using the Deduction Theorem (to $\{a, \neg a\} \vdash b$) we get

$$\{\neg a\} \vdash a \to b.$$

   Since $\neg a \in X$, $X \vdash \neg a$, so $X \vdash a \to b$, i.e. $a \to b \in X$.

3. *If* $a \in X$ *and* $b \notin X$, then $c_X(a) = 1, c_X(b) = 0$, so $c_X(a) \Longrightarrow c_X(b) = 0$. The relation $a \to b \notin X$ remains to be proven. Indeed, if $a \to b \in X, a \in X$, then $b \in X$, a contradiction.

□

Corollary 3.9. *If X is consistent, then there exists an interpretation $h : P \to \{0,1\}$ such that $h(a) = 1$, for all $a \in X$.*

Proof. Embedd the given consistent set into a maximal consistent set and then use Proposition 3.8. □

We are now able to prove Post's Completeness Theorem [34], which guaranties that our system is completely adequate.

Lemma 3.10. *For every set of propositions X and every proposition a,*

$$X \models a \text{ iff } X \vdash a.$$

Proof. By Proposition 3.1 only the direct implication has to be proven. Assume that $X \models a$. We shall prove that $X \cup \{\neg a\}$ is not consistent. If it were consistent, then we would have, by Corollary 3.9, an interpretation h such that $h(b) = 1$, for all $b \in X \cup \{\neg a\}$, i.e.

$$h(\neg a) = 1,$$

and

$$h(b) = 1, \text{ for all } b \in X.$$

From $h(\neg a) = 1$ one deduces $h(a) = 0$, so we have contradicted the hypothesis $X \models a$.

From the inconsistency of the set $X \cup \{\neg a\}$ we deduce[13]

$$X \cup \{\neg a\} \vdash f.$$

Use again the Deduction Theorem

$$X \vdash \neg a \to f = \neg\neg a,$$

and the axiom A3. to get $X \vdash a$. $\square$

Taking $X = \emptyset$ in Lemma 3.10 we get

Theorem 3.11 (Completeness Theorem). *For every proposition a,*

$$\models a \text{ iff } \vdash a.$$

Digression: *Three or many valued logics.* The proposition

$$(\neg a \to a) \to a$$

is clear a tautology (it seems to be discovered by Clavius, 1600 A.C.). If we switch the underlying logic, from binary, to, say ternary, we loose the tautological property. Indeed, assume we work with the ternary logic in which the truth values are $0, \frac{1}{2}$ (uncertain), 1. The implication interpretation will use the same formula, i.e. $m \implies n = \max\{1 - m, n\}$. This means that $\neg\frac{1}{2} = \frac{1}{2}$ and $\frac{1}{2} \implies \frac{1}{2} = \frac{1}{2}$. If the truth value of a is uncertain, then the proposition $(\neg a \to a) \to a$ is also uncertain.

[13] Does it mean that actually we have got an $X \cup \{\neg a\}$ **- proof** for f or only an assertion telling that such a **proof** does exist?

4 The Structure of Tautologies

One reason why Boolean algebras are relevant to logic is that propositional operators have properties similar to Boolean operations. Based on this analogy we cannot ask questions such as "What is a proof?" or "How can we prove?"; instead, we can study the inner "structure" of provable propositions, that is, via the Completeness Theorem, of tautologies.

To every interpretation h we associate an equivalence relation $\overset{h}{\sim}$ defined on P as follows:

$$a \overset{h}{\sim} b \text{ iff } h(a) = h(b).$$

In fact, $\overset{h}{\sim}$ is more than an equivalence relation, it is a *congruence*, in the sense that $\overset{h}{\sim}$ is compatible with the algebraic structure of P: If $a \overset{h}{\sim} b$ and $a' \overset{h}{\sim} b'$, then $a \to a' \overset{h}{\sim} b \to b'$. Indeed, from $h(a) = h(b), h(a') = h(b')$ we deduce

$$h(a \to a') = h(a) \Longrightarrow h(a') = h(b) \Longrightarrow h(b') = h(b \to b').$$

The intersection of congruences $\overset{h}{\sim}$, when h runs over all interpretations,

$$\sim = \bigcap_{h \text{ interpretation}} \overset{h}{\sim},$$

is still a congruence on P. The equivalence class of an element $a \in P$ is

$$[a] = \{b \in P | a \overset{h}{\sim} b, \text{ for every interpretation } h\}.$$

The family of all equivalence classes, $P/_{\sim} = \{[a]\}_{a \in P}$ can be endoweded, in a natural way, with the following Boolean operations:[14]

$$\neg[a] = [\neg a],$$

$$[a] \cup [b] = [\neg a \to b],$$

$$[a] \cap [b] = [\neg((\neg a) \cup (\neg b))].$$

These definitions are correct, i.e. they do not depend upon the chosen "names" for classes. For instance, if $a \sim b$, then $h(a) = h(b)$, for every interpretation h, so

$$h(\neg a) = h(a \to f) = h(a) \Longrightarrow h(f) =$$

$$h(a) \Longrightarrow 0 = h(b) \Longrightarrow 0 = h(b \to f) = h(\neg b),$$

meaning that $[\neg a] = [\neg b]$. More, $(P/_{\sim}, \cup, \cap, \neg)$ is a Boolean algebra (called *Lindenbaum algebra*).[15]

[14]Recall that $\neg a$ is an abbreviation for the proposition $a \to f$.

[15]The following identities are satisfied for all $u, v, w \in P/_{\sim}$:

$$u \cap v = v \cap u, \ u \cup v = v \cup u,$$

The distinguished element "1" of this Boolean algebra[16] is

$$\mathbf{Taut} = [a] \cup \neg[a] = [a] \cup [\neg a] = [a \cup \neg a],$$

and, as $h(a \cup \neg a) = 1$, for all $a \in P$, coincides with the set of all tautologies.

We make one more step further in our generalization: Consider an arbitrary Boolean algebra B endowed with the operations $\cup, \cap, \neg$, whose elements are identified with the propositions of some mathematical theory. Assume $F \subset B$ corresponds to the set of *provable* propositions (*theorems*). The common mathematical experience motivates the following two statements;

- If $s, t \in F$, then s **and** $t \in F$.
- If $s \in F$ and $t \in B$, then s **or** $t \in F$.

The above two properties are similar to properties defining the notion of *Boolean filter*. Is this only a superficial analogy? The argument for a negative answer is presented in the following

Theorem 4.1. *Let F be a subset of the Boolean algebra B. Then, the following two assertions are equivalent:*

1. *The set F is a filter.*[17]
2. *One has:*
   a. $1 \in F$.[18]
   b. *If $x \in F$ and $x \to y \in F$, then $y \in F$.*[19]

Proof. For the direct implication we assume that $x \in F$ and $x \to y \in F$. In view of the second property of a filter, if $p, q \in F$, then $p \cap q \in F$. A simple computation shows that $x \cap (x \to y) = x \cap (\neg x \cup y) = (x \cap \neg x) \cup (x \cap y) \in F$, i.e. $x \cap y \in F$. Finally, $y = y \cup (x \cap y)$ is in F as $x \cap y \in F$; we have used the third property of a filter.

Conversely, let $x, y \in F$. We have: $x = x \cap (x \cup y)$, so

$$\neg x = \neg x \cup \neg(x \cup y) = \neg x \cup (\neg x \cap \neg y).$$

$$u \cap (v \cap w) = (u \cap v) \cap w,\ u \cup (v \cup w) = (u \cup v) \cup w,$$
$$u \cap (u \cup v) = u, u \cup (u \cap v) = u,$$
$$u \cap (v \cup w) = (u \cap v) \cup (u \cap w),\ u \cup (v \cap w) = (u \cup v) \cap (u \cup w),$$
$$(u \cap \neg u) \cup v = v,\ (u \cup \neg u) \cap v = v.$$

[16]Recall that in every Boolean algebra the expression $x \cup \neg x$ does not depend upon the actual value of x; this is the element "1", or the maximal element of the algebra.

[17]That is, 1. $1 \in F$, 2. For all $x, y \in F, x \cap y \in F$, 3. For all $x \in F, y \in B, x \cup y \in F$.

[18]This condition says that all tautologies are provable.

[19]*Modus Ponens*.

Consequently,

$$1 = x \cup \neg x = x \cup (\neg x \cup (\neg x \cap \neg y)) = (x \cup (\neg x \cap \neg y)) \cup \neg x \in F.$$

But $x \in F$ and $1 \in F$, so $x \cup (\neg x \cap \neg y) \in F$ and

$$\neg x \cup ((\neg x \cap \neg y) \cup x) = \neg x \to ((\neg x \cap \neg y) \cup x) = 1 \in F.$$

So,

$$x \cup (\neg x \cap \neg y) = (x \cup \neg y) \cap (x \cup y) = x \cup \neg y = y \to x \in F.$$

Now we are using the second hypothesis, $y \in F$:

$$y \to (x \cap y) = \neg y \cup (x \cap y) = (\neg y \cup x) \cup (\neg y \cap x) = \neg y \cup x \in F,$$

so $x \cap y \in F$.

Let $x \in F$ and $y \in B$. In the above computation we substitute $\neg y$ for y and we obtain $x \cup \neg(\neg y) \in F$, i.e. $x \cup y \in F$. $\square$

We can now come back to our concrete example of Boolean algebra, Lindenbaum algebra $P/_\sim$. Take $X \subset P$ and

$$F(X) = \{[a] \in P/_\sim | X \vdash a\}.$$

Then $F(X)$ is a filter. Indeed, $\mathbf{Taut} \in F(X)$ (if $a \in \mathbf{Taut}$, then $\models a$, so by the Completeness Theorem, $\vdash a$, so $X \vdash a$). Next take $[a] \in F(X)$ and $[a] \to [b] = [a \to b] \in F(X)$. This means that $X \vdash a, X \vdash a \to b$, so by *Modus Ponens*, $X \vdash b$, i.e. $[b] \in F(X)$.

So, from a structural point of view, $\{\mathbf{Taut}\}$ is a filter in the Lindenbaum algebra $P/_\sim$; actually, it is an ultrafilter.

5 Ultrafilters and Constructivity

Let B be a Boolean algebra. Filters in B which are maximal with respect to inclusion are called *ultrafilters*. It is not hard to show that *a filter F is an ultrafilter iff for every $x \in B$ either $x \in F$ or $\neg x \in F$, bot not both*; compare with Proposition 3.7. The key result on ultrafilters is the Ultrafilter Theorem (see, for a proof, Bell ans Slomson [4], Theorem 3.4, p.15; again, it is instructive to compare with Proposition 3.6):

Theorem 5.1. *Every filter in a Boolean algebra can be extended to an ultrafilter.*

To illustrate this situation we consider the Lindenbaum algebra $P/_\sim$; for every interpretation h define

$$F_h = \{[a] \in P/_\sim | h(a) = 1\}.$$

A simple argument shows that F_h is a filter, in fact, an ultrafilter.

These facts actually motivate another approach to the Completeness Theorem, a path followed by Rasiowa and Sikorski [36]. Bell and Slomson [4], p. 49, wrote:

> *The proofs of Post and Kalmár*[20] *both provide explicit recipes for constructing a proof of a given tautology. The proof that we have given, which is due to Rasiowa and Sikorski [1951], does not have this character, and since it depends on the ultrafilter theorem is not a constructive proof.*

This remark calls for a more detailed explanation. The problem under discussion is the following: Having a proposition a and *knowing* that a is a tautology, is it possible to get a **proof**, within the considered system, for a? As it stands, the above question has *always* a positive answer, by the Completeness Theorem, independently of the proof of this theorem. Indeed, a dovetailing algorithm[21] running through all possible proofs does the job, as *we know* that eventually the right **proof** will be discovered. In fact, this is exactly the algorithm rejected for the general problem discussed at the beginning[22]. The main difference lies in the *extra* information given in the weaker question: we know that a is a tautology. This is a quite subtle situation, in which the difference between a constructive proof and a non-constructive proof[23] affects very little the "numerical" content of the result. To get more insight on this phenomenon we make use of some rudiments of Constructive Mathematics. According to Bridges and Richman [6] p.1:

> *We engage in constructive mathematics from a desire to clarify the meaning of mathematical terminology and practice – in particular, the meaning of existence in a mathematical context. The classical mathematician, with the freedom of methodology advocated by Hilbert, perceives an object x to exist if he can prove the impossibility of its nonexistence; the constructive mathematician must be presented with an algorithm that constructs the object x before he will recognize that x exists.*

The essential difference between a classical and constructive approach to mathematics can be grasped by considering **binary sequences** generated by an algorithm. Let $b = b_1 b_2 \dots b_n \dots$ be a binary sequence and consider the following statements:

$$S(b) : b_n = 1, \text{ for some } n,$$

[20] See [25].

[21] A *British Museum algorithm*, following Chaitin.

[22] Having a proposition a, is it possible to algorithmically decide if a is a **theorem**?

[23] The proof discussed in this paper is only apparently constructive. It avoids the use of Zorn's Lemma, but makes essential use of the *embbeding*.

$$\neg S(b) : b_n = 0, \text{ for all } n.$$

Here $\neg S(b)$ is the denial of $S(b)$: under the assumption of $S(b)$ a contradictory statement (like $0 = 1$) holds. A constructive proof of $S(b) \vee \neg S(b)$ must provide an algorithm showing that $b_n = 0$, for all n, or computing a positive integer n such that $b_n = 1$.

A **Brouwerian counterexample** to an assertion is a proof that the assertion implies some unacceptable principle in constructive mathematics. The most popular such principle is called the **Limited Principle of Omniscience, LPO**:

> *If (b_n) is a binary sequence, then either there exists n such that $b_n = 1$, or else $b_n = 0$, for all n.*

Clearly, **LPO** is simple the assertion

$$\forall b(S(b) \vee \neg S(b)).$$

Why is it constructively false? Just because it is equivalent to the **Halting Problem**, which cannot be solved algorithmically. Here is the outline of the argument. First we show that the **Halting Problem** is not decidable. Assume, for the sake of a contradiction, that there exists a **halting program** deciding if an arbitrary program eventually halts. The outputs, if any, for all our programs are supposed to be 0 or 1; also, we may assume, without loss of generality, that the inputs for the programs are part of the programs themselves.

Construct, following Chaitin [9], the program (which essentially makes use of the **halting program**):

- read a natural N;
- generate all programs up to N bits in size;
- use the **halting program** to check for each generated program whether it halts;
- simulate the running of the above generated programs;
- make sure that the running time of the current program is bigger than the running time of all halting programs, generated above.

First, notice that the above program eventually halts for every natural N. How long is the above program ? It is about $\log_2 N$ bits. Indeed, the program consists of the input data N (which requires about $\log_2 N$ bits) and a constant part. Globally, the program has $\log_2 N + O(1)$ bits. For large enough N, the above program will belong to the set of programs having less than N bits (because $\log_2 N + \mathrm{O}(1) < N$). Accordingly, the program will be generated by itself – at some stage of the computation. In this case we have got a contradiction, since the computation time for our program will be bigger than the computation time of itself!

The second step in our argument is a reduction: we prove that in case we assume **LPO**, then the **Halting Problem** is decidable. Indeed, let

$$\pi_1, \pi_2, \ldots, \pi_n, \ldots$$

be the set of all our programs and consider the following (computable) function μ:

$$\mu(m,k) = \begin{cases} 1, & \text{if } \pi_m(m) \text{ halts in time less than } k, \\ 0, & \text{otherwise.} \end{cases}$$

Applying **LPO** to the set of binary sequences

$$b_1^m, b_2^m, \ldots, b_i^m, \ldots,$$

where

$$b_i^m = \mu(m,i),$$

would solve the **Halting Problem**, which is impossible.

Markov's Principle, MP[24], which corresponds to our axiom A3., reads:

$$\neg\neg S(b) \Leftrightarrow S(b).$$

To illustrate **MP**[25] we consider an one-one enumeration of all possible proofs for tautologies:

$$p_1, p_2, \ldots$$

Let $a \in$ **Taut** and consider the predicate

$$Pred(a,i) = p_i \text{ is a proof for } a.$$

Clearly, for a fixed a, $Pred(a,i)$ is algorithmically decidable. Next, use **MP** to the statement

$$\exists i Pred(a,i),$$

saying that *it would be absurd to denny that there is a positive integer i such that $Pred(a,i)$.* From this fact we get no clue or computation bound for the construction of such an i.

To conclude, given a tautology a, we surely can get a **proof** for a; however, we can provide no indication concerning the number of proofs necessary to inspect

[24]**MP** is rejected by Brouwer, but freely used by the Russian school in constructive mathematics.

[25]It is interesting to note, following Brouwer, that the statement

$$\neg\neg\neg A \Rightarrow \neg A,$$

is constructively meaningful. Indeed, under the assumption $\neg\neg\neg A$ we can prove $\neg a$ by deriving a contradiction from A: if A, then $\neg A$ is absurd, hence $\neg\neg A$, which contradicts $\neg\neg\neg A$.

before getting the required **proof**: this state of affairs reflects the meaning of **MP**.

When considering the predicate calculus[26] we can prove a similar Completeness Theorem.[27] From a constructive point of view the situation is dramatically different: Church [12] has proven that *no proof of the Completeness Theorem for predicate calculus is constructive.* In this case the result has a devastating impact: *There is no algorithm testing the property of being a tautology, or equivalently, a theorem, for the predicate calculus.*

6 Decidability and Complexity

The formulation of the negative result cited at the end of the above section leaves the impression that the property of being a **theorem** of the propositional calculus is algorithmically decidable. Is this true?

Indeed, the above decision problem is algorithmically decidable, by virtue of the Completeness Theorem. **Theorems** coincide with tautologies and testing if an arbitrary proposition is or is not a tautology is algorithmically decidable. Apparently, switching from **theorems** to tautologies doesn't help too much, as we replace the (potential infinite) search through all possible proofs by a search through all possible interpretations of propositions (an infinite set, as well). This is only a superficial feeling! If a contains n atomic propositions, then we don't have to go through all possible interpretations h, but to examine only the restriction of these interpretations to the set of atomic propositions in a. We have arrived at a finite set, containing 2^n elements.

The immediate question is: How difficult is to decide if an arbitrary proposition a is a **theorem**? To approach this question we will discuss briefly the class **P** of polynomial algorithms. The Euclidean algorithm (for computing the greatest common divisor of two positive integers) is an example of a polynomial algorithm, in the sense that the number of basic bit operations (the *time* used by the algorithm) is a polynomial function of the number of bits in the input.[28]

Sometimes we are not able to design a polynomial algorithm for a problem; at least, we can prove that a solution for the problem can be quickly recognized if some miraculously source furnishes it to us. A good example is the problem of primality. It is not easy to determine if a positive integer having 1,000 digits is composite. But if we have got somehow two numbers and a claim that they

[26]One augments the propositional calculus with the quantifier symbols $\exists$ (there exists) and $\forall$ (for all) and all necessary extra constructions. De Morgan gave the first example of a logically valid argument which cannot be expressed in the propositional calculus: *All horses are animals. Therefore all horses' heads are animals' heads.*

[27]Due to Gödel [18].

[28]If the two inputs have at most n digits, then the larger input is less than 2^n, so the number of steps is bounded by cn. Each step involves a division, i.e. about n^2 bit operations, which gives finally a cubic polynomial. In fact, by a more involved analysis one can show that the Euclidean algorithm works in time bounded by a quadratic function of the length of inputs.

multiply to the given number, then we can very easily check if the claim is correct or not. These two numbers form a *certificate* of their compositeness. This leads to the important class **NP** of algorithms running in nondeterministic polynomial time, i.e. algorithms working in polynomial time under the assumption that a certain certificate has been given. One of the most intriguing open problems in theoretical computer science pertains exactly the relation between **P** and **NP**: **P** =? **NP**.

Testing if an arbitrary proposition a is a **theorem** along the path suggested at the beginning of this section requires an exponential computation time. Is it possible to do it better? No one knows this. We can see readily that our problem is in co-**NP**,[29] as guessing an interpretation which makes a false solves very quickly the problem.

In fact the problem **P** = ? **NP** is really meta-mathematical! Indeed, assume an appropriate coding and measure of the size of proofs. So, we may have polynomial size proofs and exponential size proofs. The difference between **P** and **NP** – if any – may be seen as a difference between *constructing* a polynomial size proof and *verifying* a polynomial size proof. If **P** = **NP**, then they are the same.

Currently, there is a lot of work devoted to the problem **P** = ? **NP**. We will confine ourselves only to a single recent result, just because it uses a nonstandard approach and gives us a concrete example of a new kind of *axiom* or *hypothesis*. To this aim we consider the exponential deterministic time-complexity classes

$$E = DTIME\left(2^{\text{linear}}\right), \text{ and } E_2 = DTIME\left(2^{\text{polynomial}}\right).$$

There are several reasons for considering these classes (Lutz [27, 28]):

1) Both classes E, E_2 have rich internal strutures.

2) E_2 is the smallest deterministic time complexity class known to contain **NP** and **PSPACE**.

3) $\mathbf{P} \subset E \subset E_2, E \neq E_2$, and E contains many **NP**-complete problems.

4) Both classes E, E_2 have been proven to contain intractable problems.

In view of the property 2) there may be well a natural "notion of smallness" for subsets of E_2 such that **P** is a small subset of E_2, but **NP** is not. Similarly, it may be that **P** is a small subset of E, but that $\mathbf{NP} \cap E$ is not! In the language of constructive measure theory smallness can be translated by "measure zero" (with respect to the induced spaces E or E_2). One can prove that indeed **P** has constructive measure zero in E and E_2, Lutz [27]. This motivates Lutz [28] to adopt the following quantitative hypothesis:

The set **NP** *has not measure zero.*

[29] co-**NP** is the class of sets X such that the predicate $x \notin X$ is in **NP**.

This is a strong hypothesis, as it implies $\mathbf{P} \neq \mathbf{NP}$. It is consistent with Zimand [40] topological analysis (with respect to a natural, constructive topology, if $\mathbf{NP} \backslash \mathbf{P}$ is non-empty, then it is a *second Baire category* set, while **NP**-complete sets form a *first category* class) and appears to have more explanatory power than traditional, qualitative hypotheses. As currently we are unable to prove or disprove this conjecture, the best strategy seems to investigate it as a scientific hypothesis; its importance is to be evaluated in terms of the extent and credibility of its consequences.

Two more problems are quite relevant for our discussion. Both belong to number theory and are currently *open*. The *prime number problem* asks for an polynomial time algorithm to check whether an arbitrary number n is prime.[30] It is plain that this problem is in **NP**; Pratt [35] has shown that it is also in co-**NP**. Miller [31] has proven that this problem is in **P** if *one assumes the extended Riemann Hypothesis*.[31] The other problem, the *factorization problem* asks for non-trivial factors of the natural number n, if n is composite. It is basic for many public-key crypto-systems ("trapdoor ones") and it is widely believed to be *intractable*. See more in Salomaa [38].[32]

It is interesting to note that:

- Much security is essentially based on a problem *believed* to be intractable, but concerning which very little is known.

- The *theoretical ignorance* supports two schools in Computer Science, the automatic proving systems based on resolution principles in AI (a school which is largely based on the belief that $\mathbf{P} = \mathbf{NP}$) and the public-key cryptography school (which assumes the opposite relation, i.e. $\mathbf{P} \neq \mathbf{NP}$).

7 Experimental Mathematics = Mathematics for the Future?

Church's theorem concerning the impossibility to prove constructively completeness for the predicate calculus is just a first result in a long list of theorems about the limits of mathematics.

A really impressive remark made by Bridges [5] is relevant for our discussion. Consider the following function F, defined on the set $\mathbf{N}$ of natural numbers:

$$F(n) = \begin{cases} 1, & \text{if the Continuum Hypothesis is true,} \\ 0, & \text{if the Continuum Hypothesis is false.} \end{cases}$$

[30]It should be emphasized that one is looking for a polynomial time algorithm in the number of digits representing the number n.

[31]The function

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots$$

has all non-real zeros on the axis $x = \frac{1}{2}$.

[32]Actually, we do not even know if this problem is **NP**-complete.

Deep work by Gödel [19] and Cohen[13] shows that neither the Continuum Hypothesis[33] nor its negation can be proved within Zermelo-Fraenkel set theory augmented with the axiom of choice. According to classical logic, F is computable because there exists an algorithm that computes it: that algorithm is either the one which always produces 0, or else the one which always produces 1. The trouble is we cannot know the correct one! And, as the Continuum Hypothesis is independent of the axioms of Zermelo-Fraenkel set theory augmented with the axiom of choice – the standard framework for mathematics – **we will never know which of the two algorithms actually is the one that computes** F.

The deepest result marking the limits of mathematics was discovered by Gödel [18]; we will present it in the stronger, information-theoretic variant due to Chaitin [9, 7, 37]:

- *An n-bit formal axiomatic system cannot enable one to exhibit any specific object with program-size complexity greater than $n + c$.*[34]
- *There exists an exponential diophantine equation*[35]

$$P(n, x, y_1, y_2, \ldots, y_m) = 0,$$

such that every n-bit formal axiomatic system cannot enable one to determine more than $n + c'$ naturals k for which the equation

$$P(k, x, y_1, y_2, \ldots, y_m) = 0$$

has an infinity of solutions.

The above results support Chaitin's claim that randomness has pervaded the inner structure of Mathematics![36] A complementary conclusion can be derived from another analysis of Gödel Incompleteness Theorem. In Calude, Jürgensen, Zimand [8] one proves that, in a quite general topological sense, incompleteness is a rather common phenomenon: *with respect to any reasonable topology the set of true and unprovable statements of a recursively enumerable, consistent, and rich enough theory is dense, and in many cases even co-rare.* These results show that the significance of axioms and proofs should be accordingly "modified". This point of view is consistent with the opinions expressed (thirty years ago) by Gödel [20, 21]:

[33] There is no cardinal number strictly in between aleph-null, the cardinal of the the set of natural numbers, and aleph-one, the cardinal of the set of reals.

[34] The program-size complexity of a finite object, e.g. a binary string, is a measure of the difficulty of specifying that object.

[35] That is an equation which is built by means of addition, mutiplication, and exponentiation of non-negative integer constants and variables.

[36] Note that the above assertion does not mean a "mandate for revolution, anarchy, and license".

> *... besides mathematical intuition there exists another (though only probable) criterion of truth of mathematical axioms, namely their fruitfulness in mathematics, and one may add, possibly also in physics ... The simplest case of an application of the criterion under discussion arises when some ... axiom has number-theoretical consequences verifiable by computation up to any given integer.*
>
> *... axioms need not be evident in themselves, but rather their justification lies (exactly as in physics) in the fact that they make it possible for these "sense perceptions" to be deduced ... I think that ... this view has been largely justified by subsequent developments, and it is to be expected that it will be still more so in the future. It has turned out that the solution of certain arithmetical problems requires the use of assumptions essentially transcending arithmetic ... Of course, under these circumstances mathematics may lose a good deal of its "absolute certainty"; but, under the influence of the modern criticism of the foundations, this has already happened to a large extent ...*

The above discussion leads naturally to the question: How should one do Mathematics? According to Chaitin [10]

> *... elementary number theory and the rest of mathematics should be pursued more in the spirit of experimental science, and ... [one] should be willing to adopt new principles.*

A new tendency in (the Philosophy of) Mathematics called **Experimental Mathematics** is emerging.[37] The emphasis on observational and experimental is not a new idea in the history of Mathematics; the novelty comes from the way and scale of experiments. This is possible due to the advent of computers; for a detailed analysis see S. Marcus [29, 30]. We have computer proofs for Gödel Incompletenss Theorem (Ammon [1]), computer proofs in Number Theory (Andrews, Ekhand, Zeilberger [2]), computer proofs for identities (Ekhand, Tre [15]). Computers were used in one of the technical steps of Louis de Branges' proof of the Bieberbach conjecture. Franz Mertens, a contemporary of Riemann, proposed a conjecture that involves only naturals; if true, this conjecture would have provided strong evidence that Riemann Hypothesis was also true. Mertens' conjecture was tested and proven true for at least the first 10 billion of naturals. However, a much larger computation revealed in 1984 that for numbers of the order of magnitute of

$$10^{(10^{70})}$$

[37] There are several journals using in their titles the adjective *experimental*, for instance, the *Journal of Experimental Mathematics*.

the pattern guessed by Mertens vanishes! Recently, Chaitin [11] showed that it is possible to write down executable programs (in C and *Mathematica*) that embody the constructions in the proofs of theorems in algorithmic information theory.

The utility of proofs in today, and, especially, tomorrow Mathematics is currently an object of debates, sometimes rather hectic (see, for instance, Horgan paper "The death of proof" [24], and one of the replies it generated, "The immortality of proof", by Kranz [26]). An important direction of this discussion is centered around the advent of a technique, developed by Lazlo Babai team, that offers not certainty, but only a statistical probability truth.

> *The philosophical cost of this efficient method is that we lose the absolute certainty of a Euclidean proof... But if you do have doubts, will you bet with me?*

says Babai.

Zeilberger [39], in a more radical attitude wrote about the **day after tomorrow**:

> *There are writings on the wall that, now that the silicon savior has arrived, a new testament is going to be written. Although there will always be a small group of "rigorous" old-style mathematicians (e.g. [16] [38]) who will insist that the true religion is theirs and that the computer is a false Messiah, they may be viewed by future mainstream mathematicians as a fringe set of harmless eccentrics, as mathematical physicists are viewed by regular physicists today. ...*
> *I speculate that ... [transparent proofs] will "trivialize" large parts of mathematics by reducing mathematical truths to routine, albeit possibly very long and exorbitantly expensive to check* "proof certificates"*. These proof certificates would also enable us, by plugging in random values, to assert "probable truths" very cheaply.*
>
> *I can envison an abstract of a paper, c. 2100, that reads,* "We show in a certain precise sense that the Goldbach conjecture is true with probability larger than 0.99999 and that its complete truth could be determined with abudget of 10 billion"*.*

We believe that there is a lot of exageration in saying that proofs are dead. *We will always need proofs! The problem is that sometimes we cannot afford them.*

[38] Jaffe and Quinn distinguishe between "Theoretical Mathematics" (referring to the speculative and intuitive work) and "Rigorous Mathematics" (the proof-oriented phase) in an attempt to build a framework assuring a positive role for speculation and experiment.

References

[1] K. Ammon. An automatic proof of Gödel's incompleteness theorem, *Artificial Intelligence* 61 (1993), 291-306.

[2] G. E. Andrews, S. B. Ekhand, D. Zeilberger. A short proof of Jacobi's formula for the number of representations of an integer as a sum of four squares, *Amer. Math. Monthly* 100 (1993), 274-276.

[3] D. W. Barnes, J. M. Mack. *An Algebraic Introduction to Mathematical Logic*, Springer-Verlag, New York, Heidelberg, Berlin, 1975.

[4] J. L. Bell, A. B. Slomson. *Models and Ultraproducts: An Introduction*, North-Holland, Amsterdam, Oxford, New York, 3rd revised printing, 1974.

[5] D. S. Bridges. *Computability – A Mathematical Sketchbook*, Springer-Verlag, Berlin, 1994.

[6] D. S. Bridges, F. Richman. *Varieties of Constructive Mathematics*, Cambridge, University Press, Cambridge, 1987.

[7] C. Calude. *Information and Randomness. An Algorithmic Perspective*, Springer-Verlag, Heidelberg, 1994. (in press)

[8] C.Calude, H. Jürgensen, M. Zimand. Is independence an exception?, *Appl. Math. Comput.* (in press)

[9] G. J. Chaitin. *Information-Theoretic Incompleteness*, World Scientific, Singapore, New Jersey, Hong Kong, 1992.

[10] G. J. Chaitin. Randomness in arithmetic and the decline and fall of reductionism in pure mathematics, *EATCS Bull.* 50(1993), 314-328.

[11] G. J. Chaitin. *The Limits of Mathematics – Course Outline & Software*, IBM Watson Center, Yorktown Heights, December 12, 1993, 127 pp.

[12] A. Church. A note on the entscheidungsproblem, *J. Symbolic Logic* 1 (1936), 40-41, 101-102.

[13] P. J. Cohen. *Set Theory and the Continuum Hypothesis*, Benjamin, New York, 1966.

[14] K. Devlin. Introduction to the column "Computers and Mathematics", *Notices Amer. Math. Soc.* 39 (1992), 1065-1066.

[15] S. B. Ekhand, S. Tre. A purely verification proof of the first Rogers - Ramanujan identity, *J. Combin. Theory*, Ser. A 54 (1990), 309-311.

[16] A. Jaffe, F. Quinn. "Theoretical mathematics": toward a cultural synthesis of mathematics and theoretical physics, *Bull. Amer. Math. Soc.* 29(1993), 1-13.

[17] K. Gödeł. Die Vollständigkeit der Axiome des logischen Funktionenkalkúlus, *Monatsh. Math. Phys.* 37 (1930), 582-591.

[18] K. Gödeł. Über formal unenscheidbare Sätze der Principia Mathematica und verwandter Systeme I, *Monatsh. Math. Phys.* 38 (1931), 173-198.

[19] K. Gödel. *The Consistency of the Continuum Hypothesis*, Princeton University Press, Princeton, 1940.

[20] K. Gödel. Russell's mathematical logic, in P. Benacerref, H. Putnam (eds.). *Philosophy of Mathematics*, Prentice-Hall, Englewood Cliffs, New Jersey, 1964, 211-232.

[21] K. Gödel. What is Cantor's continuum problem? in P. Benacerref, H. Putnam (eds.). *Philosophy of Mathematics*, Prentice-Hall, Englewood Cliffs, New Jersey, 1964, 258-273.

[22] P. R. Halmos. *Lectures on Boolean Algebras*, Van Nostrand, New Jersey, 1963.

[23] J. Herbrand. Sur la théorie de la démonstration, *C. R. Acad. Sci. Paris* 126 (1928), 1274-1276.

[24] J. Horkan. The death of proof, *Scientific American* 269(1993), 74-82.

[25] L. Kalmár. Über die axiomatisierbarkeit des Aussagenkalkülus, *Acta Sci. Math. (Szeged)* 7 (1934-5), 222-243.

[26] S. G. Kranz. The immortality of proof, *Notices Amer. Math. Soc.* 41(1994), 10-13.

[27] J. H. Lutz. Almost everywhere high nonuniform complexity, *J. Comput. System Sci.* 44(1992), 220-258.

[28] J. H. Lutz. The quantitative structure of exponential time, *Proceedings of the Eighth Annual Structure in Complexity Theory Conference*, (San Diego, CA, May 18–21, 1993), IEEE Computer Society Press, 1993, 158-175.

[29] S. Marcus. *The Mathematical Shock*, Albatros Publ. House, Bucharest, 1987. (in Romanian)

[30] S. Marcus. *Controversies in Science and Engineering*, Technical Publ. House, Bucharest, 1990. (in Romanian)

[31] G. L. Miller. Riemann's hypothesis and tests of primality, *J. Comput. System Sci.* 13(1976), 300-317.

[32] P. Odifreddi. *La prova di dio*, manuscript, January 1994, 8 pp.

[33] P. Odifreddi. *Ultrafiltri, dittatori e dei*, manuscript, January 1994, 9 pp.

[34] E. Post. Introduction to a general theory of elementary propositions, *Amer. J. Math.* 43 (1921), 1963-1985.

[35] V. Pratt. Every prime has a succinct certificate, *SIAM J. Comput.* 4(1975), 214-220.

[36] H. Rasiowa, R. Sikorski. A proof of the completeness theorem of Gödel, *Fund. Math.* 37 (1951), 193-200.

[37] G. Rozenberg, A. Salomaa. *Cornerstones of Undecidability*, Prentice-Hall, 1994.

[38] A. Salomaa. *Public-Key Cryptography*, Springer-Verlag, Berlin, 1990.

[39] D. Zeilberger. Theorems for a price: Tomorrow's semi-rigorous mathematical culture, *Notices Amer. Math. Soc.* 40 (1993), 878-891.

[40] M. Zimand. If not empty, $NP \setminus P$ is topologically large, *Theoret. Comput. Sci.* 119 (1993), 293-310.

[41] N. Wiener. *God and Golem*, MIT Press, Cambridge, Mass., 1964.