Mathematical Knowledge: Motley and Complexity of Proof

Akihiro Kanamori

May 21, 2010

Modern mathematics is, to my mind, a complex edifice based on *conceptual constructions.* The subject has undergone something like a biological evolution, an opportunistic one, to the point that the current subject matter, methods, and procedures would be patently unrecognizable a century, certainly two centuries, ago. What has been called "classical mathematics" has indeed seen its day. With its richness, variety, and complexity any discussion of the nature of modern mathematics cannot but accede to the primacy of its history and practice. As I see it, the applicability of mathematics may be a driving motivation, but in the end mathematics is autonomous. Mathematics is in a broad sense self-generating and self-authenticating, and alone competent to address issues of its correctness and authority.

What brings us mathematical knowledge? The carriers of mathematical knowledge are *proofs*, more generally arguments and constructions, as embedded in larger contexts.[1] Mathematicians and teachers of higher mathematics know this, but it should be said. Issues about competence and intuition can be raised as well as factors of knowledge involving the general dissemination of analogical or inductive reasoning or the specific conveyance of methods, approaches or ways of thinking. But in the end, *what can be directly conveyed as knowledge are proofs.*

Mathematical knowledge does not consist of theorem statements,[2] and does not consist of more and more "epistemic access", somehow, to "abstract objects" and their workings. Moreover, mathematical knowledge extends not so much into the statements, but back into the means, methods and definitions of mathematics, sometimes even to axioms. Of course, statements are significant as encapsulations or markers of arguments. However, the bare statement, no matter how striking or mundane, remains aloof and often mysterious as to what it conveys. Statements gain or absorb their senses from the proofs made on their behalf. One does not really get to *know* a statement, but rather a proof, the complex of argument taken altogether as a conceptual construction.

[1] In a perceptive paper advocating similar themes Rav [15] used the term "bearer" instead of "carrier". The former is more passive, as in "bearer of good tidings".

[2] Here, "statement" is being used to suggest mere prose expression, in preference to the weightier "proposition", which often translates Frege's "Satz" and was also used by Russell.

A statement may have several different proofs each investing the statement with a different sense, the sense reinforced by different refined versions of the statement and different corollaries from the proofs.[3] In modern mathematics, proofs and arguments often achieve an autonomous status beyond their initial contexts, with new, generalizing definitions formulated and new spaces of mathematical objects devised just so that certain proofs and, more generally, methods can be carried out in a larger context. In this sense knowledge begets knowledge, each new context a playing field for the development of new proofs. Proofs are not merely stratagems or strategies; they and thus their evolution are what carries forth mathematical knowledge.

Based on the autonomy of mathematics and anchored in its practice and history, this emphasis on proof is not to be any particular "theory". It is not to advocate a verificationism with a thick sense of meaning, for it is the myriad of verifications themselves which is the message. Nor is it to advocate a deductivism, since there is no presumption that the content of modern mathematics can be coherently axiomatized, and there is no presumption that mathematical proofs need be converted to formal deductions in a formal system. Nor is it to advocate any form of constructivism, although there is a surface affinity in the use of the word "construction" and with the basic constructive tenet that to assert a statement is to provide a proof. Mathematics is to be accounted for both as a historical and an epistemological phenomenon, with the evolution of proofs and methods at the heart.

What about truth in mathematics? Since proofs are the carriers of mathematical knowledge, whether mathematical statements are true or false is not as central to mathematics as the proofs devised on their behalf. Truth does not have an independent, *a priori* meaning in modern mathematics, but it does operate in mathematics in a primordial way. Truth is normative; statements are incipiently taken to be true or false; and bivalence is intrinsic to its basic grammar. Problems and conjectures get clarified and contextualized, and some are eventually transformed into a proof. When a mathematician proves a statement, it is true mainly in that a proof has been provided, one that can be examined. The picture then is that mathematical truth abounds everywhere, and the directions of investigations, the working out of particular truths, is a matter of historical contingency and the social context of mathematicians working with problems and conjectures. Truth serves at the beginning of investigation to intimate an initial parting of ways, but is not the end, which is the proof. Of course, one can analyze an argument as a web of implications and consider whether each implication as a statement is true or false. Truth again functions

[3] Evidently, "sense" here is being used in a common-sensical way, one not tied in any theory of meaning. Waismann [21] p.109 recorded Wittgenstein on 25 September 1930 on proof: "A proof is not a vehicle for getting anywhere, but is the thing itself. . . . two different proofs cannot lead to the same thing. Two proofs can either meet, like two paths leading to the same destination, or they prove different things: a difference between proofs corresponds to a difference between things proved." A note is added: "A transformation of two proofs into one another is the proof of their proving the same thing." In other words, it may be that one proof can be transformed into another of the same statement, but that very transformation is yet another proof.

primordially here, but invariably this pressing into the interstices comes to an end, and we take in the argument as a whole.

Truth, whether a statement has the property of being true or the property of being false, is itself too primal to be definable or otherwise characterizable. Little can be *done* with truth as such in mathematics.[4] This by no means is to dispense with truth or to advocate a deflationist theory of truth; rather, it is to point out how no general theory of truth will have any bearing on mathematics and its practice.[5]

What, finally, about existence in mathematics? Existence is surely not a predication in mathematics. Whether numbers or sets exist or not in some prior sense is devoid of mathematical interest. Questions like "What is a number?" and "What is a set?" are not mathematical questions, and any answers would have no operational significance in mathematics.[6] *Within* mathematics, an existence assertion may be an axiom, a goal of a proof, or one of the junctures of a proof. Existence is then submerged into context, and it is at most a matter of whether one regards the manner in which the existence assertion is deduced or incorporated as coherent with the context.[7] Finally, there are many junctures in proofs, especially since the turn of the 20th Century and in modern algebra, in which negations of universal statements in a variable are considered. In formal terms, one works with the equivalence of $\neg\forall$ with $\exists\neg$, and in informal terms one searches for counterexamples to deny universality — there are proofs and refutations. Existence in mathematics is embedded in the calculi of mathematics; to be is to be in the range of a variable in some mathematical system. No theory of mathematical existence, let alone any resolution of any realism vs. anti-realism debate, will have any bearing on mathematics and its practice. Varieties of structuralism may try to deal with mathematical objects as submerged in relations and structures, but there is still the "second-order"

[4]Kant, *Critique of Pure Reason* A58/B83: "What is truth? The nominal definition of truth, that it is the agreement of knowledge with its object, is assumed as granted; the question asked is as to what is the general and sure criterion of the truth of any and every knowledge.

To know what questions may reasonably be asked is already a great and necessary proof of sagacity and insight. For if a question is absurd in itself and calls for an answer where none is required, it not only brings shame to the propounder of the question, but may betray an incautious listener into absurd answers, thus presenting, as the ancients said, the ludicrous spectacle of one milking a he-goat and the other hold a sieve underneath."

[5]Wittgenstein, *Philosophical Investigations* §241: "So you are saying that human agreement decides what is true and what is false?" –It is what human beings *say* that is true and false; that is not agreement in opinions but in form of life [Lebensform].

[6]The Fields medalist Timothy Gowers [9] p.18 aptly wrote: "A mathematical object *is* what it *does*."

[7]Waismann [21] pp.172ff recorded Wittgenstein on 21 September 1931 on proof of existence: "If, on one occasion, I prove that an equation of degree n must have n solutions by giving, e.g. one of the Gaussian proofs, and if, on another, I specify a procedure for deriving the solutions and so prove their existence, I have by no means given two different proofs of the same proposition; I have proved entirely different things. What is common to them is simply the prose proposition 'There are n solutions', and that, taken by itself, means nothing, being a mere abbreviation standing for a proof. If the proofs are different, then this proposition simply *means* different things."

question of what is a structure, and in any case, the preoccupation is still with mathematical existence.

Mathematicians themselves have often described a feeling of dealing with independent, autonomous objects, some professing an avowedly realist view of mathematics. The simple reply is that this is psychological, perhaps informatively attributable to our cognitive mechanisms, and the reification, an operational attitude. Objectification is part of the practice of mathematics, the sense of existence here to be described as in any other concerted social activity, and it is particularly fostered by the precision of mathematical language. Mathematicians work with equal vigor in incompatible theories, e.g. non-Euclidean geometries, with objects "existing" in one theory but not in another, and more pointedly, there is the *counterexample phenomenon*: In order to establish a universal $\forall$ statement, one works at length on counterexamples, these "existing" in context in just as full-bodied a sense as examples, until one can dismiss them as not "existing". Some of the most complex and prolonged proofs, e.g. in finite group theory,[8] have this overall character of a *reductio ad absurdum* proof based on the equivalence of $\neg\forall$ and $\exists\neg$.

§1. At the Beginnings of Set Theory

Let me give a notable example at the heart of set theory that illustrates several of the foregoing points. In 1904 Ernst Zermelo [23] established the Well-Ordering Theorem, that every set can be well-ordered, applying the Axiom of Choice. Indeed, it was for this purpose that he made explicit the axiom, which he considered a logical principle "used everywhere in mathematical deduction". That part of the argument that does not depend on the axiom can be isolated in the following result, not made explicit by Zermelo, which establishes a basic correlation between functions "type-reducing" $\gamma\colon \mathcal{P}(M) \to M$ from the power set $\mathcal{P}(M) = \{X |\ X \subseteq M\}$ of a set M into the set and definable well-orderings.[9]

Theorem 1. *Suppose that $\gamma\colon \mathcal{P}(M) \to M$. Then there is a unique $\langle W, \prec\rangle$ such that $W \subseteq M$ and $\prec$ is a well-ordering of W satisfying:*

(a) For every $x \in W$, $\gamma(\{y \in W \mid y \prec x\}) = x$, and

(b) $\gamma(W) \in W$.

The picture here is that γ generates a well-ordering which according to (a) starts with

$$a_0 = \gamma(\emptyset),\ a_1 = \gamma(\{a_0\}),\ a_2 = \gamma(\{a_0, a_1\}),\ \ldots$$

and so continues as long as γ applied to the initial segment constructed thus far produces a new element. W is the result when according to (b) an old element is again named.

[8] The concluding section has other examples.

[9] The following analysis is drawn from Kanamori [13, §2]. Tarski [19, Theorem 3] was a version of the theorem. Substantially the same version appeared in the exposity work of Bourbaki [5, p.43] (Chapter 3, §2, Lemma3).

Proof of Theorem 1. Call $Y \subseteq M$ a *γ-set* if and only if there is a well-ordering R of Y such that for each $x \in Y$, $\gamma(\{y \in Y \mid y\ R\ x\}) = x$. We shall establish:

$(*)$ If Y is a γ-set with a witnessing well-ordering R and Z is an γ-set with a witnessing well-ordering S, then $\langle Y, R\rangle$ is an initial segment of $\langle Z, S\rangle$, or vice versa.

Taking $Y = Z$ it will follow that any γ-set has a unique witnessing well-ordering.

For establishing $(*)$, we continue to follow Zermelo: By the comparability of well-orderings we can assume without loss of generality that there is an order-preserving injection $e\colon Y \to Z$ with range an S-initial segment of Z. It then suffices to show that e is in fact the identity map on Y: If not, let t be the R-least member of Y such that $e(t) \neq t$. It follows that $\{y \in Y \mid y\ R\ t\} = \{z \in Z \mid z\ S\ e(t)\}$. But then,

$$e(t) = \gamma(\{z \in Z \mid z\ S\ e(t)\}) = \gamma(\{y \in Y \mid y\ R\ t\}) = t\,,$$

a contradiction.

To conclude the proof, let W be the union of all the γ-sets. Then W is itself a γ-set by $(*)$ and so, with $\prec$ its witnessing well-ordering, satisfies (a). For (b), note that if $\gamma(W) \notin W$, then $W \cup \{\gamma(W)\}$ would be a γ-set, contradicting the definition of W. Finally, that (a) and (b) uniquely specify $\langle W, \prec\rangle$ also follows from $(*)$. ⊣

Zermelo of course focused on choice functions as given by AC to well-order the entire set:

Corollary 2 (The Well-Ordering Theorem)(Zermelo [23]). *If $\mathcal{P}(M)$ has a choice function, then M can be well-ordered.*

Proof. Suppose that $\varphi\colon \mathcal{P}(M) \to M$ is a choice function, i.e. $\varphi(X) \in X$ whenever X is non-empty, and define a function $\gamma\colon \mathcal{P}(M) \to M$ to "choose from complements" by: $\gamma(Y) = \varphi(M - Y)$. The resulting W of the theorem must then be M itself. ⊣

Theorem 1 also leads to a new proof of Cantor's Theorem, a proof that eschews diagonalization altogether and moreover provides a definable counterexample to having a one-to-one correspondence between a set and its power set:

Corollary 3. *For any $\gamma\colon \mathcal{P}(M) \to M$, there are two distinct sets W and Y both definable from γ such that $\gamma(W) = \gamma(Y)$.*

Proof. Let $\langle W, \prec\rangle$ be as in Theorem 1, and let $Y = \{x \in W \mid x \prec \gamma(W)\}$. Then by (a) of Theorem 1, $\gamma(Y) = \gamma(W)$, yet $\gamma(W) \in W - Y$. ⊣

In the $\gamma\colon \mathcal{P}(M) \to M$ version of Cantor's diagonal argument, first given by Zermelo himself ([24, Theorem 2]), one would consider the definable set

$$A = \{\gamma(Z) \mid \gamma(Z) \notin Z\} \subseteq M.$$

If $\gamma(A) \notin A$, then we have the contradiction $\gamma(A) \in A$. If on the other hand $\gamma(A) \in A$, then $\gamma(A) = \gamma(B)$ for some B such that $\gamma(B) \notin B$. But then, $B \neq A$. However, no such B is provided with a *definition*.[10]

To emphasize an important contention about the primacy of proof for mathematical knowledge: At the heart of set theory is Cantor's Theorem, its crux being: there is no one-to-one correspondence between a set and its power set. Cantor's diagonal proof provides one sense as a *reductio* argument, one that can also be used to generate a new real from a countable sequence of reals. Corollary 3 provides another sense, with a recursive definition of a well-ordering.

Bringing out the new sense, the proof of Theorem 1 informs Cantor's Theorem with another notable consequence expressible only in the new setting where sets are not inherently well-ordered: Since the γ there need only operate on the *well-orderable* subsets of M, the $\mathcal{P}(M)$ in Corollary 3 can be replaced by the following set:

$$\{Z \subseteq M \mid Z \text{ is well-orderable}\}.$$

That this subset of $\mathcal{P}(M)$ is also not in one-to-one correspondence with M was first pointed out by Tarski [19] through a less direct proof.

§2. Proofs in Mathematics

If mathematical proofs are the carriers of mathematical knowledge, the nature of mathematical proof as embedded in mathematical practice plays a central role in epistemology. But what *is* a proof? In what ways do proofs validate statements? There can only be *descriptive* answers, as one surveys the motley of modern mathematics in all its variety and complexity and sees a motley of proofs as avenues to knowledge.

At the outset, a proof is a network of implicational connections between a series or web of statements. The connections can be fused or split, and the juncture statements themselves can be reduced, shifted, or proliferated according to how a mathematician might conceive of or teach a proof. In the direction of refinement, the connections can be split more and more with intermediary statements introduced, but this may jeopardize the surveyability of the proof. A *mathematical* proof has an irreducible semantic content that is carried by the implicational connections and juncture statements at an appropriate level of organization, one that is based on the concepts and methods of the context.

There are crucial aspects of proof beyond just the schematic picture which are brought out by the *communication* of proofs among mathematicians. Proofs ought to be communicable, and so ultimately they should be written down. But before then, proofs—generally methods and schemes—are often communicated in conversations and seminars among those in the subfield. Pictures are drawn; ideas are metaphorically described; there are telling side comments. Just a few gestures and remarks may suffice to convey a proof, as one draws on the common store of knowledge and ways of thinking that have long been assimilated as part

[10]This is also the main thrust of Boolos [4], in which the argument for Theorem 1 is given *ab initio* and not connected with Zermelo [23].

of the "language game" of the subfield. Mathematicians in a subfield are very reliable in checking each other's work and have a sharp sense of when a proof is correct based merely on a high-level configuration of ideas and methods, the details to be attended to later. Indeed, the sign of a very good mathematician is the ability to separate the steps which are procedural and unproblematic from those that require something distinctly new.

This last brings out a crucial feature of a *new* proof in the historical, evolutionary sense: Although a proof is a network of implicational connections, one or two particular connections becomes pivotal. These are the keys that unlock, the crucial gaps that are filled, or the new innovations that reorganize the implicational connections. From simple proofs to the intimation of new methods, there is often just one telling connection that clinches the proof, and this is related to the common epiphanous experience of suddenly seeing a proof whole and correct.

The writing down of proofs raises major issues for the conveyance of mathematic knowledge. Research mathematicians can be poor expositors, often adhering to presentations with overemphasis on brevity of argument or generality of applicability. One looks in vain for a discussion of themes, motivations, the wider historical context in which to place the new proofs. A strenuous effort is often required to assimilate a proof presented in a research paper, an effort that amounts to making one's own implicational connections at different conceptual levels. Mathematicians know that published accounts of proofs are often backward in that they are written forward, that the road to discovery was some new connection toward the end. So what actually *was* the proof presented? Even subsequent expositions, however well-intended, sometimes err on the side of simplicity. Simpler and simpler versions of proofs may be presented, but this can be at the the cost of emasculation or mystification; a proof as a larger conceptual construction may be shorn of its richness and consequence through streamlining, leaving an air of mystery as to how it could have been conceived. A sure sign is that structural corollaries that could have been drawn formerly are no longer possible. We are left with the realization that formal proofs are not crucial, that the correctness and authority of the modern mathematical enterprise must lie in a wider sense of proof as embedded in mathematical practice.

Mathematicians have steadily re-proved theorems, and this is a conspicuous feature of modern mathematics and significant for its epistemology. Why reprove a state if it is already true? Because the fact of the matter does not reside in its truth but in its avenues, the exploration of the conceptual constructions that see it out. Mathematical knowledge is not a roster of true statements but the web of connections among them and the techniques and methods that hold up the edifice. There are a variety of reaons why mathematicians re-prove theorems:[11]

(1) To provide a constructive or more effective demonstration. This includes

[11] See Dawson [7]; the following list amounts to a reorganization of his.

providing constructive proofs for existence statements and providing faster algorithms, like the recent primality testing in polynomial time.

(2) To eliminate hypotheses or apply methods appropriate to the statement context. This includes eliminating the Axiom of Choice, the Riemann Hypothesis, and so forth, and providing proofs for number-theoretic statements in Peano Arithmetic, like the elementary proof of the Prime Number Theorem.

(3) To provide a regressive reconstruction of historical practices. This includes Hilbert's rigorization of Euclidean geometry and the development of generalized distributions to handle Dirac's delta function. New statements are proved, as the underlying concepts themselves having been transmuted.

(4) To simplify and make more direct and surveyable earlier proofs. This involves reducing the computations and hypotheses that depended on an earlier proof having come out of a complex setting, but comes with the danger of increasing the mystery and a sense of surprise. An example is Hilbert's basis theorem, which actually goes counter to (1).

(5) To demonstrate different approaches. This includes algebraic or topological proofs of geometric statements and proofs of non-standard analysis.

(6) To generalize an earlier result into a larger context. This includes extensions of the Riemann integral and Henkin's proof of the Completeness Theorem.

Proofs at the complex end of the range of proofs raise further issues, particularly those of *surveyability*, *intelligibility*, *acceptance*, and the dependence on *authority*, i.e. the reliance on experts—and these are the significant and interesting issues, further and further away from abstract preoccupations about the relation of proof to truth. What is most striking about the evolution of mathematics in the last half-century is that it has become such a complex edifice. This complexity presumably came into mathematics with the 1962 proof of Walter Feit and John Thompson resolving the Burnside Problem: *All finite groups of odd order are solvable.*[12] The proof was non-constructive, proceeding from a minimal counterexample to draw a contradiction. This is an important, early example of existence in mathematics as informed by the *counterexample phenomenon*, the working at length on counterexamples, these "existing" in context until they can be dismissed. The publication [8] was well over two hundred pages and had to be farmed out to several referees. And this itself was just a beginning: 100 group theorists working in a cottage industry for the two subsequent decades and publishing 10,000 journal pages were said to have completed the classification of all finite simple groups: *Every finite simple group is either a group of prime order, an alternating group, a group of Lie type, or else one of the 26 sporadic groups.* No single mathematical statement hitherto had such a long proof, a proof variously featuring the counterexample phenomenon. In the 1990s a program was launched to simplify large parts of the proof and to write it all down in one place, but gaps emerged that continue to be filled.[13] This may be increasing the surveyability and intelligibility of the classification, but with the best estimates for the size of the proof still at around 4000 pages, acceptance

[12] Equivalently, every finite simple non-Abelian group is of even order.

[13] See Aschbacher [3] for the current status.

by the wider mathematical community may remain across a spectrum. "True" applied here may have a longstanding vagueness akin to words like "big". The classification has been applied in subsequent mathematics, and as a juncture statement in a proof it will very much have to be based on authority, on the reliance on experts.

Issues about the concept of proof and its possible liberalization came to fore with the 1976 proof by Kenneth Appel and Wolfgang Haken of the Four-Color Theorem: *Every planer graph is four-colorable.*[14] The counterexample phenomenon at play, they were able to reduce the infinitude of possible counterexamples to 1476 configurations, and then in 1200 hours of computing time they showed that these too are four-colorable. Going beyond finite group theory in terms of authority, computer-assisted proofs manifest reliance on experts no longer for presumably intelligible implicational connections, but also for avowedly un-intelligible connections. Understanding has been relegated to an overview of the myriad of connections mapped out, the computer completing the tasks.

On the one hand, there was debate about admitting the Appel-Haken argument into the pantheon of proofs, but on the other hand, there was the feeling that at least the door was closed on the problem. However, subsequent events interestingly provided new knowledge, as for "conventaionl" surveyable proofs. First, the 1989 741-page monograph Appel-Haken [2] significantly diminished skepticism, with its detail and overall careful account. Then in 1995, Neil Robertson, Daniel Sanders, Paul Seymour and Robin Thomas provided a new, still computer-assisted, proof featuring new techniques that initially reduced the configurations to 633 and provided a four-coloring algorithm of quadratic, $O(n^2)$ order[15] — the Appel-Haken proof had led to a quartic, $O(n^4)$ algorithm. Latterly in 2004, Georges Gonthier and Benjamin Werner wrote a formal proof script for the computer code part of the 1995 proof in a language that used logical propositions and applied a proof checking system which mechanically verified the correctness.[16]

In 2005 Gonthier in a singular advance carried out a complete, computer-assisted formalization of a proof of the Four Color Theorem in its entirety. Gonthier began with the Robertson-Sanders-Seymour-Thomas proof, and in the process implemented new approaches, as befitted the computer-assisted framework, with combinatorial hypergraphs. This remarkable development signaled the establishment of a new, notable field of mathematics devoted to the complete computer-assisted formalization of proofs. A traditional, mathematical proof is first written out in greatly expanded form with all the assumptions made explicit and all the cases treated in full. From the expanded text a computer script is prepared which generates all the logical inferences of the proof. This is done with "computer assistants", computer systems which are either declarative, in which proofs are written out in atomic steps, or procedural, in which proofs are generated interactively through dialogue. Currently, Gonthier

[14] See Appel-Haken [1], and the monograph Appel-Haken [2].
[15] See [16].
[16] See http://ralyx.inria.fr/2003/Raweb/moscova/uid23.html.

is carrying out a complete formalization of the Feit-Thompson result.

This new field of mathematics substantively realizes the ideal of formalization in the direction of actual proof implementation. Instead of "formalizable in principle" we have formalization in realization. Hilbert with his metamathematics emphasized and advanced the formalizability of mathematics, but was not interested in formalizations of actual proofs. Before him Gottlob Frege and Bertrand Russell provided formal proofs to establish the reduction of mathematics to deductive logic. The real precursor was Guiseppe Peano, who devised an efficient symbolic language and sought to provide, with his *Formulario Mathematico*, an encyclopedia of all known formulas and theorems of mathematics. Similarly, a stated goal of the new formalization field is to someday provide a library of Alexandria of complete, formalized proofs, the possibility only newly realizable through computer assistants. Another, new incentive that may become more and more prominent is to verify increasingly complex proofs, so that authority is transferred from humans to computers. This is a remarkable development, one prompted by the new complexities of proof, and it may well turn out that the very issues of surveyability, intelligibility, and authority about proof will affirm a new meta-mathematics, new mathematical knowledge generated by the subject of proof itself.

The issues of surveyability and intelligibility vis-à-vis computer-assisted proofs had become accentuated by the 1998 proof by Thomas Hales of the Kepler Conjecture: *Congruent balls in three dimensions can be packed with the highest density in rows with rectilinear or, equivalently seen from another perspective, hexagonal arrangements.*[17] This was a specific part of Hilbert's 18th Problem, and the proof involved global optimization, linear programming, and interval arithmetic, and like the proof of the Four-Color Theorem, the counterexample phenomenon. At the outset there was a reduction to about 5000 large scale nonlinear optimization problems. Then there was a further reduction to about 100,000 linear programming problems each with 100 to 200 variables. Having appealed to 12 referees the *Annals of Mathematics* [12] published the non-computer part of the argument with a footnote distancing itself from the computer part, appearing in Hales [11].[18]

Although Hales's argument for Kepler's Conjecture may become increasingly accepted as a proof by the mathematical community, it is one *without potentiality*, even more than the solutions to the Four Color Conjecture, and this perhaps is its most telling feature for epistemology: Nothing larger is learned from the argument, and it does not open up new possibilities for mathematics. But in this case, the gap with computer capability is much more pronounced, and only the future will tell how new developments in formalization will color the conjecture. With his Flyspeck Project Hales aspires to provide a complete formalization of a proof of the Kepler Conjecture and estimates it to be a a 7000 work-day project.

In contrast, there is Andrew Wiles' 1994 proof of Fermat's Last Theorem:

[17] See Hales [10] for a short and Szpiro [17] for a book-length, account.

[18] See Hales's website www.math.pitt.edu/∼thales for more on the interaction with computation.

There is no solution to $x^n + y^n = z^n$ *in positive integers for any* $n > 2$. In a substantial sense, this statement isolated and unto itself has no intrinsic interest whatsoever, and it only grew in historical significance as it withstood more and more techniques, techniques that have enriched mathematics considerably like the Kummer theory of ideals. No, what is tremendous about the Fermat is the Wiles *proof*. He actually established the Shimura–Taniyama Conjecture about elliptic curves in algebraic geometry through a beautiful synthetic proof, and this among mathematicians has been seen as the great advance. The perennial pushing for the Fermat had led to a novel observation about a connection to elliptic curves, a connection that was affirmed by the late 1980s to establish that the Shimura–Taniyama Conjecture implies Fermat's Last Theorem. Thus, Wiles's proof had a last implicational connection due to others. This is not to say that Wiles did not covet the prize. This truth among a myriad was definitely stalked, but in any case the proof considerably enriched the theory of elliptic curves, a theory that has its origins centuries ago in the study of planetary motion. There is still the issue of authority, but the understanding brought about by the proof is acknowledged in large part through its potentiality, its opening up of new possibilities.

Wiles's proof [22] has raised interesting issues about proof.[19] Wiles wrote that "the turning point in this and indeed in the whole proof came" when he was led to two cohomology invariants from Grothendieck's duality theory. The Wiles proof in fact depends on the so-called "Grothendieck Universes". In arithmetic algebraic geometry of the last fifty years the algebra and topology of *schemes*, certain spaces, have been investigated through cohomology with respect to how they are situated in large categories. A straightforward formalization of Wiles' proof thus requires several levels of above the usual cumulative hierarchy of ZFC. However, at the expense of elegance and a surveyable level of organization, the Wiles's proof can evidently be established in ZFC alone, and here, set-theoretic reflection would be the evident approach. Recently, Angus MacIntyre has claimed that the central Modularity Thesis in Wiles's proof is provable in Peano Arithmetic. If so, then there could a new proof of the Fermat Last Theorem in Peano Arithmetic, possibly by bypassing through further analysis the Modularity Thesis.

The issues aired above about proof figured fresh in the recent excitement about Grigori Perelman's proof of the Poincaré's Conjecture: *Every simply connected closed three-manifold is homeomorphic to the three-sphere.*[20] Informally, the sphere is the only type of bounded three-dimensional space possible that contains no holes. Formulated a century ago this conjecture, unlike Fermat's Last Theorem but like Kepler's Conjecture, has the immediacy of a fundamental structural characterization. But unlike, say, Riemann's Hypothesis, there was no general presumption about which way it would go; groups worked through the 1980s and into the 1990s both to try to find a proof and to try to find a counterexample. With increasing effort expended, resolution of the conjecture

[19] What follows is taken from McLarty [14].

[20] See Collins [6] for a short and Szpiro [18] for a book-length, account.

had become more and more prized, and the Clay Institute in 2000 offered a million dollars for a confirmed proof, as one of several outstanding problems for the millenium.[21]

Like Wiles's proof, Perelman's argument was actually to resolve a more general conjecture, in this case the classification of all three-manifolds according to William Thurston's *geometrization*. In 2002 and 2003 Perelman sketched his argument in three papers, amounting to 68 dense and terse pages, and gave a series of talks across the United States and Europe in 2003. Because of the centrality of geometrization, the argument began being vetted by the experts. Seminars and workshops worked their way through; sketches were filled in with detailed proof; and there were reorganized expositions.[22] All this increased the surveyability and the intelligibility, and the high-level configuration of ideas and methods together with Perelman's ability to convey verbally the local and global structures of the argument gradually led over a couple of years to a general acceptance of his proof based quite avowedly on authority. Eventually, three pairs of authors published accounts in 2006 detailing Perelman's proof: the Kleiner-Lott notes in 200 pages filled out the Perelman papers, like a Talmudic exegesis, to provide a proof of geometrization; the Cao-Zhu paper amounting to 326 pages also provided a proof of geometrization; and the Morgan-Tian monograph in 521 pages gave a careful, "self-contained" account of just the Poincaré Conjecture solution. In 2006, Perelman was awarded the Fields Medal,[23] and just March of this year, 2010, was awarded the million dollar Clay prize for the Poincaré Conjecture.

We tuck in here another example, though it does not have to do as much with proof surveyability but effectiveness. Also in 2006, Terence Tao was award the Fields Medal for his solutions of problems over work in a broad range of areas. His best-known result has been his 2004 joint result with Ben Green: *There are arbitrarily long arithmetical progressions of prime numbers*. They brought together a cocktail of sophisticated mathematical ideas to solve a very old problem, and the result *is* surveyable, but there is another issue. The Green-Tao Theorem was another non-constructive existence assertion, in that it provided no algorithmic means of providing an arithmetical progression of specified length.[24] In fact, before they had established this theorem of modern mathematics in 2004, 23 was the length of the longest known arithmetic progression of primes, and as of 12 April 2010, it is 26. On one side there is the steady work of improving specific computational procedures—in effect new mathematical arguments and proofs—and on the other, there are the enormously sophisticated methods of modern mathematics — both focused on an age old issue about the prime

[21] The See the website www.claymath.org/millennium/ for the problems and an account of their importance for mathematics.

[22] See the website http://www.math.lsa.umich.edu/ lott/ricciflow/perelman.html.

[23] The Fields Medal is the most prestigious award given to a mathematician, with several awarded every four years at the International Congress of Mathematicians. Perelman was the first to refuse to accept the medal.

[24] In fact, the other well-known result of Klaus Roth, of 1952,that any set of positive integers of positive density has arithmetic progressions of length three, was the beginning of results toward the Green-Tao result.

numbers. On the latter side, mathematicians are moving ahead toward an old conjecture of Paul Erdős, that if a set A of natural numbers has the property that $\Sigma_{n\in A}1/n = \infty$, then A contains arbitrarily long arithmetical progressions of prime numbers. One has to look for a new kind of proof, and there is even talk about undecidability, the complexity of definition of A becoming an issue.

The weight of these various examples shows how far away mathematics now is from being comprehended by any formal notion of proof and any theory of mathematical knowledge, and how the limits of human intelligibility are being put to the test. A complicated proof is like the Grand Tour: We are first given an itinerary and told that the connections can be made by straightforward means. The capitals Paris and Rome loom large, and in their terms we start to find our way about. We are soon taken in by Florence, seduced by Venice. The connections become shorter, and we explore the lesser churches and monuments. History begins to play an increasingly important role, and we put together a picture for ourselves of how it all fits. In our further travels we see more and more of the smaller towns and villages, but we also return refreshed to the large capitals. We make friends and look up relatives.

The argumentation is more important than the theorem; it is the journey, not the destination, that counts.

References

[1] Kenneth Appel and Wolfgang Haken. Every planer map is four colorable. *Illinois Journal of Mathematics*, 21:439–657, 1977.

[2] Kenneth Appel and Wolfgang Haken. *Every Planer Map is Four-Colorable*. American Mathematical Society, Providence, 1989.

[3] Michael Aschbacher. The status of the classification of the finite simple groups. *Notices of the American Mathematical Society*, 51, 2004.

[4] George S. Boolos. Constructing Cantorian counterexamples. *Journal of Philosophical Logic*, 26:237–239, 1997.

[5] Nicolas Bourbaki. *Eléments de Mathématique. I. Théorie des Ensembles. Chapter III: Ensembles ordonnés, cardinaux, nombres entiers.* Hermann, Paris, 1956.

[6] Graham P. Collins. The shapes of space. *Scientific American*, 291:94–103, 2004.

[7] John W. Dawson. Why do mathematicians re-prove theorems? *Philosophia Mathematica*, 14:269–286, 2006.

[8] Walter Feit and John Thompson. Stability of groups of odd order. *Pacific Journal of Mathematics*, 13:775–1029, 1964.

[9] Timothy Gowers. *Mathematics, A Very Short Introduction*. Oxford University Press, Oxford, 2002.

[10] Thomas C. Hales. Cannonballs and honeycombs. *Notices of the American Mathematical Society*, 47:440–449, 2000.

[11] Thomas C. Hales. Some algorithms arising in the proof of the Kepler conjecture. In *Discrete and Computational Geometry*, Algorithms and Combinatorics 25, pages 489–507, Berlin, 2003. Springer.

[12] Thomas C. Hales. A proof of the kepler conjecture. *Annals of Mathematics*, 162:1065–1185, 2005.

[13] Akihiro Kanamori. The mathematical import of Zermelo's well-ordering theorem. *The Bulletin of Symbolic Logic*, 3:281–311, 1997.

[14] Colin McLarty. What does it take to prove Fermat's Last Theorem? Goethendieck and the logic of number theory. *The Bulletin of Symbolic Logic*, 2010.

[15] Yehuda Rav. Why do we prove theorems? *Philosophia Mathematica*, 7:5–41, 1999.

[16] Neil Robertson, Daniel P. Sanders, Paul Seymour, and Robin Thomas. A new proof of the Fcour-Color Theorem. *Electronic Research Announcements of the American Mathematical Society*, 2:17–25, 1996.

[17] George G. Szpiro. *Kepler's Conjecture*. John Wiley & Sons, Hoboken, 2003.

[18] George G. Szpiro. *Poincaré's Prize: The Hundred-Year Quest to Solve One of Math's Greatest Puzzles*. Penguin Group, New York, 2007.

[19] Alfred Tarski. On well-ordered subsets of any set. *Fundamenta Mathematicae*, 32:176–183, 1939. Reprinted in [20, vol. 2, pp.551–558].

[20] Alfred Tarski. *Collected Papers*. Birhkäuser, Basel, 1986. Steven R. Givant and Ralph N. McKenzie (editors).

[21] Friedrich Waismann. *Wittgenstein and the Vienna Circle*. Basil Blackwell, 1979. Edited by Brain McGuinness.

[22] Andrew Wiles. Modular elliptic curves and Fermat's Last Theorem. *Annals of Mathematics*, 141:443–551, 1995.

[23] Ernst Zermelo. Beweis, dass jede Menge wohlgeordnet werden kann (Aus einem an Herrn Hilbert gerichteten Briefe. *Mathematische Annalen*, 59:514–516, 1904. Reprinted and translated with commentary in Zermelo [25, pp.80–119].

[24] Ernst Zermelo. Untersuchungen über die grundlagen der mengenlehre I. *Mathematische Annalen*, 65:261–281, 1908. Reprinted and translated with commentary in Zermelo [25, pp.160–229].

[25] Ernst Zermelo. *Collected Works*. Springer, 2010. Edited by Heinz-Dieter Ebbinghaus and Akihiro Kanamori.