CDMTCS Research Report Series

Workshop on Truths and Proofs

D. S. Bridges, C. S. Calude, F. Kroon (Eds.)
Christchurch University
University of Auckland
New Zealand

CDMTCS-165
November 2001

Centre for Discrete Mathematics and
Theoretical Computer Science

The Centre for Discrete Mathematics and Theoretical Computer Science
and The Department of Philosophy

WORKSHOP ON TRUTHS AND PROOFS

Auckland, 7-8 December 2001

The Workshop is part of the *Australasian Association of Philosophy (New Zealand Division) Annual Conference* to be held in Auckland, New Zealand on 2-7 December 2001.

The Workshop consists of seven talks and one roundtable discussion. The programme, including the abstracts of talks, follows.

Programme

Friday: 7 December 2001.
Morning Session: Room 421, 55 Anzac Ave.

10.00am–10.15am: Opening

SESSION I Chair: Koji Tanaka

10.15am-11.00am: Philip Catton. *Proofs, Harmony, Meaning and Truth*

Abstract: Suppose that we were to illustrate Michael Dummett's view of meaning and truth in mathematics by comparing assertions of mathematics with assertions of physics. To produce a good understanding, with respect to physics, of the doctrine about meaning that Dummett spells out with respect to mathematics, we would need to say things about physics that are, from the vantage point of philosophers of physics, roughly fifty years out of date, that is, utterly beyond the pale by now because of the advancement over recent decades of our philosophical understanding of physics. This raises doubts in my mind about Dummett's view, and the doubts that it raises seem to me well directed towards an alternative to that view. Yet the alternative is not one that I think has been canvassed by philosophers of mathematics. It seems to me therefore that the philosophy of mathematics could usefully learn something from the philosophy of physics. And if that is so then, via the link between mathematics and meaning established inter alii by Dummett, we might find the lessons we learn about mathematics pertinent to our general views about meaning and truth.

Proceeding in this way I shall take a step away from Dummett, but not so large a step as to dispel altogether the vestiges of verificationism that there are in his position or therefore so large as to land me in the realist camp. If I am not mistaken, the notions of meaning and truth could remain epistemic and yet possess qualities conspicuously different from those that either Dummett or his holist antagonist Quine bring into view.

According to a raw verificationist outlook on physics, a theory of physics, insofar as it is meaningful and true, accurately predicts what we observe. Contemporary philosophy of physics corrects this view at least to the extent of replacing 'accurately predicts' by 'concertedly harmonises' and 'what we observe' by 'phenomena'. A theory of physics insofar as it is meaningful and true concertedly harmonises phenomena. A phenomenon is as far different from what we might observe as concerted harmonisation is from mere accuracy of prediction, and the differences are very similar. Phenomena have a richness far and away beyond what can be brought under simple observation, yet phenomena also possess robust consilience features which remark a kind of harmony in what they draw together.

Proofs promote rational harmony in a science; such harmony is impossible without proofs. Thus the epistemology of physics invites attention to the nexus of proofs, harmony, meaning and truth. I indicate why I think that the same nexus is important for the philosophy of mathematics, and indeed for the general understanding of meaning and truth.

11.00am–11.15am: Coffee break

11.15am–12.00pm: Bill Barton. *Truth, Tautology, or Just Being Sensible? Some Reflections Deriving from Wittgenstein's Ideas about Mathematical Talk*

Abstract: The last forty years has seen increasing interest in mathematics as a cultural phenomenon. However standard positions in the philosophy of mathematics are at odds with such a view. If mathematics has a claim to any absolute or universal standard of rationality or truth, then mathematics cannot simply be a form of cultural expression.

This paper will discuss the shift in philosophical orientation which is required by a cultural view of mathematics, and the consequences for notions of truth and rationality. Wittgenstein's explorations of mathematical talk will be used to explore ideas of truth and proof with respect to some elementary mathematical examples.

12.15pm–1.30pm: Lunch, Room 514, Fisher International Building, 18 Waterloo Quadrant

Friday: 7 December 2001.
Early Afternoon Session: Room 611, Fisher International Building

SESSION II Chair: Douglas Bridges

2.00pm–2.45pm: Tien D. Kieu. *Quantum Principles and Mathematical Computability*

Abstract: The limits of mathematical computability have been set solely by mathematical logic and reasoning until now. Here we propose a quantum mechanical "algorithm" for one of the insoluble problems of mathematics, the Hilbert's tenth and equivalently the Turing halting problem. The algorithm, as it stands, has its limit as it cannot solve non-computable problems of other classes different than that of Turing's. But it provides an interesting and new perspective on computability. If for some fundamental physical principles or unsatisfiable requirements of physical resources (constrained by the total energy and lifetime of the universe) the algorithm cannot be carried out, then this new perspective is still very interesting as it will set the limits of mathematical computability by physics. Information, we can argue, is physical after all.

2.45pm–3.00pm: Coffee break

3.00pm-3.45pm: Cristian S. Calude, Elena Calude. *Passages of Proof*

Abstract: Classically, there are two equivalent ways to look at the mathematical notion of proof: a) as a finite sequence of sentences strictly obeying some axioms and inference rules, b) as a specific type of computation. Indeed, from a proof given as a sequence of sentences one can easily construct a machine producing that sequence as the result of some finite computation and, conversely, giving a machine computing a proof we can just print all sentences produced during the computation and arrange them in a sequence. A proof is an explicit sequence of reasoning steps that can be inspected at *leisure*; *in theory*, if followed with care, such a sequence either reveals a gap or mistake, or can convince a skeptic of its conclusion, in which case the theorem *is considered proven.*

This equivalence has stimulated the construction of programs which perform like *artificial mathematicians.* From proving simple theorems of Euclidean geometry to the proof of the four-color theorem, these "theorem provers" have been very successful. Of course, this was a good reason for sparking lots of controversies. *Artificial mathematicians* are far less ingenious and subtle than human mathematicians, but they surpass their human counterparts by being infinitely more patient and diligent. What about making errors? Are human mathematicians less prone to errors? This is a difficult question which requires more attention.

If a conventional proof is replaced by a "quantum computational proof" (or a proof produced as a result of a molecular experiment), then the conversion from a computation to a sequence of sentences may be impossible, e.g., due to the size of the computation. For example, a quantum machine could be used to create some proof that relied on quantum interference among all the computations going on in superposition. The quantum machine would say "your conjecture is true", but there will be no way to exhibit all trajectories followed by the quantum machine in reaching that conclusion. In other words,

the quantum machine has the ability to check a proof, but it may fail to reveal any "trace" of how it did it. Even worse, any attempt to *watch* the inner working of the quantum machine (e.g. by "looking" at any information concerning the state of the on going proof) may compromise for ever the proof itself!

These facts may not affect the essence of mathematical objects and constructions (which have an autonomous reality quite independent of the physical reality), but they seem to have an impact of how we learn/understand mathematics (which is thorough the physical world). Indeed, our glimpses of mathematics seem to be "revealed" through physical objects, i.e. human brains, silicon computers, quantum Turing machines, etc., hence, according to Deutsch (1985), they have to obey not only the axioms and the inference rules of the theory, but the *laws of physics* as well.

Friday: 7 December 2001.
Late Afternoon Session: Room 611, Fisher International Building

SESSION III Chair: Fred Kroon

4.15pm–6.15pm: Roundtable discussion with wine and cheese: *Recent Work in Church-Turing Thesis*

Saturday: 8 December 2001.
Morning Session: Room 246, Computer Science

SESSION IV Chair: Tien Kieu

10.00qm-10.45pm: Douglas Bridges. *Random Rambles in Constructivism*

Abstract: Beginning with two problematic classical existence proofs, I will introduce Brouwer's intuitionism and its associated proof principles (encapsulated in Heyting's axioms of intuitionistic logic). This will lead to a discussion of omniscience principles, Brouwerian examples, and the constructive reformulation of classical theorems. I will try wherever possible to bring out some of the unusual, not to say peculiar, aspects of constructive proofs. In particular, I will look closely at Ishihara's tricks, which use the method of 'flagging alternatives' to prove remarkably strong constructive results that are simple classical consequences of the law of excluded middle. The talk will conclude with some general remarks about constructive mathematics, especially in connection with choice.

10.45am–11.00pm: Coffee break

11.00am–11.45pm: Dave McIntyre. *A High-level Language for Topological Proofs*

Abstract: For several years now, Stephen Watson of York University, Canada, has been advocating what he calls a "high-level language" for proofs and constructions in topology. The name is an analogy to the development of high-level computing languages, which relieve the user from low-level details such as buffers and memory allocation and allow them to issue high-level commands.

Probably the most familiar and widespread aspect of this project is the use of elementary submodels which has become (at least in topology) a relatively standard part of the language. Many older proofs involve "closing off" arguments, in which an object is constructed inductively, adding new elements one at a time with special care taken to ensure that, on the one hand, enough elements are included to ensure a certain property of the final object, and on the other hand, because only one element is added at each stage the size of the final object is not too large. In many cases, such a construction can be considerably simplified by taking a small elementary submodel M of the universe V of all sets, and taking our final object to be $M \cap Y$ for some set Y. All of the careful balancing of putting just the

right number of elements into the object is simply taken care of by the Löwenheim–Skolem Theorem, ensuring the existence of M, allowing the reader to ignore the details and focus on a higher-level idea of the proof.

Perhaps less familiar is the use of resolutions, a general technique for building more complex topological spaces out of simpler ones. The goal here is to build a body of theorems ensuring that if the simpler spaces have certain properties then the new space will have certain properties: thus the writer can simply appeal to these theorems and the reader is spared the details of a particular instance of a general result.

More recent work involves the use of scheduled relativisation, and finite hulls. The first of these is a high-level language for direct limits, inverse limits and other constructions using transfinite induction, while the second is an extension of the ideas used in elementary submodels.

Finally, he has been advocating a drive towards a style inspired by advice for good computer programming style. A well-written program contains a number of routines, each of which has strong functional cohesion (doing only one thing well) and loose coupling (small, direct, visible and flexible relations to other routines). Similarly, a well-written proof should consist of a number of lemmas, each of which has non-trivial content, but which represents only one step in the proof.

In this talk, I will present some of these ideas.

11.45am–12.30pm: Neil Leslie. *Treating Elimination Rules as Self-Justifying*

Abstract: In 'Investigations Into Logical Deduction' Gerhard Gentzen wrote:

> The introductions represent, as it were, the 'definitions' of the symbols concerned, and the eliminations are no more, in the final analysis, than the consequences of these definitions.

This remark has formed the basis of an argument for proof-theoretical justifications of the logical laws, an argument which has been developed by Dag Prawitz, Per Martin-Löf, and Michael Dummett. We turn this argument on its head, and show, using rather simple means, that we might as well take the elimination rules as defining the meanings of the logical laws.

12.30pm–12.45pm: Closing

12.45pm–2.00pm: Lunch, Computer Science Common Room