Jean Paul VAN BENDEGEM (Belgium)
Vrije Universiteit Brussel

CHARACTERISTICS OF REAL MATHEMATICAL PROOFS

1. What real proofs are not. Formal logic provides us with a neat and clear definition of a formal, mathematical proof. A proof is a list of statements - formulated in a given language L with a clear vocabulary and a clear set of formation rules - starting with the premisses, ending with the conclusion to be proved, and such that all formulas in the list can be justified by a logical/mathematical rule, axiom and/or definition of the logical, mathematical theory under consideration. As is well known, real mathematical proofs in general do not satisfy this definition. Except for trivial cases, a real proof never lists *all logically necessary* steps.

Apart from factual considerations on the actual development of mathematics - proofs tend to be become longer, and more and more specialized - general arguments relying on complexity considerations show why this is unavoidably so. (See [6], [7]). An example: To check whether a proof does or does not contain circularities is equivalent to detect a Hamiltonian circuit in a network. The arrows in the network represent the derivability relation, and a Hamiltonian circuit is quite simply a closed sequence of arrows, i.e. a circular path. This problem is known to be NP-complete (see [4]), hence the only full solution known is exponentially difficult. Thus, checking proofs is a hard and difficult task, as is equally well known in the computer sciences. To show that a program does the job it has been designed to do, is usually a much more complex task than the design of the program itself (see e.g. 1]).

Hence, it is a legitimate question to ask what properties characterize a real mathematical proof. In other words, what do real proofs look like, and, most importantly, how do mathematicians decide that a proof is correct, given that the only reliable procedure - step-by-step control - is not accessible?

2. Some properties of real proofs. No doubt, Imre Lakatos' *Proofs and Refutations* remains the first, and quite seminal study on the nature of real proofs. However, his approach was limited to a mathematical problem - the Euler conjecture - for which a proof was found almost right from the start, and, such that counter-examples were easily accessible. Not all mathematical problems share these features. Thus, Lakatos' model does not tell the whole story. In [8], I looked at Fermat's Last Theorem (FLT) and found a new (relative to Lakatos' framework) heuristic: Mathematicians have *expectations* that guide their search for a proof or disproof. They make judgments of the following nature: It is likely that this problem will be proved in the language of number theory? E.g., no professional mathematician today believes that FLT will be proved in elementary number theory. A similar effect was at work, according to my analysis in [9], in the reception of the proof of Roger Apéry on the irrationality of the Zeta-function for z = 3. All the elements in the proof were "around" for almost two centuries. It was, therefore, judged to be extremely unlikely that the proof was correct.

Another element that came out of the Apéry case, is the fact that mathematicians rely on, what I have called, *quality considerations*. That is, proofs have a proof quality. There are low quality proofs and high quality proofs. An important element to raise the quality is whether the proof can be *summarized*, i.e. whether the proof has a *proof-outline*. There was an apparent agreement among mathematicians that Apéry's proof was a low quality proof. A proof considered generally of high quality, is the irrationality proof of $\sqrt{2}$.

3. **Implicit assumptions or shared background knowledge.** In this paper, I want to look at another element that *must* play its part in mathematical practice. Mathematical proofs can be seen as (a special kind of) texts. It needs hardly be stated that all texts face the problem of implicit knowledge, or, in different wordings, background knowledge, and/or unmentioned, implicit assumptions. I have already mentioned computer science in connection with the complexity of proofs. The *frame problem* (see [2]) in computer science is the analog of the problem of background knowledge in linguistics and text analysis.

What I have in mind is the following. It is my expectation that in a real mathematical proof, a set of implicit assumptions is made concerning, among other things, the use, notation and interpretation of mathematical concepts (variables, functions, operators, etc.), concerning the way(s) arguments are formulated (e.g. whether or not examples are admitted as supporting evidence), concerning the use of drawings and diagrams to support an argument. Note that these features, although related to, are to be distinguished from the hidden lemma notion in Lakatos' *Proofs and Refutations*. For, in Lakatos' view, progress is made by making the hidden lemmas explicit, whereas in the case of background knowledge, this could turn out to be a bad strategy. Rather, the point is that background assumptions are an *integral* part of mathematical activity and cannot be eliminated.

However, one might object that the considerations above constitute only a possibility argument. It remains to be shown that indeed background knowledge does play its part. The next paragraph presents a specific example. I want to argue that the evidence presented is best understood in terms of shared or, in this case, rather *not* shared, background knowledge.

4. **A case study: Herbert A. Simon vs. the mathematicians.** During 1988-1989, an interesting discussion, or should one say controversy, took place in the columns of the well-known journal, *The Mathematical Intelligencer*. ([a]: volume 10, 1, 1988, pp.4-16, [b]: volume 10, 2, 1988, pp.10-12, [c]: volume 10, 3, 1988, pp.3-5, [d]: volume 10, 4, 1988, pp.3-6, and [e]: volume 11, 1, 1989, pp.3-4). The discussion started out between the economist, and computer scientist, Herbert A. Simon, and the mathematician Neal Koblitz. Other mathematicians, mainly through letters, contributed to the discussion. Two remarks. First, as I am primarily interested in the use of mathematics in this discussion, I have not tried to take sides (although I have to admit, that I do have an opinion on the matter). Second, I will look into the mathematical side of the discussion and not into the general discussion. The latter - and actually the origin of the controversy - concerns a paper by Samuel Huntington ("The Change to Change: Modernization, Development and Politics"). In this paper, according to Neal Koblitz, Huntington uses, or rather misuses, mathematics to support his right-wing views. Herbert A. Simon then wrote an article to defend Huntington's use of mathematics without taking political sides. In [a], both

Koblitz and Simon present their case with a reply of Koblitz, followed by reply from Simon in [b]. What turns this discussion into an interesting problem for a philosopher of mathematics, is that some of Koblitz's arguments are meant to show that Simon himself, defending Huntington's use of mathematics, has a poor grasp of the mathematical machinery. Here are three examples in some detail.

4.1. **The monotonic transformation problem.** In Simon's paper "Some Trivial But Useful Mathematics", (in [a], p.6) the following definition is given. X and Y are sets equipped with an order relation, $<$. Then "consider $x \in X$ and $y \in Y$. The $f(x)$: $X \to Y$ is a positive strict monotonic transformation if $y_i = f(x_i) > y_j = f(x_j)$, whenever $x_i > x_j$ and vice versa." Koblitz in his reply ([a], p. 8) argues that this definition allows the following case. Let f be a function that increases on an interval (a,b) and decreases on an interval (c,d). Then the positive strict monotonic transformation: $g: x \to (a + bx)/(1 + x)$, transforms f to a monotonically increasing function on R^+. But the function $h: x \to (c + dx)/(1 + x)$ transforms f into a monotonically decreasing function. In his reply, [a], p. 11-12, Simon replies that Koblitz's example does not work, since the functions g and h do not transform the original function f because the range of g and h are different and he adds "that is odd, because the domain and range of a function are ordinarily considered part of its definition." Koblitz reply is that "this is the first we have heard that the set of values taken by a function is supposed to play a role in the definition of the transformed function." ([a], p. 15). Koblitz offers another example, again dismissed by Simon on the same grounds. Koblitz does not reply believing it is pointless to do so (see [b], p.11).

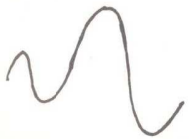
The important element in this discussion is that Koblitz is amazed by Simon's formulations. The point is not that Simon is *wrong*, or *mistaken*, but, rather that his use of the mathematical language is not the *proper* use of it. "This is the first we have heard that ..." expresses, it seems, an unconventional use of terminology rather than a misunderstanding. That is, according to Koblitz, Simon uses the function concept in a way that is not *customary*. But that really is a reference to a *shared use of mathematical language*. In an almost Wittgensteinian fashion, Koblitz reproaches Simon that he "is using the logic of Humpty Dumpty, who says: "When *I* use a word, it means just what I choose it to mean"" ([b], p.11). As said before, I do not wish to take sides in the discussion. The point is that I want to draw attention to the fact that terminology, meaning, and correct use of language are at the core of this discussion. In other words, not the truth of the statements *per se*, but their formulation is the issue.

4.2. **The simple proof problem.** In Simon's original paper, a proof involving derivatives is given of the statement that, given a function $z = f(x,y)$, it is impossible by monotonic transformations of x, y, and z to transform f into a sum, or multiplication, i.e. $z^* = x^* + y^*$, or $z^* = x^*.y^*$, where x^*, y^*, and z^* are the transformed variables. In [a], p. 8, Koblitz claims that shorter proofs can be produced (he actually gives three examples), e.g.: "Choose $f(x,y) =$ constant, which is not equivalent to $z^* = x^* + y^*$. (Any function such that $f(x,y_0)$ is constant on an interval for some y_0 will do.)" Here, it seems, the focus of disagreement between Simon and Koblitz is whether his proofs prove what they are supposed to prove. Neither of them has any problems with the fact that Koblitz's proofs are indeed *shorter*. Are they?

They are, if one shares the same background. That is, if one accepts that a statement such as: f(x,y) = constant is not equivalent to z = x + y, needs not be explicated any further. Perhaps one thinks one is unreasonable to ask for a proof. This may be so in the context of elementary analysis, but, say from the perspective of set theory, the question ceases to be obvious. Does, e.g., the proof depend on the axiom of choice? If the proof starts with "Take two couples (x,y) and (x',y') such that ..." then, yes, it does. But is another proof possible? Clearly, the question becomes an interesting one. Both discussants have apparently assumed implicitly, that *their language is to be the language of elementary analysis*. This assumption must be *shared*, otherwise, it is not clear why Simon would accept Koblitz's proofs as one-line proofs.

4.3. **The continuity problem.** In [b], in response to a critique of Neal Koblitz, Simon wants to present an example of a function or transformation "that maps the integers 1 and 7 onto the integers 2 and 8, respectively, is bijective, order-preserving, and hardly continuous" ([b] p.11). Neal Koblitz in his reply suggests "to advise Simon to read an introductory book for undergraduates on the use of functional *notation*, composition of functions, continuity, and so on." (my emphasis). In [d], p.4, Andrew J. Lazarus in a letter states that he "was shocked to read H. Simon's assertion that the adding-one map from {1,2,3,4,5,6,7} to {2,3,4,5,6,7,8} is not continuous. My conclusion is that Professor Simon's smug, arrogant tone is a cover for complete ignorance of elementary analysis." (Note, by the way, that Lazarus talks about another function than Simon does). Finally, in [d] itself, Simon admits the mistake, but claims (rightly so) that it "does not invalidate my point: that a bijective order-preserving mapping of one subset of the reals onto another need not be continuous."

Although this may seem a quite clear-cut case - Simon made a mistake, period - it is interesting to raise the question why Simon believes that the function f: {1,2} -> {7,8} is not continuous. My hypothesis is that the meaning of the term "continuous" has shifted from a rather intuitive content to a rather abstract idea. Ivor Grattan-Guinness in [5] summarizes the situation quite well (E: Euler, M: Modern):



E: "continuous"
M: "differentiable"

E: "discontinuous"
M: "continuous"

M: "discontinuous"

It seems likely that Simon used a way of speaking that is closer to our intuitive understanding of continuity and that was, in the not so far away past, even appropriate within the mathematical community itself. The point is not Simon's "complete ignorance of elementary analysis", but, rather, Simon speaking a different language although using the very same words. In short, *a problem of meaning*.

5. Conclusion. Obviously, a couple of examples are insufficient in support of my thesis. Rather, it was my aim to show what type of evidence one should look for. Further investigation is needed. Let me just draw your attention to an important consequence of this short study. If indeed *shared* background knowledge does play such a crucial role as claimed, then mathematical practice should be characterized as a *social* activity (see also [3]). The mathematical community is a *community* of mathematicians, not an equivalence class of interchangeable identical elements. In other words, the *individual* mathematician is not the proper concept to use to describe what mathematicians do, but rather the mathematician in a particular position in the mathematical community. In short, the *social* mathematician.

REFERENCES

[1] Michael A. ARBIB, A.J. KFOURY & Robert N. MOLL, *A Basis for Theoretical Computer Science*, Springer, Heidelberg, 1981.

[2] F.M. BROWN (ed.), *The Frame Problem in Artificial Intelligence*, Morgan Kaufman, Los Altos, 1987.

[3] Steve FULLER, *Social Epistemology*, Indiana University Press, Bloomington, 1988.

[4] Michael R. GAREY & David S. JOHNSON, *Computers and Intractibility. A Guide to the Theory of NP-Completeness*, Freeman, San Francisco, 1979.

[5] Ivor GRATTAN-GUINNESS, *The Development of the Foundations of Mathematical Analysis from Euler to Riemann*, MIT Press, Cambridge, Mass., 1970.

[6] Jean Paul VAN BENDEGEM, Pragmatics and Mathematics or how do mathematicians talk?, *Philosophica* 29, 1982, pp. 97-118.

[7] ---, Foundations of Mathematics or Mathematical Practice: Is One Forced to Choose?, *Philosophica* 43, 1989, pp. 197-213.

[8] ---, Fermat's Last Theorem seen as an Exercise in Evolutionary Epistemology, in: Werner CALLEBAUT & Rik PINXTEN (eds.), *Evolutionary Epistemology*, Kluwer, Dordrecht, 1987, pp. 337-363.

[9] ---, Non-formal Properties of Real Mathematical Proofs, in: Arthur FINE & Jarrett LEPLIN (eds.), *PSA 1988, volume one*, PSA, East Lansing, 1988, pp. 249-254.