Simpler-to-Describe Cases are Often More Difficult to Prove: A Possible Explanation

Olga Kosheleva and Vladik Kreinovich
University of Texas at El Paso
500 W. University
El Paso, TX 79968, USA
olgak@utep.edu, vladik@utep.edu

Abstract
In many areas of mathematics, simpler-to-describe cases are often more difficult to prove. In this paper, we provide examples of such phenomena (Bieberbach’s Conjecture, Poincaré Conjecture, Fermat’s Last Theorem), and we provide a possible explanation for this empirical fact.

1 Empirical Fact
Simpler-to-describe cases are often more difficult to prove: an empirical fact. In [10], L. Kazdan attracts the reader’s attention to the fact that in mathematics, simpler-to-describe cases are often more difficult to prove. He illustrates this phenomenon on the example of the Bieberbach Conjecture, that each analytical function \( f(z) = z + a_2 \cdot z^2 + a_3 \cdot z^3 + \ldots \) which is defined on the unit disk \( \{ z : |z| \leq 1 \} \) and which is injective on this disk (i.e., \( f(z_1) \neq f(z_2) \) whenever \( z_1 \neq z_2 \)) satisfies the inequalities \( |a_n| \leq n \) for all \( n \). This conjecture also states that for each \( n \), the equality \( |a_n| = n \) is attained only for the function

\[
f(z) = \frac{z}{(1-z)^2} = z + 2z^2 + 3z^3 + \ldots
\]

For \( n = 2 \), this statement was proven by L. Bieberbach himself [2].

The next proven case was \( n = 3 \), for this case the hypothesis was proven in 1923 by C. Löwner [13]. The case \( n = 4 \) was proven in 1955 by R. Garabedian and M. Schiffer [7]. The original \( n = 4 \) proof involved tedious computations, but soon, this proof has been simplified [3]. Interestingly, the simplifying idea cannot be applied to \( n = 3 \). As a result, the \( n = 4 \) proof is much shorter and simpler than the proof for \( n = 3 \). In other words, it looks like the simpler-to-describe case \( n = 3 \) is more difficult to prove.

Such an irregularity continued: the case \( n = 6 \) turned out to be simpler to prove than the case \( n = 5 \): the case \( n = 6 \) was proven in 1968–69 [14, 15], while the case \( n = 5 \) was proven only in 1972 [16].
The whole problem was solved when the Bieberbach Conjecture was proven by L. de Branges in 1985 [4]; see also [1, 5, 8, 9, 11, 12, 21]. However, a similar phenomenon can be found in many other areas of mathematics:

- In Topology, the Poincaré Conjecture [19] – that every close \( n \)-dimensional manifold which has the homotopy type of the \( n \)-dimensional sphere is homeomorphic to this sphere – was first proven, by S. Smale, for all dimensions higher than 4 [20]; for \( n = 4 \), it was proven by M. H. Freedman [6], and the case \( n = 3 \) was only recently famously solved by G. Perelman [17, 18].

- In Number Theory, the famous Fermat’s Last Theorem – that the equation \( a^n + b^n = c^n \) has not solutions in natural numbers when \( n > 2 \) – was first proven by P. Fermat himself for \( n = 4 \) in 1637, and the case \( n = 3 \) was proven (by L. Euler) only in 1770. Such “jumps” between values \( n \) continued until the Fermat’s Last Theorem was finally proven by A. Wiles for all \( n \), in 1995 [23].

How can we explain that simpler-to-describe cases are often more difficult to prove?

2 Possible Explanation

What does it mean that a proof is more difficult? In a reasonable first approximation, a natural way to describe the difficulty of a proof is by its length – as described in some appropriate formal proof system. This is, in effect, what L. Kazdan does in [10].

Let \( \ell(S) \) denote the length of the shortest possible proof of a statement \( S \) or its negation \( \neg S \) in the selected formal system. If a statement \( S \) is independent on the selected formal system, so that neither \( S \) not its negation \( \neg S \) can be proven in this system, then we take \( \ell(S) = \infty \).

Precise formulation of the problem. Let us consider a general situation, when we have a sequence of statements \( A(1), A(2), \ldots \), that we are interested in proving (or disproving). We are interested in the sequence of values \( \ell(A(n)) \) corresponding to different cases \( n \).

Preliminary analysis of the problem. The very formulation \( A(n) \) – and thus, a proof of \( A(n) \) – includes the description of the number \( n \) itself. Thus, the length of a proof of \( A(n) \) cannot be shorter than the length \( \approx \log_2(n) \) of describing the number \( n \). Therefore, \( \ell(A(n)) \geq \log_2(n) \) and hence, \( \ell(A(n)) \to \infty \) when \( n \to \infty \).

Crudely speaking, this means that, in general, the length \( \ell(A(n)) \) increases with \( n \) – overall, the complexity of the proof grows. However, this general statement is consistent both:

- with a monotonic growth (which seem to be intuitively expected) and

\[ \]
• with the actually observed growth which, as we mentioned, is often non-monotonic.

How can we explain this non-monotonicity?

A reasonable assumption. In general – just like in the case of the Bieberbach conjecture – there seems to be relation between the statements \( A(n) \) and \( A(m) \) which correspond to different cases \( n \neq m \). We can describe this independence by assuming that if \( n \neq m \) and we have proven that \( A(n) \) is true, this should not help us prove that \( A(m) \) is true or that \( A(m) \) is not true – it should not even help us to decide that the statement \( A(m) \) is decidable within the given formal theory (i.e., that either the statement \( A(m) \) or its negation \( \neg A(m) \) can be deduced from this theory).

Let us show that this seemingly reasonable assumption can explain why the sequence \( \ell(A(n)) \) is often non-monotonic. We will prove this by reduction to a contradiction.

**Desired explanation.** Let us assume that the length \( \ell(A(n)) \) of the shortest proof is monotonically increasing with \( n \). In this case, once we have a proof that \( A(n) \) is true, then we know that the shortest proof \( \ell(A(n)) \) cannot exceed the length \( \ell_0 \) of our proof: \( \ell(A(n)) \leq \ell_0 \). Since we assumed that the shortest proof length \( \ell(A(x)) \) is a monotonic function of \( x \), we thus conclude that for all \( m < n \), we have \( \ell(A(m)) \leq \ell(A(n)) \), and therefore, that \( \ell(A(m)) \leq \ell_0 \).

Since the case when \( A(m) \) is independent of the given theory corresponds to \( \ell(A(m)) = \infty \), the fact that we have \( \ell(A(m)) \leq \ell_0 < \infty \) means that either the statement \( A(m) \) or its negation \( \neg A(m) \) can be deduced from the formal theory – which contradicts to our assumption that we cannot deduce this from the proof of \( A(n) \). This contradiction shows that the independence assumption is indeed incompatible with monotonicity of \( \ell(A(n)) \) and therefore, under this assumption, the function \( \ell(A(n)) \) is, in general, not monotonic.

**Comment.** Once we know that either \( A(m) \) or \( \neg A(m) \) are provable, we can, in principle, find the corresponding proof by simply trying all possible combinations of symbols – and in the above case, we know that we will succeed once we have tried all combinations of length \( \leq \ell_0 \).

**Conclusion.** We have shown that the above seemingly reasonable independence assumption indeed implies that, in general, the length \( \ell(A(n)) \) of the shortest proof is not monotonically depending on \( n \). Thus, we have values \( m < n \) for which \( \ell(A(m)) > \ell(A(n)) \), i.e., we have situations in which simpler-to-describe cases are more difficult to prove.

**Acknowledgments.** This work was supported in part by the National Science Foundation grants HRD-0734825 and HRD-1242122 (Cyber-ShARE Center of Excellence) and DUE-0926721.
References


