Gödel and the Lengths of Proofs

Sam Buss
U.C. San Diego

Celebrating 90 Years of Gödel's Incompleteness Theorems
Universität Tübingen
July 8, 2021

Talk outline

Proof complexity and proof length are very actively studied in the present time due especially to their connections to complexity theory and automated theorem proving.

Gödel was the first one to study the lengths of proofs — albeit in only a single, short paper.

This talk touches on:

- Partial (finistic) consistency statements (symbol length).
- Separations in higher-order theories of arithmetic (step length) from Gödel's 1936 paper.
- A result stated by Gödel in a 1956 letter to von Neumann related to the P versus NP question.

"The length of a proof ought not to be measured by the yard. It is easy to make a proof look short on paper by skipping over many links in the chain of inference and merely indicating large parts of it. Generally people are satisfied if every step in the proof is evidently correct, and this is permissable if one merely wishes to be persuaded that the proposition to be proved is true. But if it is a matter of gaining an insight into the nature of this 'being evident', this procedure does not suffice; we must put down all the intermediate steps, that the full light of consciousness may fall upon them." [G. Frege, *Grundgesetze*, 1893; translation by M. Furth]

Preliminaries

We work in theories in first-order or higher-order logic, extending PRA or S^1_2, with any of the usual Hilbert-style formalizations.

Notation:

- $T \vdash^n \varphi$ means T has a proof of φ of ***symbol*** length $\leq n$.
- $T \vdash_n \varphi$ means T has a proof of φ of ***step*** length $\leq n$.
- $Con_T(n)$ is the first-order formula expressing "T has no proof of a contradiction of symbol length $\leq n$."

$$\neg\exists x[Proof_T(x, \ulcorner 0 = 1 \urcorner) \,\&\, |x|_{sym} \leq n]$$

- $Con^{step}_T(n)$ is the same for step length instead of symbol length

These are called "partial consistency" or "finitistic consistency" statements.

I. Lower and upper bounds for partial consistency

Let T be one of the usual theories of arithmetic. We let $n \in \mathbb{N}$ and t be a closed term or be a value defined by a Δ_0 formula.

Theorem ([H. Friedman'79; Pudlák'86])

There is an $\epsilon > 0$ so that:

- *It is not the case that $T \vdash^{n^\epsilon} Con_T(\underline{n})$.*
- *It is not the case that $T \vdash^{t^\epsilon} Con_T(t)$.*

[Pudlák '87] improves this from n^ϵ to $\Omega(n/\log^2 n)$ under a suitable formalization of arithmetic (with Rosser's Rule C).

Letting t be given via a formula defining a very large integer, we can form short sentences that are true but require very long proofs.

Remark: We use efficient binary encodings for numerals, so $\underline{n}$ has $|n|$ symbols, where $|n|$ denotes the length of n.

Proof Sketch

By diagonalization, let φ assert that it does not have a short proof:

$$T \vdash \varphi \leftrightarrow \neg(\exists x)[Proof_T(x, \ulcorner\varphi\urcorner) \,\&\, |x|_{sym} \leq \underline{n^\delta}].$$

We have φ is true since T is consistent.

- T proves $\neg\varphi \rightarrow T \stackrel{n^\delta}{\vdash} \varphi$ by definition of φ.
- T proves $\neg\varphi \rightarrow T \stackrel{n^{\delta k}}{\vdash} \neg\varphi$, for some constant k, since φ is a true Σ_1-formula, and T contains PRA or S^1_2.
- Thus T proves $Con_T(\underline{n}) \rightarrow \varphi$ for $\delta < 1/k$.
- Thus we cannot have $T \stackrel{n^\epsilon}{\vdash} Con_T(\underline{n})$ for $\epsilon < \delta$.

Q.E.D.

Note that the above argument follows one of the usual proofs of the Gödel Incompleteness Theorem.

A polynomial upper bound holds too:

Theorem (Pudlák '86)

For some constant k,

- $T \vdash^{n^k} Con_T(\underline{n})$.

Proof idea: Use partial truth definitions – for formulas of symbol length $\leq n$. □

[Pudlák'87] improves this n^k to $O(n)$ – based on bounds on formula complexity from unification ([Parikh'73]) and constructions of Krajíček-Pudlák.

The theorem also holds for $Con_T^{step}(\underline{n})$. (!)
The proof uses unification techniques to limit the complexity of formulas in the proof.

II. [Gödel'36] on the Lengths of Proofs

Gödel used ***step length***, not symbol length.

Let Z_i be $(i+1)^{st}$ order arithmetic. So Z_0 is Peano arithmetic; Z_1 is second-order arithmetic, etc.

Theorem ([Gödel'36])

Z_{i+1} has super-recursive speed-up over Z_i.
Namely, for theorems φ of Z_i, there is no recursive function bounding the step length of the shortest Z_i proof of φ in terms of the step length of a Z_{i+1} proof of φ.

Gödel never provided a proof of this theorem.

[Mostowski'52], [Ehrenfeucht-Mycielski'71] proved it for *symbol length*. For ***symbol length***, it can be proved using the Friedman-Pudlák method using partial consistency statements $Con_{Z_i}(\underline{n})$ as φ's. (see [B'94])

[Parikh'73] and [Krajíček'89] proved Gödel's theorem for step length, but for languages with only ***unary*** function symbols.

Gödel's theorem on proof length also holds for non-recursive functions.

Theorem (Gödel'36], [B'94])

Z_{i+1} has unbounded step-length proof speedup over Z_i. Namely, there are Π^0_1-formulas φ_j, which are provable in Z_i so that

- *There is a k s.t. $Z_{i+1} \vdash_k \varphi_j$ for all j.*
- *There is no k s.t. $Z_i \vdash_k \varphi_j$ for all j.*

Proof ingredients: It does not seem to work to use consistency statement $Con_{Z_i}(\cdot)$.
Instead work directly with with formulas φ_j asserting they need long Z_i-proofs.
Use the MDPR theorem about diophantine equations to get Π^0_1-formulas for φ_j and to get the constant k for Z_{i+1}.

Open Problem: Let the theory T be PA, PRA or S^1_2, etc. Find lower bounds $k(n)$ such that

$$\neg T \not\vdash_{k(n)} Con^{step}_T(\underline{n}).$$

Does this hold with $k(n) = n^\epsilon$?

Remark: This can fail for some formalizations of PA. For instance, if Kreisel's conjecture holds. One way it can fail is if all true sentences $\underline{n} + \underline{m} = \underline{n + m}$ and $\underline{n} \cdot \underline{m} = \underline{n \cdot m}$ are added as axioms. (See [B'94].)

III. Gödel's 1956 letter to von Neumann

One can obviously easily construct a Turing machine, which for every formula F in first order predicate logic and every natural number n, allows one to decide if there is a proof of F of length n (length = number of symbols). Let $\psi(F, n)$ be the number of steps the machine requires for this and let $\varphi(n) = \max_F \psi(F, n)$. The question is how fast $\varphi(n)$ grows for an optimal machine. One can show that $\varphi(n) \geq k \cdot n$. If there really were a machine with $\varphi(n) \sim k \cdot n$ (or even $\sim k \cdot n^2$), this would have consequences of the greatest importance [Tragweite]. Namely, it would obviously mean that in spite of the undecidability of the Entscheidungsproblem, the mental work of a mathematician concerning Yes-or-No questions could be completely (footnote: except for the setting up of axioms) replaced by a machine. After all, one would simply have to choose the natural number n so large that when the machine does not deliver a result, it makes no sense to think more about the problem. Now it seems to me, however, to be completely within the realm of possibility that $\varphi(n)$ grows that slowly. Since (1) it seems that $\varphi(n) \geq k \cdot n$ is the only estimation which one can obtain by a generalization of the proof of the undecidability of the Entscheidungsproblem; and (2) after all $\varphi(n) \sim k \cdot n$ (or $\sim k \cdot n^2$) only means that the number of steps as opposed to trial and error can be reduced from N to $\log N$ (or $(\log N)^2$). However, such strong reductions appear in other finite problems, for example in the computation of the quadratic residue symbol using repeated application of the law of reciprocity. It would be interesting to know, for instance, the situation concerning the determination of primality of a number and how strongly in general the number of steps in finite combinatorial problems can be reduced with respect to simple exhaustive search.

First part of letter:

"One can obviously easily construct a Turing machine, which for every formula F in first order predicate logic and every natural number n, allows one to decide if there is a proof of F of length n (length = number of symbols). Let $\psi(F, n)$ be the number of steps the machine requires for this and let $\varphi(n) = \max_F \psi(F, n)$. The question is how fast $\varphi(n)$ grows for an optimal machine. One can show that $\varphi(n) \geq k \cdot n$.

Theorem (Gödel'56],[B'95])

Work with a Hilbert-style first-order logic. The decision problem of whether a first-order formula F has a proof of $\leq n$ symbols cannot be solved

- *By a deterministic k-tape Turing machine in time $o(n)$.*
- *By a non-deterministic k-tape Turing machine in time $o(n/\log n)$.* *(Conjectured by S. Cook in letter to H. Wang.)*

Proof ingredients: Proof is by contradiction, forming a formula F that states "I am not accepted by Turing Machine M in δn steps". Then show that if F is true, it has a proof of symbol length $\leq n$.

- The tapes of the Turing machine M can be assumed to be partitioned into "blocks", each block with $\ell = \alpha \log n$ symbols.
- Tape heads must stay within a pair of adjacent blocks within each epoch of computation. Each epoch lasts between ℓ and 4ℓ steps. Tape heads can transition to a new pair of blocks only at epoch boundaries.
- Using unary function symbols, first-order terms can represent block contents and can count epochs.
- All facts about the Turing machine computation at the n/ℓ epoch boundaries can be encoded using these terms and other relation symbols. Only ϵn many symbols are need to write out all these facts.
- A special technique is used to keep track of the "topology" of blocks, namely, to track tape head positions correctly (to avoid quadratic blowup).

Middle part of letter:

> *"If there really were a machine with $\varphi(n) \sim k \cdot n$ (or even $\sim k \cdot n^2$), this would have consequences of the greatest importance [Tragweite]. Namely, it would obviously mean that in spite of the undecidability of the Entscheidungsproblem, the mental work of a mathematician concerning Yes-or-No questions could be completely (footnote: except for the setting up of axioms) replaced by a machine. After all, one would simply have to choose the natural number n so large that when the machine does not deliver a result, it makes no sense to think more about the problem. Now it seems to me, however, to be completely within the realm of possibility that $\varphi(n)$ grows that slowly.*

Here Gödel is saying it is completely with the realm of possibility ("durchaus im Bereich der Möglichkeit liegt") that this NP-complete problem is in time $O(n)$ or $O(n^2)$, in which case P=NP.

Final part of letter:

"Now it seems to me, however, to be completely within the realm of possibility that $\varphi(n)$ grows that slowly. Since (1) it seems that $\varphi(n) \geq k \cdot n$ is the only estimation which one can obtain by a generalization of the proof of the undecidability of the Entscheidungsproblem; and (2) after all $\varphi(n) \sim k \cdot n$ (or $\sim k \cdot n^2$) only means that the number of steps as opposed to trial and error can be reduced from N to $\log N$ (or $(\log N)^2$). However, such strong reductions appear in other finite problems, for example in the computation of the quadratic residue symbol using repeated application of the law of reciprocity. It would be interesting to know, for instance, the situation concerning the determination of primality of a number and how strongly in general the number of steps in finite combinatorial problems can be reduced with respect to simple exhaustive search."

To argue against the possibility (Möglichkeit) [B'95]:

PREMISE 1: *Mathematics (especially the discovery of mathematical truths) is inherently difficult for humans and for Turing machines, even working in concert.*

PREMISE 2: *Some of the inherently difficult aspects of mathematics can be phrased as questions of the form "* $\vdash^{n \text{ symbols}} \phi$*?" where n is not excessively large.*

CONCLUSION: *The question "* $\vdash^{n \text{ symbols}} \phi$*?" can not be reliably decided in time* $k \cdot n$ *or* $k \cdot n^2$ *with k not excessively large. More generally, "* $\vdash^{n \text{ symbols}} \phi$*?" can not be feasibly decided.*

Thank you!

References:

S. Buss, "On Gödel's Theorems on Lengths of Proofs I: Number of Lines and Speedups for Arithmetic". Journal of Symbolic Logic 39 (1994) 737-756.

S. Buss, On Gödel's Theorems on Lengths of Proofs II: Lower Bounds for Recognizing k Symbol Provability. In Feasible Mathematics II, Birkhauser, 1995, pp. 57-90.

A. Ehrenfeucht and J. Mycielski, "Abbreviating Proofs by Adding New Axioms", Bulletin of the AMS, 77 (1971), pp. 366–367.

H. Friedman, "On the Consistency, Completeness and Correctness Problems", Ohio State University, 1979.

K. Gödel, "Über die Länge von Beweisen", Ergebnisse eines Mathematischen Kolloquiums, (1936), pp. 23–24.

K. Gödel, *Letter to von Neumann*, 1956.

A. Mostowski, *Sentences Undecidable in Formalized Arithmetic: An Exposition of the Theory of Kurt Gödel*, North-Holland, 1952.

R. Parikh, "Some Results on the Lengths of Proofs", Transactions of the AMS, 177 (1973), pp. 29–36.

P. Pudlák, "On the Lengths of Proofs of Finitistic Consistency Statements in First Order Theories", in Logic Colloquium '84, North-Holland, 1986, pp. 165–196

P. Pudlák, "Improved Bounds to the Lengths of Proofs of Finitistic Consistency Statements", in Logic and Combinatorics, Contemporary Mathematics 65, AMS, 1987, pp. 309–331.