

Shattering Hilbert's Spirit: Natural Independence Phenomena and the Goodstein Sequence (or My Function Grows Too Fast For Your Formal System)

Abstract:

While Godel's theorem demonstrated that Hilbert's goals were impossible, it did so in a self-referential way which bothered many mathematicians. The discovery of natural propositions which were independent of arithmetic demonstrated that arithmetic did lack power as a formal system, there were true theorems within it that required a more powerful formal system to prove. Such proofs tend to involve fast-growing functions, and there is a poorly understood but potentially fruitful connection between the speed of growth of functions and the power of the formal systems required to prove their properties. We explore these topics and present our own intuitive explanation of the convergence of the Goodstein sequence, which requires little mathematical background.

Background:

"...the conviction (which every mathematician shares, but which no one has as yet supported by a proof) that every definite mathematical problem must necessarily be susceptible of an exact settlement, either in the form of an actual answer to the question asked, or by the proof of the impossibility of its solution and therewith the necessary failure of all attempts."

[Hilbert, 1900]

In the late 19th century, mathematics had been axiomatized - changed from an informal system of reasoning to an explicit set of starting axioms and allowable transformations. This allowed mathematicians to formally investigate properties of a system, such as its completeness, which could not be done with ad-hoc systems. Hilbert proposed that we investigate the consistency of arithmetic by considering it as a mathematical problem.

He also had strong feelings about what mathematics could do. He felt that all mathematical problems ought to be solvable by mathematics (with a proof of impossibility counting as a solution). The basis of mathematics was held to be arithmetic with natural numbers. "*God made the natural numbers, all the rest is the work of man.*", said Kronecker. Hilbert's program was very ambitious, he wanted to show that mathematics was complete using itself. He hoped to prove that adding things to arithmetic ("ideal mathematics") might make proofs easier, but did not increase the *proving power* of the system as a whole. That is, to prove using arithmetic that anything you could prove, you could prove with arithmetic.

Then came Godel's epochal 1931 paper, "On formally undecidable propositions of

Principia Mathematica and related systems", in which he demonstrated that any sufficiently powerful formal system was either incomplete or inconsistent. This was an explicit impossibility proof to the goal of showing that arithmetic was complete and consistent. His method relied on cleverly encoding the axioms and deductive rules of the system within itself, so that a number could also be viewed meta-mathematically as a proof or theorem. He then generated a self-referential statement of the form "I can not be proved in this formal system". In a consistent system of course, this statement can never be proved.

"The statements constructed by Godel suffered the defect of being unnatural and for the past half century a somewhat raggedy debate ensued concerning whether or not Godel's result applied to statements of real mathematical interest." [Spencer]

"The (self-referential) formally-undecidable statements - implied by Gödel's original incompleteness results - strike many people as being too artificial and contrived to be of interest. The question arises: does Gödel's theorem actually matter to mathematics of the kind we normally come across? In other words, are the only undecidable statements ones which are somewhat obscure and removed from 'ordinary' mathematics?" [Burbanks]

The strength of his method, however, was in some ways its weakness. It seemed like a dirty trick, of a sort. Its self-referential nature meant that it could be applied to any formal system which could encapsulate basic arithmetic, but it also raised doubt in some people's minds about to what extent it demonstrated the failings of arithmetic and the incompleteness of mathematics. Perhaps mathematics could somehow be proved complete modulo self-reference - we could prove, within arithmetic, that all true non-self-referential statements can be proved by arithmetic. This would at least fulfill some of the spirit of Hilbert's program.

This is not as far-fetched as it sounds. Set theory was successfully rescued from the self-referential trap set by Bertrand Russell. Russell's paradox bears a great similarity to Godel's theorem and the classic Liar's Paradox, which can be most easily understood by considering the truth-value of the sentence "This sentence is false". If its false, its true, if its true, its false - clearly a quandary. In naive set theory, we create this by defining a good set as a set that is not a member of itself. Now consider the set of all good sets. Is it good? If its good, its bad, if its bad, its good - again the vicious circle.

The problem stems from the question of what we allow as the definition of a set, and can be resolved through restricting how sets can be generated. There are a number of solutions, including type theory by Russell himself, which result in a set theory that is powerful without being vulnerable to the paradox. Perhaps, says the optimist, something similar could be done with arithmetic, or the definition of completeness, to sweep these tangled loops under the rug.

Natural Independence Phenomena

It was not until 1977, almost half a century after Godel's result, that Paris and Harrington found a statement that was true for the integers but unprovable in Peano Arithmetic. Peano Arithmetic is a formal system which epitomizes what Hilbert considered "real math", it defines only the Kronecker-ordained set of ordinals known as the natural numbers (0, 1, 2...), along with addition and multiplication. Infinity is implicit but not explicit, the closest PA comes to recognizing it is the induction axiom, which says that if a statement is true for 0, and when true for x is true for $(x+1)$, it is true for all natural numbers.

The Paris and Harrington result was based on an extension of Ramsey's Theorem having to do with graph theory. Ramsey's Theorem states that for all k, r, t , there exists n such that given any r -coloring of the k -sets of $[n]$, there exists a monochromatic t -set B . [Spencer] In a graph theoretic sense, this says that given any t (clique size) and r (number of colors), we can find an n (graph size) such that any r -coloring of n contains a monochromatic clique of size t .

It turns out that a small modification of this results in a theorem which is independent of PA. The PH theorem is that for all k, r , there exists n such that given any r -coloring of the k -sets of $[k+1, n]$, there exists a "large" monochromatic B (where a set of natural numbers is large if $|S| > \min(S)$) Solovay proved this via a combinatorial argument, where he defined the function $PH(k, r)$ as the least n which satisfies the criterion. He then "showed that PH grows too fast for PA" [Spencer].

A few years later, in 1982, Kirby and Paris proved that a number-theoretic proposition called Goodstein's Theorem was independent of PA. Goodstein had proved his theorem in 1944 using methods stronger than arithmetic. GST is stated and defined entirely in arithmetical terms, so one might expect it to be provable with arithmetic, but this is not the case.

"While most of the other independent statements preceding Goodstein's Theorem are combinatorial in nature, Goodstein's Theorem is purely number-theoretic, having a greater aesthetic appeal and impact on mathematics as a whole" [Miller]

It is quite easy to intuitively understand why the theorem itself is true, and we will present an explanation which requires very little mathematical background. Unfortunately the proof that GST is independent of PA is rather involved, so we will only sketch it, attempting to intuitively contrast the finite nature of PA with the transfinite ordinals.

Goodstein's Theorem

Given any natural number a , we can write it in base b , which means we express a as:

$$a = t_n * b^n + t_{n-1} * b^{n-1} + \dots + t_1 * b^1 + t_0 * b^0$$

where $0 \leq a_i < b$. Each number has a unique representation in this form. We can go further, and whenever one of the exponents $e_i \geq b$, rewrite it in base b . If we repeat this procedure until all exponents are strictly less than b , we obtain the Cantor Normal Form of a , for example:

$$10 = 2^3 + 2^1 = 2^{2^1+2^0} + 2^1$$

Goodstein used this representation to create the Goodstein sequence. For any initial a , the sequence a^i for $i > n$ is created by setting $a_0 = a$, and iterating the following procedure. Increasing the base of a_0 by 1, then subtracting 1 from the resulting number. Continue doing this to produce the sequence. If subtracting one ever results in a value of zero, succeeding terms are zero as well. Formally we can define a "bumping" function which takes a number and bumps its base from b_i to b_{i+1} . To generate a_{i+1} , we bump a_i from b_i to b_{i+1} and subtract one. So if the starting base is always 2 (it turns out not to matter), we have:

$$[a_0 = a, a_{i+1} = \{ b_{i+2} [a_i] \text{ if } a_i > 0, \text{ or } 0 \text{ if } a_i = 0 \}]$$

For very small initial numbers, the sequence converges quickly to zero:

$$a = 2. \quad a_0 = 1 * 2^1, \quad a_1 = 1 * 3^1 - 1 = 2, \quad a_2 = 2 - 1 = 1, \quad a_3 = 1 - 1 = 0, \quad a_i = 0 \text{ for } i \geq 3$$

$$a = 3. \quad a_0 = 1 * 2^1 + 1, \quad a_1 = 1 * 3^1 + 1 - 1 = 1 * 3^1, \quad a_2 = 1 * 4^1 - 1 = 3, \quad a_3 = 2, \quad a_4 = 1, \quad a_5 = 0, \quad a_i = 0 \text{ for } i \geq 5$$

For larger starting numbers the sequence grows very quickly and the rate of growth appears to accelerate. For example:

$$a = 16, \quad a_0 = 1 * 2^{2^2}, \quad a_1 = 1 * 3^{3^3} - 1 = 3^{27} - 1, \text{ or about } 7.6 \times 10^{12} \text{ (wow!)}$$

Despite this extraordinarily rapid initial rate of growth, Goodstein's Theorem states that:

For any starting a and base b , the Goodstein sequence eventually converges to 0.

While inevitable, this convergence is extremely slow. For example when $a = 4$ it does not become zero until $k = 3 * 2^{402653211}$ [Miller].

We can intuitively demonstrate the truth of this theorem without needing advanced mathematics. First, we will deal with a simplified version in which we don't write numbers in Cantor Normal Form, but simply in a base representation where e_i can be $\geq b$. This has the same characteristic we desire of growing very rapidly yet converging to zero. Let us ignore the huge numbers produced by calculating the value of a base representation and focus solely on the representation itself, which shown in list form,

where we represent the number $a = t_n * b^n + t_{n-1} * b^{n-1} + \dots + t_1 * b^1 + t_0 * b^0$ as the list $(t_n, t_{n-1}, \dots, t_1, t_0)_b$. So the number 439 we might think of in base 3 as:

$$(1, 2, 1, 0, 2, 1)_3$$

Since $439 = 1 * 3^5 + 2 * 3^4 + 1 * 3^3 + 0 * 3^2 + 2 * 3^1 + 1 * 3^0$. Let us examine what happens when we generate a Goodstein sequence and focus on this list representation. The base goes up by 1 each time. The rightmost entry is the 1's column, so it decreases by 1. When it is 0, we have a number of the form $\dots + t_1 * b^1$, and subtracting 1 from this yields $\dots + (t_1 - 1) * b^1 + (b - 1)$. Thus we subtract one from the t_1 and add $b - 1$ to t_0 . Similarly when we need to decrement $t_1 = 0$, and so forth. So from the starting number, we have:

$$\begin{aligned} &(1, 2, 1, 0, 2, 1)_3 \\ &(1, 2, 1, 0, 2, 0)_4 \\ &(1, 2, 1, 0, 1, 4)_5 \\ &(1, 2, 1, 0, 1, 3)_6 \\ &(1, 2, 1, 0, 1, 2)_7 \\ &(1, 2, 1, 0, 1, 1)_8 \\ &(1, 2, 1, 0, 1, 0)_9 \\ &(1, 2, 1, 0, 0, 9)_{10} \\ &(1, 2, 1, 0, 0, 8)_{11} \\ &(1, 2, 1, 0, 0, 7)_{12} \\ &(1, 2, 1, 0, 0, 6)_{13} \\ &(1, 2, 1, 0, 0, 5)_{14} \\ &(1, 2, 1, 0, 0, 4)_{15} \\ &(1, 2, 1, 0, 0, 3)_{16} \\ &(1, 2, 1, 0, 0, 2)_{17} \\ &(1, 2, 1, 0, 0, 1)_{18} \\ &(1, 2, 1, 0, 0, 0)_{19} \\ &(1, 2, 0, 19, 19, 19)_{20} \end{aligned}$$

Viewed in this manner, we can clearly see what is happening. The base is getting bigger and bigger, which means that the number expressed as an integer has grown a great deal. Here the leading term has gone from $1 * 3^5$ to $1 * 20^5$, an increase of approx. 13,000 times. Examining the base representation, however, tells another story. We can see that the sequence is inexorably (if erratically) counting down.

The rightmost term t_0 decrements once each step, from some positive number down to zero. Each time it hits zero, it subtracts one from the place on its left (t_1), and changes to some new positive number (one less than the base). If we start with $t_1 = x$, then when t_0 has completed x cycles, $t_1 = x - 1$. Since t_1 is decrementing by one after successive finite periods, it must be cycling as well. t_2 must be cycling for the same reason, and this recursive argument holds for the rest of the terms. We can think of mass or value moving always from left to right, and draining slowly from t_0 without being replaced.

A more formal way of considering the matter is to define an ordering on pairs of numbers written in list form. We ignore the base and use a lexical comparison. This means that if the leftmost terms t_n are different, we order the lists by largest t_n (if one list is shorter, we can prepend zero's to it until they are the same size). If the t_n are equal, we compare t_{n-1} , and so forth. If all terms are identical, the lists are identical (although

the numbers are only identical if the bases are the same). So, for example, $(1, 0, 0) > (0, i, j)$ for any i, j . $(1, 1, 0) > (1, 0, 42)$, and $(1, 0, 0) > (72)$. $(3, 3, 3) = (3, 3, 3)$. Using this ordering function, we can see that the Goodstein sequence is strictly decreasing. Each term in list form is smaller than the previous, because some term t_i has always decreased, and only terms t_j with $i > j$ (less significant terms) have increased. Since it is monotonically strictly decreasing, it must eventually go to the zero list $(0, 0, \dots 0)_b$, for some base b . No matter what the base (and it will be mind-bogglingly large), this list still represents the natural number zero.

This ordering function suggests why bumping numbers in full Cantor Normal Form does not change the convergence of the function. We can use the same list notation to represent numbers being bumped in CNF, and note that the only time the integer value of a "place" mattered was when carrying over due to the next term being decremented from zero. We had used the identity $x*b^n - b^{n-1} = (x-1)*b^n + (b-1)*b^{n-1}$. Now, however, our n 's are being increased by the bumping. We have $x*b^{[n]} - b^{[n-1]}$ where $[n]$, for term i of the Goodstein sequence, is the result of bumping n 's base i times. We can observe that $n-1$ is some integer ≥ 0 , and $[n-1]$ is some integer ≥ 0 , so $b^{[n-1]}$ is some integer > 0 . So we must have $x*b^{[n]} - b^{[n-1]} = (y)*b^{[n]} + k$ where $y < x$ and $k < b^{[n]}$. (In fact, since $b^{[n-1]} < b^{[n]}$, we must have $y = x-1$). k 's actual value is irrelevant, as it simply adds some finite integer values to $t_{n-1}, t_{n-2}, \dots t_0$. Using our lexical metric, the sequence is still monotonically decreasing, and $(0, 0, \dots 0)_b$ is still the representation of the natural number 0, so we have still demonstrated convergence

Having seen why the Goodstein Sequence converges to zero, it is then natural to wonder why this cannot be proved in Peano Arithmetic. While limited by space, we can briefly sketch the answer, though it will not be rigorous. The lexical metric was simple to define and intuitive to anyone who has ever looked words up in the dictionary, but it implies certain properties that do not hold on the natural numbers. Notice that $(2,0) > (1, n)$ for all n . Based on how list notation was defined, this is like saying that $2*w + 0 > 1*w + n$ for all n , where w is the multiplier for being in place t_1 , used to convert a number from list notation into a natural number. This is simply not valid when doing arithmetic with natural numbers. When $n > w$, the inequality should not hold. If the inequality always holds, then $n < w$ for all n . This w is not a natural number.

In fact, that is exactly how we can model the lexical metric arithmetically in a more powerful axiomatic system, one which includes the so-called transfinite numbers. w is the first transfinite number, and it is defined by $w > n$ for all n . Similar definitions let us define (or generate) an infinite family of these transfinite numbers. The lexical metric corresponds nicely to treating our lists as writing numbers in base w , which have the desired comparison properties: $i*w + j > p*w + q$ for i, j, p, q natural numbers and $i > p$, no matter what the values of j, q .

We've just seen the intuitive connection between Goodstein's Theorem and transfinite numbers by considering the implications of the lexical metric with list notation. It turns out that the connection is strong in that proving the convergence of the Goodstein Sequence is equivalent to generating transfinite numbers. Thus Goodstein's Theorem

is equivalent to saying that the transfinite numbers exist.

Using this same set of transfinite numbers in addition to the axioms of Peano Arithmetic, Gentzen proved the consistency of PA. That is, Gentzen showed that PA + transfinite numbers prove the consistency of PA. However, Godel proved that no consistent formal system with power at least equal to arithmetic can prove its own consistency. Since extending PA with transfinite numbers enables the consistency of PA to be proved, transfinite numbers must not be part of PA, otherwise PA would contradict Godel's Theorem by being able to prove its own consistency (or be incomplete, which it is not). Since PA cannot generate transfinite numbers, it cannot prove the convergence of the Goodstein Sequence, and GST is independent of PA.

Note that despite fleeing from self-reference, we have not succeeded in hiding from the wily Godel. Far from being irrelevant, even when discussing more natural phenomena his theorems are still intimately related to independence. We require his proof that PA cannot prove its own consistency to establish the independence of Goodstein's Theorem.

Note also that the independence of GST is different from the independence of something like Euclid's Fifth Postulate, which is neither true nor false. We can assume it as an axiom, and derive an intuitive and consistent geometry. Or we can assume other, contradictory postulates which result in less-intuitive but still consistent geometries. The postulate is not merely not provable within the system, it is neither true nor false. In contrast, the independent theorems which we are studying are true within a system they cannot be proved in.

Aside On Fast-Growing Functions

The astute reader will have noticed some common threads at this point between the natural independence phenomena discussed. They all have to do with functions that grow extremely quickly, so quickly that arithmetic somehow cannot keep up. Those with a background in complexity theory may recall the proof that the Ackermann function is not primitive recursive, which involves showing that it dominates every primitively recursive function. It just grows "too fast" to be primitively recursive. There is something rather strange about the idea that how fast a function grows is related to the complexity of the system needed to prove things about it, but it is a fascinating recent area in mathematics which is open for further development.

"...we can show that proving the growth of fast growing functions involves undecidability...this seemsto hint to a deep relationship between the speedof growth of a function and the complexity of the proof system required to prove it...it apparently ties in research in logic theory to complexity theory and is somekind of deepbridge theorem." [Vladimir Nuri]

"The strength of a formal system is intimately connected with the size of a

certain ordinal (a). Unprovable theorems have associated fast growing functions. Some important theorems remain unprovable even in very strong formal systems." [Burbanks]

One of the most important current unsolved problems is the complexity theory question of whether $P=NP$. After studying independence, a natural hypothesis which explains our failure to prove the answer to $P=NP$ might be that this proposition is independent of the axiom systems we are using to study it (at least ZFC set theory). Some research is being done attempting to proving this using fast-growing functions by F. A. Doria and N. C. A. da Costa. While little information on his research is available, the approach seems to be based on the idea of enumerating all polynomial-time SAT solving Turing Machines. If $P \neq NP$, then for each of these TM's there must exist a SAT-problem for which that TM gives the incorrect answer. The size of these counterexamples grows extremely rapidly, and so proving that one exists may be independent for similar reasons to the problems above. A first paper will soon appear in print [Doria].

Further Research

As with Godel's Theorem, the strength of natural independence phenomena is also their weakness. They are "natural" and thus intuitive, but they are also specific, they apply only to certain axiom systems. Goodstein's Theorem only demonstrates something about the incompleteness of Peano Arithmetic. Might there be some non-self-referential way of generating independent statements? Is such a thing possible, or does it take reference to (as well as knowledge of) an axiom system in order to defeat it?

There remain many open problems in this area, such as characterizing the undecidable propositions for particular axiom systems such as PA. The proof of GST's undecidability by showing that it implies transfinite induction, which we know is not possible in PA, is an example of how such characterizations make it much easier to show that statements are undecidable. Characterizing undecidability based on the rate of growth is particularly interesting. We know that any function which grows faster than a certain bound cannot be primitively recursive. Kriesel showed that functions which dominate f_{ϵ_0} lead to unprovable theorems. Can we find similar bounds for ZFC? Can we find a way of generating such bounds for any axiom system? How does this relate to complexity theory in computer science?

Conclusions

The optimist, as usual, does not get his way. We cannot rescue real mathematics, even were we to restrict our goals to proving all non-self-referential propositions, or somehow modify our formal systems to cleverly protect them against Godel. It is simply a fact that there are statements made in arithmetic that are true, yet require stronger axiom systems to prove them. This makes life more complicated but also more interesting. Normally when faced with a mathematical question, we have two options - prove that it is true or prove that it is false. We now have a tricky third path to resort to when the well-worn ways fail. We can attempt to prove that we cannot prove that it is true or false

using our current axiom system, and find a stronger system which demonstrates that it is true (or false). Perhaps the discovery of new formal systems will become driven by independence phenomena, as the existence of propositions which appear true but seem tantalizingly unprovable motivates our search.

References

Burbanks, Andrew D: "*Fast-Growing Functions and Unprovable Theorems (How Hercules Beat the Hydra.)*" an online seminar available at <http://www2.maths.bris.ac.uk/~maadb/research/seminars/online/fgfut/>

Doria, Francisco Antonio (private email correspondence)

Miller, Justin T. "*On the independence of Goodstein's Theorem*", an undergraduate thesis available at <http://www.u.arizona.edu/~miller/thesis/thesis.html>

Nuri, Vladimir - Internet Mailing list post: <http://www.cs.nyu.edu/pipermail/fom/2002-November/006070.html> (also private email correspondence).

Spencer, J: "*Large Numbers and Unprovable Theorems*", American Mathematical Monthly, 90:669-675