Unprovability, phase transitions and the Riemann zeta-function

Andrey Bovykin and Andreas Weiermann

Abstract

Unprovability Theory started with Kurt Gödel's incompleteness theorems in 1931 but only gained mathematical significance since the late 1970s when Jeff Paris and Harvey Friedman discovered the first few families of interesting combinatorial statements that cannot be proved using the axioms of Peano Arithmetic or even some stronger axiomatic systems. In this survey article we briefly introduce the subject of Unprovability Theory to non-logicians and describe two of its directions that have recently been pursued by the authors, namely phase transitions and encodings of Ramsey-like statements using the Riemann zeta-function. Phase transitions between provability and unprovability of parameterised families of assertions were introduced by the second author in 2000. We give several examples and sketch some explanations of the reasons behind this phenomenon. Unprovability results that involve the Riemann zeta function are consequences of classical results about the Riemann zeta-function: Bohr's almost periodicity and Voronin's universality theorems. We also indicate how the universality phenomenon will give us many more unprovable assertions in the future.

1 Introduction

In this note we briefly survey some classical unprovability results in mathematics with the aim of explaining what these results might mean and, to some extent, how such results are usually obtained.

Unlike the early days of Unprovability Theory, unprovable statements discovered nowadays are more relevant to concrete mathematical disciplines, and are occasionally very interesting in their own right, not just because they are unprovable. Also, the mathematics around them suggests questions of independent mathematical interest, for example in complex analysis.

The 'amount of unprovability' a statement possesses is a rough measure of its 'true inner difficulty': a statement provable in a weak theory is in this sense "simple", even if its proof is a long chain of sophisticated ingenious arguments. But statements that possess a lot of unprovability can be thought of as fundamentally more difficult and having more complex mathematical 'gear-mechanisms' inside them.

Axiomatic systems are the underlying basis of all mathematical disciplines, ensuring that all assumptions (axioms) that are used during mathematical proofs are made explicit and stipulating the exact rules that constitute valid reasoning. Of course, in axiomatic systems designed to describe vast classes of diverse mathematical objects, unprovable statements come as no surprise. Take for example the axioms for groups and consider the commutativity statement $(\forall x)(\forall y)(x \cdot y = y \cdot x)$. Clearly, this statement cannot be proved or refuted from the axioms of groups because, as we know, some groups are commutative and some are non-commutative.

The story becomes very different when we formulate all-embracing axiomatic systems with the aim of formalising all our intuitions about (what we might think to be) one particular mathematical object, for example "*the natural numbers*". What should we think about a theorem that says that a certain statement φ cannot be proved or refuted in such an all-embracing system? Should we say that the actual 'truth' about our object exists somewhere out there but our mathematical tools and intuitions are not sufficient to discover which alternative φ or $\neg\varphi$ is true (the "Platonist" or "realist" belief)? Or should we say that because each of the two alternatives is consistent with our most comprehensive, list of axioms that we wanted to have, we should think in terms of "parallel universes" with φ being true in some universes and $\neg\varphi$ being true in other universes (a picture common among various "pluralist" views)? We have seen many exciting stories of unprovability results in the last two centuries: Euclid's Fifth Postulate (cannot be proved or refuted using the first four postulates), the Axiom of Choice (cannot be proved or disproved in ZF), the Axiom of Determinacy (cannot be proved or disproved[1] in ZF), Cantor's Continuum Hypothesis (independent of ZFC), etc. The 'age of innocence' in mathematics is now long over. Mathematical statements are no longer 'true or false' but form a complex net of implications, equivalences and other complicated interdependencies.

In this paper we deal with another all-embracing axiomatic system: Peano Arithmetic. The axioms of Peano Arithmetic, formulated in the first-order language $\{+, \cdot, <, s, 0, 1\}$, state all basic properties we want of our natural numbers, i.e. successors are never zero, the successor function is injective, the defining recursive equations for addition and multiplication are as expected, distributivity, linear order, and finally the scheme of mathematical induction: $\forall\vec{x}\Big(\varphi(0,\vec{x}) \wedge \forall y(\varphi(y,\vec{x}) \to \varphi(y+1,\vec{x})) \to \forall y\varphi(y,\vec{x})\Big)$, that is, for every formula $\varphi(y,\vec{x})$ we state the above instance of mathematical induction as an axiom. PA is an extremely strong system for carrying out mathematics. It is possible to define rationals, pairs of rationals, functions on rationals, sequences of rationals that converge in themselves, hence also continuity of functions, all classical functions of calculus (approximating them by partial sums of their Taylor expansions), differentiation of functions, etc., using formulas of the first-order language of arithmetic, and prove all the usual theorems about these objects using axioms of PA. Also, speaking and reasoning about finite structures, sequences, trees, graphs, constructive real numbers, finite cardinalities, as well as any 'infinite' objects that have approximations by finite sets is straightforward in PA. In particular, PA can perform all usual proofs of analytic combinatorics, number theory, complex analysis, etc.

For a long time it was presumed without much thought that every question about natural numbers (and hence also about any object encoded by approximations by finite sets) can be answered using PA. It was Kurt Gödel who strongly refuted this belief by constructing the first examples of statements G in the language of arithmetic such that PA can neither prove nor refute G. Gödel's first example was constructed by a diagonalisation argument and has a strong logical, syntactic flavour. Essentially G expresses its own unprovability in PA, so perhaps its unprovability is not too surprising a posteriori.

2 Two fundamental examples of PA-unprovable combinatorial statements

Gödel's Incompleteness Theorem did not have dramatic effect on mainstream mathematics at the time, mostly because the first unprovable statement G was built by a purely logical, syntactic construction, using a diagonal argument, and for many decades there were no other methods to produce unprovable statements. This situation even prompted

[1] but its consistency is equivalent to consistency of existence of some large cardinals

some people of that era to declare that unprovability will never concern real mathematical practice and that no meaningful interesting mathematical statements will ever turn out to be unprovable, that unprovability will be forever locked in its syntactic dungeon.

This situation changed in the late 1970s when Jeff Paris invented a model-theoretic method of building PA-unprovable combinatorial statements and, jointly with Leo Harrington, provided a mathematically appealing example of an assertion that is not provable or refutable in PA [21]. Let us formulate this unprovable statement (the Paris-Harrington Principle, denoted PH). For a set X, let $[X]^n$ be the set of all n-element subsets of X. Let us identify every natural number m with the set of its predecessors $\{0, \dots, m-1\}$. The finite Ramsey theorem FRT says "for every triple of natural numbers d, c, s (dimension, number of colours and size), there is a natural number R such that for every partition $P\colon [R]^d \to c$, there exists a set $H \subseteq R$ such that $|H| = s$ and the restriction $P|_{[H]^d}$ is constant". The set H is called P-homogeneous or P-monochromatic. The minimal value of R is called the corresponding Ramsey number and will be denoted by $R(d, c, s)$. A classical theorem of Erdös and Rado gives us the upper bound:

$$R(d, c, s) \leq 2_{d-1}(d \cdot c \cdot \log_2(c) \cdot s).$$

Here, $2_n(x)$ denotes the tower of n twos with an x on the top (i.e. $2_0(x) = x$ and $2_{n+1}(x) = 2^{2_n(x)}$). Since the tower-function is provably computable in PA, PA proves FRT. A finite set X of natural numbers is called relatively large if $|X| \geq \min X$. So $\{3, 33, 333, 3333\}$ is relatively large but $\{11, 111, 1111, 11111, 111111\}$ is not and clearly relative largeness is a property which is not closed under order-preserving bijections but depends on the position of our set among natural numbers. The Paris-Harrington assertion PH is the Finite Ramsey Theorem with the extra condition that the monochromatic set is relatively large. That is, PH says "for every triple of natural numbers d, c, s, there is a natural number R such that for every partition $P\colon [R]^d \to c$ there exists a *relatively large* set $H \subseteq R$ such that $|H| \geq s$ and $P|_{[H]^d}$ is constant".

The Paris-Harrington assertion is unprovable in PA. We can easily use infinitary 'set-theoretic' methods (stronger than PA) to prove PH, so the potential trivial case that PH is unprovable because it is outright contradictory doesn't happen. The proof goes by a standard compactness argument applied to the infinitary Ramsey theorem "for all natural numbers d and c and all partitions $P\colon [\mathbb{N}]^d \to c$ there exists an infinite set $H \subseteq \mathbb{N}$ which is P-monochromatic".

At this moment two questions are immediate. Why is PH unprovable from PA? Is it possible to find some rationale behind the largeness condition?

We address these questions later but first let us discuss another striking unprovable combinatorial assertion, the Finite Kruskal Theorem, discovered around 1980 by Harvey Friedman. Define a finite tree as a finite partially ordered set $\langle T, \leq_T \rangle$ with a minimal element r (the root, which satisfies $r \leq_T t$ for all $t \in T$) and such that for every element $t \in T$, the set of its predecessors $\{s \in T \mid s \leq_T t\}$ is linearly ordered by $\leq_T$. For two given nodes t, t' there exists a uniquely determined least upper bound $\inf_T(t, t')$ of t and t' in T (i.e., the first point where the paths from t and t' to the root meet). Given two trees $\mathcal{S} = \langle S, \leq_S \rangle$ and $\mathcal{T} = \langle T, \leq_T \rangle$ we call $\mathcal{S}$ embeddable into $\mathcal{T}$ (and write $\mathcal{S} \trianglelefteq \mathcal{T}$ for this) if there exists an injective mapping $h\colon S \to T$ such that $h(\inf_S(s, s')) = \inf_T(h(s), h(s'))$ for all $s, s' \in S$. This is the natural notion of embeddability for this notion of a tree. For example, if $\mathcal{S} \trianglelefteq \mathcal{T}$ then of course $|S| \leq |T|$, the height of $\mathcal{S}$ does not exceed the height of $\mathcal{T}$ and the outdegree of $\mathcal{S}$ does not exceed the outdegree of $\mathcal{T}$.

Harvey Friedman's assertion FKT is the statement: "for any natural number K there exists a natural number M such that for any sequence $\mathcal{T}_0, \dots, \mathcal{T}_M$ of finite trees there are natural numbers $i < j \leq M$ such that $\mathcal{T}_i \trianglelefteq \mathcal{T}_j$, provided that this sequence satisfies the condition that the number of nodes in $\mathcal{T}_i$ does not exceed $K + i$ for all $i \leq M$".

This assertion is unprovable in PA and even in some stronger theories [23, 24]. To exclude the trivial reason for unprovability (that is, that the assertion could be refuted), it is possible to check that FKT can be proved using much stronger methods. The proof goes by a routine application of compactness to the infinitary tree theorem of Kruskal: "for any infinite sequence $(\mathcal{T}_i)_{i<\omega}$ of finite trees, there exist natural numbers $i < j$ such that $\mathcal{T}_i \trianglelefteq \mathcal{T}_j$". Kruskal's theorem is a highlight in combinatorics and the proof provided by Nash-Williams (which is based on a *minimal bad sequence argument*) is one of the most beautiful proofs in mathematics (a proof can be found, for example, in [23]).

To get a first taste of FKT, let us fix $K = 100$ and ask for the smallest possible $M = M_{100}$ in the assertion FKT. It is known that M_{100} is quite big. The precise value is unknown but a lower bound is 2_{1000} where $2_1 = 2$ and $2_{k+1} = 2^{2_k}$. It is known that PA proves all "true" existential statements (namely: if for some natural number n, an arithmetical statement $\varphi(n)$ without unbounded quantifiers is verified by the computation of the corresponding truth value on input n then PA proves $\exists x \varphi(x)$) and therefore PA proves the existence of M_{100}. Still it would take quite some time to write down the proof of this, since Harvey Friedman showed that the number of symbols used in a PA-proof of existence of M_{100} would necessarily be bigger than 2_{1000}.

Again, two questions are immediate. Why is FKT unprovable from PA? Is it possible to find some rationale behind the linear growth rate condition?

3 A simple paradigm for some independence results: growth rates of functions

There are many more families of unprovable statements and it would be convenient to see a common reason behind different unprovability phenomena.

To prove that an assertion A is independent from a set of axioms T (that is not provable and not refutable in T) it is usually possible to construct two models of T such that one model makes A true and the other model makes the negation of A true. A classical example is from geometry. Euclid's Fifth Postulate (in its Playfair's formulation) says that given a line and a point outside this line, there exists a unique parallel line passing through this point. $\mathbb{R}^2$ with the standard interpretation of lines and points is a model of geometry where Euclid's Fifth Postulate holds. The Beltrami-Klein model and two models by Poincare are models of hyperbolic geometry (the parallel line passing through our point is not unique) thus satisfying the negation of Euclid's Fifth Postulate, and the sphere with lines interpreted as great circles is a model of elliptic geometry (any two lines intersect) thus also satisfying the negation of Euclid's Fifth Postulate.

We can see the same story in the solution of Cantor's Continuum Problem (which was also Hilbert's First Problem in Hilbert's list). CH is the assertion that every infinite subset of $\mathbb{R}$ is either in bijective correspondence with the rationals or in bijective correspondence with the whole set $\mathbb{R}$. Kurt Gödel showed that there is a model of the axioms of set theory ZFC in which CH holds and Paul Cohen produced a model of ZFC in which CH fails.

Similarly, in the study of arithmetical statements, nowadays there is already a whole machinery of building models that satisfy or refute our statements. (The paper [4] by the first author, contains some full and accessible model-theoretic unprovability proofs, in particular a simple unprovability proof for the Paris-Harrington assertion PH.)

However, at the level of PA, there is another, much simpler picture or reason that explains how you *may* think about unprovability of arithmetical statements of the form $\forall x \exists y \ \varphi(x, y)$. This is growth rate of functions. (However for theories like ZFC that have much higher arithmetical strength than PA, and prone to philosophical controversies (various questions of meaning, 'truth', justification of axioms, etc), this explanation might

fail but at the level of PA, which we are discussing here, it is neat and clear.)

Before we start our discussion of fast-growing functions, here is a word of warning: "fast" will mean very fast. Functions like $2^{2^{2^x}}$ or 2_k will be considered very slow.

To start, we need the following hierarchy at the bottom level:

$$\begin{aligned} F_0(n) &= n+1 && (1)\\ F_{k+1}(n) &= \underbrace{F_k(\ldots F_k}_{n \text{ times}}(n)) \text{ (the } \textit{iteration} \text{ step)} && (2) \end{aligned}$$

The hierarchy starts modestly, but then even F_3 grows faster than the usual functions that show up in calculus. Now consider the *diagonal* function $F(n) = F_n(n)$. The function F eventually dominates every F_k (for every fixed natural number k). No computer is able to calculate the decimal representation of $F(10)$, so $F(10)$ is quite big. The number $F(10)$ is even greater than the famous Graham number.

But for our purposes, functions from this hierarchy and its diagonal function F are still too slow. We need a *transfinitely* extended process of combining iteration and diagonalisation. (In a certain sense that can be made precise, transfinite methods are unavoidable here.) To introduce the required notions (without going explicitly into ordinal numbers) let us consider a subclass of Hardy's orders of infinity [14].

Let $\mathcal{E}$ be the least set of functions $f\colon \mathbb{N} \to \mathbb{N}$ such that:

1. the constant zero function (which we shall denote by 0) is an element of $\mathcal{E}$;
2. if $f, g \in \mathcal{E}$ then the function h defined as $h(n) = n^{f(n)} + g(n)$ is an element of $\mathcal{E}$.

This class contains all polynomials with natural number coefficients and all sorts of mixtures of exponentials with such polynomials. $\mathcal{E}$ is ordered by eventual domination in the natural way: set $f \prec g$ if and only if there exists a natural number K such that for all $n > K$ we have $f(n) < g(n)$. Hardy showed that $\prec$ is a linear order. Actually, $\prec$ is a well-order (there are no infinite strictly descending sequences of elements of $\mathcal{E}$) by Ehrenfeucht's classical argument based on Kruskal's theorem [10]. (Well-orderedness of $\mathcal{E}$ can also be proved using König's Lemma, or one may employ ordinals for the same purpose.)

It can be shown that every non-zero function f in $\mathcal{E}$ can be written uniquely as

$$f = id^{f_1} + \cdots + id^{f_m},$$

where $f_1 \succeq \ldots \succeq f_m$ and id is the identity function. If in this expression f_m is the zero function then f is called a successor and otherwise a limit. For limit elements $f \in \mathcal{E}$ and every $k \in \mathbb{N}$, we introduce an element $f[k] \in \mathcal{E}$ such that the sequence $f[k]$ converges to f in the order topology. This means that whenever $g \prec f$, there will be $k \in \mathbb{N}$ such that $g \prec f[k]$. Let f be as above.

1. If f_m is a limit, we assume that $f_m[k]$ has been defined and set $f[k] = id^{f_1} + \cdots + id^{f_m[k]}$.
2. If f_m is a successor of the form $f_m = f'_m + id^0$ then set $f[k] = id^{f_1} + \cdots + id^{f'_m[k]} \cdot k$.

In the rest of the paper we abbreviate id^0 as 1. For technical reasons we set $(f+1)[k] = f$ and $0[k] = 0$ for non-limit elements of $\mathcal{E}$. Over $\mathcal{E}$ we can build up the following hierarchy:

$$\begin{aligned} F_0(n) &= n+1\\ F_{f+1}(n) &= \underbrace{F_f(\ldots F_f}_{n \text{ times}}(n))\\ F_f(n) &= F_{f[n]}(n) \text{ if } f \text{ is a limit.} \end{aligned}$$

Define $\omega_1(n) = n$ and $\omega_{k+1}(n) = \omega^{\omega_k(n)}$. Then $(\omega_k)_{k<\omega}$ is a cofinal sequence in $\mathcal{E}$. Define a new function $F_{\mathcal{E}}$ as follows: $F_{\mathcal{E}}(n) = F_{\omega_n}(n)$. Then $F_{\mathcal{E}}$ eventually dominates every F_f for any $f \in \mathcal{E}$.

About $F_{\mathcal{E}}$ many logicians would agree that it is indeed fast-growing. It turns out that for any function $G\colon \mathbb{N} \to \mathbb{N}$ which is provably computable in PA (i.e. such that PA proves $\forall x \exists y\, G(x) = y$), there exists $f \in \mathcal{E}$ such that $G(n) < F_f(n)$ for all n. (This fundamental result goes back to Ackermann [1] and Kreisel [18]. A more polished proof for this result using so called cut-elimination can be found in [7] or [27]. The details are still intricate and beyond the scope of the present survey.) The upshot is that PA cannot prove the totality of the function $F_{\mathcal{E}}$ itself. Let $\mathrm{TOT}(F_{\mathcal{E}})$ be the assertion: "for all K, there exists a natural number M such that $F_{\mathcal{E}}(K) = M$". Here, $F_{\mathcal{E}}(K) = M$ should be read as a formula in the language of arithmetic and so it stands for the assertion that there exists a natural number coding a successful computation of $F_{\mathcal{E}}(K)$ which leads to the result M. In this situation $\mathrm{TOT}(F_{\mathcal{E}})$ is a paradigm for a PA-unprovable statement.

Having argued that $\mathrm{TOT}(F_{\mathcal{E}})$ is of paradigmatic importance, it is important to recognise that $\mathrm{TOT}(F_{\mathcal{E}})$ can be easily written as a statement about natural numbers. For this purpose one has to code the elements of $\mathcal{E}$ by positive integers. One solution runs as follows. Let p_i be the i-th prime number, $p_1 = 2$. Define the following relation $\lhd$ on the positive integers: $m \lhd n$ if and only if m is different from n and either $m = 1$ or for every prime divisor p_i of $\frac{m}{(m,n)}$, there exists a prime divisor p_j of $\frac{n}{(m,n)}$ such that $i < j$. Here (m, n) denotes the greatest common divisor of m and n. So, the ordering looks like this:

$$1 \lhd 2 \lhd 4 \lhd \ldots 3 \lhd 3 \cdot 2 \lhd 3 \cdot 4 \lhd \ldots 3^2 \lhd 3^2 \cdot 2 \lhd 3^2 \cdot 4 \lhd \ldots 3^n \lhd 3^n \cdot 2 \lhd \ldots p_{2^k}^m \lhd p_{2^k}^m \cdot 2 \lhd \ldots \quad 5 \lhd \ldots$$

It turns out that the positive integers ordered by $\lhd$ are order-isomorphic to $(\mathcal{E}, \prec)$. The isomorphism $\varphi\colon \mathcal{E} \to \mathbb{N}\backslash\{0\}$ can be defined as follows: $\varphi(0) = 1$ and $\varphi(id^f + g) = p_{\varphi(f)} \cdot \varphi(g)$.

Over $\mathcal{E}$ we can build up the following alternative hierarchy:

$$\begin{aligned} H_0(n) &= n \\ H_{f+1}(n) &= H_f(n+1) \\ H_f(n) &= H_{f[n]}(n) \text{ if } f \text{ is a limit.} \end{aligned}$$

Let $H_{\mathcal{E}}(n) = H_{\omega_n}(n)$.

By a simple calculation, it turns out that $F_f(n) = H_{id^f}(n)$. Therefore $\mathrm{TOT}(F_{\mathcal{E}})$ is equivalent to the assertion $\mathrm{TOT}(H_{\mathcal{E}})$: "for all x there exists y such that $H_{\mathcal{E}}(x) = y$". In general, writing down a formula for $H_f(x) = y$ is a routine matter using tools available in PA. Indeed, $H_f(x) = y$ means that there exists a sequence of pairs of natural numbers coding the calculation of $H_f(x) = y$. So the first entry of this sequence may consist of $(0, x)$, and the last may consist of $(\varphi(f), y)$ and for all intermediate entries one has to repeat the recursive clauses of the definition of the H-functions (see, for example, [27] for an exposition).

Let HYDRA be the following assertion: "for all $f \in \mathcal{E}$ there exists a natural number K such that $f[0][1]\ldots[K] = 0$". It is easy to show that HYDRA is equivalent to the famous Paris-Kirby assertion that Hercules wins any battle against any hydra [17]. It can be shown (by specialising the first quantifier to functions of the form ω_{x+x}) that HYDRA implies $\mathrm{TOT}(H_{\mathcal{E}})$ and so HYDRA is a PA-unprovable statement. Of course HYDRA can be proved using a stronger argument (well-orderedness of $\mathcal{E}$): since $\mathcal{E}$ is well-ordered, there is no infinite descending chain $f \succ f[0] \succ \ldots \succ f[0][1]\ldots[K] \succ f[0][1]\ldots[K][K+1] \succ \ldots$. (A systematic treatment of the Hardy hierarchy and related topics can be found in [6].)

A first unprovability result for PA that looks to some extent number-theoretic is now within reach. Pick your favourite number m and perform the following steps. Assume we are at step $k \geq 1$. First subtract 1 from the number under consideration if your number is not zero. Then rewrite the result completely with respect to base $k + 1$ (and do this

iteratively also in the exponents and exponents of exponents etc.) and then replace the base $k+1$ at all of its occurrences by $k+2$, and go to the next step. The first entries of the resulting sequence indicate that this sequence is quickly diverging. This is supported by any computer experiment when one starts with, say, $m = 10$. But this impression is a perception trick. Let GOODSTEIN be the assertion "for all m, there is n such that the process for m hits zero after fewer than n steps". Then GOODSTEIN follows from the well-orderedness of $\mathcal{E}$. By a non-trivial translation argument, one can show that GOODSTEIN implies TOT($H_{\mathcal{E}}$) by elementary means and so GOODSTEIN is PA-unprovable [9].

It is now a natural question whether PH and FKT might imply TOT($H_{\mathcal{E}}$) in an elementary way, so that their PA-unprovability would follow from PA-unprovability of TOT($H_{\mathcal{E}}$). This is true but this time the proofs are more complicated. A translation of PH to TOT($H_{\mathcal{E}}$) was provided by J. Ketonen and R. Solovay but their argument is quite involved [16]. Later, M. Loebl and J. Nesetril simplified the Ketonen-Solovay proof in [19] but the proof still remains somewhat mysterious since partitions of all d-element subsets of finite sets of natural numbers are induced by partitions of sets of subsets of ordinals. An alternative way of proving PA-unprovability of PH is model-theoretic. This was the original method that gave rise to PH and many related statements equivalent to PH. A streamlined treatment of PH using this approach is given in [4].

It is much easier to show that Friedman's assertion FKT implies TOT($H_{\mathcal{E}}$), and hence is PA-unprovable. (This is not surprising since FKT is strictly much stronger than PH or TOT($H_{\mathcal{E}}$).) Let us define the norm $N(f)$ of an element of $\mathcal{E}$ as follows: $N(0) = 0$ and $N(id^f + g) = 1 + N(f) + N(g)$. Let SWO ("slow well-orderedness") be the following assertion: "for all natural numbers K there exists a natural number M such that for all $f_0, \ldots, f_M \in \mathcal{E}$ there exists a natural number $i < M$ such that $f_i \preceq f_{i+1}$, provided that $N(f_i) \leq K + i$ for all $i \leq M$".

It can be shown that SWO implies TOT($H_{\mathcal{E}}$) by elementary means and therefore SWO is PA-unprovable. Now, introduce the canonical bijection ψ between finite trees and $\mathcal{E}$: $\psi(0)$ is the singleton tree and if $f = id^{f_1} + \ldots + id^{f_m}$ with $f_1 \succeq \ldots \succeq f_m$ then $\psi(f)$ is the tree consisting of the root and immediate subtrees $\psi(f_1), \ldots, \psi(f_n)$. It turns out that $N(f)$ is the number of edges in $\psi(f)$. Under this bijection, $\trianglelefteq$-embeddability of trees implies the $\preceq$-relation on their inverse images. Therefore we have an elementary proof of SWO from FKT, and thus FKT is PA-unprovable.

We have seen many interesting unprovable statements so far (and there exist many more!) but despite logicians' hopes, these phenomena did not receive much attention in mainstream mathematics. We shall now describe a connection of the above unprovability results with analytic combinatorics and complex analysis. This may look unbelievable since all objects in our unprovable statements seemed discrete and the high growth rates of functions have not had any connection with functions from analysis.

4 Phase transitions for independence results

Around 2000, the second author introduced a new aspect of Unprovability Theory: phase transitions between provability and unprovability.

Let $A(r)$ be an assertion in the language of arithmetic which is parametrised with a non-negative rational number r, the *order parameter*, and suppose "for every positive $r \in \mathbb{Q}$, $A(r)$ holds" has been proved using some extremely strong theory, like ZFC or Z_2. Let us suppose that $A(r)$ is monotone, that is for $r < s$, $A(s)$ implies $A(r)$. Assume that for some small values of r, $A(r)$ is PA-provable but for some other values of r, $A(r)$ is PA-unprovable. Now we can define the phase transition threshold $\rho \in \mathbb{R}$ given by the

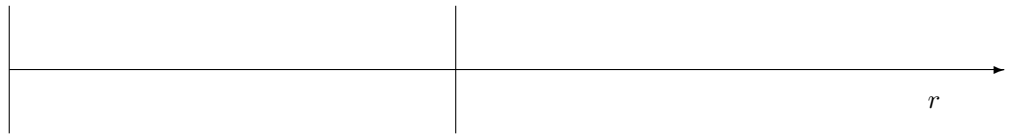
resulting Dedekind cut:

$$\rho = \sup\{r \mid \text{PA proves } A(r)\} = \inf\{r \mid \text{PA does not prove } A(r)\}.$$

Let us study the first concrete example of such phase transition: the formula FKT that expresses the finite Kruskal theorem. Let us fix a primitive recursive (so that it has a description within PA) real number r and let FKT_r be the following assertion: "for any natural number K there exists a natural number M such that for any sequence $\mathcal{T}_0, \ldots, \mathcal{T}_M$ of finite trees, there are natural numbers $i < j \leq M$ such that $\mathcal{T}_i \trianglelefteq \mathcal{T}_j$, provided that this sequence satisfies the condition that the number of nodes in $\mathcal{T}_i$ does not exceed $K + r \cdot \log_2(i)$ for all $i \leq M$".

Of course FKT_r follows from the Infinite Kruskal Theorem for every r (in the same way as FKT does) and thus is provable in the same very strong theory as the Infinite Kruskal Theorem.

J. Matousek and M. Loebl proved that $\text{FKT}_{\frac{1}{2}}$ is provable in PA but FKT_4 is PA-unprovable. So for FKT_r there will be a critical constant ρ. In [25] the critical value for ρ has been determined as $\frac{\ln(2)}{\ln(\alpha)} \approx 0.6395781750\ldots$, where α is the Otter's tree constant [20], $\alpha = 2.95576\ldots$. It is currently not known whether α is rational, irrational, algebraic or transcendental).



0 PA proves A_r ρ PA does not prove A_r

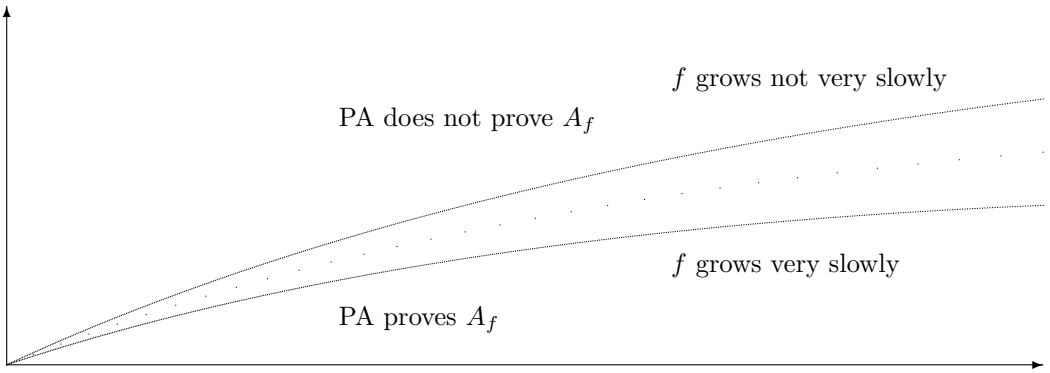
Explaining the nature of α leads naturally to the first point where analysis enters. Let $T(z) = \sum_{n=0}^{\infty} t_n z^n$ be the power series such that $T(z) = z \cdot \exp(\sum_{i=1}^{\infty} \frac{T(z^i)}{i})$. This is an implicit description of T which fixes its coefficients. It can be shown that the radius of convergence η of T is larger than zero. Now, $\frac{1}{\eta} = \alpha$ is called Otter's tree constant. Analytic combinatorics yields that $t_n \sim const \cdot \frac{\alpha^n}{n^{\frac{3}{2}}}$ and this combinatorial result eventually leads to the proof of the threshold result [25]:

1. for all $r \leq \rho$, PA proves FKT_r;
2. for any $\varepsilon > 0$, PA does not prove $\text{FKT}_{\rho+\varepsilon}$.

To make this phase transition result even sharper, let us consider contexts in which ε is replaced by a sequence that slowly converges to zero.

To study such questions in a more general context we may try to arrange that our assertion A depends on a function parameter f. Suppose, like before, that "for all $f\colon \mathbb{N} \to \mathbb{N}$, the statement A_f holds" has been proved in some extremely strong theory. Suppose that for some slow-growing f, A_f is PA-provable and for some faster-growing f, A_f is PA-unprovable. Also suppose monotonicity: if f eventually dominates g then A_f implies A_g. In this set-up, we can now expect to have a functional threshold between provability and unprovability.

Determining the threshold for A_f seems to give us some insights about the general philosophical question: *What makes an assertion* PA*-unprovable?*



Returning now to our example of the Finite Kruskal theorem, the following refinement emerges. Let FKT_G be the following assertion: "for any natural number K there exists a natural number M such that for any sequence $\mathcal{T}_0, \ldots, \mathcal{T}_M$ of finite trees, there are $i < j \leq M$ such that $\mathcal{T}_i \trianglelefteq \mathcal{T}_j$, provided that this sequence satisfies the condition that for all $i \leq M$, the number of nodes in $\mathcal{T}_i$ does not exceed $K + G(i)$".

For any unbounded nondecreasing function $H\colon \mathbb{N} \to \mathbb{N}$, let H^{-1} denote the functional inverse of H (i.e, $H^{-1}(m) = \min\{n \mid H(n) > m\}$). The function $\frac{1}{H_f^{-1}(n)}$ will serve as a dynamic ε which slowly converges to zero. Now, here is the ultimate refined phase transition theorem for the Finite Kruskal Theorem.

1. For any $f \in \mathcal{E}$, let $G_f(n) = \big(\rho + \frac{1}{H_f^{-1}(n)}\big) \cdot \log_2(n)$. Then PA proves FKT_{G_f}.

2. But if we put $G_{\mathcal{E}}(n) = \big(\rho + \frac{1}{H_{\mathcal{E}}^{-1}(n)}\big) \cdot \log_2(n)$ then suddenly PA does not prove $\mathrm{FKT}_{G_{\mathcal{E}}}$.

The proof of the first half of the theorem employed a recent unpublished result by Schlage Puchta [22].

Another appealing phase transition is related to SWO. Let SWO_G be the assertion: "for all natural numbers K there exists a natural number M such that for all $f_0, \ldots, f_M \in \mathcal{E}$, there exists $i < M$ such that $f_i \preceq f_{i+1}$, provided that $N(f_i) \leq K + G(i)$ for all $i \leq M$". Here is the phase transition result.

1. For $f \in \mathcal{E}$, let $G_f(n) = \log_2(i) \cdot \log_2^{(H_f^{-1}(n))}(i)$, where the upper index denotes the number of iterated applications of the logarithm function. Then PA proves SWO_{G_f}.

2. But if we let $G_{\mathcal{E}}(n) = \log_2(i) \cdot \log_2^{(H_{\mathcal{E}}^{-1}(n))}(i)$, then PA does not prove $\mathrm{SWO}_{G_{\mathcal{E}}}$.

To obtain these results, we needed asymptotic information on the function

$$c_f(n) = |\{g \prec f \mid N(g) = n\}|.$$

It turns out that such information is available by methods dating back to Hardy and Ramanunjan. Since $c_{id^{id}}(n)$ is the partition function, we obtain

$$c_{id^{id}}(n) \sim \frac{\exp(\pi\sqrt{\frac{2}{3}n})}{4\sqrt{3}n}.$$

Moreover

$$\log(c_{\omega_3}(n)) \sim \frac{\pi^2}{6} \cdot \frac{n}{\log(n)}$$

and

$$\log(c_{\omega_4}(n)) \sim \frac{\pi^2}{6} \cdot \frac{n}{\log\log(n)}$$

etc. These weak asymptotic results follow by exploiting the corresponding fundamental identities for the generating functions in question. In general one has:

$$\sum_{n=0}^{\infty} c_{idf}(n) z^n = \prod_{i=1}^{\infty} \frac{1}{(1-z^i)^{c_f(i)}}.$$

From this, one can extract the desired asymptotic information on $\log(c_{idf}(n))$ recursively from previously proved asymptotic information on $\log(c_f(i))$ [25].

The above phase transition threshold for SWO_G is essentially computed from the functional inverse of the count functions for c_{ω_k}.

Now let us come back to the Paris-Harrington assertion. To study its phase transition, let us call a set of natural numbers relatively G-large if $|H| \geq G(\min X)$. The assertion PH_G says "for every triple of natural numbers d, c, s, there is a natural number R such that for every partition $P\colon [R]^d \to c$ there exists a *relatively G-large* set $H \subseteq R$ such that $|H| \geq s$ and the restriction $P|_{[H]^d}$ is constant". It turns out, and this is crucial for understanding of the largeness condition, that if we take for G the inverse of the function $s \mapsto R(s,s,s)$, hence essentially the inverse of the tower function, then PH_G follows by elementary means from FRT and so PA proves PH_G in this case. But if we take for G a fixed iterate of the log function then the provability argument no longer applies and it has been shown in [26] that for such G, PH_G suddenly becomes PA-unprovable. The ultimate phase transition result for PH is now as follows.

1. For $f \in \mathcal{E}$, if $G_f(n) = \log_2^{(H_f^{-1}(n))}(n)$, then PA proves PH_{G_f}.

2. But for $G_{\mathcal{E}}(n) = \log_2^{(H_{\mathcal{E}}^{-1}(n))}(n)$, PA does not prove $\mathrm{PH}_{G_{\mathcal{E}}}$.

There are many more threshold results being proved nowadays. Very often, once we find an instance of unprovability, a threshold conjecture can be formulated. It may depend on some counting results in combinatorics, but often lower bounds and upper bounds are within easy reach. Let us finish the story of phase transitions by one more illustration.

We say that a graph G is a minor of a graph H if G can be obtained from H be deleting edges, contracting edges and deleting isolated vertices. A famous theorem by N. Robertson and P. Seymour says that in every infinite sequence of finite graphs, there is an earlier graph that is isomorphic to a minor of a later graph. It was proved by H. Friedman, N. Robertson and P. Seymour that the following finite graph minor theorem "for every K there is N such that whenever $G_1, G_2, \ldots, G_N$ are graphs with $|G_i| < K + i$ then for some $i < j \leq N$, G_i is isomorphic to a minor of G_j" is unprovable in PA and in certain much stronger systems. Also, if you restrict this statement to planar graphs it remains unprovable.

The first author recently established the unprovability threshold for this statement restricted to planar graphs, connected planar graphs and graphs embeddable into a given surface, assuming an unproved conjecture (*): 'for all $k \geq 3$, a random unlabelled planar graph omitting the k-element circle as minor is connected with positive probability'. Let γ be the unlabelled planar growth constant, a classical constant in graph enumeration theory (a number somewhere between 26 and 32). Let $P(c)$ be the following first-order arithmetical statement with real parameter c: "for every K there is N such that whenever

$G_1, G_2, \ldots, G_N$ are planar graphs with $|G_i| < K + c \cdot \log_2 i$ then for some $i < j \leq N$, G_i is isomorphic to a minor of G_j". Then

1. for every $c \leq \frac{1}{\log_2 \gamma}$, $P(c)$ is provable in PA;
2. for every $c > \frac{1}{\log_2 \gamma}$, $P(c)$ is unprovable in PA.

The unprovability clause can be improved to talk about unprovability in a much stronger theory. The same threshold constant $\frac{1}{\log_2 \gamma}$ separates provable and unprovable instances when you formulate the same statement $P(c)$ for connected planar graphs or for graphs embeddable into a given surface.

5 Reformulating unprovable combinatorial statements to talk about zeta

We shall now discuss encodings of Ramsey-like statements using number-theoretic objects. We could use the Paris-Harrington Principle for such encodings, but a more convenient unprovable statement for these purposes turns out to be the Kanamori-McAloon principle. For $X \subseteq \mathbb{N}$, we call a partition $P\colon [X]^d \to \mathbb{N}$ regressive if $P(x_1, \ldots, x_d) \leq x_1$ where we assume that $x_1 < \ldots < x_d$. We call a set H min-homogeneous for P if $P(x_1, x_2, \ldots, x_d) = P(x_1, y_2, \ldots, y_d)$ for all $x_1 < x_2 < \ldots < x_d$ and $x_1 < y_2 < \ldots < y_d$ in H. The Kanamori-McAloon Principle is the following assertion (denoted KM): "for all natural numbers d and m there exists a natural number R such that for all regressive partitions $P\colon [R]^d \to \mathbb{N}$ there exists a subset $H \subset R$ of size at least m which is min-homogeneous for P". It can be shown by elementary combinatorial manipulations that KM is equivalent to PH. (Also, there is a canonical notion of G-regressive partitions and the resulting phase transition for KM is the same as for PH.)

An interesting reformulation of a version of the Kanamori-McAloon Principle was suggested by Harvey Friedman [12]. Let us formulate it in our way, more resembling KM. The statement "for all m and d there exists N such that whenever $a_1 < a_2 < \ldots < a_N$ are rational numbers, there is a subset $H \subset \{0, 1, 2, \ldots, N-1\}$ such that for any $i_1 < i_2 < \ldots < i_d$ and $i_1 < k_2 < \ldots < k_d$ in H,

$$|\sin(a_{i_1} \cdot a_{i_2} \cdot \ldots \cdot a_{i_d}) - \sin(a_{i_1} \cdot a_{k_2} \cdot \ldots \cdot a_{k_d})| < 2^{-i_1}"$$

is PA-unprovable. You can find some discussion of Friedman's sine-principle in [3]. Notice that the true Ramseyan character of this statement (that is responsible for unprovability gear-mechanisms) is moderately well-hidden (you see no quantification over all possible partitions, since no partitions are mentioned in it). It turns out that similar statements can be written for many other functions, including the Riemann zeta-function. This is what we shall do in the rest of this section.

Investigations on PA-unprovability lead to some natural questions about analytic objects which can be investigated by mathematicians without any experience in logic. It is our hope that some of these results and some open questions needed for future advances in this direction might prompt a back-and-forth exchange between the two subjects.

Lemma 1. *Let $\sigma > 1$ and let I_σ be a non-trivial interval (which exists according to [2]) on the real line in which the zeta values $\zeta(\sigma + it)$ are dense. Let $\varepsilon > 0$ and $R > n \geq 2$ be two arbitrary natural numbers and $F\colon [R]^n \to I_\sigma$ be an arbitrary function. Let N be so large that $|\prod_{i=N+1}^{\infty} \frac{1}{1-p_i^{-\sigma-it}}| < \frac{\varepsilon}{6}$ uniformly in t. Let $K = \mathbb{Q}(\log(p_1), \log(p_2), \ldots, \log(p_N))$*

where p_i denotes the i-th prime. Then there exist K-algebraic irrationals $a_1, \ldots, a_R$ over K such that $deg_K(a_i) = 3^{3^{n^i}}$ for $1 \leq i \leq R$ and such that

$$|F(i_1, \ldots, i_n) - \zeta(\sigma + i \cdot a_{i_1} \cdot \ldots \cdot a_{i_n})| < \varepsilon$$

for $1 \leq i_1 < \ldots < i_n \leq R$.

Proof. By [2] find for all sequences $i_1 < \ldots < i_n$ rational numbers $t(i_1, \ldots, i_n)$ such that $|\zeta(\sigma + i \cdot t(i_1, \ldots, i_n)) - F(i_1, i_2, \ldots, q+1)| < \varepsilon/6$.

The proof is now by induction on i_n. Assume $i_n = n$. Pick K-algebraic irrationals $a_1, \ldots, a_{n-1}$ such that $deg(a_i) = 3^{3^{n^i}}$. By [2] we know that $t \mapsto \zeta(\sigma + it)$ is dense in I_σ. Then by density of the algebraic irrationals involved, we can pick a suitable a_n which has to satisfy only $|F(1, 2, \ldots, n) - \zeta(\sigma + ia_1 \cdot \ldots \cdot a_n)| < \varepsilon$.

Now consider $i_n = q + 1$ and assume that $a_1, \ldots, a_q$ have been constructed with the desired properties.

Put $\zeta_N(\sigma + i \cdot t) := \prod_{i=1}^{N} \frac{1}{1 - p_i^{-\sigma - i \cdot t}}$ and $R_N(\sigma + i \cdot t) := \frac{\zeta(\sigma + i \cdot t)}{\zeta_N(\sigma + i \cdot t)}$.

By the condition on degrees, the products $\log(p_j) \cdot a_{i_1} \cdot \ldots \cdot a_{i_n}$ are linearly independent. Hence by Kronecker's result on simultaneous Diophantine approximation (in the effective form) and continuity considerations we find a rational number t with effective bounds on numerator and denominator such that

$$|\zeta_N(\sigma + i \cdot a_{i_1} \cdot \ldots \cdot a_{i_{n-1}}) - \zeta_N(\sigma + i \cdot t(i_1, \ldots, i_{n-1}, q+1)| < \varepsilon/6$$

for all relevant indices. By continuity find a positive δ such that for all γ with $|\gamma| \leq \delta$ we have

$$|\zeta(\sigma + i(t + \gamma) \cdot a_{i_1} \cdot \ldots \cdot a_{i_{n-1}}) - F(i_1, i_2, \ldots, i_{n-1}, q+1)| < \varepsilon.$$

Find a_{q+1} of appropriate degree in a δ neighbourhood of t

$$|\zeta(\sigma + i \cdot a_{i_1} \cdot \ldots \cdot a_{i_{n-1}} \cdot a_{i_{q+1}}) - F(i_1, i_2, \ldots, q+1)| < \varepsilon/6.$$

We finally obtain

$$\begin{aligned} & |\zeta(\sigma + i \cdot a_{i_1} \cdot \ldots \cdot a_{i_n}) - F(i_1, \ldots, i_n)| \\ \leq\ & |\zeta_N(\sigma + i \cdot a_{i_1} \cdot \ldots \cdot a_{i_n}) - \zeta_N(\sigma + i \cdot t(i_1, \ldots, i_n))| \\ +\ & |\zeta(\sigma + i \cdot t(i_1, \ldots, i_n)) - F(i_1, \ldots, i_n)| \\ +\ & |R_N(\sigma + i \cdot a_{i_1} \cdot \ldots \cdot a_{i_n})| \\ +\ & |R_N(\sigma + i \cdot t(i_1, \ldots, i_n)| < \varepsilon. \end{aligned}$$

□

Lemma 2. *Let $\sigma > 1$ and let I_σ be a non-trivial interval (which exists, as above [2]) on the real line in which the zeta values $\zeta(\sigma + it)$ are dense. Let $\varepsilon > 0$. Assume that $F\colon [R]^n \to I_\sigma$. Then there exist rationals $r_1, \ldots, r_R$ such that numerators and denominators are bounded by a primitive recursive function of R and such that $|F(i_1, \ldots, i_n) - \zeta(\sigma + i \cdot r_{i_1} \cdot \ldots \cdot r_{i_n})| < \varepsilon$ for $1 \leq i_1 < \ldots < i_n \leq R$.*

Proof. Apply the previous lemma and pick the a_i. By Dirichlet's result on simultaneous Diophantine approximation we can find nice rationals r_i close to a_i. Then do a continuity argument. □

Theorem 3.
The following assertion is provable using the Infinite Ramsey Theorem but not provable in PA. *Fix $\sigma > 1$ and a natural number $n \geq 2$. For all natural numbers K there exists a natural number R such that for all rational numbers $r_1 < \ldots < r_R$ (which have numerators and denominators bounded primitive recursively in R), there exists a subset H of cardinality K such that for all choices $r_{i_1} < r_{i_2}, \ldots < r_{i_K} \in H$ and all $r_{i_1} < r_{j_2} < \ldots < r_{j_K} \in H$, we have $|\zeta(\sigma + i \cdot r_{i_1} \cdot r_{i_2} \cdot \ldots \cdot r_{i_K}) - \zeta(\sigma + i \cdot r_{i_1} \cdot r_{j_2} \cdot \ldots \cdot r_{j_K})| < 2^{-i_1}$.*

Proof. The proof of our statement using the Infinite Ramsey Theorem is straightforward (as in [3]) and we omit it.

The unprovability proof follows similar lines as in [3] and uses Lemma 2. For convenience we give some details. Assume our assertion holds. Given K find $2R$ as wished. Assume that $F\colon [R, 2R]^n \to 2R$ is regressive. We show that F has a min-homogeneous set of cardinality K. This is a version of KM and we are done. Put $g(x_1, \ldots, x_n) := \frac{1}{F(x_1, \ldots, x_n)}$. Choose, by Lemma 2, $r_1, \ldots, r_R$ such that for all $i_1 < \ldots < i_n$ we have $|g(i_1, \ldots, i_n) - \zeta(\sigma + i \cdot r_{i_1} \cdot \ldots \cdot r_{i_n})| < \frac{1}{R}$. By assumption of Theorem 3, extract H of cardinality K such that $|\zeta(\sigma + i \cdot r_{i_1} \cdot \ldots \cdot r_{i_n}) - \zeta(\sigma + i \cdot r_{i_1} \cdot r_{j_2} \cdot \ldots \cdot r_{j_n})| < \frac{1}{2^R}$ for members in H. Then for all relevant indices $|g(i_1, \ldots, i_n) - g(i_1, j_2 \ldots, j_n)| < \frac{3}{R}$ hence $g(i_1, \ldots, i_n) = g(i_1, j_2 \ldots, j_n)$ and $F(i_1, \ldots, i_n) = F(i_1, j_2 \ldots, j_n)$. □

In a next step we extend Theorem 3 to the case where $\sigma \in (\frac{1}{2}, 1]$. The proof will now have a slightly different flavour since $|\prod_{i=N+1}^{\infty} \frac{1}{1-p_i^{-\sigma - it}}|$ does not converge uniformly for $\sigma \in (\frac{1}{2}, 1]$ and any fixed N.

Let as before $R_N(s) := \zeta(s) \cdot \prod_{i=1}^{N}(1 - p_i^{-s})$. The following three lemmas can be found in Bohr-Courant [2]. We only need these weak predecessors of universality to prove our next theorem.

Lemma 4. *Assume that $0.5 < \sigma \leq 1$. Assume that ε, δ are strictly positive reals. Then there exists N_0 depending on $\sigma, \varepsilon, \delta$ such that for every fixed $N > N_0$ we have that for T large enough, the sum of the lengths of the intervals $I \subseteq [-T, T]$, such that for $t \in I$ we have $|R_N(\sigma + it) - 1| \geq \varepsilon$, is smaller than $\delta \cdot T$.*

Lemma 5. *Assume that $\lambda_1, \ldots, \lambda_N$ are linearly independent over the rationals. Assume that we have given an N-dimensional cube Q,with side length d, contained in the unit cube. Assume that the sides of Q are parallel to the axes. Let $M := \{t \in [0, T] : (t\lambda_1, \ldots, t\lambda_N) \in Q(\mod 1)\}$. Then M consists of a finite number of intervals. Let $M(T)$ be the sum of the lengths of these intervals. Then $\lim_{T\to\infty} \frac{M(T)}{T} = d^N$.*

Lemma 6. *Assume that $(r_i)_{i=1}^{\infty}$ is a sequence of positive reals such that $\sum_{i=1}^{\infty} r_i$ diverges and such that $\sum_{i=1}^{\infty} r_i$ converges. Let $S_N(\eta_1, \ldots, \eta_N) := \sum_{i=1}^{N} \log(1 - r_i \exp(2 \cdot \pi \cdot i \cdot \eta_i))$. Assume that I_0 is a finite collection of cubes with non zero diameter. Then the Lebesgue measure of $\{(\eta_1, \ldots, \eta_N) \in [0, 1]^N : S_N(\eta_1, \ldots, \eta_N) \in I_0\}$ is strictly positive.*

Lemma 7. *Let $0.5 < \sigma \leq 1$. Let $\varepsilon > 0$. Assume that $F\colon [R]^n \to [1, 2]$. Let $N \geq N_0$. Let $K := \mathbb{Q}(\log(p_1), \log(p_2), \ldots, \log(p_N))$. Here p_i denotes the i-th prime. Then there exist K-algebraic irrationals $a_1, \ldots, a_R$ over K such that $deg_K(a_i) = 3^{3^{n^i}}$ for $1 \leq i \leq R$ and such that*

$$|F(i_1, \ldots, i_n) - \zeta(\sigma + i \cdot a_{i_1} \cdot \ldots \cdot a_{i_n})| < \varepsilon$$

for $1 \leq i_1 < \ldots < i_n \leq R$.

Proof. The proof is again by induction on i_n and can be established by the previous lemmas. An alternative route is to apply Voronin's result here. Details will be deferred to another paper which is in preparation. □

Lemma 8. *Let $0.5 < \sigma \leq 1$, $\varepsilon > 0$. Assume that $F\colon [R]^n \to [1,2]$. Then there exist rationals $r_1, \ldots, r_R$ such that numerators and denominators are bounded by a primitive recursive function of R and such that $|F(i_1, \ldots, i_n) - \zeta(\sigma + i \cdot r_{i_1} \cdot \ldots \cdot r_{i_n})| < \varepsilon$ for $1 \leq i_1 < \ldots < i_n \leq R$.*

Proof. Apply the previous Lemma and pick the a_i. By Dirichlet's result on simultaneous Diophantine approximation we can find nice rationals r_i close to a_i. Then do a continuity argument.

□

Denote the fractional part of a real number x by $\{x\}$ (i.e. $x = [x] + \{x\}$ where $[x]$ is the least integer not exceeding x). Let $\{\zeta\}(z) := \{Re(z)\} + i \cdot \{Im(z)\}$ be a mod one version of ζ.

Theorem 9.
The following assertion is unprovable in PA. *Fix $\sigma \in (\frac{1}{2}, 1]$ and a natural number $n \geq 2$. For all natural numbers K, there exists a natural number R such that for all rational numbers $r_1 < \ldots < r_R$ which numerators and denominators bounded primitive recursively in R, there exists a subset H of cardinality K such that for all choices $r_{i_1} < r_{i_2} < \ldots < r_{i_n} \in H$ and all $r_{i_1} < r_{j_2} < \ldots < r_{j_n} \in H$ we have*

$$|\{\zeta\}(\sigma + i \cdot r_{i_1} \cdot r_{i_2} \cdot \ldots \cdot r_{i_n}) - \{\zeta\}(\sigma + i \cdot r_{i_1} \cdot r_{j_2} \cdot \ldots \cdot r_{j_n})| < 2^{-i_1}.$$

Again, the above assertion follows from the Infinite Ramsey Theorem as in [3]. To make this work it is useful to work with a bounded version of ζ. The unprovability proof is similar to the proof of Theorem 3.

We close with two conjectures which are plausible by standard results from universality theory.

Define $I\Sigma_k$ as the subsystem of PA in which all induction axioms have at most k unrestricted quantifiers. The theory $I\Sigma_1$ is commonly identified with 'elementary methods' in mathematics and $I\Sigma_2$ is believed to be the subsystem of PA where all usual concrete mathematics (elementary and non-elementary alike) can be conducted.

It is known that $\mathrm{KM}^{(2)}$, the Kanamori-McAloon principle restricted to dimension 2 is unprovable in $I\Sigma_1$ but is provable in $I\Sigma_2$. We shall use this fact to gain new unprovable statements.

Conjecture 1. *The following is not provable in $I\Sigma_1$ but provable in $I\Sigma_2$: "for all natural numbers K there exists a natural number R so large that for all natural numbers $3 \leq m_1 < \ldots < m_R$ there exists a subset H of cardinality K such that for all choices $m, k, l \in H$ such that $m < k < l$ we have $|\{\zeta^{(m)}\}(0.75 + i \cdot l) - \{\zeta^{(m)}\}(0.75 + i \cdot k)| < 2^{-m}$". Here $\{\zeta^{(m)}\}$ denotes the suitably cut off m-th derivative of ζ.*

Conjecture 2. *The following is not provable in $I\Sigma_1$ but provable in $I\Sigma_2$: "for all natural numbers K there exists a natural number R so large that for all natural numbers $3 \leq m_1 < \ldots < m_R$ there exists a subset H of cardinality K such that for all choices $2 < m < l \in H$ and all $2 < m < k \in H$ we have $|\{\zeta\}(\frac{1}{2} + \frac{1}{m} + i \cdot l) - \{\zeta\}(\frac{1}{2} + \frac{1}{m} + i \cdot k)| < 2^{-m}$".*

It is often straightforward to encode unprovable Ramseyan statements in other settings that provide some degree of randomness or universality in the broad sense of the word (all possible configurations realised infinitely-often). For example, a recent series of results by the first author uses Dirichlet's theorem on primes in arithmetic progressions and some yet unproved conjectures about constellations of primes to formulate unprovable statements

that on the surface look like statements about primes and whose true Ramseyan nature is somewhat hidden [5]. Here's the simplest example illustrating it. The second-order statement "for any infinite set $B \subseteq \mathbb{N}$, there is an infinite subset $A \subseteq B$ such that for any $k < m < n$ in A, we have $p_m \equiv p_n \mod p_k$", where p_i is the ith prime, is equivalent to the Infinite Ramsey Theorem for triples, thus implying all theorems of Peano Arithmetic. There are such unprovable statements in the language of first-order arithmetic too, and there are versions that encode Ramsey-type statements differently, using the Hardy-Littlewood k-tuple Conjecture, Buniakovskiy's Conjecture on infinitude of prime values of any irreducible polynomial and Hypothesis H. These initial observations are perhaps not very deep but they established some yet-unseen connections and thus may offer new information about primes in the future (for example PA-unprovability of some classical hypotheses about primes).

However, the most striking and mysterious future development we can already anticipate is finding number-theoretic statements φ such that there are two genuinely alternative axiomatic theories T_1 and T_2 (say, both containing a very strong theory consisting of all axioms we already committed ourselves to) such that T_1 proves φ and T_2 proves $\neg\varphi$. We saw such bifurcations in the examples of Euclid's Fifth Postulate and Continuum-Hypothesis, but there isn't yet an arithmetical first-order example. There are some technical, perhaps temporary, obstacles to achieving it at the moment but in principle nothing prevents us from eventually discovering such dream-bifurcations. (Harvey Friedman's striking recent results [13] providing first-order arithmetical statements unprovable in very strong theories (ZFC+large cardinals) is a crucial first step along this road.)

Acknowledgement. Both authors would like to thank the John Templeton Foundation for financial support.

References

[1] W. Ackermann. (1940). Zur Widerspruchsfreiheit der reinen Zahlentheorie, *Mathematische Annalen*, 117.

[2] H. Bohr and R. Courant. (1914). Neue Anwendungen der Theorie der Diophantischen Approximation auf die Riemannsche Zetafunktion. *J. Reine Angew. Math.*, 144, 249-274.

[3] A. Bovykin (2007). Unprovability of sharp versions of Friedman's sine-principle. *Proceedings of the American Mathematical Society*, 135, no. 9, pp. 2967–2973.

[4] A. Bovykin. (2009). Brief introduction to unprovability. Logic Colloquium 2006, *Lecture Notes in Logic*, pp. 38–64.

[5] A. Bovykin (2009). Unprovable Ramsey-type statements reformulated to talk about primes. To appear in Mints Festschrift.

[6] W. Buchholz, A. Cichon and A. Weiermann. (1994). A uniform approach to fundamental sequences and hierarchies. *Mathematical Logic Quarterly*, 40, 273-286.

[7] W. Buchholz and S. Wainer. (1987). Provably computable functions and the fast growing hierarchy. Logic and Combinatorics. *Contemporary Mathematics* 65, American Mathematical Society, 179-198.

[8] L. Carlucci, G. Lee and A. Weiermann. Classifying the phase transition threshold for regressive Ramsey functions (submitted).

[9] E. A. Cichon. (1983). A short proof of two recently discovered independence results using recursion theoretic methods. *Proceedings of the American Mathematical Society*, 87, 704-706.

[10] A. Ehrenfeucht. (1973). Polynomial functions with exponentiation are well ordered. *Algebra Universalis*. 3, 261-262.

[11] H. Friedman and M. Sheard. (1995). Elementary descent recursion and proof theory. *Annals of Pure and Applied Logic*, 71, 1-45.

[12] H. Friedman: a posting on the FOM forum, June 8, 2002.

[13] H. Friedman (2008). Boolean Relation Theory and the Incompleteness Phenomena. A book manuscript. To appear.

[14] G. H. Hardy. (1910). Orders of infinity: The 'Infinitärcalcül' of *Paul du Bois-Reymond*. Cambridge University Press. (Nr. 12 of the Cambridge Tracts in Mathematics and Mathematical Physics).

[15] T. Jech. (1997). Set theory. Second Edition. Springer-Verlag.

[16] J. Ketonen and R. Solovay. (1981). Rapidly growing Ramsey functions. *Annals of Mathematics*, 113 (2): 267-314.

[17] L. Kirby and J. Paris. (1982). Accessible independence results for Peano Arithmetic. *Bulletin of the London Mathematical Society*, 14, 285-293.

[18] G. Kreisel. (1952). On the interpretation of non-finitist proofs II. *Journal of Symbolic Logic*, 17, 43-58.

[19] M. Loebl and J. Nesetril. (1992). An unprovable Ramsey-type theorem. *Proceedings of the American Mathematical Society*, 116, no. 3, 819–824.

[20] R. Otter. (1948). The number of trees, *Annals of Mathematics* 49, 583–599.

[21] J. Paris and L. Harrington. (1977). A mathematical incompleteness in Peano arithmetic, *Handbook for Mathematical Logic*, North-Holland, Amsterdam.

[22] J. C. Schlage Puchta. (2009). Unpublished manuscript.

[23] S. Simpson. (1985). Non-provability of certain combinatorial properties of finite trees. In: *Harvey Friedman's research on the foundations of mathematics*, 87–117. North-Holland, Amsterdam.

[24] R. Smith. (1985). The consistency strength of some finite forms of the Higman and Kruskal theorems. In: *Harvey Friedman's research on the foundations of mathematics*, 119-136. North-Holland, Amsterdam.

[25] A. Weiermann. (2003). An application of graphical enumeration to PA. *Journal of Symbolic Logic* 68, 5-16.

[26] A. Weiermann. (2004). A classification of rapidly growing Ramsey functions. *Proceedings of the American Mathematical Society*, 132, pp. 553-561.

[27] A. Weiermann. (2006). Classifying the provably total functions of PA. *Bulletin of Symbolic Logic* 12 (2), 177-190.

Andrey Bovykin
Department of Mathematics,
University of Bristol, BS8 1TW, England.

Andreas Weiermann
Department of Pure Mathematics and Computer Algebra,
Ghent University,
Krijgslaan 281 - Gebouw S22
B9000 Ghent, Belgium.