# Some Applications of Computability in Mathematics

Rod Downey
Victoria University
Wellington, New Zealand
Dedicated to Paul Schupp for his Birthday

Hoboken, June 2017

# Overview

- Recently there has been a lot of activity taking computability theory back into its roots: Understanding the algorithmic content of mathematics.
- Examples include algorithmic randomness, differential geometry, analysis, ergodic theory, etc.
- Of course this goes way back to the work of von Mises, Dehn, Kronecker, Herrmann, etc in the years up to 1920.
- I remark that we have seen a number of new results proven using computational methods.
- Personally, I've always been fascinated by the combination of computation and classical mathematics in any form.
- I recall being inspired by reading all those wonderful books Combinatorial Group Theory (it seems that the authors had trouble thinking of original names..)
- I Think it is fair to say that Paul shares this spirit, and his work has inspired me.

# This lecture

- I will mainly concentrate on invariants.
- Mathematics is replete with "invariants."
- Think: dimension, rank, Ulm sequences, spectral sequences, etc, etc.
- What is an invariant? I recognize one when I see it.
- How to show that
- no invariants are possible? How to quantify how complex invariants must be if they have them?
- Logic is good for telling people things they cannot do.
- You make a mathematical model of what the thing is, and then show that you cannot realize this model.
- Witness the Church-Turing work. The hard part is modelling computation, the easy part (sometimes) demonstrating that objects can be constructed which emulate this model.
- This modelling is why logic is so used in computer science. (Vardi etc)

# No Invariants

- We concentrate on isomorphism.
- What is the use of an invariant, like e.g. dimension, Ulm invariants, etc.
- Arguably, they should make a classification problem easier.
- For example, one invariant for isomorphism type of a class of structures e.g. vector spaces over $\mathbb{Q}$ is the isomorphism type, but that's useless.
- We choose dimension as it completely classifies the type.
- So for countable vector spaces, we classify by $n \in \mathbb{N} \cup \{\infty\}$.
- How to show NO invariants?
- We give one answer in the context of computable mathematics, and mention some other approaches using logic.

# A First Pass

- Stuff beyond my ken.
- If we consider models of a first order theory $T$, then structures like vector spaces over $F$ of, say, cardinality $\aleph_0$ have only a countable number of models because of the invariants, things like trees have many more : $2^{\aleph_0}$.
- Shelah formalized all of this by showing that

**Theorem (Dichotomy Theorem)**

*For a complete theory $T$, either the number of models of cardinality $\kappa$ is always $2^\kappa$ for all uncountable $\kappa$, or the number is "small". (Shelah $I(T, \aleph_\xi) < \beth_{\omega_1}(|\xi|)$, Hrshovsky and others have refined this.)*

- Moreover, to prove this he describes a set of "invariants" roughly corresponding to dimension or "rank" in a kind of matroid, that control the number of models of that cardinality. ("does not fork over")

# Reductions

- All the methods below use reductions.
- $A$ reduces to $B$ ($A \leq B$) means that a method for solving $B$ gives one for solving $A$.
- Typically, there is a function $f$ such that for all instances $x$, $x \in A$ iff $f(x) \in B$. (meaning "yes" instances go to "yes" instances).
- Example from classical mathematics: map square matrices to determinants. $A$=nonsingular matrices and $B$ nonzero reals.
- Important that the function $f$ should be "simpler" than the problems in question.
- For classical computability theory, $f$ is computable. For complexity theory, $f$ might be poly-time.

# Method 2

- We leave outer space, and concentrate on "normal" things.
- We can think of problems having isomorphism types as corresponding to "numbers" corresponding to equivalence classes (i.e. isomorphism types).
- Thus a problem $A$ reduces to a problem $B$ if I can map the isomorphism types correspnding to $A$ to those of $B$. So determining if two $B$-instances are isomorphic gives the ability to do this for $A$. That is (in the simplest form) $xAy$ iff $f(x)Bf(y)$.
- This is called Borel cardinality theory.
- Why? What is a reasonable choice for functions $f$? Answer: $f$ should be Borel (at least when studying equivalence relations on Polish spaces-complete metrizable with countable dense set).
- Classical mathematics regards countable unions and intersections of basic open sets as "building blocks."

# Examples

- All on $\omega^\omega$.
- Identity $E_=$.
- Vitali operation: $E_1$ $\overline{x} =^* \overline{y}$ iff they agree for almost all positions. $E_= <_B E_1$ and $E_1$ captures the complexity of rank one torsion free groups (more later).
- $E_\infty$ the maximal. For example trees. There are also algebraic problems here such as the orbits of the 2 generator free group $\mathbb{Z}^2$ acting on $2^{\mathbb{Z}^2}$.
- This is an area of significant resent research (Hjorth, Thomas, Kechris, Pestov) and is still ongoing.

# Method 3-Refining things

- As a logician I am more interested in deeper understanding of complexity.
- The plan is to understand invariants computationally.
- Invariants should make problems *simpler*.
- Let's interpret this as computationally simpler.

# Computable mathematics

- Arguably Turing 1936: Computable analysis.
- Mal'cev 1962 A computable abelian group is computably presented if we have $G = (G, +, 0)$ has $+$ and $=$ computable functions/relations on $G = \mathbb{N}$. ("The open diagram is computable, with "=" in the signature")
- Be careful with terminology. In this language, a computable group is one with a solvable word problem.
- When can an abelian group be computably presented? (Relative to an oracle) Is there any reasonable answer?
- Do different computable presentations have different computable properties?
- Mal'cev produced examples presentations of $\mathbb{Q}^\infty$ that were not computably isomorphic, as we see later.
- Along with Rabin and Frölich and Shepherdson, began the theory of presentations of computable structures, though arguably back to Emmy Noether, Kronecker as recycled in van der Waerden (1ed).
- See Matakides and Nerode "Effective Content of Field Theory".

# Why should we care?

- If we are interested in actual processes on algebraic structures then surely we need to understand the extent to which they are algorithmic.
- Effective algorithmics requires more detailed understanding of the model theory. Witness the resurrection of the study of invariants despite Hilbert's celebrated "destruction" of the programme.
- The Hilbert basis (or nulstellensatz) theorem(s) are fine, but suppose we need to calculate the relevant basis.
- Examples of this include the whole edifice of combinatorial group theory. The theory of Gröbner bases etc. New constructions in combinatorics, algebra, etc.
- As we will see a backdoor into establishing classical results about the existence/nonexistence of invariants in mathematics. Computability is used to establish classical result.
- Establishing calibrations of complexity of algebraic constructions.... reverse mathematics.

# $\Sigma_1^0$-completeness?

- The halting problem is $\Sigma_1^0$. This means it can be described by an existential quantifier on numbers around a computable predicate. "There is a stage $s$ where the $e$-th machine with input $y$ halts in at most $s$ steps-Halt$(e, y)$ iff $\exists s \in \mathbb{N}(\varphi_e(y) \downarrow [s])$"
- Showing that a problem $A$ is $\Sigma_1^0$ complete means that there is a computable $f$ such that for each instance $I$ of a $\Sigma_1^0$ problem $B$, I can compute $f(I)$ which is an instance of $A$ such that $I$ is a yes for $B$ iff $f(I)$ is a yes for $A$. $A$ is the "most complex" $\Sigma_1^0$ problem.
- For example, the word problem for finitely presented groups, can be $\Sigma_1^0$ complete for a finitely presented group.
- To wit: with relations $r_1, \ldots r_n$, $x \equiv w$ iff there exists a sequence of applications of the relations taking $x$ to $y$.

- Down thru the years many examples of problems of the same complexity as the halting problem.
- Hilbert's 10th Problem (Matiyasevich)
- Word problems in groups (Novikov-Boone)
- Homeomorphism problems in 3 space (Reubel)
- more recently DNA self assembly (Adelman, Lutz)
- boundaries of Julia Sets (Braverman, Yampolsky)
- Some general meta-theorems, e.g. Rice's Theorem, Markov Properties.
- Recently spectra in quantum mechanics. (Cubitt, Perez-Garcia and Wolf)

# Sometimes more complexity needed

- Sometimes what is needed is more intricate understanding of (c.e.) computably enumerable ($\Sigma_1^0$) sets for an application.
- The c.e. sets and their "degrees of unsolvability" each form extremely complex structures.
- At Chicago, Soare provided the computability needed for "settling times" of families of c.e. sets, for work on Riemannian metrics on a smooth manifold under reparameterization.
- See Nauktovsky and Weinberger-Geometrica Dedicata.
- Sometimes stronger reducibilties are needed, or "limitwise monotonic" functions.

# But does it matter?

- Various approaches to quantify the fact that undecidability/intractability is rare in practice.
- For example most group theoretical questions for finitely presented groups are generically decidable. (Karpovich, Myasnikov, Schupp and Shpilrain)
- Here one asks for an algorithm which is always right, but only halts on a set of Borel density 1.
- Similar questions arise about NP completeness. Why do SAT SOLVERS work so well?
- What is the topology of hard instances of real life problems... e.g. Parameterized complexity

# The duty of theory

- It is not widely known that "modulo some reasonable complexity assumptions" many algorithms are in some sense optimal.
- Because practioners don't completely care. Not only does this make it hard to get a job in a CS department, but it points at our serious lack of theory explaining practice.
- I like the fact that PC now has implementation contests.
- Of course one trouble is that you need to beat the big teams, Google, etc. Witness Jeopardy for example.
- There is still a major project here.
- Anyway, back to mathematics.

# Problems higher up

- If a problem can be expressed as a finite number of alternations of number quantifiers, it is called arithmetical, "$\Delta_n^0$" for some $n$, and $\Sigma_n^0$ if the first quantifier is a $\exists$, with $n$ alternations, and $\Pi_n^0$ if it begins with a $\forall$.
- For example: is $\varphi_x$ total? provably needs an alternation of quantifiers. To wit: $\mathrm{Tot}(x)$ iff $\forall s \exists t (\wedge_{y \leq s} \varphi_x(y) \downarrow [t])$. It is in $\Pi_2^0$ and $\Pi_2^0$-complete.
- I have a question:

**Question**

*For each $n$, is there a finitely presented group $G$, which is $\Delta_n^0$-decidable, but not $\Delta_{n+1}^0$? Is there one which is $\Delta_n^0$ decidable for each $n$, but not decidable?*

- These sets occur naturally in problems:

# Computable abelian groups

- (Maltsev) Describe computably presentable Abelian groups.

**Theorem (Khisamiev 1970's, Ash-Knight-Oates 1980's)**

*A certain characterization of computable reduced abelian p-groups of finite Ulm type in terms of limitwise monotonic approximations of functions.*

- (Khisamiev) A set $S$ is limitwise monotonic iff $S = \mathrm{ra}(f)$ for some computable $f = f(\cdot, \cdot)$, where for $\lim_s f(n, s)$ exists for all $n$, and $f(n, s+1) \geq f(n, s)$ for all $s$.
- Sometimes the function $f$ has only elements of $\omega$ in its range and sometimes for convenience we have $\infty$ there.
- Fact: the finite members of the range of one of these functions is a $\Sigma^0_2$ set.

# Equivalence relations/structures

- Will be of relevance and interest later.
- $E$ is a structure with cells $c_i$ for $i \in \omega$. As above, note that they only get bigger.

**Theorem (Calvert, Cenzer, Harizanov, and Morozov 2006)**

*An equivalence structure $\mathcal{E}$ with infinitely many classes is computable if and only if there is a limitwise monotonic function $F$ (with range $\omega \cup \{\infty\}$) for which there are exactly $|\{x : F(x) = \kappa\}|$ many classes of size $\kappa$ (for each $\kappa \in \omega \cup \{\infty\}$) in $\mathcal{E}$.*

- Limitwise monotonic approximations found applications:
- in computable linear orders (Downey-Khoussainov, Harris, Kach-Turetsky),
- in computable models of $\aleph_1$-categorical theories (Khoussainov, Nies, Shore),
- in computable equivalence structures (Harizanova et al.),
- in a characterization of high c.e. degrees (Downey, Kach, Turetsky).
- Khisamiev's classification of Ulms sequences for computable abelian groups.

# $\Sigma_1^1$ Completeness

- Some problems are too complex to be arithmetical. Classical isomorphism of infinite structures: "There is a function such that ...."
- If we allow function quantifiers, we put a "1" on top.
- Thus we enter the realm of second order logic.
- Note now we are searching through the uncountably many possible functions $f : \mathbb{N} \to \mathbb{N}$.

$$\exists f \in \mathbb{N}^{\mathbb{N}}(\forall x, y(f(x+y) = f(x) + f(y))).$$

- Analogously, a problem is $\Sigma_1^1$ complete if every other $\Sigma_1^1$ problem reduces to it.

# Consequences of $\Sigma^1_1$-completeness

- The idea of an invariant is that is ought to make the problem simpler.
- Classical isomorphism is always $\Sigma^1_1$.
- Invariants make this easier, you would expect. Dimension in a vector space makes the problem $\Delta^0_3$.
- The point is that a $\Sigma^1_1$-completeness result result means that the cannot be reasonable invariants for the isomorphism problem.

# Torsion-free abelian groups

- In general the isomorphism problem is very complex:

**Theorem (Downey and Montalbán-J. Algebra)**

*The isomorphism problem for torsion-free abelian groups is $\Sigma^1_1$ complete.*

- That is a computational "proof" that there cannot be invariants.
- As explained in the DM paper, group theorists try to understand finitely presented groups via spectral sequences, one called the integral homology sequence (Stallings etc)

- Digression: (The true computational depth of finitely presented groups.) This consequence involves the *integral homology sequence of finitely presented groups,*

$$H_1 G, H_2 G, \ldots,$$

  where $H_n G$ denotes the $n$-th homology group of $G$ with trivial integer coefficients. (Certain subquotients of the integral group ring $\mathbb{Z}F$ of the free group $F$ on $X$, where $G$ is presented by $\langle X, R \rangle$.
- Stallings constructed a finitely presented group where $H_3$ was a free abelian group of infinite rank.
- Amongst other things, Baumslag, Dyer, and Miller showed that $H_3 G$ can be any torsion-free abelian group. Thus determining $H_3 G$ is as bad as the classification of any countable isomorphism problem!

- The computational mentality
- This methodology understands invariant theory computationally.
- Also used by Slaman and Woodin, Friedman, Stanley, Knight and others in many other settings.
- There are other programmes like this as we now will see.

# Better algebraic classes

- Okay, so the general classification problem is intractable, then can we measure how complex the classically "understood" classes are.
- Recall that if $G$ is a torsion-free then $G$ embeds into $\oplus_{i\in F}(\mathbb{Q},+)$. The cardinality of the least such $F$ is called the (Prüfer) rank of $G$. Some Good news:
- Khisamiev proved that there is an effective embedding. (That is if $G$ is a computable torsion-free abelian group then $G$ can be computably embedded into a computable copy of $\oplus_{i\in F}(\mathbb{Q},+)$.
- He also proved that if a torsion-free abelain group has a $\Pi^0_{n+1}$ presentation, it has a $\Sigma^0_n$ one.

# Rank One Groups

- The only groups we understand well are the rank one groups (and certain mild generalizations) If $g \in G$, define $t(g) = (a_1, a_2, \dots)$ where $a_i \in \{\infty\} \cup \omega$ and represents the maximum number of times $p_i$ divides $g$. Say that $t(g) = t(h)$ if they are $=^*$, meaning that they must be $\infty$ in the same places, but otherwise are finitely often different. Thus we can write $t(G)$.
- For example, a divisible group would have $(\infty, \infty, \dots)$ as its type.

**Theorem (Baer, Levi)**

*For rank 1 torsion-free abelian groups, $G \cong H$ iff they have the same type.*

- One corollary is that if we consider $T(G) = \{\langle x, y\rangle \mid x \leq t(G)_y\}$, then $G$ is computably presentable iff $T(G)$ is $\Sigma^0_1$. (Mal'tsev)

# Two Corollaries

- A structure is called computably categorical iff any two computable copies are computably isomorphic. e.g. dense linear orderings without end points.
- A Torsion-free abelian group is computably categorical iff it has finite rank.
- If a structure is not computably categorical, we might ask what computational power is needed to classify it up to isomorphism. $\Delta^0_n$-categorical, or assign some kind of least degree.

- Degrees of structures:

**Definition**

A structure $\mathcal{A}$ has a degree iff $\min\{\deg(\mathcal{B}) \mid \mathcal{B} \cong \mathcal{A}\}$ exists.

- Strictly speaking, we would mean the isomorphism type here. For example, finitely generated groups always have degrees.
- (Jockusch) Can define jump degree by replacing $\deg(\mathcal{B})$ by $\deg(\mathcal{B})'$. The same for $\alpha$-th jump degree. Proper if no $\beta$-th jump degree for $\beta < \alpha$. The "jump" of a set is the halting problem with the set as an oracle.
- (Coles, Downey and Slaman-Bull LMS) Every torsion free abelian group of finite rank has first jump degree.
- (Anderson, Kach, Melnikov, Solomon-APAL) For each computable $\alpha$ and $\mathbf{a} > \mathbf{0}^\alpha$ there is a torsion-free abelian group with proper $\alpha$-th jump degree $\mathbf{a}$.

# General stuff about structures

Computably categorical structures might seem simple, and in "normal circumstances" they are

**Theorem (Goncharov, 1975)**

*If $\mathcal{A}$ is $2-$decidable, then $\mathcal{A}$ is computable cat iff it is relatively computably cat iff it has an effective naming, that is a c.e. Scott family of existential formulae with parameters $\overline{c}$, such that for all $\overline{a}, \overline{b}$ if they satisfy the same $\phi$, then they are automorphic.*

But:

**Theorem (D, Kach, Lempp, Lewis-Pye, Montalban and Turetsky-Advances in Math)**

*The index set of computably categorical structures is $\Sigma^1_1$ complete.*

The following theorem is concerned with important classes of models. I won't give the definitions here.

**Theorem (Hirschfeldt and White)**

*The index sets of classes of computable homogeneous structures, computable atomic structures, and computable computably saturated structures are all $\Pi^0_{\omega+2}$-complete.*

I remark that pretty well all of the results above apply to familiar classes like division rings, groups, lattices, partial orderings, etc due to work of oHirschfeldt, Khoussainov, Shore, and Slinko.
Now back to abelian groups:

# The infinite rank case

- It could be hoped that if $G$ has infinite rank, then $G \cong \oplus_{i \in \omega} H_i$ with $H_i$ of rank one.
- Alas, this is not true, however, there is a class of groups for which this is true, called completely decomposable for which this does happen.
- What about categoricity for such groups?
- We cannot hope for computable categoricity, but can hope for things "higher up".

# The homogeneous case

- If $G \cong \oplus H$ for a fixed $H$ then $G$ is called homogeneous

**Theorem (Downey and Melnikov-J. Algebra)**

*Homogeneous computable torsion free abelian groups are $\Delta^0_3$ categorical.*

- The proof relies on a new notion of independence called $S$-independence generalizing a notion of Fuchs to sets $S$ of primes.
- $B$, a set of elements, is $S$-independent (in $G$) iff for all $p \in S$ and $b_1, \ldots, b_k \in G$,

$$p | \sum_{i=1}^{k} m_i b_i \text{ implies } p | m_i \text{ for all } i.$$

- This bound is tight.

# But when can it be $\Delta^0_2$ categorical?

- Recall that a set $S$ is called semilow if $\{e \mid W_e \cap S \neq \emptyset\} \leq \emptyset'$.
- Semilow sets allow for a certain kind of local guessing, and arose in (i) automorphisms of the lattice of computably enumerable sets (Soare) and in (ii) computational complexity as non-speedable ones. (Soare, Blum-Marques, etc.)

**Theorem (Downey and Melnikov-J. Algebra)**

*$G$ is $\Delta^0_2$ categorical iff the type of $H$ consists of only 0's and $\infty$'s and the position of the 0's is semilow.*

- The proof is tricky and splits into 5 cases depending on "settling times".
- We remark that this is one of the very few known examples of when $\Delta^0_2$ categoricity of structures has been classified.

# The general completely decomposable case

**Theorem (Downey and Melnikov-TAMS)**

*A completely decomposable $G$ is $\Delta^0_5$ categorical. The bound is tight.*

The proof uses methods from the homogeneous case, plus some new ideas. The sharpness is a coding argument. For sharpness we use copies of $\oplus_{i\in\omega}\mathbb{Z} \oplus \oplus_{i\in\omega}\mathbb{Q}^{(p)} \oplus \oplus_{i\in\omega}\mathbb{Q}^{(q)}$., where $p \neq q$ primes and $\mathbb{Q}^{(r)}$ denotes the additive group of the localization of $\mathbb{Z}$ by $r$. Then a relation $\theta$ on this group which is decidable in one copy and very bad in another.
With some extra work we can also prove the following. We don't know if the bound is sharp here.

**Corollary (Downey and Melnikov-TAMS)**

*The index set of completely decomposable groups is $\Sigma^0_7$.*

# Algorithmic Randomness

- Can we give meaning to the notion of an individual random sequence?
- The idea is to use computability theory to define a real $\alpha$ to be random if no computable betting strategy (computable martingale) can succeed in making infinite capital.
- Can use simple martingales effective functions $f : 2^\omega \to \mathbb{R}^+ \cup \{0\}$,

$$f(\sigma) = \frac{f(\sigma 0) + f(\sigma 1)}{2}.$$

- Large amount of theory, and we know this correlates to e.g. initial segments being incompressible (Levin), or the real having no computably rare properties (Matin-Löf).
- The analog of the halting set is Chaitin's halting probability $\Omega$, the Lebesgue measure of the collection of strings (names or programmes) which halt.

$$\Omega = \sum_{U(\sigma)\downarrow} 2^{-|\sigma|}.$$

# A couple of recent theoretical advances

- A classical theorem is that every real can be computed from a Martin-Löf random one. Seems strange.
- Randoms split into two classes, "false randoms like $\Omega$ which can compute the halting problem", and those that are "really random and provable stupid in a technical sense."
- Using computable martingales $s$-gales (betting with tax) with a weighting $s$ to give a meaning to the effective Hausdorff dimension of an individual real. (Lutz, Schnorr)

# Effective dimension

- We can also ascribe meaning to Hausdorff (and other) dimensions to individual strings and reals using $K$. e.g $\liminf_{n\to\infty} \frac{K(X\upharpoonright n)}{n}$.
- E.g. putting 0 after every bit of $\Omega$ has dimension $\frac{1}{2}$.
- It was thought that the only way to make a real of broken dimension was to mess up a random.

**Theorem (Miller)**

*There is a Turing degree* $\mathbf{a}$ *of proper dimension* $\frac{1}{2}$*, i.e. computing no random.*

- Can have a degree of dimension 1 with no random. (Greenberg, Miller)
- A fabulous recent advance is due to Greenberg, Kuyper and Miller that if $X$ has effective Hausdorff dimension 1, then $X$ differs from a random by a density 0 set.
- It turns out there are correspondence principles.

# Application

- (Symbolic Dynamics) A $d$-dimensional *shift* of finite type is a collection of colourings of $\mathbb{Z}^d$ defined by local rules and a shift action (basically saying certain colourings are illegal). Its (Shannon) entropy is the asymptotic growth in the number of legal colourings.
- More formally, consider $G = (\mathbb{N}^d, +)$ or $(\mathbb{Z}^d, +)$, and $A$ a finite set of symbols. We give $A$ the discrete topology and $A^G$ the product topology. The shift action of $G$ on $A^G$ is

$$(S^g x)(h) = x(h + g), \text{ for } g, h \in G \wedge x \in A^G.$$

A *subshift* is $X \subseteq A^G$ such that $x \in X$ implies $S^g x \in X$ (invariant).

**Theorem (Simpson-J Ergodic Theory)**

*If $X$ is a subshift (closed and shift invariant), then the effective Hausdorff dimension of $X$ is equal to the classical Hausdorff dimension of $X$ is equal to the entropy, moreover there are calculable relationships between the effective and classical quantities. (See Simpson's home page for his recent talks and more precise details.)*

- Simpson used this to give new elementary proofs and then extensions to difficult results of Furstenberg.
- Day has similar recent work on "amenable" groups.
- Johanna Franklin will tell us about other work on ergodic theory later today.

# Some other applications

- Braverman and Yampolsky showed that the halting probabilities correspond exactly to Julia sets from effective initial conditions. (JAMS)
- In symbolic dynamics again:

**Theorem (Hochman and Meyerovitch, Ann Math)**

*The values of entropies of subshifts of finite type over $\mathbb{Z}^d$ for $d \geq 2$ are exactly the complements of halting probabilities.*

- Recently Day used a similar method to give a very short proof of the Kolmogorov-Sinai theorem relating Shannon entropy to equivalence of Bernoulli systems from Ergodic theory.
- Niel and Jack Lutz also proved new classical results about classical Hausdorff dimension using effective methods.

# High up Low down

Allender and others began a program under the idea that random oracles can't be usefuli under eficient reductions..

**Theorem (Buhrman, Fortnow, Koucký and Loff; Allender, Buhrman, Koucký, van Melkebeek and Ronneburger 2006; Allender, Buhrman and Koucký 2006)**

*Let $R$ be the set of all random strings for either plain or prefix-free complexity.*

- $\mathrm{BPP} \subseteq \mathrm{P}^R_{tt}$.
- $\mathrm{PSPACE} \subseteq \mathrm{P}^R$.
- $\mathrm{NEXP} \subseteq \mathrm{NP}^R$.

## Theorem (Allender, Friedman and Gasarch)

- $\Delta_1^0 \cap \bigcap_U \mathrm{P}_{tt}^{R_{K_U}} \subseteq \mathrm{PSPACE}$.
- $\Delta_1^0 \cap \bigcap_U \mathrm{NP}^{R_{K_U}} \subseteq \mathrm{EXPSPACE}$. *Here $U$ ranges over universal prefix-free machines, $K_U$ is prefix-free complexity as determined by $U$, and $R_{K_U}$ is the corresponding set of random strings.*

## Theorem (Cai,D,Epstein,Lempp,Miller)

*For any universal $U$ there is a noncomputable set $X \not\leq_{tt} R_K^U$. Hence if $X \leq_{tt}$ all $R_K^V$'s it is computable.*

# Computable Analysis

- Roots go back to Turing's original paper!

**Definition (Kleene, essentially)**

$f$ is computable it there is a uniform algorithm taking fast converging Cauchy sequences (i.e. $q_k \in B(q_n, 2^{-n})$ for all $k > n$) to fast converging Cauchy sequences.

(This is in. e.g. a separable metric space with a countable computable base, like the reals and the base $\mathbb{Q}$.)

- In fact "$f$ continuous" $=$ "$f$ computable relative to an oracle".

**Theorem (Pour-E and Richards)**

*In this setting an operator is computable iff it is bounded.*

- Thus there is a computable ODE with computable initial conditions but no computable solution. (Myhill)

- Some things are perhaps surprisingly computable. For example, the graph $G$ of a computable function on a closed interval is computable as a set, in the sense that the distance function $d(x, G)$ is computable from it.
- It is also possible to look at effective $L^p$-computability, Fine computability, ....
- New initiatives in computable structures in Polish spaces, e.g. Pontryagin duality. (Melnikov, etc)

# Derivatives

- If you look at e.g. the Dini derivative the correct way, then it looks like a Martingale. This observation was by Demuth.

**Theorem (Demuth-Brattka, Miller, Nies-TAMS)**

*A computable $f$ of bounded variation is differentiable at each Martin-Löf random set, and this is tight.*

- That is "differentiable=random"!!
- Westrick has shown that the differentiation/continuity hierarchy aligns exactly with the arithmetic/analytic hierarchy.
- Lots of new work on computational aspect of Ergodic Theorems, Brownian motion and the like. But no time.
- Think about the "almost everywhere" behaviour you have seen...

Thank You
Congratulations Paul