Generic Decision Complexity

Rod Downey
Victoria University
Wellington
New Zealand

References

- Asymptotic Density for c.e. Sets (with Jockusch and Schupp) in preparation.
- Generic Computability, Turing Degrees and Asymptotic Density (Jockusch and Schupp), to appear.
- Generic case complexity, decision problems in group theory and random walks, (Kapovich, Miasnikov, Schupp and Shpilrain) J. Algebra, (2003)
- Genericity, the Arshantseva-Ol'shanskii technique and the isomorphism problem for one relator groups, (Kapovich and Schupp) Math Ann (2005)

Background

- Classical complexity, P, NP etc seems often the wrong model for actual behaviour of problems.
- E.g Simplex Algo, Polynomial Identity Testing etc.
- Other models: Parameterized complexity (Downey-Fellows), average case complexity (Gurevich-Levin), smoothed analysis (Spielman-modern version of average case)
- The first does not always explain things it seems, and the last two are hard to apply (distributions etc)
- New method suggested by Kapovich, Miasnikov, Schupp and Shpilrain in 2003.

Asymptotic density

- A finite alphabet Σ
- Let S be a subset of Σ^*. For every $n \geq 0$ let $S\lceil n$ denote the set of all words in S of length at most n.
- Let

$$\rho_n(S) = \frac{|S\lceil n|}{|\Sigma^*\lceil n|}$$

- Upper density (Borel)

$$\overline{\rho}(S) := \limsup_{n\to\infty} \rho_n(S)$$

- Similarly, Lower density
- (asymptotic) density If the actual limit

$$\rho(S) = lim_{n\to\infty}\rho_n(S) \text{ exists}$$

Generic Case Complexity

- A subset S of Σ^* is generic if $\rho(S) = 1$ and S is negligible if $\rho(S) = 0$
- exponentially fast Exist $0 \leq \sigma < 1$ and $C > 0$ such that for every $n \geq 1$ we have $1 - \rho_n(S) \leq C\sigma^n$. In this case we say that S is strongly generic.
- A (partial) $\Phi \mid \Sigma^* \to \{0, 1\}$ is a generic description of S if $\Phi(x) \downarrow \to \Phi(x) = S(x)$ and the domain of Φ is generic.
- A set S is called generically computable if there exists a *partial computable* function Φ which is a generic description of S.

An Example

- $G = \langle a, b; R \rangle$ be any 2-generator group.
- Note Any countable group is embeddable in a 2-generator group so there are uncountably many such G.
- Let $F = \langle x, y \mid \rangle$ be the free group of rank 2.
- $H = G * \langle x, y \rangle := \langle a, b, x, y; R \rangle$ be the free product of G and F.
- Then the word problem for H is strongly generically solvable in linear time.

A generic case algorithm

- Take a long word w on the alphabet $\{a, b, x, y\}^{\pm 1}$, e.g. $abx^{-1}bxyaxbby$.
- Erase the a, b symbols, freely reduce the remaining word on $\{x, y\}^{\pm 1}$, and if any letters remain, output “no”.
- This partial algorithm gives no incorrect answers because if the image of w under the projection homomorphism to the free group F is not 1, then $w \neq 1$ in H.

$$abx^{-1}bxyaxbby \to x^{-1}xyxy \to yxy \neq 1$$

- The successive letters on $\{x, y\}^{\pm 1}$ in a long random word $w \in H$ is a long random word in F which is not equal to the identity. So the algorithm answers “No” on a strongly generic set and gives no answer if the image in F is equal to the identity.

Other examples

- The above is called the quotient method and can be used for any $G = \langle X, R \rangle$ subgroup of K of finite index for which there is an epimorphism $K \to H$ hyperbolic and not virtually cyclic, to show generically solvable word problem.
- Applies also to 1-relator groups with ≥ 3 generators similarly (no bound for Magnus' solution), plus isomorphism problem; and braid groups, and automorphism problems for free groups etc.
- Boone's group also, unknown if there is a one without a generically solvable word problem. (See also Gilman, Miasnikov and Osin for the strong case)
- See the papers by Schupp, Kapovich etc.

Easy Observations

- Every degree contains a generically computable set. $S \subseteq \{0,1\}^*$ be the set $\{0^n : n \in A\}$.
- (Jockusch-Schupp; Miasnikov-Rybalov) Every nonzero Turing degree contains a set which is not generically computable. Let A be any noncomputable subset of ω and let $T = \{0^n 1 w : n \in A, w \in \{0,1\}^*\}$.
- Clearly A and T are Turing equivalent.
- For a fixed n_0, $\rho(\{0^{n_0} 1 w : w \in \{0,1\}^*\}) = 2^{-(n_0+1)} > 0$. A generic algorithm for a set must give an answer on some members of any set of positive density.

Generic computability of subsets of ω

- density is now Borel density.

Definition (Jockusch-Schupp)

Let $\mathcal{C}$ be a family of subsets of ω. A set $A \subseteq \omega$ is densely $\mathcal{C}$-approximable if there exist sets

$$C_0, C_1 \in \mathcal{C} \text{ such that } C_0 \subseteq \overline{A},\ C_1 \subseteq A \text{ and } C_0 \cup C_1 \text{ has density } 1.$$

Theorem (Jockusch-Schupp)

A set A is generically computable if and only if A is densely approximable by c.e. sets. Hence every c.e. set of density 1 is generically computable.

A Key player

- Jockusch-Schupp defined the following set:

$$R_k = \{m : \; 2^k | m, \; 2^{(k+1)} \nmid m\}$$

- The collection of sets $\{R_k\}$ forms a partition of unity for $\omega - \{0\}$ since these sets are pairwise disjoint and $\bigcup_{k=0}^{\infty} R_k = \omega - \{0\}$.
- As JS observed they have the following nice additivity: If $\{S_i\}, i = 0, 1, \ldots$ is a countable collection of pairwise disjoint subsets of ω such that each $\rho(S_i)$ exists and $\overline{\rho}(\bigcup_{i=N}^{\infty} S_i) \to 0$ as $N \to \infty$, then

$$\rho(\bigcup_{i=0}^{\infty} S_i) = \sum_{i=0}^{\infty} \rho(S_i).$$

Definition

If $A \subseteq \omega$ then $\mathcal{R}(A) = \bigcup_{n \in A} R_n$

- $\rho(\mathcal{R}(A)) = \sum_{n \in A} 2^{-(n+1)}$

A simple application

- (JS) If $r = .b_0 b_1 b_2 ... b_i ...$ is the binary expansion of r, let $A = \{i : b_i = 1\}$ and then $\rho(\mathcal{R}(A)) = r_A$.
- The density r_A of $\mathcal{R}(A)$, i.e. $\sum_{n \in A} \rho(R_n)$, is a computable real if and only if A is computable. Hence every real in $[0,1]$ is a density.

Theorem (Jockusch-Schupp)

A real number $r \in [0,1]$ is the density of some computable set if and only if r is a Δ^0_2 real.

- If A is computable

$$q_n = \rho_n(A) = \frac{|\{k : k \leq n,\ k \in A\}|}{n+1}$$

for all n. Thus, if $\rho(A) = lim_{n\to\infty}\rho_n(A)$ exists, its value r is a Δ^0_2 real.

- Let $r = lim_n q_n \in (0,1)$ a limit of a computable sequence of rationals
- there is a computable set A with $\rho(A) = r$.

- (Interpolating sequences) A computable increasing sequence $\{s_n\}$ of positive integers such that

$$\left|\frac{|A\lceil s_n|}{s_n+1} - q_n\right| \leq \frac{1}{n} \text{ and } lim_{n\to\infty}\frac{|A\lceil s_n|}{s_n+1} = r.$$

  Take $s_1 = 1$ and put 0 in A. If $A\lceil s_n$ is already defined there are two cases.
  If $\frac{|A\lceil s_n|}{s_n+1} < q_{n+1}$ find the least k such that

$$\frac{|A\lceil s_n| + k}{s_n+k+1} \geq q_{n+1}.$$

  (Such a k exists because $q_{n+1} < 1$.) Let $s_{n+1} = s_n + k$ and let $A\lceil s_{n+1} = A\lceil s_n \cup \{s_n+1, \ldots, s_n+k\}$.
  If $\frac{|A\lceil s_n|}{s_n+1} \geq q_{n+1}$ find the least k such that

$$\frac{|A\lceil s_n|}{s_n+k+1} < q_{n+1}.$$

  Let $s_{n+1} = s_n + k$ and let $A\lceil s_{n+1} = A\lceil s_n$.

A starting point

Theorem (Jockusch-Schupp)

There exists a c.e. set A of density 1 which has no computable subset of density 1. Hence, generically computable sets need not be densely approximable by computable sets. Hence, there exists a generically computable set A of density 1 such that no generic algorithm for A has computable domain.

- $$P_n : R_n \subseteq^* A$$
- N_e: If $W_e \cup A = \omega$ then W_e does not have upper density 0 on R_e.

The N_e strategy

- Work in cycles. Pick a big interval in R_e, say $I_{e,1}$.
- Keep this out of A but put the rest of R_e into A (i.e. below s) until W_e eats $I_{e,1}$.
- Then put $I_{e,1}$ into A and repeat with another big interval $I_{e,2}$.
- Finite outcome W_e is bad, infinite outcome $I_{e,i} \cap W_e = \emptyset$ for all i and hence W_e does not have density 1.

A characterization of lowness

Theorem (Downey-Jockusch-Schupp)

A c.e. degree $\mathbf{a}$ *contains a c.e. set* A *of density* 1 *which has no computable subset of density* 1
iff
$\mathbf{a}$ *is nonlow..*

One direction

- We are given nonlow A and build $B \leq_T A$.

$$Q_e : \overline{W_e} \text{ density } 1 \rightarrow \overline{W_e} \not\subseteq B.$$

- For the sake of Q_e, we will set aside infinitely many rows, $R_{e,i}$ where $i \in \omega$.
- The idea is that row $R_{e,i}$ will be devoted to argument i of the jump, $\Phi_i(i)$ with use $\varphi_i(\cdot, \cdot)$.
- For each e we will build a (potential) limit lemma reduction $\Gamma_e(i, s)$ trying to compute A' predicated on the *failure* of Q_e being met.
- All of the strategies work completely independently, though all the $R_{e,i}$ use the same Γ_e.

- $\Gamma_e(i, 0) = 0$
- $\Phi^A(i) \downarrow [s_0]$. (If not then fine)
- Then we will pick a *big* interval I in $R_{e,i}$ (so that, in particular, $\varphi_i(i, s) < \min I$. We restrain this interval from B, at present. We wait for one of two things to happen.
  - (I) W_e eats the interval, at stage t.
  - (II) $\Phi^A(i) \uparrow [t]$ using the hat convention here.
- If (ii) occurs, we will release all restraint on B and enumerate all of I immediately into B. (A-permitted)
- If (i) occurs, we will enumerate $\Gamma_e(i, t) = 1$, and declare i as *active*. If (i) occurs, we will then do nothing more unless a stage $v > t$ occurs where $\Phi^A(i) \uparrow [v]$, (the hat convention applies) in which case we immediately enumerate I into B, declare i as no longer active, make $\Gamma_e(i, v) = 0$ and repeat.

How tight?

Theorem (Downey-Jockusch-Schupp)

If A is c.e. and has density q and $q' < q$, A has a computable subset of density q'.

- Use a method of “big interval bootstrapping”
- Divide the universe into $I_0, I_1, \ldots$.
- Work from the point where the density is above q', say I_0.
- Ask that A achieves high density on all of I_{i+2} before enumerating C on I_i.
- Choose the sizes I_j so that the combinatorics works.

The other direction of the lowness result

- Suppose that we had a computable function f telling us that above $f(n)$ A had density $1 - 2^{-n}$, on the I_n above chosen like Ackermann's function. Then we could wait for the elements to enter A and then put them into a computable set $C \subseteq A$.
- The statement that for all $m > \min I_n$ the density of $A \upharpoonright m > 1 - 2^{-n}$ is A'-computable and hence approximable if A is low.
- Now run the construction using a $\emptyset'$ approximation to f^A as above.

What are the densities of c.e. sets?

Theorem (Downey-Jockusch-Schupp)

Let $g(n,s)$ be a computable function with rational values such that:

(i) *For all $n, s, 0 \leq g(n,s) \leq g(n,s+1) \leq 1$,*

(ii) *For all $n, \exists^{<\infty} s[g(n,s) \neq g(n,s+1)]$*

Let $h(n) = \lim_s g(n,s)$ Then there is a c.e. set A such that the lower density of A is $\lim inf_n h(n)$ and the upper density is $\lim sup_n h(n)$.

- Note that changing $g(n,s)$ by at most $1/n$ can assume that $g(n,s)$ has the form k/n, where k is an integer.
- Partition the interval $[n!,(n+1)!)$ into consecutive subintervals of size n . Let A consist of the first $nh(n)$ elements of each such subinterval, over all n .
- A is c.e. because, by (i), $h(n) = \max_s g(n,s)$.
- Clearly the density of A on each interval $[n!,(n+1)!)$ is exactly $h(n)$, since this is the density of A on each subinterval.
- Hence the density of A on $[0,(n+1)!)$ is close to $h(n)$, since $n!$ is negligible in comparison with $(n+1)!$, for large n.
- For i in the interval $(n!,(n+1)!)$ the density of A on $[0,i)$ is approximately between $h(n-1)$ and $h(n)$ (if $n > 0$), with error which approaches 0.

A Corollary

Corollary (Downey-Jockusch-Schupp)

TFAE for r a real in $[0,1]$

(i) *r is the upper density of a c.e. set*

(ii) *r is the density of a c.e. set*

(iii) *r is the upper density of a computable set*

(iv) *r is left Π_2.*

Corollary (Downey-Jockusch-Schupp)

There is a Δ^0_3 real that is not the density of a c.e. set.

Corollary (Downey-Jockusch-Schupp)

There is a real which is the density of a c.e. set but not of any computable set.

Other directions

- (JS) A of natural numbers *coarsely computable* if there is a computable set B such that the symmetric difference of A and B has density 0.
- Thus there exists a *total* algorithm Φ which may make mistakes on membership in A but the mistakes occur only on a negligible set.

Theorem (Jockusch-Schupp)

The word problem of any finitely generated group $G = \langle X : R \rangle$ is coarsely computable.

- If G is an infinite group, the set of words on $(X \cup X^{-1})^*$ which are not equal to the identity in G has density 1 and hence is coarsely computable.
- Generic computability and coarse computability are independent for c.e. sets (JS)

Coarse vs generic

- JS coarse but not generic: take e.g. a simple set and say no for all inputs.
- The other direction looks a bit like the the theorem above. Build $A_1 \sqcup A_2$ and kill Ψ_e's using their totality and big intervals.

Theorem (Jockusch-Schupp)

Every nonzero degree contains a set that is not coarsely computable. (and of course one that is)

- Their proof breaks down into two cases. $\mathcal{R}(A)$ is coarsely computable iff $A \leq_T \emptyset'$, and if $A \leq_T \emptyset'$ use the fact that A is hyperimmune to directly meet requirements. See the JS paper.

Another characterization of lowness

Theorem (Downey-Jocksuch-Schupp)

Let r be a computable real. A c.e. degree **a** *contains a c.e generically computable set and the density of A is r, which is not coarsely computable iff* **a** *is non-low.*

- The proof is similar to the other one, in some sense.

- However, if we remove the r from the above only one direction holds. *If* **a** *is nonlow it computes a c.e generically computable set which is not coarsely computable*. This is not surprising:

Theorem (Downey-Jocksuch-Schupp)

If **a** *is a nonzero degree then* **a** *computes a c.e generically computable set which is not coarsely computable.*

Where to?

- Reductions are problematical. Most generally to be transitive should be enumeration operators which generically take a generic description of A to one for B.
- Even if full access to A, B questions like minimal pairs, degrees all open and seem quite hard.
- Provably need to be in hyperimmune-free degrees so loved by Frank Stephan.
- What about generic algos for other algebraic objects?
- Lots of other nice results in the Jockusch-Schupp paper about associated degree structures, etc.

- Thanks!