

Solovay Functions, Triviality and Traceability

Rod Downey
Victoria University
Wellington
New Zealand

REFERENCES

- ▶ Kolmogorov complexity and Solovay functions, (with Laurent Bienvenu) to appear *Proceedings STACS 2009*
- ▶ K-trivial degrees and the jump traceability hierarchy, (with George Barmpalias and Noam Greenberg), to appear, *Proceedings of the American Mathematical Society*.
- ▶ Also L. Bienvenu, W. Merkle. Reconciling data compression and Kolmogorov complexity. 34th International Colloquium on Automata, Languages and programming (ICALP 2007), LNCS 4596, pp 643-654 (2007).
- ▶ L. Bienvenu, W. Merkle. Effective randomness for computable probability measures. 3rd International Conference on Computability and Complexity in Analysis (CCA 2006), ENTCS 167, pp 117-130
- ▶ Hölzl, R., T. Kräling and W. Merkle, Time bounded Kolmogorov complexity and Solovay functions, to appear.

REFERENCES TO BUY

- ▶ Randomness and Computability, Andre Nies, OUP.
- ▶ Algorithmic Randomness and Complexity, Downey and Hirschfeldt, Springer, last 75 pages of proof reading being done as we speak.

PLAIN KOLMOGOROV COMPLEXITY

- ▶ Capture the incompressibility paradigm. Random means hard to describe, incompressible: e.g. 1010101010.... (10000 times) would have a short program.
- ▶ A string σ is random iff the only way to describe it is by hardwiring it. (Formalizing the Berry paradox)

PLAIN KOLMOGOROV COMPLEXITY

- ▶ Capture the incompressibility paradigm. Random means hard to describe, incompressible: e.g. 1010101010.... (10000 times) would have a short program.
- ▶ A string σ is random iff the only way to describe it is by hardwiring it. (Formalizing the Berry paradox)
- ▶ For a fixed machine N , we can define
- ▶ The **Kolmogorov complexity** $C(\sigma)$ of $\sigma \in \{0, 1\}^*$ with respect to N , is $|\tau|$ for the shortest τ s.t. $N(\tau) \downarrow = \sigma$. (Kolmogorov)

- ▶ A string σ is N -random iff $C_N(\sigma) \geq |\sigma|$.
- ▶ A machine U is called weakly universal iff for all N , there is a d such that for all σ , $C_U(\sigma) \leq C_N(\sigma) + d$.

- ▶ A string σ is N -random iff $C_N(\sigma) \geq |\sigma|$.
- ▶ A machine U is called weakly universal iff for all N , there is a d such that for all σ , $C_U(\sigma) \leq C_N(\sigma) + d$.
- ▶ Actually we will always use universal machines where the e -th machine is coded in a computable way.

- ▶ A string σ is N -random iff $C_N(\sigma) \geq |\sigma|$.
- ▶ A machine U is called weakly universal iff for all N , there is a d such that for all σ , $C_U(\sigma) \leq C_N(\sigma) + d$.
- ▶ Actually we will always use universal machines where the e -th machine is coded in a computable way.
- ▶ They exist (Kolmogorov). Hence there is a notion of Kolmogorov randomness for strings up to a constant.

- ▶ A string σ is N -random iff $C_N(\sigma) \geq |\sigma|$.
- ▶ A machine U is called weakly universal iff for all N , there is a d such that for all σ , $C_U(\sigma) \leq C_N(\sigma) + d$.
- ▶ Actually we will always use universal machines where the e -th machine is coded in a computable way.
- ▶ They exist (Kolmogorov). Hence there is a notion of Kolmogorov randomness for strings up to a constant.
- ▶ Proof: We can enumerate the Turing machines $\{M_e : e \in \mathbb{N}\}$. Define

$$U(1^e 0 \sigma) = M_e(\sigma).$$

This particular coding gives $C(\tau) \leq M_e(\tau) + e + 1$.

DEFINITION

Thus we can define the **plain Kolmogorov complexity** of a string σ as $C(\sigma)$ for a fixed universal machine U .

- ▶ We can similarly do an oracle version of this and can define $C(x|y)$ as the Kolmogorov complexity of x **given** y .

PLAIN COUNTING THEOREM

- ▶ The following is the basic fact that makes the theory work.

THEOREM (PLAIN COUNTING THEOREM-KOLMOGOROV)

$$|\{\tau \mid |\tau| = n \wedge C(\tau) \leq n - d\}| \leq O(1)2^{n-d}.$$

- ▶ Proof: pigeonhole principle.

DEFINITION (KOLMOGOROV)

We say that σ is **C-random** iff $C(\sigma) \geq |\sigma|$.

PREFIX-FREE RANDOMNESS

- ▶ Levin, Gaács, Chaitin, Schnorr.
- ▶ Computers have alphabet $\{0, 1\}$.
- ▶ A computer M is **prefix-free** if

$$(M(\sigma)\downarrow \wedge \sigma' \supsetneq \sigma) \Rightarrow M(\sigma')\uparrow.$$

- ▶ A prefix-free machine is universal if every other one is coded in it.
- ▶ They exist, same proof.
- ▶ Building them uses what is now called KC. (Kraft-Computable)

THEOREM (KRAFT, LEVIN, SCHNORR, PIPPINGER)

- (I) *If A is prefix-free then $\sum_{n \in A} 2^{-|n|} \leq 1$.*
- (II) *(This part is now called KC) Let d_1, d_2, \dots be a collection of lengths, possibly with repetitions, Then $\sum 2^{-d_i} \leq 1$ iff there is a prefix-free set A with members σ_i and σ_i has length d_i . Furthermore from the sequence d_i we can effectively compute the set A .*
- (Restatement) Suppose that we are effectively given a set of “requirements” $\langle n_k, \sigma_k \rangle$ for $k \in \omega$ with $\sum_k 2^{-n_k} \leq 1$. Then we can (primitive recursively) build a prefix-free machine M and a collection of strings τ_k with $|\tau_k| = n_k$ and $M(\tau_k) = \sigma_k$.

PREFIX-FREE RANDOMNESS

- ▶ Prefix freeness gets rid of the use of length as extra information:
- ▶ The **prefix-free complexity** $K(\sigma)$ of $\sigma \in \{0, 1\}^*$ is $|\tau|$ for the shortest τ s.t. $M(\tau) \downarrow = \sigma$.
- ▶ Note now $K(\sigma) \leq |\sigma| + K(|\sigma|) + d$, about $n + 2 \log n$, for $|\sigma| = n$.
- ▶ Also $K(\sigma\tau) \leq^+ K(\sigma) + K(\tau)$. Machines concatenate!
- ▶ Build M , $M(z\sigma) = \sigma$ if $U(z) = |\sigma|$.

THEOREM (COUNTING THEOREM-CHAITIN)

$$|\{\sigma : |\sigma| = n \wedge K(\sigma) \leq n + K(n) - c\}| \leq O(1)2^{n+K(n)-c}.$$

MARTIN-LÖF RANDOMNESS

- ▶ We say that a real (member of 2^ω) is ML- or 1- random iff it passes all Martin-Löf tests
- ▶ A ML -test is a collection $\{U_n : n \in \omega\}$ of uniformly c.e. open sets with $\mu(U_n) \leq 2^{-n}$. A passes the test if $A \notin \bigcap_n U_n$.

REMINDERS

THEOREM (LEVIN-SCHNORR)

A is 1-random iff $K(A \upharpoonright n) \geq n - O(1)$ for all n .

- ▶ We will often write $=^+$, or \leq^+ where we mean $\pm O(1)$.

THEOREM (MILLER + NIES, STEPHAN TERWIJN)

A is 2-random (ie 1-random relative to \emptyset') iff

$\exists^\infty n (C(A \upharpoonright n) \geq^+ n)$.

- ▶ Chaitin proved that a real A is computable iff for all n , $C(A \upharpoonright n) \leq^+ \log n$ iff $C(A \upharpoonright n) \leq^+ C(n)$.
- ▶ This is proven using the fact that a Π_1^0 class with a finite number of paths has computable paths, combined with the Counting Theorem $\{\sigma : C(\sigma) \leq C(n) + d \wedge |\sigma| = n\} \leq A2^d$. (The Loveland Technique)
- ▶ Loveland A is computable iff $C(A \upharpoonright n \mid n) \leq c$ for some constant c .
- ▶ eg if $c = 2$ then there are only 4 possible programmes for $A \upharpoonright n$ given n . Suppose only 2 is the maximum hit infinitely often.
- ▶ Then from this parameter we can build a Π_1^0 class with at most 2 elements, and hence both computable.

K-TRIVIALITY

- ▶ What is $K(A \upharpoonright n) \leq^+ K(n)$ for all n ? We call such reals K -trivial. Does A K -trivial imply A computable?
- ▶ Write $A \in KT(d)$ iff for all n , $K(A \upharpoonright n) \leq K(n) + d$.

THE ARGUMENT FAILS

- ▶ It is still true that $\{\sigma : K(\sigma) \leq K(|\sigma|) + d\}$ is $O(2^d)$, so it would appear that we could run the Π_1^0 class argument used for C . But no...
- ▶ The **problem** is that we don't know $K(n)$ in any computable interval, therefore the tree of K -trivials we would construct would be a Π_1^0 class **relative to \emptyset'** .

THEOREM (CHAITIN, ZAMBELLA)

There are only $O(2^d)$ members of $KT(d)$. They are all Δ_2^0 .

THEOREM (SOLOVAY)

There are noncomputable K -trivial reals.

THEOREM (ZAMBELLA)

Such reals can be c.e. sets.

THEOREM (NIES PLUS MANY OTHERS)

They form an amazing Σ_3^0 ideal in the superlow Turing degrees.

COMPUTABLE UPPER BOUNDS

- ▶ In algorithmic randomness, we have already a lot of examples of upper bounds.
- ▶ n is an upper bound for $C(\sigma)$ if $|\sigma| = n$ so that $f(m) = \log m$ is a function bounding $C(m)$ an infinitely often agreeing with it.
- ▶ Miller and Yu proved that A is 1-random iff $C(A \upharpoonright n) \geq n - g(n) - O(1)$ for every computable function g such that $\sum_n 2^{-g(n)} < \infty$.
- ▶ In fact there is a fixed computable G which works.

THEOREM (BIENVENU AND MERKLE)

α is 1-random iff for all computable f with $\sum_{n \in \omega} 2^{-f(n)} < \infty$, $f(\alpha \upharpoonright n) \geq^+ n$.

- ▶ Downey and Greenberg showed that A is K -trivial if J^A can be traced at order $\sqrt{\log n}$. (more later)

SOLOVAY FUNCTIONS

- ▶ To what extent can algorithmic randomness be developed by the use of computable functions alone?
- ▶ (Aside) Compare with decidable machines of Beinvenu and Merkle, quick process machines of Day, computable measure machines of Downey-Griffiths.
- ▶ For instance what is a **good** upperbound for K ? Certainly $f(n) = n + 2 \log n$ is aznd upperbound, but is it good?
- ▶ We will say that a computable function f is a **Solovay function** if $K(\sigma) \leq^+ f(\sigma)$ for all σ , and $\exists^\infty \sigma (K(\sigma) =^+ f(\sigma))$.

SOLOVAY FUNCTIONS

THEOREM (SOLOVAY)

Solovay functions exist.

- ▶ Think of the machine M which is specified by
 - If $U_s(\sigma) = \tau$ it will enumerate $\langle |\sigma| + 1, \tau \rangle$.
 - whenever $K_s(n) < K_{s-1}(n)$, **also** enumerate $\langle K_s(n), 1^s \rangle$, assuming at most one new computation of U at s .
- ▶ This defines a function $f(n) = K_n(n)$, **and a polynomial time machine M .**

CHARACTERIZING SOLOVAY FUNCTIONS

- ▶ Early work of Levin showed that a computable $f \leq^+ K$ iff $\sum_{n \in \omega} 2^{-f(n)} < \infty$.

THEOREM (BIENVENU AND DOWNEY)

Computable f is a Solovay function iff

- (I) $\sum_{n \in \omega} 2^{-f(n)} < \infty$.
- (II) $\sum_{n \in \omega} 2^{-f(n)}$ is Martin-Löf random.

- ▶ Suppose f is a Solovay function and $\sum_{n \in \omega} 2^{-f(n)} = \alpha$.
prove that α is 1-random. Suppose not.
- ▶ For each c there is a k such that $K(\alpha \upharpoonright k) \leq k - c$. Given $\alpha \upharpoonright k$, we can effectively find an s such that $\sum_{n > s} 2^{-f(n)} \leq 2^{-k}$.
- ▶ Hence, by a standard KC Theorem argument, we have $K(n \mid \alpha \upharpoonright k) \leq f(n) - k + O(1)$ for all $n > s$. Thus, for all $n > s$,

$$K(n) \leq f(n) + K(\alpha \upharpoonright k) - k + O(1) \leq f(n) + (k - c) - k + O(1) \leq f(n) - c + O(1).$$

- ▶ Since c can be taken arbitrarily large, $\lim_n f(n) - K(n) = \infty$; i.e., f is not a Solovay function.

- ▶ Suppose that f is computable, $\alpha = \sum_{n \in \omega} 2^{-f(n)}$ is random and f not Solovay.
- ▶ By Kučera-Slaman $\Omega \leq_S \alpha$. That is, there is a partial computable g such that for some d , if q is a rational less than α , then $g(q) \downarrow < \Omega$ and $\Omega - g(q) < 2^d(\alpha - q)$.
- ▶ This implies from $\alpha \upharpoonright k$ we can compute an $s(k)$ such that $\sum_{n > s(k)} 2^{-K(n)} \leq 2^{-k+d}$.
- ▶ As f not Solovay, if k is large, $n > s(k) \Rightarrow K(n) \leq f(n) - c - d$.
- ▶ Hence $\sum_{n > s(k)} 2^{-f(n)} \leq 2^{-c-d} \sum_{n > s(k)} 2^{-K(n)} \leq 2^{-c-d} 2^{-k+d} \leq 2^{-k-c}$.
- ▶ That is, for large enough k , $\alpha \upharpoonright (k + c)$ can be computed from $\alpha \upharpoonright k$ and c .

- ▶ Therefore, for all large enough k ,

$$K(\alpha \upharpoonright (k+c)) \leq K(\alpha \upharpoonright k, c) + O(1) \leq K(\alpha \upharpoonright k) + 2 \log c + O(1).$$

- ▶ The $O(1)$ is independent of c and hence we can choose c such that the expression $2 \log c + O(1)$ in the above inequality is smaller than $c/2$.
- ▶ Then, for all large enough k ,

$$K(\alpha \upharpoonright (k+c)) \leq K(\alpha \upharpoonright k) + \frac{c}{2}.$$

- ▶ An easy induction then shows that $K(\alpha \upharpoonright k) \leq O\left(\frac{k}{2}\right)$, contradicting the assumption that α is 1-random.

COROLLARY (BIENVENU AND DOWNEY)

There exist nondecreasing Solovay functions.

- ▶ **Also:** New proof by Bienvenu of Miller: A is 2-rnd iff A has infinitely often $K(A \upharpoonright n) \geq^+ n + K(n)$. (Book)
- ▶ Further work by Hölzl, Kräling, Merkle looked at time bounded Kolmogorov complexity
- ▶ E.g. the method above was adapted by them to show that

THEOREM (HÖLZL, KRÄLING, MERKLE)

K^t is any reasonable time bounded version of K then the halting probability for this is 1-random.

- ▶ also results related to K -triviality.

SOLOVAY FUNCTIONS AND TRIVIALITY

THEOREM (BIENVENU AND DOWNEY)

A set A is K -trivial iff for all computable functions f such that $\sum_n 2^{-f(n)} < \infty$, we have $K(\alpha \upharpoonright n) \leq f(n) + O(1)$. Moreover, there exists a single function g such that

$$A \text{ is } K\text{-trivial} \Leftrightarrow K(A \upharpoonright n) \leq g(n) + O(1). \quad (1)$$

- ▶ It is unknown if the “Moreover” statement holds for **any** Solovay function. The particular one used is “Solovay’s Solovay function.”

- ▶ Suppose that f is Solovay's Solovay function, and $K(A \upharpoonright n) \leq K(n) + c$. There are only d many strings with $K(\sigma) \leq K(n) + c$, by Chaitin.
- ▶ We enumerate markers m_i , and KC with index e .
- ▶ For cycle i we enumerate $m_i = m_i[s]$ and assume that $K_s(m_i) = K(m_i)$. Then for strings σ of length m_i when for all $k \leq m_i$ we see $K_s(\sigma \upharpoonright k) \leq K_s(k) + c$ we enumerate (e.g.) $\langle K_s(k), \sigma \rangle$ (if not already there)
- ▶ If ever there are more than d such strings then we know that $K_s(m_i) \neq K(m_i)$, so we wait for that to happen. If $K_s(m_i) < K_t(m_i)$, we reset m_i and start again.
- ▶ This works.

TRACEABILITY

THEOREM (NIES)

All K -trivials are superlow $A' \equiv_{tt} \emptyset'$, and are tt -bounded by c.e. K -trivials.

- ▶ Thus triviality is essentially an “enumerable” phenomenon.
- ▶ Actually Nies proved more.
- ▶ $J^A(e)$ is the jump function: ie the actual value of the e -procedure with oracle A on input e .
- ▶ A c.e. **trace** for a partial function f is a computable collection of c.e. finite sets $T_x = W_{g(x)}$ with $f(e) \in W_{g(e)}$. If h is a function with $|T_x| \leq h(x)$ all x we say f is traceable at order h .

JUMP TRACING

- ▶ Nies proved that if A is K -trivial then A is **jump traceable** at order $n \log n$: J^A is traceable at order $n \log n$.
- ▶ Figueira, Nies Stephan there are continuum many reals jump traceable at order 2^{2^n} .

THEOREM (FNS)

There are **strongly jump traceable** reals, jump traceable at **all** computable orders.

- ▶ (For the cognoscenti) the c.e. SJT's = (superlow) $^\diamond$ = (superhigh) $^\diamond$. (Greenberg, Nies, Hirschfeldt)

LIMITS

THEOREM (CHOLAK, DOWNEY, GREENBERG)

There is an order approximately $h(n) = \log \log n$ with a K -trivial A not jump traceable at order h .

THEOREM (NG)

In fact the index set of SJT c.e. reals is Π_4^0 complete.

THEOREM (CDG)

There is an order roughly $h(n) = \sqrt{\log n}$ where if A is jump traceable at order h , then A is K -trivial.

Question[CDG] Is there a combinatorial characterization of K -triviality using jump tracing?

- ▶ Here you must be careful about tracing. To be jump traceable at order h we need that **all A -partial computable** functions are so traceable.

THEOREM (BARMPLIAS, DOWNEY, GREENBERG)

If $\sum_n \frac{1}{h(n)} < \infty$ every K -trivial is jump traceable at this order.

- ▶ Proof uses Nies characterization of K -trivials as having low cost enumerations.

THEOREM (BARMPLIAS, DOWNEY, GREENBERG)

*There is a c.e. real A which is jump tracable at every (computable) order with $\sum_n \frac{1}{h(n)} < \infty$ and is **not** K -trivial.*

- ▶ Actually the argument works for all h which is superlinear.
- ▶ Π_2^0 argument using strategies a bit like the ones to show that SJT and K -trivial are distinct.

- ▶ Enumerate Π_1^0 classes of measure less than 1 effectively as $\{V_j : j \in \omega\}$
- ▶ For each j we enumerate a Π_1^A class G_j^A and ensure that $\sum_j \mu(G_j^A) < 1$. The requirement is

$$P_j \mid G_j^A \not\subseteq V_j$$

So if we let $G^A = \bigcup_j G_j^A$ then the requirement P is met.

- ▶ The basic module is easy: If we want $\mu(G_j^A) \leq q_j$, break the universe in clopen sets of that size.
- ▶ Put them in, wait for V_j , take them out, etc.

- ▶ For the tracing:

Q_e | If h_e is superlinear, then $\{T_i^{e''} \mid i \in \omega\}$ traces Φ^A .

- ▶ Lowness: see a computation try to preserve it.
- ▶ Place the P_j sporadically. if it is $Q_{e,0}, \dots, Q_{e,k}$ then there are $k + 1$ many possible re-starts. So need $h_e(k) > \frac{k+1}{q_j}$.
- ▶ Combining requirements needs geometric re-starting of the q_j 's and then also a Π_2^0 guess for h being superlinear.

QUESTIONS

- ▶ What about A is K -trivial iff A is jump traceable at all (computable) orders h with $\sum_n 2^{-h(n)} < \infty$? What about all Solovay functions h ?
- ▶ Note

THEOREM (HÖLZL, KRÄLING, MERKLE)

A is K -trivial iff A is $O(g(n) - K(n))$ jump traceable for all Solovay functions g .

- ▶ More general programme: (Bienvenu) Re-do randomness using things like Solovay functions and computable orders.
- ▶ Is there a class of reals C where K -trivials are the same as C^\diamond ?

Thank You,
and Happy Birthday CT

BUT WAIT THERE IS MORE!

Next Asian Logic Meeting
Wellington, December (late) 2011