

RANDOM NON-CUPPING REVISITED

GEORGE BARMPALIAS

ABSTRACT. Say that Y has the strong random anticupping property if there is a set A such that for every Martin-Löf random set R

$$Y \leq_T A \oplus R \Rightarrow Y \leq_T R$$

(in this case A is an anticupping witness for Y). Nies has shown that every random Δ_2^0 set has the strong random anticupping property via a promptly simple anticupping witness. We show that every Δ_2^0 set has the random anticupping property via a promptly simple anticupping witness. Moreover, we prove the following stronger statement: for every noncomputable $Y \leq_T \emptyset'$ there exists a promptly simple A such that

$$Y \leq_T A \oplus R \Rightarrow A \leq_T R$$

for all Martin-Löf random sets R .

1. INTRODUCTION

In classical computability theory of c.e. sets and degrees we say that a c.e. set Y has the *anticupping property* via an anticupping witness $A <_T Y$ if for all $B <_T Y$, $A \oplus B \not\leq_T Y$ (see [10]). If the condition $B <_T Y$ is replaced by $B \not\leq_T Y$ we get the *strong anticupping property* and witness; these notions extend naturally to the c.e. degrees. Cooper and Yates (unpublished notes of Cooper from the 1970s) showed that $\mathbf{0}'$ has the anticupping property. Then Harrington followed with a proof that every high c.e. degree has the strong anticupping property with a high strong anticupping witness. Finally Ladner and Sasso [9] showed that below any non-computable c.e. degree there is a non-computable low_2 predecessor with the anticupping property. In the following we discuss a randomized version of anticupping in the Δ_2^0 degrees. Kučera was probably the first to ask about cupping below $\mathbf{0}'$ with random degrees and Nies [13] gave the first results. The general question of which Δ_2^0 degrees can be cupped to $\mathbf{0}'$ by random Δ_2^0 degrees also appears in [11] where the following terminology is used.

Definition 1. ([11]) *A set A is weakly ML-cuppable if $A \oplus Z \geq_T \emptyset'$ for some Martin-Löf random set $Z \not\leq_T \emptyset'$. Also, A is ML-cuppable if one can choose $Z <_T \emptyset'$.*

Date: November 2005.

The author was supported by EPSRC Research Grant No. EP/C001389/1 and partially supported by the NSFC Grand International Joint Project, No. 60310213, “New Directions in the Theory and Applications of Models of Computation”.

In accordance with the terminology in the classical case, and since this notion was not defined explicitly in [13] we adopt the following definition.

Definition 2. *We say that Y has the strong random anticupping property if there is a set A such that for every Martin-Löf random set R*

$$Y \leq_T A \oplus R \Rightarrow Y \leq_T R.$$

In this case we say that A is a (randomized) strong anticupping witness for Y .

We prefer not to use the term ‘random anticupping witness’ in order to avoid confusion, since such a witness is not necessarily (and in fact it cannot be, see [13]) Martin-Löf random. Note that A is a randomized strong anticupping witness for \emptyset' iff it is not weakly ML-cupppable. For a discussion on questions related to cupping with random reals we refer to [8]. Nies’ main result in [13] was the following theorem.

Theorem 1. *(Nies [13]) Every random Δ_2^0 set has the strong random anticupping property and a promptly simple anticupping witness.*

We present the following generalization of Nies’ non-cupping result.

Theorem 2. *Every Δ_2^0 set has the strong random anticupping property via a promptly simple anticupping witness. That is, for every Δ_2^0 set Y there is a promptly simple set A such that*

$$Y \leq_T A \oplus R \Rightarrow Y \leq_T R.$$

for every random set R .

Let $K(x)$ be the prefix-free complexity of the string x . That is, $K(x)$ is the length of the shortest string which produces x via a fixed universal prefix-free machine. A set $A \subseteq \mathbb{N}$ is *K -trivial* if (up to a constant) the initial segments of A have minimum complexity. That is,

$$(\forall n) K(A \upharpoonright n) \leq K(n) + \mathcal{O}(1)$$

(where we suitably identify numbers with strings). Note that this notion is opposite to 1-randomness (randomness from now on) since A is random iff there is a constant c such that

$$(\forall n) K(A \upharpoonright n) \geq n - c$$

that is, the initial segments of A have nearly maximal complexity. The class \mathcal{K} of K -trivial sets is known to be equal to the class of *low for random* sets; that is, those sets A for which A -randomness (i.e. randomness relativized in a standard way to oracle A) coincides with (oracle-free) randomness. For background on algorithmic randomness we refer to [2, 3, 12].

Note that the proof below is just a cost-management construction, much like a direct construction of a K -trivial or a low for random set. However our cost function *cost* is somewhat different from the cost functions used for the construction of K -trivials or low for random sets (see [7, 12, 3]). The

reader should notice that the cost functions used in the proof of theorem 2 are essentially the following

$$C_\Gamma(n, s) = \mu\{\sigma \mid \exists v, t < s((\Gamma^{A, \sigma} = v)[t] \wedge v \subset Y_t \wedge (A_t = A_s) \upharpoonright u \wedge n < u)\}$$

where Γ is a Turing functional, Y is a non-computable Δ_2^0 set (with a role as in definition 2), A is the set being constructed, u is the use of the computation mentioned and μ is the Lebesgue measure. The difference is that, although they still have (at least when Γ is a typical functional, in the sense of lemma 1) the vital property

$$(1) \quad \limsup_n \inf_s cost(n, s) = 0$$

which allows us to get a chance to diagonalize, we may have $cost(n, s) < cost(n, s + 1)$ while $cost(m, s) = cost(m, s + 1)$ for some $m < n$ and some s . We note that K -trivials and low for random sets are exactly those which can be constructed via cost functions (a result of Nies, for more details see [12]) and that any c.e. set A which is not ML-cuppable is K -trivial (see [13]).

Our proof is largely based on Nies'; the new ingredient is that we deal directly with the cost functions C_Γ and show that they have the property (1) with the help of a generalization of Sacks' theorem on the measure of upper cones in the Turing degrees (theorem 1). Thus we avoid the assumption that Y is random: incomputability suffices and in fact, if Y is computable the claim holds trivially. Nies followed an indirect approach: he explicitly required the set A to be K -trivial and used this along with the randomness of Y to ensure that the cost (associated with non-cupping) from the enumeration into A is bounded.

Proof of theorem 2. We may assume that Y is non-computable (otherwise the claim is trivial). Assume a computable approximation (Y_s) of Y . We consider any one-oracle Turing functional Θ as a consistent c.e. set of axioms $\langle \tau, v \rangle$ where τ, v are strings. Consistent means that if $\langle \tau_1, v_1 \rangle, \langle \tau_2, v_2 \rangle \in \Theta$ and τ_1, τ_2 are comparable (i.e. one is a prefix of the other) then v_1, v_2 are comparable. An axiom $\langle \tau, v \rangle$ means that all reals which are prefixed by τ must be mapped (via Θ) to a real which is prefixed by v . Analogous definitions hold for functionals of more oracles (e.g. a two-oracle functional will be a consistent set of axioms $\langle \tau, \sigma, v \rangle$).

Moreover, we say that a (for example) two-oracle Turing functional Γ (with enumeration (Γ_s)) *does not enumerate any superfluous axioms* if for any stage s of its enumeration the following holds: if $\langle \tau_1, \sigma_1, v \rangle \in \Gamma_s$ then no axiom $\langle \tau_2, \sigma_2, v \rangle$ with $\tau_2 \supseteq \tau_1$ and $\sigma_2 \supseteq \sigma_1$ is going to be enumerated into Γ at a later stage. Such an axiom is called *superfluous* since it does not add any information about the map Γ to what we already know at stage s . It is obvious that given any Turing functional Γ we can effectively get a Turing functional Θ which does not enumerate any superfluous axioms and is identical to Γ , as a map from reals to reals. Let μ be the Lebesgue measure. We often identify strings with basic open sets of the Cantor space 2^ω (e.g. σ is the set of reals whose binary expansion extends σ) and sets of

strings with the union of the corresponding sets of reals. Thus, for example, we can consider the measure of a set of strings.

Lemma 1. *Suppose that Γ is a two-oracle Turing functional which does not enumerate any superfluous axioms and A is a set. Then for every string ρ and $e > 0$ there is some stage t such that*

$$\mu\{\sigma \mid (\exists \tau, v)[\tau \subset A \wedge |\tau| > u \wedge v \subseteq \rho \wedge \langle \tau, \sigma, v \rangle \in \Gamma - \Gamma_t]\} < 2^{-e}$$

where u is the length of the longest τ such that $\langle \tau, \sigma, v \rangle \in \Gamma_t$ for some σ, v .

Proof. Obviously it is enough to show that for every string ρ and $e > 0$ there is some stage t such that

$$(2) \quad \mu\{\sigma \mid (\exists \tau)[\tau \subset A \wedge |\tau| > u \wedge \langle \tau, \sigma, \rho \rangle \in \Gamma - \Gamma_t]\} < 2^{-e}.$$

Consider the set \mathcal{S} of all strings σ such that there exists $\tau \subset A$ with $\langle \tau, \sigma, \rho \rangle \in \Gamma$ and no $\sigma' \subset \sigma$ has this property. Note that the set of reals corresponding to \mathcal{S} (i.e. the reals which are extensions of the strings in \mathcal{S}) is the set of reals corresponding to

$$\mathcal{G} = \{\sigma \mid (\exists \tau)[\tau \subset A \wedge \langle \tau, \sigma, \rho \rangle \in \Gamma]\}.$$

Consider the approximation $(\mathcal{S}_t) \rightarrow \mathcal{S}$ where $\sigma \in \mathcal{S}_t$ if $\sigma \in \mathcal{S}$ and $\langle \tau, \sigma, \rho \rangle \in \Gamma_t$ for some $\tau \subset A$. Since $\lim_t \mathcal{S}_t = \mathcal{S}$ we can choose a stage t_0 such that

$$\mu\mathcal{S} - \mu\mathcal{S}_t < 2^{-e}$$

for all $t > t_0$. We claim that (2) holds for $t = t_0$. Indeed it is enough to show that any real β of the set in (2) belongs to $\mathcal{S} - \mathcal{S}_{t_0}$. We know that β belongs to \mathcal{S} (since \mathcal{S} and \mathcal{G} contain the same reals). If it belonged to \mathcal{S}_{t_0} then there would be a $\sigma \subset \beta$ such that $\sigma \in \mathcal{S}_{t_0}$ and $\langle \tau, \sigma, \rho \rangle \in \Gamma_{t_0}$ for some $\tau \subset A$. But since β belongs to the set in (2) there must be some $\tau' \subset A$, $\sigma' \subset \beta'$ such that $\langle \tau', \sigma', \rho \rangle \in \Gamma - \Gamma_{t_0}$ and $|\tau'| > u > |\tau|$. Then $\tau \subset \tau'$ and, by the properties of \mathcal{S} , $\sigma \subseteq \sigma'$. This is a contradiction since we assumed that Γ does not enumerate any superfluous axioms. \square

For each two-oracle partial computable functional Γ we will construct a consistent Δ_2^0 set of axioms Δ_Γ (in particular, a one-oracle functional) such that the following requirement holds:

$$N_\Gamma : [\langle \tau, \sigma, v \rangle \in \Gamma \wedge \tau \subset A \wedge v \subset Y] \Rightarrow \langle \sigma, v \rangle \in \Delta_\Gamma$$

and if $I_\Gamma(s)$ is the set of uses (as strings σ) of the axioms that are removed from Δ_Γ at stage s then

$$(3) \quad \sum_s \mu I_\Gamma(s) < \infty.$$

The relation (3) asserts that $(I_\Gamma(s))$ is a Solovay test. We recall that a real β is Solovay random (which is equivalent to Martin-Löf random, see [2]) if for every sequence of intervals which is a Solovay test, only finitely many intervals contain β . So (3) says that for any Martin-Löf random R only finitely many axioms with use comparable to R will ever be extracted from

Δ_Γ . From the discussion above we can restrict the functionals Γ to those which do not enumerate any superfluous axioms (something we will assume from now on without special notice) without losing any generality. Of course we also have the prompt simplicity requirements for A :

$$P_W : |W| = \infty \Rightarrow \exists s, n [n \in W_s - W_{s-1} \wedge n \in A_s]$$

where W runs over all c.e. sets. The functionals Δ will be fed tagged axioms of the form $\langle \sigma, v \rangle_\tau$ where $\langle \tau, \sigma, v \rangle$ belongs to Γ . We use tags in order to reduce consistency of Δ to the consistency of Γ . In particular, at any stage we will only allow in Δ axioms whose tags agree with the current approximation to A . This way Δ will be consistent so long as Γ is consistent.

The requirements above are sufficient to guarantee the claim. Indeed, if $\Gamma^{A,R} = Y$ then $\Delta^R = Y$ (by the satisfaction of N_Γ). If R is random then we can compute Y as follows: after some stage no axiom with use an initial segment of R is going to be extracted from Δ (otherwise, by (3) R would not be random). So we can run the approximation to Δ after that stage and every axiom which applies to R will be indeed in Δ and will give us the correct answer about Y . The cost function (for requirement N_Γ) will be as follows:

$$(4) \quad \text{cost}_\Gamma(n, s) = \mu\{\sigma \mid (\exists v, \tau)(\langle \sigma, v \rangle_\tau \in \Delta_{\Gamma, s-1} \wedge n < |\tau|)\}.$$

Assume an effective ordering of the requirements of the form

$$P_0 > N_0 > P_1 > N_1 > \dots$$

and say that the e -th P -strategy requires attention at stage s if there is some n such that

$$n \in W_s - W_{s-1} \wedge \text{cost}_\Gamma(n, s) \leq 2^{-e}$$

for all N -requirements of higher priority than P . Such a number n is called *P-suitable*. The construction is as follows.

Construction: At stage s ,

- (1) For each N_Γ -requirement (of priority order $< s$) do the following:
 - (*removing from Δ_Γ*) Remove from Δ_Γ every axiom $\langle \sigma, v \rangle_\tau$ such that $\tau \not\subset A_s$.
 - (*adding to Δ_Γ*) For every $\langle \tau, \sigma, v \rangle \in \Gamma_s$ such that $\tau \subset A_s$ and $v \subset Y_s$ add $\langle \sigma, v \rangle_\tau$ to Δ_Γ .
- (2) find the least P -strategy (of priority order $< s$) requiring attention (if such exists) and enumerate the least P -suitable number into A .

Verification. For the verification, first note that every Δ tends to a limit since (A_s) tends to a limit. Also every Δ is consistent since it is consistent at each stage (due to the consistency of Γ and the tags). Note that all requirements N are satisfied by the construction. Also, the condition on I_Γ

is satisfied since there is a stage s_0 such that for all $t > s_0$ no P -requirement of higher priority than N_Γ acts and

$$\sum_{t > s_0} \mu I_\Gamma(s) \leq \sum_s 2^{-e}$$

(because every P acts at most once and only with suitable witnesses). Now if we show that for every N_Γ and e there exists some n_0 such that

$$(5) \quad (\forall n > n_0)(\forall s > n) \text{ cost}_\Gamma(n, s) \leq 2^{-e}$$

the satisfaction of all P follows and we are done. Fix $N_\Gamma = N_t$, $e > t$ and consider

$$T_n = \{\sigma \mid (\Gamma^{A,\sigma} = Y) \upharpoonright n\}$$

i.e.

$$T_n = \{\sigma \mid (\exists \tau, v)(\langle \tau, \sigma, v \rangle \in \Gamma \wedge \tau \subset A \wedge v \supseteq Y \upharpoonright n)\}.$$

Then $T_{n+1} \subseteq T_n$ and if $T = \lim_n T_n$ then

$$T = \{\beta \mid \Gamma^{A,\beta} = Y\}.$$

Notice that $Y \not\leq_T A$. Indeed, otherwise we can choose a random $R \not\leq_T Y$ (since Y is non-computable) and we would have $Y \leq_T A \oplus R$ which contradicts the satisfaction of the N -requirements that we showed above. The following is a generalization of Sacks' theorem that the measure of non-trivial upper cones of Turing degrees is 0.

Theorem 3. (*Stillwell* [17]) *If $Y \not\leq_T A$ then $\mu\{\beta \mid Y \leq_T A \oplus \beta\} = 0$.*

So $\mu T = 0$ and $\lim_n \mu T_n = 0$. Choose some m such that $\mu T_m < 2^{-e-2}$ and a stage t_0 after $Y \upharpoonright m$ has settled (in the approximation of Y that we have). Recall lemma 1 and choose a stage t_1 such that if

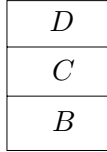
$$M = \mu\{\sigma \mid (\exists \tau, v)[\tau \subset A \wedge |\tau| > u \wedge v \subseteq Y \upharpoonright m \wedge \langle \tau, \sigma, v \rangle \in \Gamma - \Gamma_{t_1}]\}$$

where u is the length of the longest τ such that $\langle \tau, \sigma, v \rangle \in \Gamma_{t_1}$ for some σ, v , then

$$(6) \quad M < 2^{-e-2}.$$

If t_2 is the last stage where some P_i , $i \leq e+1$ acts and $n_0 > t_0, t_1, t_2, u$ then (5) holds. Indeed, consider any $n > n_0$, $s > n$. Then $\Delta_s \subseteq B \cup C \cup D$ (we drop the subscript Γ from Δ for simplicity) where

- (1) B is the set of axioms $\langle \sigma, v \rangle_\tau$ with $\tau \subset A$ such that $\langle \tau, \sigma, v \rangle \in \Gamma_{t_1}$.
- (2) C is the set of axioms $\langle \sigma, v \rangle_\tau$ with $\tau \subset A$, $v \subseteq Y \upharpoonright m$ or $v \supset Y \upharpoonright m$ (i.e. v is *comparable* to $Y \upharpoonright m$), and such that $\langle \tau, \sigma, v \rangle \in \Gamma - \Gamma_{t_1}$. Let C^1 be the set of those axioms $\langle \sigma, v \rangle_\tau \in C$ that have $v \subseteq Y \upharpoonright m$ and $C^2 = C - C^1$.
- (3) D is the set of axioms of Δ_s which are going to be removed in stages $> s$ (i.e. those $\langle \sigma, v \rangle_\tau \in \Delta_s$ such that $\tau \not\subset A$).

Figure 1: Δ_s and its partition

Note that B, C^1, C^2, D are pairwise disjoint as sets of tagged axioms. If $B_\sigma, C_\sigma^i, D_\sigma$ are the sets of uses of the axioms in B, C^i, D respectively then $C_\sigma^2 \subset T_m$, $\mu C_\sigma^2 < 2^{-e-2}$ and by the choice of t_2 , $\mu D_\sigma < 2^{-e-1}$. Also $\mu C_\sigma^1 \leq 2^{-e-2}$ by (6) and the choice of t_1 . If

$$E = \{\langle \sigma, v \rangle_\tau \in \Delta_s \mid n < |\tau|\}$$

and E_σ the set of uses of the axioms in E then $E \subseteq B \cup C^1 \cup C^2 \cup D$ and $E \cap B = \emptyset$ (since n bounds the lengths of the tags of all axioms in B). So $E \subseteq C^1 \cup C^2 \cup D$ and by (4),

$$\text{cost}_\Gamma(n, s) = \mu E_\sigma \leq \mu C_\sigma^1 + \mu C_\sigma^2 + \mu D_\sigma < 2^{-e}$$

which concludes the proof of theorem 2. \square

After the submission of this paper, the referee suggested that the proof of theorem 2 (with a minor modification) actually shows the following stronger statement.

Theorem 4. *For every Δ_2^0 noncomputable set Y there is a promptly simple set A such that*

$$Y \leq_T A \oplus R \Rightarrow A \leq_T R.$$

for every random set R .

The only modification we have to do is that we require the functionals Γ to have the following two properties (instead of just the first one):

- Γ does not enumerate superfluous axioms
- if $\langle \tau, \sigma, v \rangle \in \Gamma$ then $|\tau| \geq |v|$.

It is not hard to show that each partial computable functional Γ can be effectively filtered so that we get a partial computable functional Γ' which has these two properties and gives exactly the same reductions as the functional it came from. Indeed, stage by stage we pour the axioms appearing in Γ into Γ' with the following exceptions:

- if an axiom is superfluous we do not enumerate it in Γ'
- if $\langle \tau, \sigma, v \rangle$ with $|\tau| < |v|$ appears in Γ we consider the set of extensions (τ_i) of τ such that $|\tau_i| = |v|$ and enumerate $\langle \tau_i, \sigma, v \rangle$ into Γ' for each i unless this axiom is superfluous for Γ' .

Now one can inductively verify that Γ' has the required properties. So we have an effective list of all such typical functionals which we can use

without loss of generality (since they give all possible reductions). The proof proceeds exactly as before and we only need to verify that

$$Y \leq_T A \oplus R \Rightarrow A \leq_T R.$$

for every random set R . Assuming that $\Gamma^{A \oplus R} = Y$ we show how to compute A given R . Every time that an axiom $\langle \sigma, v \rangle_\tau$ appears in Δ_Γ with $\sigma \subset R$ we enumerate τ into a set M . Now by the assumptions M contains strings of unbounded length. Moreover, if infinitely many of these strings are not prefixes of A , the set R must be a member of infinitely many terms of the Solovay test I_Γ (by the same argument as in the proof of theorem 2). Since R is random almost all strings in M are prefixes of A and thus $A \leq_T R$.

REFERENCES

- [1] R. Downey, D. Hirschfeldt and A. Nies, Randomness, computability, and density *SIAM Journal of Computation*, Vol. **31** No. 4, pp. 1169–1183 (2002)
- [2] R. Downey, D. Hirschfeldt, Algorithmic Randomness and Complexity, Springer monograph in preparation. Current draft available at <http://www.mcs.vuw.ac.nz/~downey/>
- [3] Downey, R., D. Hirschfeldt, A. Nies, and F. Stephan, *Trivial reals*, extended abstract in Computability and Complexity in Analysis Malaga, (*Electronic Notes in Theoretical Computer Science*, and proceedings, edited by Brattka, Schröder, Weihrauch, FernUniversität, 294-6/2002, 37–55), July, 2002. Final version appears in [4] 2003, 103–131.
- [4] Downey, R., Ding Decheng, Tung Shi Ping, Qiu Yu Hui, Mariko Yasugi, and Guohua Wu (eds), *Proceedings of the 7th and 8th Asian Logic Conferences*, World Scientific, 2003, viii+471 pages.
- [5] Kučera, A., Measure, Π_1^0 classes and complete extensions of PA, *Springer Lecture Notes in Mathematics*, Vol. 1141, 245–259, Springer-Verlag 1985.
- [6] Kučera, A. and Slaman, T., Randomness and recursive enumerability, *SIAM Journal of Computing*, Vol. **31** (2001) 199–211
- [7] Kučera, A. and Terwijn, S., Lowness for the class of random sets, *Journal of Symbolic Logic*, vol. **64** (1999) 1396–1402.
- [8] A. Kučera, PA sets, 1-random sets, Π_1^0 classes, slides from a talk in the *Computational Prospects of Infinity* meeting in Singapore, 20 Jun – 15 Aug 2005. Available at <http://www.ims.nus.edu.sg/Programs/infinity/visitors.htm>
- [9] R. E. Ladner and L. P. Sasso, The weak truth table degrees of recursively enumerable sets, *Ann. Math. Logic* **4** (1975), 429–448
- [10] D. P. Miller, High recursively enumerable degrees and the anti-cupping property, Logic Year 1979-80: University of Connecticut (editors), Lecture Notes in Mathematics No. 859, Springer-Verlag, Berlin, Heidelberg, Tokyo, New York, 1981.
- [11] Miller, J. and Nies, A., Randomness and computability: open questions, *preprint*.
- [12] Nies, A., Reals which compute little, *to appear*.
- [13] Nies, A., Non-Cupping and Randomness, to appear in the *Proceedings of the American Mathematical Society*
- [14] Odifreddi, P., “Classical recursion theory”, Amsterdam Oxford: North-Holland, 1989
- [15] Odifreddi, P., “Classical recursion theory Vol.II”, Amsterdam Oxford: North-Holland, 1999
- [16] Soare, R. I., “Recursively enumerable sets and degrees”, Berlin London: Springer-Verlag, 1987
- [17] Stillwell, J., Decidability of almost all theory of degrees, *J. Symb. Logic*, Vol. **37** (1972), 501–506.

E-mail address: `georgeb@maths.leeds.ac.uk`

SCHOOL OF MATHEMATICS, UNIVERSITY OF LEEDS, LEEDS LS2 9JT, U.K.