Demuth's path to algorithmic randomness*

Antonín Kučera and André Nies

[1] Faculty of Mathematics and Physics, Charles University, Prague, Czech Republic
antonin.kucera@mff.cuni.cz
[2] Department of Computer Science, University of Auckland, Auckland, New Zealand
andre@cs.auckland.ac.nz

Abstract. Osvald Demuth (1936–1988) studied constructive analysis in the Russian style. For this he introduced notions of effective null sets which, when phrased in classical language, yield major algorithmic randomness notions. He proved several results connecting constructive analysis and randomness that were rediscovered only much later.
We give an overview in mostly chronological order. We sketch a proof that Demuth's notion of Denjoy sets (or reals) coincides with computable randomness. We show that he worked with a test notion that is equivalent to Schnorr tests relative to the halting problem. We also discuss the invention of Demuth randomness, and Demuth's and Kučera's work on semigenericity.

1 Who was Demuth?

The mathematician Osvald Demuth worked mainly on constructive analysis in the Russian style, which was initiated by Markov, Šanin, Ceĭtin, and others. Demuth was born 1936 in Prague. In 1959 he graduated from the Faculty of Mathematics and Physics at Charles University, Prague with the equivalent of a masters degree. Thereafter he studied constructive mathematics in Moscow under the supervision of A. A. Markov jr., where he successfully defended his doctoral thesis (equivalent to a PhD thesis) in 1964. After that he returned to Charles University, where he worked, mostly in isolation, until the end of his life in 1988.

2 Demuth's world

Demuth used the Russian style terminology of constructive mathematics, adding some of his own terms and notions. In this paper, his definitions will be phrased in the language of modern computable analysis, developed for instance in [34,6]. We will also use present-day terminology in algorithmic randomness as in [28].

* A. Kučera is partially supported by the Research project of the Ministry of Education of the Czech Republic MSM0021620838. Nies is partially supported by the Marsden Foundation of New Zealand under grant 09-UOA-184. We wish to dedicate this paper to Cris Calude on the occasion of his 60th birthday. We are grateful to Cris because he brought randomness to New Zealand.

From the beginning through the 1970s, in line with Russian style constructivism, Demuth only believed in computable reals, which he called constructive real numbers, and sometimes, simply, numbers.

Definition 1. A *computable real* z is given by a computable Cauchy name, i.e., a sequence $(q_n)_{n\in\mathbb{N}}$ of rationals converging to z such that $|q_r - q_n| \leq 2^{-n}$ for each $r \geq n$.

Demuth still accepted talking about Δ^0_2 reals, which he called pseudo-numbers. They are given as limits of computable sequences of rationals, so it was not necessary to view them as entities of their own. Later on, in the 1980s, he relaxed his standpoint somewhat, also admitting arithmetical reals.

The following is a central notion of Russian-style constructivism. Since in that context only computable reals actually exist, it is the most natural notion of computability for a function.

Definition 2. A function g defined on the computable reals is called *Markov computable* if from an index for a computable Cauchy name for x one can compute an index for a computable Cauchy name for $g(x)$.

Demuth called such functions *constructive*. By a *c-function* he meant a constructive function that is constant on $(-\infty, 0]$ and on $[1, \infty)$. This in effect restricts the domain to the unit interval (but a constructivist cannot write that into the definition since it is not decidable whether a given computable real is negative). By a result of Ceĭtin, and also a similar result of Kreisel, Shoenfield and Lacombe, each c-function is continuous on the computable reals. However, since such a function only needs to be defined on the computable reals, it is not necessarily uniformly continuous.

A *modulus of uniform continuity* for a function f is a function θ on positive rationals such that $|x-y| \leq \theta(\epsilon)$ implies $|f(x)-f(y)| \leq \epsilon$ for each rational $\epsilon > 0$. If a c-function is uniformly continuous (or equivalently, if it can be extended to a continuous function on $[0,1]$) then it has a modulus of uniform continuity that is computable in $\emptyset'$. Demuth also considered $\emptyset$-uniformly continuous c-functions, i.e. c-functions which even have a computable modulus of uniform continuity; this is equivalent to computable functions on the unit interval in the usual sense of computable analysis (see [34,6]).

3 The Denjoy alternative, and pseudo-differentiability

The Denjoy alternative motivated a lot of Demuth's work on algorithmic randomness.

3.1 Background

For a function f, the *slope* at a pair a, b of distinct reals in its domain is

$$S_f(a,b) = \frac{f(a) - f(b)}{a - b}.$$

Recall that if z is in the domain of f then

$$\overline{D}f(z) = \limsup_{h\to 0} S_f(z, z+h)$$
$$\underline{D}f(z) = \liminf_{h\to 0} S_f(z, z+h)$$

Note that we allow the values $\pm\infty$. By the definition, a function f is differentiable at z if $\underline{D}f(z) = \overline{D}f(z)$ and this value is finite.

One simple version of the Denjoy alternative for a function f defined on the unit interval says that

$$\text{either } f'(z) \text{ exists, or } \overline{D}f(z) = \infty \text{ and } \underline{D}f(z) = -\infty. \tag{1}$$

It is a consequence of the classical Denjoy (1907), Young (1912), and Saks (1937) Theorem that for *any* function defined on the unit interval, the Denjoy alternative holds at almost every z. The full result is in terms of right and left upper and lower Dini derivatives denoted $D^+f(z)$ (right upper) etc. Denjoy himself obtained the Denjoy alternative for continuous functions, Young for measurable functions, and Saks for all functions. For a proof see for instance Bogachev [5, p. 371]. One application of this result is to show that f' is Borel (as a partial function) for any function f. A paper by Alberti et al. [1] revisits the Denjoy alternative. They provide a version that is in a sense optimal.

3.2 Pseudo-differentiability

If one wants to study the Denjoy alternative for Markov computable functions, one runs into the problem that they are only defined on computable reals. So one has to introduce upper and lower"pseudo-derivatives" at a real z, taking the limit of slopes close to z where the function is defined. This is presumably what Demuth did. Consider a function g defined on $I_{\mathbb{Q}}$, the rationals in $[0, 1]$. For $z \in [0, 1]$ let

$$\widetilde{D}g(z) = \limsup\nolimits_{h\to 0^+}\{S_g(a, b)\colon a, b \in I_{\mathbb{Q}} \,\wedge\, a \le x \le b \,\wedge\, 0 < b - a \le h\}.$$
$$\underset{\sim}{D}g(z) = \liminf\nolimits_{h\to 0^+}\{S_g(a, b)\colon a, b \in I_{\mathbb{Q}} \,\wedge\, a \le x \le b \,\wedge\, 0 < b - a \le h\}.$$

Definition 3. We say that a function f with domain containing $I_{\mathbb{Q}}$ is *pseudo-differentiable at x* if $-\infty < \underset{\sim}{D}f(x) = \widetilde{D}f(x) < \infty$.

Since Markov computable functions are continuous on the computable reals, it does not matter which dense set of computable reals one takes in the definition of these upper and lower pseudo-derivatives. For instance, one could take all computable reals, or only the dyadic rationals. For a total continuous function g, we have $\underset{\sim}{D}g(z) = \underline{D}g(z)$ and $\widetilde{D}g(z) = \overline{D}g(z)$. The last section of [7] contains more detail on pseudo-derivatives.

Definition 4. Suppose the domain of a function f contains $I_{\mathbb{Q}}$. We say that the *Denjoy alternative* holds for f at z if

$$\text{either } \widetilde{D}f(z) = \underset{\sim}{D}f(z) < \infty, \text{ or } \widetilde{D}f(z) = \infty \text{ and } \underset{\sim}{D}f(z) = -\infty. \tag{2}$$

This is equivalent to (1) if the function is total and continuous.

4 Martin-Löf randomness and differentiability

Demuth introduced a randomness notion equivalent to Martin-Löf (ML) randomness in the paper [10]. He was not aware of Martin-Löf's earlier definition in [27]. Among other things, Demuth gave his own proof that there is a universal Martin-Löf test.

The notion was originally only considered for pseudo-numbers (i.e., Δ^0_2 reals). As a constructivist, Demuth found it more natural to define the *non*-Martin-Löf random pseudo-numbers first. He called them Π_1 numbers. Pseudonumbers that are not Π_1 numbers were called Π_2 numbers. Thus, in modern language, the Π_2 numbers are exactly the Martin-Löf random Δ^0_2-reals.

As already noted, from around 1980 on Demuth also admitted arithmetical reals (possibly in parallel with the decline of communism, and thereby its background of philosophical materialism). In [14] he called the arithmetical *non*-ML-random reals $\mathcal{A}_1$ numbers, and the arithmetical ML-random reals $\mathcal{A}_2$ numbers. For instance, the definition of $\mathcal{A}_1$ can be found in [14, page 457]. By then, Demuth knew of Martin-Löf's work: he defined $\mathcal{A}_1$ to be $\bigcap_k [W_{\langle g \rangle (k)}]$, where g is a computable function determining a universal ML-test, and $[X]$ is the set of arithmetical reals extending a string in X. In the English language papers such as [18], the non-ML random reals were called AP (for approximable, or approximable in measure), and the ML-random reals were called NAP (for non-approximable).

Demuth needed Martin-Löf randomness for his study of differentiability of Markov computable functions (Definition 2), which he called constructive. The abstract of the paper [11], translated literally, is as follows:

> It is shown that every constructive function f which cannot fail to be a function of weakly bounded variation is finitely pseudo-differentiable on each Π_2 number.
> For almost every pseudo-number ξ there is a pseudo-number which is a value of pseudo-derivative of function f on ξ, where the differentiation is almost uniform.

Converted into modern language, the first paragraph says that each Markov computable function of bounded variation is (pseudo-)differentiable at each Martin-Löf random real. We do not know how Demuth proved this. However, his result has been recently reproved in [7] in an indirect way, relying on a similar result on computable randomness in the same paper [7]: each Markov computable nondecreasing function is differentiable at each computably random real.

The first part of the second paragraph expresses that for almost every Δ^0_2 real z, the derivative $f'(z)$ is also Δ^0_2. It is not clear what Demuth means by the second part, that "the differentiation is almost uniform". One might guess it is similar to the definition of Markov computablility: from an index for z as a limit of a computable sequence of rationals, one can compute such an index for $f'(z)$.

The notion that a property $\mathcal{S}$ holds for "almost every" pseudo-number (i.e., Δ^0_2 real) is defined in [11, page 584]; see Figure 1.

We rephrase this definition in modern (but classical) language. Demuth introduces a notion of tests; let us call them *interval sequence tests*. In the following

<u>Определние.</u> Пусть $\mathcal{S}$ свойство псевдочисел, а $x \Delta y$ сегмент. Мы скажем, что $\mathcal{S}(\xi)$ выполнено для почти всех псевдочисел ξ (соотв. ξ из $x \Delta y$), если для всякого НЧ m существуют последовательность последовательностей рациональных сегментов $\{\{Q^n_k\}_k\}_n$ и последовательность неинфинитных рекурсивно перечислимых (р.п.) множеств НЧ $\{D_n\}_n$ такие, что $\forall n \ell \left(\sum_{1 \le k \le \ell \,\&\, \neg(k \in D_n)} |Q^n_k| < \frac{1}{2^{m+n}}\right)$ и для всякого ПЧ ξ (соотв. ПЧ ξ из $x \Delta y$) верно
$(\neg \exists n k (\neg(k \in D_n) \,\&\, \xi \in Q^n_k) \supset \mathcal{S}(\xi))$
(см. лемму 7 из [2]).

Fig. 1. [11, page 584]: Definition of interval sequence tests

let m, r, k range over the set $\mathbb{N}^+$ of positive integers. An interval sequence test uniformly in a number $m \in \mathbb{N}^+$ provides a computable sequence of rational intervals $(Q^m_r(k))_{r,k\in\mathbb{N}^+}$, and a uniformly c.e. sequence of finite sets $(E^m_r)_{r\in\mathbb{N}^+}$, such that

$$\lambda(\bigcup\{Q^m_r(k)\colon\ k \notin E^m_r\}) \le 2^{-(m+r)} \tag{3}$$

(where λ denotes Lebesgue measure). A real z *fails* the test if for each m there is r such that for some $k \notin E^m_r$ we have $z \in Q^m_r(k)$. In other words, for each m,

$$z \in \bigcup_r \bigcup_{k \notin E^m_r} Q^m_r(k). \tag{4}$$

Note that the class in (4) has measure at most 2^{-m}, hence the reals z failing the test form a null set. If z does not fail the test we say that z *passes* the test. Demuth says that a property $\mathcal{S}$ holds for *almost all* reals z if there is an interval sequence test (depending on $\mathcal{S}$) such that $\mathcal{S}$ holds for all z passing the test.

Recall that a Schnorr test is a Martin-Löf test $(G_m)_{m\in\mathbb{N}^+}$ such that λG_m is a computable real uniformly in m. We say that a real z fails the Schnorr test if $z \in \bigcap_m G_m$. (See [28, 3.5.8].)

Corollary 5 (with Hirschfeldt) *Interval sequence tests are uniformly equivalent to Schnorr tests relative to $\emptyset'$. That is, given a test of one kind, we can effectively determine a test of the other kind so that every real fails the first test if and only if it fails the second test.*

Proof. Firstly, suppose we are given an interval sequence test

$$(Q_r^m(k))_{r,k\in\mathbb{N}^+},\ (E_r^m)_{r\in\mathbb{N}^+}\ (m\in\mathbb{N}^+).$$

Let G_m be the class in (4). Then G_m is $\Sigma_1^0(\emptyset')$ uniformly in m, and λG_m is computable relative to $\emptyset'$ by (3).

Secondly, suppose we are given a Schnorr test $(G_m)_{m\in\mathbb{N}^+}$ relative to $\emptyset'$. Uniformly in m, using $\emptyset'$ as an oracle we can compute λG_m for each $m\in\mathbb{N}^+$. Hence we can for each $r,m\in\mathbb{N}^+$ determine $u_r\in\mathbb{N}$ and, by possibly splitting into pieces some intervals from G_m, a finite sequence of rational intervals $P_r^m(i)$, $u_r<i\leq u_{r+1}$, such that $\lambda(\bigcup_{u_r<i\leq u_{r+1}} P_r^m(i))\leq 2^{-(m+r)}$ and $G_m=\bigcup_r\bigcup_{u_r<i\leq u_{r+1}} P_r^m(i)$. By the Limit Lemma we have a computable sequence of intervals $P_r^m(i,t)$ and a computable sequence $u_r(t)$, $t\in\mathbb{N}$, such that for large enough t, $u_r(t)=u_r$ and $P_r^m(i,t)=P_r^m(t)$ for $i\leq u_r$. From this we can build an interval sequence test as required: the uniformly c.e. finite sets E_r^m correspond to the intervals we want to remove because of the mind changes of the approximations $u_r(t)$ and $P_r^m(i,t)$ for $i\leq u_r(t)$.

Above we quoted the abstract of the paper [11]. The first part of the second paragraph asserts that for almost every Δ_2^0 real z, the derivative $f'(z)$ is also Δ_2^0. Since f is Markov computable, it is easy to verify that

$$f'(z)\leq_T z',$$

namely, the value of the pseudo-derivative of f at z is computable in the Turing jump of z, whenever this pseudo-derivative exists. Thus $f'(z)$ is Δ_2^0 whenever z is low. By [18, Remark 10, part 3b], or [28, 3.6.26], there is a single Schnorr test relative to $\emptyset'$ (in fact, a Demuth test as defined in 11 below) such that each real z passing it is generalized low (i.e., $z'\leq z\oplus\emptyset'$). Thus, we know how to obtain the first part of that paragraph; the point is the *second* part, that the derivative can be obtained uniformly.

5 Denjoy alternative and Denjoy sets

For any function $g\colon [0,1]\to\mathbb{R}$, the reals z such that $\underline{D}g(z)=\infty$ form a null set. This well-known fact from classical analysis is usually proved via covering theorems, such as Vitali's or Sierpinskis's. Cater [8] has given an alternative proof of a stronger fact: the reals z where the right lower derivative $D_+(z)$ is infinite form a null set.

Demuth knew results of this kind. He studied the question which type of null class is needed to make an analog of this classic fact hold for Markov computable functions (see Definition 2). The following definition originates in [13]. As usual, for functions not defined everywhere we have to work with pseudo-derivatives defined in Subsection 3.2.

Definition 6. A real $z\in[0,1]$ is called Denjoy random (or a Denjoy set) if for no Markov computable function g we have $\underset{\sim}{D}g(z)=\infty$.

The paper [13] is entitled "The constructive analogue of a theorem by Garg on derived numbers". Garg's Theorem, a variant of the Denjoy-Young-Saks theorem discussed in Subsection 3.1, has the somewhat obscure reference [22].

The work of Demuth on the Denjoy alternative for effective functions is described in the preprint survey "Remarks on Denjoy sets" [17]. This is based on a talk Demuth gave at the Logic Colloquium 1988 in Padova, Italy (close to the end of communist era in 1989, it became easier to travel to the "West"). He later turned the preprint survey into the paper [19] with the same title, but it contains only part of the preprint survey.

In the preprint survey [17, page 6] it is shown that if $z \in [0,1]$ is Denjoy random, then for every computable $f\colon [0,1] \to \mathbb{R}$ the Denjoy alternative (1) holds at z. Combining this with the results in [7] we can now figure out what Denjoy randomness is, and also obtain a pleasing new characterization of computable randomness of reals through differentiability of computable functions. Joseph S. Miller also contributed to the theorem.

Theorem 7. *The following are equivalent for a real $z \in [0,1]$*

(i) z is Denjoy random.
(ii) z is computably random
(iii) for every computable $f\colon [0,1] \to \mathbb{R}$ the Denjoy alternative (1) holds at z.

Proof. (i)→(iii) is Demuth's result. For (iii)→(ii), let f be a nondecreasing computable function. Then f satisfies the Denjoy alternative at z. Since $\underline{D}f(z) \geq 0$, this means that $f'(z)$ exists. This implies that z is computably random by [7, Thm. 4.1].

The implication (ii)→(i) is proved by contraposition: if g is Markov computable and $\underset{\sim}{D}g(z) = \infty$ then one builds a computable betting strategy showing that z is not computably random. See [4, Thm. 15] or Section 2 of the Logic Blog [2] for proofs.

Remark 8. For the contraposition of the implication (ii)→(i), actually the weaker hypothesis on g suffices that $g(q)$ is a computable real uniformly in a rational $q \in I_{\mathbb{Q}}$.

We do not know at present how Demuth obtained (i)→(iii) of the theorem; a proof of this using classical language would be useful. However, a direct proof of the contraposition of (i)→(ii) is in [7, Thm. 3.6]: if z is not computably random then a martingale M with the so-called "savings property" succeeds on (the binary expansion of) a real z. The authors now build in fact a computable function g such that $\underline{D}g(z) = \underset{\sim}{D}g(z) = \infty$. Together with Remark 8 we obtain:

Corollary 9 *The following are equivalent for a real z:*

(i) For no function g such that $g(q)$ is uniformly computable for $q \in I_{\mathbb{Q}}$ we have $\underset{\sim}{D}g(z) = \infty$.
(ii) z is Denjoy random, i.e., for no Markov computable function g we have $\underset{\sim}{D}g(z) = \infty$.

(iii) For no computable function g we have $\underline{D}g(z) = \infty$.

This implies that the particular choice of Markov computable functions in Definition 6 is irrelevant. Similar equivalences stating that the exact level of effectivity of functions does not matter have been obtained in the article [7]. For instance, in [7, Thm. 7.3], extending a result of Demuth [11] the authors characterize Martin-Löf randomness via differentiability of effective functions of bounded variation. This works with any of the three particular effectiveness properties above: computable, Markov computable, and uniformly computable on the rationals. For nondecreasing *continuous* functions, the three effectiveness properties coincide as observed in [7, Prop. 2.2]

Because of Theorem 7 one could assert that Demuth studied computable randomness indirectly via his Denjoy sets. Presumably he didn't know the notion of computable randomness, which was introduced by Schnorr in [32], a monograph in German (see [28, Ch. 7]). Demuth also proved in [18, Thm. 2] that every Denjoy set that is AP (i.e., non ML-random) must be high. The analogous result for computable randomness was later obtained in [30]. There the authors also show a kind of converse: each high degree contains a computably random set that is not ML-random. This fact was apparently not known to Demuth.

6 Demuth randomness and weak Demuth randomness

As told above, Demuth knew that Denjoy randomness of a real z implies the Denjoy alternative at z for all computable functions. The next question for Demuth to ask was the following:

How much randomness for a real z is needed to ensure the Denjoy alternative at z for all Markov computable functions?

Demuth showed the following (see preprint survey, page 7, Thm 5, item 4), which refers to [12].

Corollary 10 *There is a Markov computable function f such that the Denjoy alternative fails at some ML-random real z. Moreover, f is extendable to a continuous function on $[0,1]$.*

This has been reproved by Bienvenu, Hölzl, Miller and Nies [4]. In their proof, z can be taken to be the least element of an arbitrary effectively closed set of reals containing all the ML-random reals but no computable reals. In particular, one can make z left-c.e.

6.1 The definition of (weak) Demuth randomness

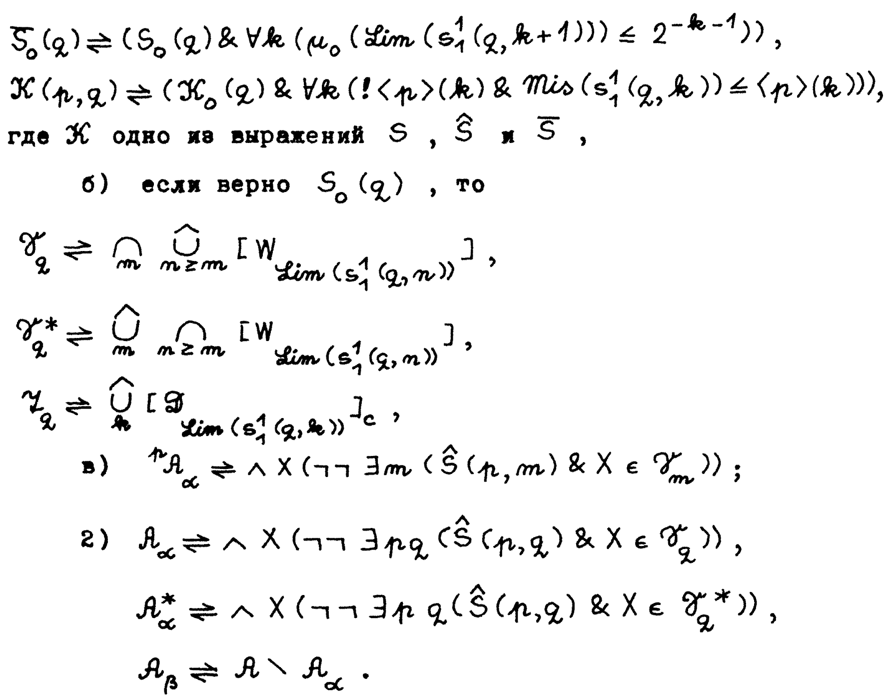
It was now clear to Demuth that a randomness notion stronger than Martin-Löf's was needed. Weak 2-randomness may have seemed ignoble to him because a Δ^0_2 real cannot be weakly 2-random. He needed a notion compatible with being Δ^0_2. Such a notion was introduced in the paper "Some classes of arithmetical reals" [14, page 458]. The definition is reproduced in the preprint survey [17, page 4].

For X a set of binary strings, let $[X]^{\prec}$ denote the collection of infinite binary sequences (sets) extending a string in X. In modern (but classical) language the definitions are as follows.

Definition 11. *A* Demuth test *is a sequence of c.e. open sets* $(S_m)_{m\in\mathbb{N}}$ *such that* $\forall m\, \lambda S_m \le 2^{-m}$, *and there is a function* $f\colon \mathbb{N} \to \mathbb{N}$ *with* $f \le_{\mathrm{wtt}} \emptyset'$ *such that* $S_m = [W_{f(m)}]^{\prec}$.

A set Z passes *the test if* $Z \notin S_m$ *for almost every* m. *We say that* Z *is* Demuth random *if* Z *passes each Demuth test.*

Recall that $f \le_{\mathrm{wtt}} \emptyset'$ if and only if f is ω-c.e., namely, $f(x) = \lim_t g(x,t)$ for some computable function g such that the number of stages t with $g(x,t) \neq g(x,t-1)$ is bounded in x. Hence the intuition is that we can change the m-th component S_m for a computably bounded number of times.


$\bar{S}_0(q) \rightleftharpoons (S_0(q) \,\&\, \forall k (\mu_0(\mathcal{L}im(s_1^1(q,k+1))) \le 2^{-k-1}))$,

$\mathcal{K}(p,q) \rightleftharpoons (\mathcal{K}_0(q) \,\&\, \forall k (!\langle p\rangle(k) \,\&\, \mathcal{M}is(s_1^1(q,k)) \le \langle p\rangle(k)))$,

где $\mathcal{K}$ одно из выражений S , $\hat{S}$ и $\bar{S}$,

б) если верно $S_0(q)$, то

$\gamma_q \rightleftharpoons \bigcap_m \hat{\bigcup}_{n\ge m} [W_{\mathcal{L}im(s_1^1(q,n))}]$,

$\gamma_q^* \rightleftharpoons \hat{\bigcup}_m \bigcap_{n\ge m} [W_{\mathcal{L}im(s_1^1(q,n))}]$,

$\chi_q \rightleftharpoons \hat{\bigcup}_k [\mathcal{D}_{\mathcal{L}im(s_1^1(q,k))}]_c$,

в) ${}^{p}\mathcal{A}_\alpha \rightleftharpoons \wedge X(\neg\neg\exists m(\hat{S}(p,m) \,\&\, X \in \gamma_m))$;

г) $\mathcal{A}_\alpha \rightleftharpoons \wedge X(\neg\neg\exists p q(\hat{S}(p,q) \,\&\, X \in \gamma_q))$,

$\mathcal{A}_\alpha^* \rightleftharpoons \wedge X(\neg\neg\exists p\, q(\hat{S}(p,q) \,\&\, X \in \gamma_q^*))$,

$\mathcal{A}_\beta \rightleftharpoons \mathcal{A} \setminus \mathcal{A}_\alpha$.

Fig. 2. [14, page 458]: $\mathcal{A}_\beta$ is the definition of Demuth randomness

Fig. 2 shows what the definition of Demuth randomness looks like in the 1982 paper [14, p. 458]. Demuth first defines tests via certain conditions γ_q, where q

is an index for a binary computable function $\phi_q(x,k)$. The condition γ_q holds for a real z if

$$\forall m \exists k \geq m \ z \text{ is in } [W_{\lim(s^1_1(q,k))}]$$

(where his notation $[X]$ is equivalent to our notation $[X]^{\prec}$). The expression in the subscript in the same line simply means $\lim_x \phi_q(x,k)$, which is the final version r of the test. A further condition $\mathcal{K}(p,q)$, involving an index p for a computable unary function, yields the bound $\phi_p(k)$ on the number of changes. The bound 2^{-k} on measures of the k-th component can be found in the top line. The notation $Mis(s^1_1(q,k))$ in Fig. 2 refers to the number of "mistakes", i.e. changes, and Demuth requires it be bounded by $\langle p\rangle(k)$, meaning $\phi_p(k)$.

If we apply the usual passing condition for tests, we obtain the following notion which only occurs in [14, page 458].

Definition 12. *We say that a set $Z \subseteq \mathbb{N}$ is* weakly Demuth random *if for each Demuth test $(S_m)_{m\in\mathbb{N}}$ there is an m such that $Z \notin S_m$.*

In [14] this is given by conditions γ^*_q, where the quantifiers are switched compared to γ_q:

$$\exists m \forall k \geq m \ z \text{ is in } [W_{\lim(s^1_1(q,k))}].$$

The class of arithmetical non-Demuth randoms is called $\mathcal{A}_\alpha$, and the class of arithmetical non-weakly Demuth randoms is called $\mathcal{A}^*_\alpha$. The complement of $\mathcal{A}_\alpha$ within the arithmetical reals is called $\mathcal{A}_\beta$ and, similarly, the complement of $\mathcal{A}^*_\alpha$ within the arithmetical reals is called $\mathcal{A}^*_\beta$. Later on, in the preprint survey, Demuth used the terms WAP sets (weakly approximable) for the non-Demuth randoms, and NWAP for the Demuth randoms and analogously, in an obviuous sense, the terms WAP* sets and NWAP* sets.

6.2 The Denjoy alternative for Markov computable functions

In the preprint survey [17, page 7, Thm 5, item 5)], Demuth states that Demuth randomness is sufficient to get the Denjoy alternative for Markov computable functions. This refers to the paper [15].

Corollary 13 *Let z be a Demuth random real. Then the Denjoy Alternative holds at z for every Markov computable function.*

This result is actually hard to pin down in [15]. Theorem 2 on page 399 comes close, but has some extra conditions not present in the original Denjoy alternative.

Remark 14. Franklin and Ng [21] introduced difference randomness, a concept much weaker than even weak Demuth randomness, but still stronger than Martin-Löf randomness. Bienvenu, Hölzl and Nies [4, Thm. 1] have shown that difference randomness is sufficient as a hypothesis on the real z in Theorem 13. No converse holds. They also show that the "randomness notion" to make the Denjoy Alternative hold for each Markov computable function is incomparable with ML-randomness!

6.3 Demuth randomness finds itself

We have seen that Demuth randomness of a real is way too strong for its original purpose, ensuring that the Denjoy alternative holds at this real for all Markov computable functions. However, Demuth randomness has recently turned out to be a very interesting notion on its own. Since it is stronger than ML-randomness but still allows the real to be Δ^0_2, it interacts nicely with computability theoretic notions. For instance, Kučera and Nies [25] proved that every c.e. set Turing below a Demuth random is strongly jump traceable (see [28, Section 8.4] for a definition of this lowness notion). Greenberg and Turetsky have recently provided a converse of this result of Kučera and Nies: every c.e. strongly jump traceable set has a Demuth random set Turing above. Nies [29] showed that each base for Demuth randomness is strongly jump traceable. Greenberg and Turetsky proved that this inclusion is proper.

Lowness for Demuth randomness and weak Demuth randomness have been characterized by Bienvenu et al. [3]. The former is given by a notion called BLR-traceability, in conjunction with being computably dominated. The latter is the same as being computable.

7 Late work related to computability theory

In the 1980s the mathematics department at Charles University had a seminar on recursion theory, which was based on Rogers' book [31] and some draft of Soare's book [33]. Because of this, Demuth became more interested in computability theory and the computational complexity of random sets.

7.1 Randomness and computational complexity

Demuth proved the following.

Corollary 15 *(i) Each Demuth random real z satisfies $z' \le z \oplus \emptyset'$.*
(ii) Each Demuth random set is of hyperimmune T-degree.

(i). Demuth [18, Remark 10, part 3b] gives a sketch of a proof. As mentioned, a full proof can be found in [28, 3.6.26].
(ii). Only a sketch of a proof is given in Remark 2 and Remark 11 of the preprint survey. It seems that a single Demuth test is sufficient here. An alternative proof can be derived from (i) and the result of Miller and Nies [28, Thm. 8.1.19] that no GL_1 set of hyperimmune-free degree is d.n.c.

It is of interest that Kučera and Demuth ([20], Theorem 18) proved a result very similar to a later result of Miller and Yu (see, [28], 5.1.14). For a Turing functional Φ and $n > 0$, consider the open set

$$S^A_{\Phi,n} = [\{\sigma \colon\ A\upharpoonright_n \preceq \Phi^\sigma\}]^\prec.$$

If A is ML-random then there is a constant c such that $\forall n\, \lambda S^A_{\Phi,n} \le 2^{-n+c}$.

7.2 Work on semigenericity

The following direction of Demuth's late work is only loosely connected to randomness. An incomputable set Z is called *semigeneric* [16] if every Π^0_1 class containing Z has a computable member. Any ML-random set is contained in a whole Π^0_1 class of ML-randoms, and is therefore not semigeneric. Intuitively, to be semigeneric means to be close to computable in the sense that the set cannot be separated from the computable sets by a Π^0_1 class.

Demuth proved in [16, Thm. 9] that if a set Z is semigeneric then any set B such that $\emptyset <_{tt} B \leq_{tt} Z$ is also semigeneric. In particular, its tt-degree only contains semigeneric sets.

Demuth and Kučera [20] studied semigenericity and its relationship with other types of genericity. We review some of their results.

Ceĭtin's notion of strong undecidability. Ceĭtin [9] called a set Z *strongly undecidable* if there is a computable function p such that for any computable set M and any index v of its characteristic function, $p(v)$ is defined and $Z\restriction_{p(v)} \neq M\restriction_{p(v)}$.

By Demuth and Kučera [20, Cor. 2], an incomputable set Z is semigeneric if and only if Z is not strongly undecidable. Furthermore, strong undecidability can be characterized by some kind of "uniform non-hyperimmunity": by [20, Thm. 5], a set Z is strongly undecidable if and only if there is a computable function f such that for each computable set M and any index v of its characteristic function, the symmetric difference $M \triangle Z$ is infinite, and its listing in order of magnitude dominated by the computable function with index $f(v)$.

Demuth and Kučera [20, Thm. 14] characterize the sets Z such that the Turing-degree of Z contains a strongly undecidable set: this happens precisely when there is a Π^0_2 class containing Z but no computable sets. So we have a weaker form of separation from the computable sets than for incomputable sets that are not semigeneric (i.e. strongly undecidable sets per se), where the separating class is Π^0_1 by definition.

The result [20, Thm. 14] was actually proved in terms of so-called V-coverings (where V stands for Vitali). A set Z is V-covered by a c.e. set of strings A if for all k there is a string $\sigma \in A$ such that $|\sigma| \geq k$ and $\sigma \prec Z$. It is easy to see that a class of sets $\mathcal{A}$ is a Π^0_2 class if and only if there is a c.e. set of strings B such that $\mathcal{A}$ is equal to the class of sets V-covered by B (see [28, 1.8.60]).

Connection to weak 1-genericity and hyperimmunity. Recall that a set Z is weakly 1-generic if Z is in each dense Σ^0_1 class (see [28, 1.8.47]). Clearly any weakly 1-generic set is semigeneric. The converse fails.

Demuth [16, Thm. 16] showed that a set Z is weakly 1-generic if and only if for any computable set M the symmetric difference $M \triangle Z$ is hyperimmune. Kurtz [23,24] proved that a Turing-degree contains a weakly 1-generic set if and only if it is hyperimmune. It follows from Kurtz's results, using a fact of Martin-Miller [26], that the weakly 1-generic T-degrees are closed upwards. As a corollary we have that there are weakly 1-generic Turing degrees which do contain ML-random sets and, thus, they can compute d.n.c. functions. On the other hand, Kučera and Demuth showed that the classes of 1-generic Turing degrees and of

Turing degrees of d.n.c. functions are disjoint. In fact, they proved in [20, Cor. 2] that no d.n.c. function (and, thus, no ML-random set) is computable in a 1-generic set (also see [28, 4.1.6]).

Demuth [16, Cor. 12] proved that any hyperimmune or co-hyperimmune set is semigeneric. Furthermore, he showed in [16, Thm. 21] that there is a semigeneric set E (even hypersimple) such that no set $A \leq_{tt} E$ is weakly 1-generic.

Final remarks. The searchable database at http://www.dml.cz contains most papers of Demuth. We plan to submit an extended journal version of this paper to the Bull. Symb. Logic in 2012.

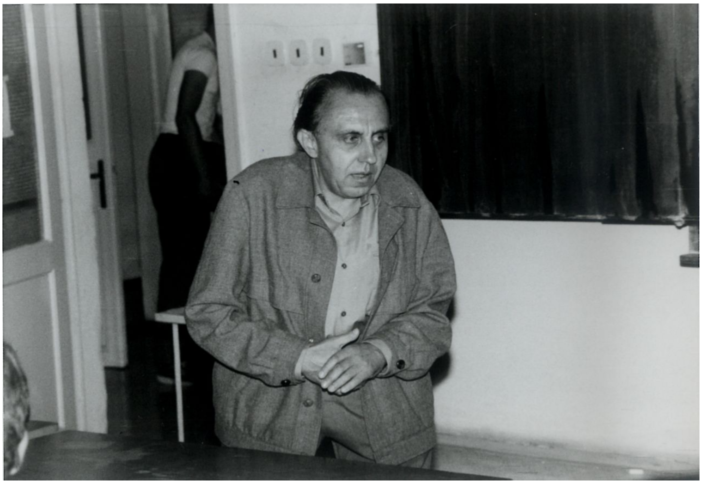


Fig. 3. Demuth by the blackboard

References

1. G. Alberti, M. Csörnyei, M. Laczkovich, and D. Preiss. The Denjoy-Young-Saks theorem for approximate derivatives revisited. *Real Anal. Exchange*, 26(1):485–488, 2000/01.
2. Various Authors. Logic Blog. http://dl.dropbox.com/u/370127/Blog/Blog2011.pdf, 2011.
3. L. Bienvenu, R. Downey, N. Greenberg, A. Nies, and D. Turetsky. Lowness for Demuth randomness. Unpublished, 20xx.
4. L. Bienvenu, R. Hoelzl, J. Miller, and A. Nies. The Denjoy alternative for computable functions. http://dl.dropbox.com/u/370127/papers/BHMNStacsFinal.pdf, 2012.
5. V. I. Bogachev. *Measure theory. Vol. I, II.* Springer-Verlag, Berlin, 2007.

6. V. Brattka, P. Hertling, and K. Weihrauch. A tutorial on computable analysis. In S. Barry Cooper, Benedikt Löwe, and Andrea Sorbi, editors, *New Computational Paradigms: Changing Conceptions of What is Computable*, pages 425–491. Springer, New York, 2008.
7. V. Brattka, J. Miller, and A. Nies. Randomness and differentiability. Submitted.
8. F. S. Cater. Some analysis without covering theorems. *Real Anal. Exchange*, 12(2):533–540, 1986/87.
9. G.S. Ceĭtin. On upper bounds of recursively enumerable sets of constructive real numbers. In *Proc. Steklov Inst. Math*, volume 113, pages 119–194, 1970.
10. O. Demuth. Constructive pseudonumbers. *Comment. Math. Univ. Carolinae*, 16:315–331, 1975.
11. O. Demuth. The differentiability of constructive functions of weakly bounded variation on pseudo numbers. *Comment. Math. Univ. Carolin.*, 16(3):583–599, 1975. Russian.
12. O. Demuth. The constructive analogue of the Denjoy-Young theorem on derived numbers. *Comment. Math. Univ. Carolinae*, 17(1):111–126, 1976.
13. O. Demuth. The constructive analogue of a theorem by Garg on derived numbers. *Comment. Math. Univ. Carolinae*, 21(3):457–472, 1980.
14. O. Demuth. Some classes of arithmetical real numbers. *Comment. Math. Univ. Carolin.*, 23(3):453–465, 1982.
15. O. Demuth. On the pseudodifferentiability of pseudo-uniformly continuous constructive functions from functions of the same type. *Comment. Math. Univ. Carolin.*, 24(3):391–406, 1983.
16. O. Demuth. A notion of semigenericity. *Comment. Math. Univ. Carolin.*, 28(1):71–84, 1987.
17. O. Demuth. Remarks on Denjoy sets (preprint). http://dl.dropbox.com/u/370127/DemuthPapers/Demuth88PreprintDenjoySets.pdf, 1988.
18. O. Demuth. Remarks on the structure of tt-degrees based on constructive measure theory. *Comment. Math. Univ. Carolin.*, 29(2):233–247, 1988.
19. O. Demuth. Remarks on Denjoy sets. In *Mathematical logic*, pages 267–280. Plenum, New York, 1990.
20. Osvald Demuth and A. Kučera. Remarks on 1-genericity, semigenericity and related concepts. *Commentationes Mathematicae Universitatis Carolinae*, 28(1):85–94, 1987.
21. Johanna N.Y. Franklin and Keng Meng Ng. Difference randomness. *Proceedings of the American Mathematical Society*. To appear.
22. K. M. Garg. An analogue of Denjoy's theorem. *Ganita*, 12:9–14, 1961.
23. S. Kurtz. *Randomness and genericity in the degrees of unsolvability*. Ph.D. Dissertation, University of Illinois, Urbana, 1981.
24. S. Kurtz. Notions of weak genericity. *J. Symbolic Logic*, 48:764–770, September 1983.
25. A. Kučera and A Nies. Demuth randomness and computational complexity. *Ann. Pure Appl. Logic*, 162:504–513, 2011.
26. D. A. Martin and W. Miller. The degrees of hyperimmune sets. *Z. Math. Logik Grundlag. Math.*, 14:159–166, 1968.
27. P. Martin-Löf. The definition of random sequences. *Inform. and Control*, 9:602–619, 1966.
28. A. Nies. *Computability and randomness*, volume 51 of *Oxford Logic Guides*. Oxford University Press, Oxford, 2009.
29. A. Nies. Computably enumerable sets below random sets. *Ann. Pure Appl. Logic*, 2011. To appear.

30. A. Nies, F. Stephan, and S. Terwijn. Randomness, relativization and Turing degrees. *J. Symbolic Logic*, 70(2):515–535, 2005.
31. H. Rogers, Jr. *Theory of Recursive Functions and Effective Computability.* McGraw-Hill, New York, 1967.
32. C.P. Schnorr. *Zufälligkeit und Wahrscheinlichkeit. Eine algorithmische Begründung der Wahrscheinlichkeitstheorie.* Springer-Verlag, Berlin, 1971. Lecture Notes in Mathematics, Vol. 218.
33. Robert I. Soare. *Recursively Enumerable Sets and Degrees.* Perspectives in Mathematical Logic, Omega Series. Springer–Verlag, Heidelberg, 1987.
34. K. Weihrauch. *Computable Analysis.* Springer, Berlin, 2000.