Random semicomputable reals revisited

Laurent Bienvenu, Alexander Shen

July 14, 2010

Abstract

The aim of this paper is to present a nice series of results, obtained in the papers of Chaitin [2], Solovay [5], Calude et al. [1], Kucera and Slaman [3]. This joint effort led to a full characterization of lower semicomputable random reals, both as those that can be expressed as a "Chaitin Omega" and those that are maximal for Solovay reducibility. The original proofs were somewhat involved; in this paper, we present these results in an elementary way, in particular requiring no prior knowledge of algorithmic randomness. We add also several simple observations relating lower semicomputable random reals and busy beaver functions.

1 Lower semicomputable reals and the $\preceq_1$-relation

A real number α is *lower semicomputable* if it is a limit of a computable increasing sequence of rational numbers. (Equivalent definition: if the set of all rational numbers less than α is enumerable).

There exist lower semicomputable but not computable reals. Corresponding sequences of rational numbers have non-computable convergence (there is no algorithm that produces $N(\varepsilon)$ given ε).

We want to classify computable sequences according to their convergence speed and formalize the intuitive idea "one sequence converges better (not worse) than the other one".

Definition 1 *Let $a_i \to \alpha$ and $b_j \to \beta$ be two computable strictly increasing sequences. We say that (a_i) [resp. (b_i)] is a* computable approximation from below *of α [resp. of β]. We say that the approximation $a_n \to \alpha$ converges "better" (not worse) than the approximation $b_n \to \beta$ if there exists a total computable function h such that*

$$\alpha - a_{h(i)} \leqslant \beta - b_i$$

for every i.

In other terms, we require that for each term of the second sequence one may algorithmically find a term of the first one that approaches the limit as close as the given term of the second sequence. Note that this relation is transitive (take the composition of two reducing functions).

In fact, the choice of specific sequences that approximate α and β is irrelevant: *any two increasing computable sequences that have the same limit, are equivalent with respect to this quasi-ordering*. Indeed, we can just wait to get a term of a second sequence that exceeds a given term of the first one. We can thus set the following definition.

Definition 2 *Let α and β be two lower semicomputable reals, and let (a_n), (b_n) be approximations of α and β respectively. If (a_n) converges better than (b_n), we write $\alpha \preceq_1 \beta$ (by the above paragraph, this does not depend on the particular approximations we chose).*

This definition can be reformulated in different ways. First, we can eliminate sequences from the defintion and say that $\alpha \preceq_1 \beta$ if there exists a partial computable function φ defined on all rational numbers $r < \beta$ such that

$$\varphi(r) < \alpha \text{ and } \alpha - \varphi(r) \leqslant \beta - r$$

for all of them (below, we refer to φ as the *reduction function*).

The following lemma is yet another characterization of the order (perhaps less intuitive but useful).

Lemma 3 *$\alpha \preceq_1 \beta$ if and only if $\beta - \alpha$ is lower semicomputable (or said otherwise, if and only if $\beta = \alpha + \rho$ for some lower semicomputable real ρ).*

Proof. To show the equivalence, note first that *for every two lower semicomputable reals α and ρ we have $\alpha \preceq_1 \alpha + \rho$*. Indeed, consider approximations (a_n) to α, (r_n) to ρ. Now, given a rational $s < \alpha + \rho$, we wait for a stage n such that $a_n + r_n > s$. Setting $\varphi(s) = a_n$, it is easy to check that φ is a suitable reduction function witnessing $\alpha \preceq_1 \alpha + \rho$.

It remains to prove the reverse implication: *if $\alpha \preceq_1 \beta$ then $\gamma = \beta - \alpha$ is lower semicomputable*. Indeed, if (b_n) is a computable approximation (from below) of β and φ is the reduction function that witnesses $\alpha \preceq_1 \beta$, then all terms $b_n - \varphi(b_n)$ are less than or equal to $\beta - \alpha$ and converge to $\beta - \alpha$. (The sequence may not be increasing, but still its limit is lower semicomputable, since all its terms do not exceed the limit, and we may replace nth term by the maximum of the first n terms.) $\square$

A special case of this Lemma: let $\sum a_i$ and $\sum b_i$ are computable series with non-negative terms (for $i > 0$; terms a_0 and b_0 are starting points and may be negative) that converge to (lower semicomputable) α and β. If $a_i \leqslant b_i$ for all $i > 0$, then $\alpha \preceq_1 \beta$, since $\beta - \alpha = \sum_i (b_i - a_i)$ is lower semicomputable.

The reverse statement is also true: if $\alpha \preceq_1 \beta$, one can find series $\sum a_i = \alpha$ and $\sum b_i = \beta$ with these properties ($0 \leqslant a_i \leqslant b_i$). Indeed, $\beta = \alpha + \rho$ for lower semicomputable ρ; take $\alpha = \sum a_i$ and $\rho = \sum b_i$ and let $b_i = a_i + r_i$.

In fact, stronger statement is also true; one of the series can be chosen in an arbitrary way. If $\alpha \preceq_1 \beta = \sum b_i$ for $b_i \geqslant 0$, then one can find a decomposition $\alpha = \sum a_i$ where $a_i \geqslant 0$ and $a_i \leqslant b_i$ for $i > 0$. [Hint: we construct a_i sequentially using the following invariant: the current approximation A to α should be at least as close (to α) as the current approximation of B (to β). Getting a new B, we use reduction to find next candidate for A and use it if the resulting a_i does not exceed b_i; if not, we let $a_i = b_i$ and keep the invariant. The invariant guarantees that the reduction will be used infinitely many times.]

The same is true for the other direction: if $\alpha = \sum a_i \preceq_1 \beta$ (for $a_i \geqslant 0$), then one can find computable $b_i \geqslant a_i$ such that $\beta = \sum b_i$. (Again all inequalities are for $i > 0$.) [Hint: use the same invariant; take $b_i = a_i$ unless some bigger b_i is found such the the reduction still gives something less than current value of A.]

2 Solovay reducibility and complete reals

Let α be a lower semicomputable but not computable real. By the results of the previous section, one has

$$\alpha \preceq_1 2\alpha \preceq_1 3\alpha \preceq_1 \ldots$$

because for all k the difference $(k+1)\alpha - k\alpha = \alpha$ is lower semicomputable (so Lemma 3 applies). The reverse relations are not true, because $k\alpha - (k+1)\alpha = -\alpha$ is not lower semicomputable (if it were, then α would be computable).

One may argue that this relation is therefore a bit too sharp. For example, α and 2α have essentially the same binary expansion (just shifted by one position), so one may want α and 2α to be equivalent. In other words, one may look for a less fine-grained relation. A natural candidate for this is *Solovay reducibility*.

Definition 4 (Solovay reducibility) *We say that $\alpha \preceq \beta$ if $\alpha \preceq_1 c\beta$ for some positive integer $c > 0$.*

(We may also say that $\alpha \preceq_c \beta$ if $\alpha \preceq_1 c\beta$. Then $\alpha \preceq \beta$ if $\alpha \preceq_c \beta$ for some c.)

Like for lower semicomputable semimeasures, one can easily prove the existence of maximal elements.

Theorem 5 *There exists a $\preceq$-biggest lower semicomputable real.*

Proof. Indeed, we can enumerate all lower semicomputable reals α_i in $[0,1]$ and then take their sum $\alpha = \sum w_i\alpha_i$ with computable positive weights w_i such that $\sum w_i$ converges. This α can be represented as $w_i\alpha_i$ plus lower semicomputable real, so $\alpha_i \preceq_1 (1/w_i)\alpha$. □

The biggest elements in $\preceq$-preorder are also called (Solovay) *complete* lower semicomputable reals. They have an alternative description:

Theorem 6 *Complete semicomputable reals are sums of universal semimeasures on $\mathbb{N}$ and vice versa.*

(Here we do not require the sum of a semimeasure to be less than 1; only finiteness is required.)

Proof. Any lower semicomputable real α is a sum of a computable series of rationals; this series (up to a constant factor that does not matter due to the definition of Solovay reducibility) is bounded by a universal semimeasure. The difference between the upper bound and the series itself is a lower semicomputable semimeasure, and therefore α is reducible to the sum of the universal semimeasure.

On the other hand, if $m_0, m_1, \ldots$ is a computable semimeasure and α is a (Solovay) complete real, then $m_0 \preceq_1 c\alpha$, so $\alpha = m_0/c + \tau$ for some integer $c > 0$ and lower semicomputable τ. Dividing m by c and then adding τ to one of the values, we get an universal semimeasure with sum α. □

Chaitin denoted the sum of a universal semimeasure by Ω. Since there is no such thing as *the* universal semimeasure, it is better to speak about Ω-reals defined as sums of universal semimeasures. We have shown therefore that the class of Ω-reals coincides with the class of complete lower semicomputable reals (with respect to Solovay reducibility).

It turns out that this class has third equivalent definition: Martin-Löf random semicomputable reals.

Theorem 7 *A lower semicomputable real is complete if and only if it is Martin-Löf random.*

We provide the proof of this result below.

3 Complete lower semicomputable reals are random

This in fact is Chaitin's theorem (randomness of Ω) usually proved by using complexity characterization of randomness. However, there is a direct argument that does not involves complexity (it is in the footnote in Levin's "Forbidden information" paper [4]; this footnote compressed the most important facts about lower semicomputable random reals into few lines!).

First, we prove that *there exists a lower semicomputable random real*. For that we consider an effectively open set U of measure less than (say) $1/2$ that covers all non-random reals in $[0,1]$. (The definition of Martin-Löf randomness guarantees that for every $\varepsilon > 0$ one can find an effectively open set that has measure less than ε and covers all non-random reals. We need only one such set for some $\varepsilon < 1$, say, $\varepsilon = 1/2$.) Then take the minimal element α in a closed set $[0,1] \setminus U$. This number is random (by definition) and lower semicomputable: compactness argument implies that any segment $[0,r]$ with rational $r < \alpha$ is covered by finitely many intervals of U and all those r's can be enumerated.

Second, we prove that *randomness is upward-closed*: if $\alpha \preceq \beta$ and α is random, then β is random. We may assume without less of generality that $\alpha \preceq_1 \beta$ (randomness does not change if we multiply the number by a rational factor).

So let $b_i \to \beta$ be a computable increasing sequence of rational numbers that converges to β. Assume that somebody gives us a sequence of rational intervals and guarantees that one of them covers β. How to transform it into a sequence of intervals that covers α (i.e., one of the intervals covers α) and has the same (or smaller) total length? If an interval appears that is entirely on the left of the current approximation b_i, it can be ignored (since it cannot cover β anyway). If the interval is entirely on the right of b_i, it can be postponed until the current approximation b_j enters it (this may happen or not, in the latter case the interval does not cover β). If the interval contains b_i, we can convert it into the interval of the same length that starts at a_j, where a_j is a rational approximation to α that has the same or better precision as b_i (as an approximation to β): if β is in the original interval, α is in the converted interval.

So randomness is upward-closed and therefore complete lower semicomputable reals are random.

Remark. The second part can be refomulated: if α and β are lower semicomputable reals and at least one of them is random, then the sum $\alpha + \beta$ is random, too. The reverse is also true: if both α and β are non-random, then $\alpha + \beta$ is not random. (We will see later different proofs of this statement.)

4 Randomness and prediction game

Before proving the reverse implication, let us make a digression and look more closely on the last argument. Consider the following game: an observer watches the increasing sequence of rationals (given one by one) and from time to time makes predictions of the following type: "the sequence will never increase more than by δ" (compared to its current value). Here δ is some non-negative rational. The observer wins this game if (1) one of the predictions remains true forever; (2) the sum of all numbers δ used in the predictions is small (less that some rational $\varepsilon > 0$ that is given to the observer in advance).

It is not required that at any moment a valid prediction exists, though one could guarantee this by making predictions with zero or very small (and decreasing fast) δ at each step. Note also that every prediction can be safely postponed, so we may assume that the next

prediction is made only if the previous one becomes invalid. Then at any moment there is only one valid prediction.

Theorem 8 *Let a_i be a computable increasing sequence of rational numbers that converges to some* (*lower semicomputable*) *real α. The observer has a computable winning strategy in the game if and only if α is not random.*

Proof. A computable winning strategy gives us a computable sequence of prediction intervals of small total measure and guarantees that one of these (closed) intervals contains α. On the other hand, having a sequence of intervals that covers α and has small total measure, we may use it for predictions. To make the prediction, we wait until the current approximation a_i gets into the already discovered part of the cover (this will happen since the limit is covered). Then for prediction we use maximal δ such that $(a_i, a_i + \delta)$ is covered completely at the moment, and then wait until this prediction becomes invalid. (Then the same procedure is used again). At some point α is covered by some interval in the sequence and the current approximation enters this interval; the prediction made after this moment will remain valid forever. The total length of all prediction interval is bounded by the measure of the cover (prediction intervals are disjoint and all are covered). □

A reformulation of the same observation that does not use game terminology:

Theorem 9 *Let a_i be a computable increasing sequence of rational numbers that converges to α. The number α is non-random if and only if for every rational $\varepsilon > 0$ one can effectively find a computable sequence $h_0, h_1, \ldots$ of non-negative rational numbers such that $\sum_i h_i < \varepsilon$ and $\alpha \leqslant a_i + h_i$ for some i.*

(Here the predictions h_i are made on every step; it does not matter since we may use zeros.)

There is a Solovay criterion of randomness (a constructive version of Borel–Cantelli lemma): a real number α is non-random if and only if there exists a computable sequence of intervals that have finite total measure and cover α infinitely many times. It also can be reformulated in the style of our previous theorem:

Theorem 10 *Let a_i be a computable increasing sequence of rational numbers that converges to α. The number α is non-random if and only if there exists a computable sequence $h_0, h_1, \ldots$ of non-negative rational numbers such that $\sum_i h_i < \infty$ and $\alpha \leqslant a + h_i$ for infinitely many i.*

Proof. If α is non-random, we apply the preceding result for $\varepsilon = 1, 1/2, 1/4, 1/8, \ldots$ and then combine the resulting sequences (with shifts $0, 1, 2, \ldots$ to the right). Each of them provides one value of i such that $\alpha \leqslant a + h_i$, and these values cannot be bounded due to shifts. On the other hand, if $\alpha \leqslant a + h_i$ for infinitely many i, we get a sequence of intervals with finite sum of measures that covers α infinitely many times (technically, we should replace closed intervals by slightly bigger open intervals). It remains to use Solovay's criterion or recall its proof: the effectively open set of points that are covered with multiplicity m has measure at most $O(1/m)$. □

The randomness criterion given in this section implies the following observation (that looks strange at first). Consider a sum of a computable series of positive rational numbers. *The randomness of the sum cannot change if all summands are changed by $\Theta(1)$-factor.* (Indeed, all h_i can be multiplied by a constant.)

Now let us prove that if α and β are non-random lower semicomputable reals, their sum $\alpha+\beta$ is non-random, too. (See the discussion in the previous section). The natural idea: make prediction in the game for α and β, and then take their sum as prediction for $\alpha+\beta$, does not work. (The problem is that the same prediction for α can be combined with many predictions for β and therefore will be counted many times in the sum.)

The solution is to make predictions for α and β of the same size. Let a_i and b_i be computable increasing sequences that converge to α and β. To make a prediction for the sequence a_i+b_i (after the previous prediction became invalid) we wait until the current approximations a_i and b_i become covered by the sequences of intervals that have small measures and cover α and β (such sequences exist since both α and β are non-random). We take the maximal h and k such that (a_i, a_i+h) and (b_i, b_i+k) are entirely covered (by the unions of currently appeared intervals). The prediction interval is then $(a_i+b_i, a_i+b_i+\delta)$ where $\delta = 2\min(h,k)$.

Let us show that one of the predictions will remain valid. Indeed, the limit values α and β are covered by some intervals. This interval appear in the sequences at some point and cover α and β with some neighborhoods, say, σ-neighborhoods. If the prediction is made after a_i and b_i enter these neighborhoods, δ is greater than 2σ and the prediction is final: a_i+b_i never increases more than by δ.

It remains to estimate the sum of all δs used during the prediction. It can be done using the following observation: if a prediction interval $(a_i+b_i, a_i+b_i+\delta)$ becomes invalid, this means that either a_i or b_i increased by $\delta/2$, so the total measure of the cover on the right of a_i and b_i decreased at least by $\delta/2$. (Here we use that $(a_i, a_i+\delta/2)$ and $(b_i, b_i+\delta/2)$ are covered completely because $\delta/2$ does not exceed both h and k: it is important here that we take the minimum.)

Let us return to the criterion for randomness provided by Theorem 9. The condition for non-randomness given there can be weakened in two aspects: first, we can replace computable sequence by a semicomputable sequence; second, we can replace h_i by the entire tail $h_i+h_{i+1}+\ldots$ of the corresponding series:

Theorem 11 *Let a_i be an increasing computable sequence of rational numbers that converges to α. Assume that for every rational $\varepsilon>0$ one can effectively find a lower semicomputable sequence h_i of non-negative reals such that $\sum_i h_i<\varepsilon$ and $\alpha \leqslant a_i+h_i+h_{i+1}+\ldots$ for some i. Then α is not random.*

Proof. Assume that for every i there is a painter who get h_i units of paint and the instruction to paint the line starting at a_i, going to the right and skipping the parts already painted by other painters (but making no other gaps). (Since h_i is only semicomputable, the paint is provided step by step.) The painted zone is an effectively open set of total measure $\sum_i h_i$. If $\alpha < a_i+h_i+h_{i+1}+\ldots$, then α is painted since we cannot use $h_i+h_{i+1}+\ldots$ paint starting between a_i and α and not crossing α. (In the condition we have $\leqslant$ instead of $<$, but this does not matter since we can increase all h_i, say, twice.) $\square$

This result implies one more criterion of randomness for lower semicomputable reals:

Theorem 12 *Let $\alpha=\sum d_i$ be a computable series of non-negative rational numbers. The number α is non-random if and only if for every $\varepsilon>0$ one can effectively produce an enumerable set $W\subset\mathbb{N}$ of indices such that (1) $\sum_{i\in W} d_i<\varepsilon$ and (2) W is co-finite, i.e., contains all sufficiently large integers.*

Proof. If α is not random, it can be covered by intervals with arbitrarily small total measure. It remains to consider the set W of all i such that $(d_0+\ldots+d_{i-1}, d_0+\ldots+d_{i-1}+$

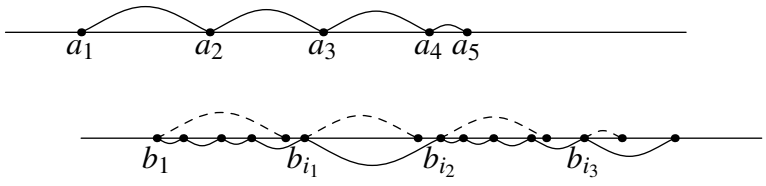
d_i) is entirely covered by one of those intervals. In the other direction the statement is a direct consequence of Theorem 11, just let $a_i = d_0 + \ldots + d_{i-1}$ and $h_i = d_i$. $\square$

This result shows again that the sum of two non-random lower semicomputable reals is not random (take the intersection of two sets W_1 and W_2 provided by this criterion for each of the reals).

5 Random lower semicomputable reals are complete

To prove this stamement, consider two lower semicomputable reals α and β presented as limits of increasing computable sequences $a_i \to \alpha$ and $b_i \to \beta$.

Let $h_i = a_{i+1} - a_i$ be the increases in the first sequence. We use h_i for prediction game against the second sequence. In other terms, we shift the interval (a_1, a_2) to get the interval of the same length that starts at b_1. Then we wait until b_i at the right of this interval appears; let it be b_{i_1}. Then shift the interval (a_2, a_3) to get the interval of the same length that starts at b_{i_1}; let b_{i_2} be the first b_i on the right of it, etc.



There are two possibilities: either

(1) observer wins in the prediction game, i.e., some of the shifted intervals covers the rest of b_i and the next b_{i_k} is undefined, or

(2) this process continues indefinitely.

In the second case $\alpha \preceq_1 \beta$ since the difference $\beta - \alpha$ is represented as a sum of a computable series ("holes" between neighbor intervals; note that the endpoints of the shifted intervals also converge to β).

So, if β is not complete, for complete α the second case is impossible, and the observer wins. In other terms, we get a computable sequence of (closed) intervals that covers β. Repeating the same argument for $\alpha/2$, $\alpha/4$,... (they are complete, too) we effectively get a cover of β with arbitrary small measure (since α has a computable upper bound even being non-computable), therefore β is not random.

Remark. This argument probably gives some quantitative connection between randomness deficiency of a random lower semicomputable real and another parameter that can be called *completeness deficiency*. It can be defined as follows: fix some complete α and for every β consider the minimal c such that $\alpha \preceq_1 c\beta$. (The connection also involves the complexity of the sequence of approximations to α.)

6 Slow convergence: Solovay functions

We have seen several results of the following type: the limit of an increasing computable sequence of rationals is random if and only if the convergence is slow. In this section we provide one more result of this type.

Consider a computable converging series $\sum r_i$ of positive rational numbers. Note that r_i is bounded by $O(m_i)$ where m_i is an a priori probability of integer i, therefore prefix complexity $\mathrm{K}(i) = -\log_2 m_i$ is bounded by $-\log_2 r_i + O(1)$. We say that the series $\sum r_i$

converges slowly in Solovay sense (has *Solovay property*) if this bound is tight infinitely often, i.e., if $r_i > \varepsilon m_i$ for some $\varepsilon > 0$ and for infinitely many i.

Historically the name *Solovay function* is used for a computable bound $S(i)$ for prefix complexity $\mathrm{K}(i)$ that is tight infinitely often, i.e., $\mathrm{K}(i) \leqslant S(i) + O(1)$ for every i and $\mathrm{K}(i) \geqslant S(i) - c$ for some c and for infinitely many values of i. Thus, a computable series $\sum a_i$ of positive rational numbers has Solovay property if and only if $i \mapsto -\log_2 a_i$ is a Solovay function.

Theorem 13 *Let $\alpha = \sum_i r_i$ be a computable converging series of positive rational numbers. The number α is random if and only if this series converges slowly in Solovay sense.*

In other terms, the sum is non-random if and only if the ratio r_i/m_i tends to 0.

Proof. Assume that $r_i/m_i \to 0$. Then for every ε we can let $h_i = \varepsilon m_i$ and get a lower semicomputable sequence that satisfies the conditions of Theorem 11. Therefore α is not random.

We can also prove that α is not complete (thus providing an alternative proof of its non-randomness). Recall the argument used in the proof of Theorem 6: if $r_i \leqslant m_i$, then $\sum r_i \preceq_1 \sum m_i$. And if $r_i \leqslant cm_i$, then $\sum r_i \preceq_c \sum m_i$. This remains true if the inequality $r_i \leqslant cm_i$ is true for all sufficiently large i. So for a fast (non-Solovay) converging series and its sum α we have $\alpha \preceq_c \sum m_i$ *for every* c. If α were complete, we would have also $\sum m_i \preceq_d \alpha$ for some d and therefore $\alpha \preceq_{cd} \alpha$ for some d and all $c > 0$. For small enough c we have $cd < 1/2$ and therefore $\alpha \preceq_{1/2} \alpha$. Then α should be computable, since we know how to find twice better approximation for any given one and can iterate this procedure.

It remains to show the reverse implication. Assuming that $\alpha = \sum r_i$ is not random, we need to prove that $r_i/m_i \to 0$. Consider the interval $[0, \alpha]$ split into intervals of length $r_0, r_1, \ldots$. Given an open cover of α with small measure, we consider those intervals (of length $r_0, r_1, \ldots$) that are completely covered (endpoints including). They form an enumerable set and the sum of their lengths does not exceed the measure of the cover. If the cover has measure 2^{-2n} for some n, we may multiply the corresponding r_i by 2^n and still their sum remains at most 2^{-n}. Note also that for large enough i the ith interval is covered (since it is close to α and α is covered). So for each n we get a semimeasure $M^n = M^n_0, M^n_1, \ldots$ such that $M^n_i/r_i > 2^n$ for sufficiently large i and $\sum_i M^n_i < 2^{-n}$. Taking the sum of all M^n, we get a lower semicomputable semimeasure M such that $r_i/M_i \to 0$. □

This result provides yet another proof that a sum of two non-random lower semicomputable reals is non-random (since the sum of two series that converge to 0 also converges to 0).

It shows also that Solovay functions exist (which is not immediately obvious from the definition; for comparison a direct proof is provided in the next section). Moreover, it shows that there exist computable non-decreasing Solovay functions: take a computable series of rational numbers with random sum and make this series non-increasing not changing the sum (by splitting too big terms into small pieces).

It also implies that slow convergence (in Solovay sense) is not a property of a series itself, but only of its sum. It looks strange: some property of a computable series (of positive rational numbers), *infinitely many terms come close to the upper bound provided by a priori probability*, depends only on the sum of this series. At first it seems that by splitting the terms into small parts we can destroy the property not changing the sum, but it is not so. In the next section we try to understand this phenomenon providing a direct proof for it (and as a byproduct get some improvements in the result of this section).

7 Solovay property as a property of the sum

First, let us note Solovay property is invariant under computable permutations. Indeed, computable permutation π changes a priori probability only by a constant factor: $m_{\pi(i)} = \Theta(m_i)$. Then let us consider grouping. Since we want to allow infinite groups, let us consider a computable series $\sum_{i,j} a_{ij}$ of non-negative rational numbers. Then

$$\alpha = \sum_{i,j} a_{ij} = (a_{00} + a_{01} + \ldots) + (a_{10} + a_{11} + \ldots) + \ldots = \sum_i A_i,$$

where $A_i = \sum_j a_{ij}$.

We want to show that A_i and a_{ij} are slowly converging series (in Solovay sense) at the same time. Note that slow convergence is permutation-invariant, so it is well defined for two-dimensional series.

However, some clarifications and restrictions are needed. First, $\sum A_i$ in general is not a computable series, it is only a lower semicomputable one. We can extend the definition of Solovay property: still $A_i = O(m_i)$, and we can ask whether this bound is $O(1)$-tight infinitely often. Second, such a general statement is not true: imagine that all non-negative terms are in the first group A_0 and all $A_1, A_2, \ldots$ are zeros. Then $\sum A_i$ does not have Solovay property while $\sum a_{ij}$ could have it.

Theorem 14 *Assume that each group A_i contains only finitely many non-zero terms. Then the properties $A_i/m_i \to 0$ and $a_{ij}/m_{ij} \to 0$ are equivalent.*

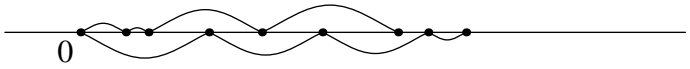
Here m_{ij} is the a priori probability of pair $\langle i, j\rangle$ (or its number in some computable numbering, this does not matter up to $O(1)$-factor). The convergence means that for every $\varepsilon > 0$ the inequality $a_{ij}/m_{ij} > \varepsilon$ is true only for finitely many pairs $\langle i, j\rangle$.

Proof. Let us recall first that $m_i = \sum_j m_{ij}$ up to a $O(1)$-factor. (Indeed, the sum in the right hand side is lower semicomputable, so it is $O(m_i)$ due to the maximality. On the other hand, already the first term m_{i0} is $\Omega(m_i)$.) So if a_{ij}/m_{ij} tends to zero, the ratio $A_i/\sum_j m_{ij}$ does the same (only finitely many pairs have $a_{ij} > \varepsilon m_{ij}$ and they appear only in finitely many groups).

It remains to show that $A_i/m_i \to 0$ implies $a_{ij}/m_{ij} \to 0$. (Here we need to use that only finitely many terms in each group are non-zero.) For this it is enough to construct some lower semicomputable $\tilde{m}_{ij}$ such that $a_{ij}/\tilde{m}_{ij} \to 0$, somehow using the fact that $A_i/m_i \to 0$. The natural idea would be to split m_i between $\tilde{m}_{ij}$ in the same proportion as A_i is split between a_{ij}. However, for this we need to know how many terms among $a_{i0}, a_{i1}, \ldots$ are non-zero, and in general this is a non-computable information. (For finite grouping this argument indeed works.)

So we go in the other direction. For some constant c we may let $\tilde{m}_{ij}$ to be ca_{ij} while this does not violate the property $\sum_j \tilde{m}_{ij} \leqslant m_i$. (When m_i increases, we increase $\tilde{m}_{ij}$ when possible.) If indeed $A_i/m_i \to 0$, for every constant c we have $cA_i \leqslant m_i$ for large i, so $a_{ij}/\tilde{m}_{ij} \leqslant 1/c$ for large i (and only finitely many pair $\langle i, j\rangle$ violate this requirement, because each A_i has only finitely many non-zero terms). So we are close to our goal ($a_{ij}/\tilde{m}_{ij} \to 0$): it remains to perform this construction for all $c = 2^{2n}$ and combine the resulting $\tilde{m}$ with coefficients 2^{-n}. □

As a corollary of Theorem 14 we see (in an alternative way) that Solovay property depends only on the sum of the series. Indeed, if $\sum_i a_i = \sum_j b_j$, these two series could be obtained by a different grouping of the third one (with combined partition points):



In this way we get not only the alternative invariance proof, but also can strengthen Theorem 13. It dealt with computable series of rational numbers. Now we consider series of rational terms but the summands are presented as lower semicomputable numbers and each has only finitely many different approximations. (So $r_i = \lim_n r(i,n)$ where r is a computable function of i and n with rational values which is non-decreasing as a function of n and for every i there are only finitely many different values $r(i,n)$.)

Theorem 15 *Let $\alpha = \sum_i r_i$ be a converging semicomputable series of rational numbers in the sense explained above. The number α is random if and only if this series converges slowly in Solovay sense* (*i.e., r_i/m_i does not converge to* 0).

Proof. Indeed, each r_i is a sum of a computable series of non-negative rational numbers with only finitely many non-zero terms. So we can split $\sum r_i$ into a double series not changing the sum (evidently) and Solovay property (due to Theorem 14). □

In particular, we get the following corollary: *an upper semicomputable function $n \mapsto f(n)$ with integer values is an upper bound for* $\mathrm{K}(n)$ *if and only if $\sum_n 2^{-f(n)}$ is finite*; *this bound is tight infinitely often if and only if this sum is random*.

Now we can show an alternative proof that all complete reals have Solovay property. First we observe that Solovay property is upward closed with respect to Solovay reducibility. Indeed, if $\sum a_i$ and $\sum b_i$ are computable series of non-negative rational numbers, and a_i converges slowly, then $\sum(a_i + b_i)$ converges slowly, too (its terms are bigger). So it remains to prove directly that at least one slowly converging series (or, in other terms, computable Solovay function) exists. To construct it, we watch how the values of a priori probability increase (it is convenient again to consider a priori probability of pairs):

$$\begin{array}{ccccc} m_{00} & m_{01} & m_{02} & m_{03} & \ldots \\ m_{10} & m_{11} & m_{12} & m_{13} & \ldots \\ m_{20} & m_{21} & m_{22} & m_{23} & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots \end{array}$$

and fill a similar table with rational numbers a_{ij} in such a way that $a_{ij}/m_{ij} \not\to 0$. How do we fill this table? For each row we compute the sum of current values $m_{i,*}$; if it crosses one of the thresholds $1/2, 1/4, 1/8\ldots$, we put the crossed threshold value into a-table (filling it with zeros from left to right while waiting for the next threshold crossed). In this way we guarantee that a_{ij} is a computable function of i and j; the sum of a-values is at most twice bigger than the sum of m-values; finally, in every row there exists at least one a-value that is at least half of the corresponding m-value. Logarithms of a-values form a Solovay function (and a_{ij} itself form a slowly convergent series).

Note that this construction does not give a *nondecreasing* Solovay function directly (it seems that we still need to use the arguments from the preceding section).

8 Busy beavers and convergence regulators

We had several definitions that formalize the intuitive idea of a "slowly converging series". However, the following one (probably the most straightforward) was not considered yet. If $a_n \to a$, for every $\varepsilon > 0$ there exists some N such that $|a - a_n| < \varepsilon$ for all $n > N$. The minimal N with this property (considered as a function of ε) is called *modulus of convergence*. A sequence (or a series) should be considered slowly converging if this function grows fast. Indeed, slow convergence (defined as Solovay property) could be equivalently characterized in these terms.

Definition 16 *Let m be a natural number. Define $BP(m)$ as the minimal value of N such that $\mathrm{K}(n) > m$ for all $n > N$.*

In other terms, $BP(m)$ is the maximal number n whose prefix complexity $\mathrm{K}(n)$ does not exceed m. Let us recall a natural interpretation of $BP(m)$ in terms of "busy beavers":

Theorem 17 *Fix an optimal prefix-free universal machine M. Let $T(m)$ be the maximal time needed for termination of (terminating) programs of length at most m. Then*

$$BP(m-c) \leqslant T(m) \leqslant BP(m+c)$$

for some c and all m.

Proof. First we prove that for all $t > T(m)$ the compexity of t is at least $m - O(1)$, thus showing that $T(m) \geqslant BP(m-c)$. Indeed, let $\mathrm{K}(t) = m - d$. Appending the shortest program for t to the prefix-free description of d, we get a prefix free description of the pair $\langle t, m\rangle$. Indeed, we can reconstruct t and $m-d$ from the shortest program of t (the second is its length) and then add d and get m. Then, knowing t and m, we wait t steps for all programs of length at most m, and then look for the first string that is not among their outputs. This string by construction has prefix complexity greater than m, and it is (prefix-freely) described by $m - d + O(\log d)$ bits, so $d = O(1)$.

On the other hand, $T(m)$ can be (prefix-freely) described by most long-playing program of size at most m (program determines its execution time), so $\mathrm{K}(T(m)) \leqslant m + O(1)$ and therefore $T(m) \leqslant BP(m + O(1))$. □

Now we can prove the equivalence of two notions of "slow convergence":

Theorem 18 *The computable series of non-negative rational numbers $\sum r_i$ has Solovay property ($\Leftrightarrow$ has a random sum) if and only its modulus of convergence satisfies the inequality $N(2^{-m}) > BP(m-c)$ for some c and for all m.*

Proof. Let $\alpha = \sum r_i = \lim a_i$, where $a_i = r_0 + \ldots + r_{i-1}$. Assume that α is random. We have to show that $|\alpha - a_i| < 2^{-m}$ implies $\mathrm{K}(i) > m - O(1)$ (and therefore $N(2^{-m}) \geqslant m - O(1)$). Since $\mathrm{K}(i) = \mathrm{K}(a_i) + O(1)$, it is enough to show that every rational 2^{-m}-approximation to α has complexity at least $m - O(1)$. This is a bit stronger condition than the condition $\mathrm{K}(\alpha_0 \ldots \alpha_{m-1}) \geqslant m - O(1)$ (used in Levin–Schnorr theorem) since now we consider *all* approximations, not only the prefix of the binary expansion. However, it can be proven in a similar way.

Let c be some integer. Consider an effectively open set U_c constructed as follows. For every rational r we consider neighborhood around r of radius $2^{-\mathrm{K}(r)-c}$; the set U_c is the union of these neighborhoods. (Since $\mathrm{K}(r)$ is upper semicomputable, it is indeed an effectively open set.) The total length of all intervals is $2 \cdot 2^{-c} \sum_r 2^{-\mathrm{K}(r)} \leqslant 2^{-(c-1)}$. Therefore, U_c form a Martin-Löf test, and random α does not belong to U_c for some c. This means that complexity of 2^{-m}-approximations of α is at least $m - O(1)$.

In the other direction we can use Schnorr–Levin theorem without any changes: if $N(2^{-m}) \geqslant BP(m-c)$, then $\mathrm{K}(i) \geqslant m - O(1)$ for every i such that a_i is a 2^{-m}-approximation to α. Therefore m-bit prefix of α has complexity at least $m - O(1)$, since knowing this prefix we can effectively find a_i that exceeds it (and the corresponding i). □

Question. Note that this theorem shows equivalence between two formalizations of an intuitive idea of "slowly converging series" (or three, if we consider Solovay reducibility

as a way to compare the rate of convergence). However, the proof goes through Martin-Löf randomness of the sum (where the series itself disappears). Can we have a more direct proof? Can we connect Solovay reducibility (not only completeness) to the properties of the modulus of convergence?

Reformulating the definition of $BP(m)$ in terms of a priori probability, we say that $BP(m)$ is the minimal N such that all $n > N$ have a priori probability less than 2^{-m}. However, in terms of a priori probability the other definition looks more natural: let $BP'(m)$ be the minimal N such that the total a priori probability of all $n > N$ is less than 2^{-m}. Generally speaking, $BP'(m)$ can be greater that $BP(m)$, but it turns out that it still can be used to characterize randomness in the same way:

Theorem 19 *Let a_i be a computable increasing sequence of rational numbers that converges to a random number α. Then $N(2^{-m}) \geqslant BP'(m-c)$.*

Proof. Since all $i > N(2^{-m})$ have the same a priori probability as the corresponding a_i (up to $O(1)$-factor), it is enough to show that the sum of a priori probabilities of all rational numbers in 2^{-m}-neighborhood of a random α is $O(2^{-m})$ (recall for all $i > N(2^{-m})$ corresponding a_i belong to this neighborhood).

As usual, we go in the other direction and cover all α such that the required inequality is not true for some m by a set of small measure. Let us fix some c and consider all intervals with rational endpoints that have the following property: *the sum of a priori probabilities of all rational numbers in this interval is at least c times bigger than its length.* It is enough to show that the union of all such intervals has measure $O(1/c)$, in fact, at most $2/c$.

It is enough to consider a finite union of intervals with this property. Moreover, we may assume that this union does not contain redundant intervals (that can be deleted without changing the union). Let us order all the intervals according to their left endpoints:

$$(l_0, r_0), (l_1, r_1), (l_2, r_2), \ldots$$

where $l_0 \leqslant l_1 \leqslant l_2 \leqslant \ldots$ It is easy to see that right endpoints go in the same order (otherwise one of the intervals would be redundant). So $r_0 \leqslant r_1 \leqslant r_2 \leqslant \ldots$ Now note that $r_i \leqslant l_{i+2}$, otherwise the interval (l_{i+1}, r_{i+1}) would be redundant. Therefore, intervals with even numbers $(l_0, r_0), (l_2, r_2), (l_4, r_4) \ldots$ are disjoint, and for each of them the length is c times less than the sum of a priori probabilities of rational numbers inside it. Therefore, the total length of these intervals does not exceed $1/c$, since the sum of all priori probabilities is at most 1. The same is true for intervals with odd numbers, so in total we get the bound $2/c$. □

Questions: how much could BP and BP' differ? How the last result follows from Schnorr–Levin theorem with a priori complexity? How all this can help to prove that $\sum_{x \in X} 2^{-|x|}$ is random for every enumerable prefix-free X that contains the domain of an optimal prefix-free function?

References

[1] Cristian Calude, Peter Hertling, Bakhadyr Khoussainov, and Yongge Wang. Recursively enumerable reals and Chaitin Omega numbers. In *Symposium on Theoretical Aspects of Computer Science (STACS 1998)*, volume 1373 of *Lecture Notes in Computer Science*, pages 596–606. Springer, 1998.

[2] Gregory Chaitin. Information-theoretical characterizations of recursive infinte strings. *Theoretical Computer Science*, 2:45–48, 1976.

[3] Antonin Kučera and Ted Slaman. Randomness and recursive enumerability. *SIAM Journal on Computing*, 31:199–211, 2001.

[4] Leonid Levin. Forbidden information.

[5] Robert Solovay. Draft of a paper (or series of papers) on Chaitin's work. Unpublished notes, 215 pages, 1975.