



ELSEVIER

Theoretical Computer Science 255 (2001) 125–149

Theoretical  
Computer Science

www.elsevier.com/locate/tcs

## Recursively enumerable reals and Chaitin $\Omega$ numbers<sup>☆,☆☆</sup>

Cristian S. Calude\*, Peter H. Hertling, Bakhadyr Khoussainov, Yongge Wang

*Department of Computer Science, University of Auckland, Private Bag 92019, Auckland, New Zealand*

Received April 1998; revised April 1999

Communicated by M. Ito

### Abstract

A real  $\alpha$  is called recursively enumerable if it is the limit of a recursive, increasing, converging sequence of rationals. Following Solovay (unpublished manuscript, IBM Thomas J. Watson Research Center, Yorktown Heights, New York, May 1975, 215 pp.) and Chaitin (IBM J. Res. Develop. 21 (1977) 350–359, 496.) we say that an r.e. real  $\alpha$  *dominates* an r.e. real  $\beta$  if from a good approximation of  $\alpha$  from below one can compute a good approximation of  $\beta$  from below. We shall study this relation and characterize it in terms of relations between r.e. sets. Solovay's (unpublished manuscript, IBM Thomas J. Watson Research Center, Yorktown Heights, New York, May 1975, 215 pp.)  $\Omega$ -like numbers are the maximal r.e. real numbers with respect to this order. They are random r.e. real numbers. The halting probability of a universal self-delimiting Turing machine (Chaitin's  $\Omega$  number (J. Assoc. Comput. Mach. 22 (1975) 329–340)) is also a random r.e. real. Solovay showed that any Chaitin  $\Omega$  number is  $\Omega$ -like. In this paper we show that the converse implication is true as well: any  $\Omega$ -like real in the unit interval is the halting probability of a universal self-delimiting Turing machine. © 2001 Elsevier Science B.V. All rights reserved.

### 1. Introduction

Algorithmic information theory, as developed by Chaitin [10, 11, 14], Kolmogorov [19], Solomonoff [29], Martin-Löf [22], and others (see [4]), gives a satisfactory description of the quantity of information of individual finite strings and infinite sequences. The same quantity of information may be organised in various ways; in order

<sup>☆</sup>An extended abstract of this paper has been presented at STACS 98, see [6]. To be consistent with [6] we use “recursively enumerable set”, “recursive set”, etc., instead of the more realistic terms “computably enumerable set”, “computable set”, etc., see [28].

<sup>☆☆</sup>The first and third authors were partially supported by AURC A18/XXXXX/62090/F3414056, 1996. The second author was supported by DFG Research Grant No. HE 2489/2-1, and the fourth author was supported by a UARC Post-Doctoral Fellowship.

\* Corresponding author.

*E-mail addresses:* cristian@cs.auckland.ac.nz (C.S. Calude), hertling@cs.auckland.ac.nz (P.H. Hertling), bm@cs.auckland.ac.nz (B. Khoussainov), wang@cs.auckland.ac.nz (Y. Wang).

to quantify the degree of organisation of the information in a string or a sequence, Bennett [1], Juedes et al. [16], and others, have considered the computational depth. Roughly speaking, the computational depth of an object is the amount of time required by an algorithm to derive the object from its shortest description. Bennett [1] showed that the characteristic sequence  $\chi_K$  of the halting problem is strongly deep, while no random sequence is strongly deep. Investigating this matter further, Juedes et al. [16] have considered the notion of “usefulness” of infinite sequences. A sequence  $\mathbf{x}$  is useful if all recursive sequences can be computed with oracle access to  $\mathbf{x}$  within a fixed recursive time bound. For example  $\chi_K$  is useful, while no recursive or random sequence is useful.

It is well known that the halting probability of a universal self-delimiting Turing machine, called Chaitin  $\Omega$  number (see [11, 15, 23, 4]), is random, but  $\chi_K$  is not;  $\Omega$  and  $\chi_K$  contain the same quantity of information but codified in vastly different ways. As we noted before,  $\chi_K$  is useful but  $\Omega$  is not useful in the sense of Juedes et al. [16]. However, when one is interested in approximating sequences<sup>1</sup>  $\Omega$  is more “useful” than  $\chi_K$ ; it is one of the aims of this paper to give a mathematical sense to this statement.

A real  $\alpha$  is called r.e. if it is the limit of a recursive increasing sequence of rationals. R.e. reals are extensively used in computable analysis, see [33, 18]. We will characterize r.e. reals in various ways. In order to compare the “usefulness” of r.e. reals for approximation purposes, Solovay [30] (see also [12]) has introduced the following notion. A real  $\beta$  *dominates* a real  $\alpha$  if there exists a partial recursive function  $f$  on rationals and a constant  $c > 0$  such that if  $p$  is a rational number less than  $\beta$ , then  $f(p)$  is (defined and) less than  $\alpha$ , and the inequality

$$c(\beta - p) \geq \alpha - f(p)$$

holds. In this case we write  $\alpha \leq_{dom} \beta$ . Informally, a real  $\beta$  *dominates* a real  $\alpha$  if from a good approximation of  $\beta$  from below one can compute a good approximation of  $\alpha$  from below. The relation  $\leq_{dom}$  is transitive and reflexive, hence it naturally defines a partially ordered set  $\langle \mathbf{R}_{r.e.}; \leq_{dom} \rangle$  whose elements are the  $=_{dom}$ -equivalence classes of r.e. reals. We shall see that this partially ordered set possesses natural properties. It has a minimum element which is the equivalence class containing exactly all recursive reals. It has a maximum element which is the equivalence class containing exactly all Chaitin  $\Omega$  numbers. It is an upper semilattice. The least upper bound of any two classes containing r.e. reals  $\alpha$  and  $\beta$ , respectively, is the class containing the r.e. real  $\alpha + \beta$ . This implies that addition is compatible with domination, that is if  $\alpha_1 \leq_{dom} \beta_1$  and  $\alpha_2 \leq_{dom} \beta_2$ , then  $\alpha_1 + \alpha_2 \leq_{dom} \beta_1 + \beta_2$ . We also stress that there is an important relationship between domination and randomness. Indeed, if  $\alpha \leq_{dom} \beta$ , then  $\beta$  is “more random” than  $\alpha$  in the sense that the Chaitin complexity of the first  $n$  digits of  $\alpha$  does *not* exceed the Chaitin complexity of the first  $n$  digits of  $\beta$  by more than a constant. In this respect, the partially ordered set  $\langle \mathbf{R}_{r.e.}; \leq_{dom} \rangle$  can be thought of as the world where effective objects (r.e. reals) are compared according to their degree

<sup>1</sup> As in constructive mathematics, see [3, 33, 18], and many other areas.

of randomness. The more random an effective object is, the closer it is to Chaitin  $\Omega$  numbers; the less random an effective object is, the closer it is to recursive reals. We study the domination relation  $\leq_{dom}$  further and characterize it in terms of certain reducibilities between r.e. sets.

Solovay [30] (see also [12]) called an r.e. real  $\Omega$ -like if it dominates every r.e. real. He showed that every Chaitin  $\Omega$  number is  $\Omega$ -like. In this paper we prove the converse implication by showing that any  $\Omega$ -like real in the unit interval is the halting probability of a universal self-delimiting Turing machine. This shows the strength of all  $\Omega$ 's for approximation purposes: from a good approximation of  $\Omega$  one can obtain a good approximation of any r.e. real, and no other r.e. reals have this property. Consequently, compared with a non- $\Omega$ -like r.e. real number, any number  $\Omega$  either contains more information or at least the information contained in  $\Omega$  is structured in a more useful way. However, the situation is different if we do not wish just to compute an arbitrary rational approximation of an r.e. real but rational approximations of a very special type, namely finite prefixes of its binary representation: we cannot compute with a total recursive function the first  $n$  digits of the r.e. real  $0.\chi_K$  (the characteristic sequence of the halting problem) from the first  $g(n)$  digits of  $\Omega$ , for any total recursive function  $g$ .

We give a brief summary of the paper. The next section introduces some basic notation. In Section 3 we define the program size complexity of strings, we define Chaitin  $\Omega$  numbers, and state some basic known results. We give a short proof of the well-known result that Chaitin  $\Omega$  numbers are random. In Section 4, we introduce r.e. reals and give several characterizations of r.e. reals. In this section we also introduce the domination relation and prove some basic and important facts about this relation and the induced partially ordered set  $\langle \mathbf{R}_{r.e.}; \leq_{dom} \rangle$ . In Section 5, we exhibit a relationship between this partially ordered set and Turing reducibility. We also give a characterization of  $\leq_{dom}$  in terms of certain reducibilities between sets of strings. In the next section, we prove that any  $\Omega$ -like real is in fact the halting probability of some universal self-delimiting Turing machine. We also consider the question whether  $\Omega$ -like reals are also good for computing the digits of the binary representation of r.e. reals. The last section contains some open problems and comments.

## 2. Notation

By  $\mathbf{N}$ ,  $\mathbf{Q}$  and  $\mathbf{R}$  we denote the set of non-negative integers, the set of rational numbers, and the set of real numbers, respectively. A sequence  $q_0, q_1, q_2, \dots$  of numbers (integers, rationals, or reals) is said to be increasing (to be non-decreasing) if  $q_i < q_{i+1}$  (if  $q_i \leq q_{i+1}$ ) for all  $i$ . If  $f$  and  $g$  are natural number functions, the formula  $f(n) \leq g(n) + O(1)$  means that there is a constant  $c > 0$  with  $f(n) \leq g(n) + c$ , for all  $n$ . If  $X$  and  $Y$  are sets, then  $f: X \overset{\circ}{\rightarrow} Y$  denotes a possibly partial function defined on a subset of  $X$ .

Let  $\Sigma = \{0, 1\}$  denote the binary alphabet.  $\Sigma^*$  is the set of (finite) binary strings,  $\Sigma^n$  is the set of binary strings of length  $n$ , and  $\Sigma^\omega$  the set of infinite binary sequences. The length of a string  $x$  is denoted by  $|x|$ ;  $\lambda$  is the empty string. Let  $<$  be the quasi-lexicographical order on  $\Sigma^*$  and let  $string_n (n \geq 0)$  be the  $n$ th string under this ordering. For strings  $x, y \in \Sigma^*$ ,  $xy$  is the concatenation of  $x$  and  $y$ . For a sequence  $\mathbf{x} = x_0x_1 \cdots x_n \cdots \in \Sigma^\omega$  and an integer number  $n \geq 0$ ,  $\mathbf{x}(n)$  denotes the initial segment of length  $n + 1$  of  $\mathbf{x}$  and  $x_i$  denotes the  $i$ th digit of  $\mathbf{x}$ , i.e.,  $\mathbf{x}(n) = x_0x_1 \cdots x_n$ . Lower case letters  $k, l, m, n$  will denote non-negative integers, and  $x, y, z$  strings. By  $\mathbf{x}, \mathbf{y}, \dots$  we denote infinite sequences from  $\Sigma^\omega$ ; finally, we reserve  $\alpha, \beta, \gamma$  for reals. A subset of  $\Sigma^*$  is called a language. Capital letters are used to denote languages. For languages  $A$  and  $B$ ,  $A \subseteq B$  denotes that  $A$  is a subset of  $B$ . We fix a standard recursive pairing function  $\lambda k, y \langle k, y \rangle$  defined on  $\mathbf{N} \times \Sigma^*$  with values in  $\Sigma^*$ . For a set  $A \subseteq \Sigma^*$  let  $A_k = \{x \mid \langle k, x \rangle \in A\}$ . For a language  $A$ ,  $\chi_A$  denotes the infinite characteristic sequence of  $A$ , that is,  $(\chi_A)_n = 1$  if  $string_n \in A$  and  $(\chi_A)_n = 0$  otherwise. For  $A \subseteq \Sigma^*$ ,  $A\Sigma^\omega$  denotes the set of sequences  $\{w\mathbf{x} \mid w \in A, \mathbf{x} \in \Sigma^\omega\}$ .

We assume that the reader is familiar with Turing machine computations, including oracle computations. We use  $K$  to denote the halting problem, that is,  $string_n \in K$  if and only if the  $n$ th Turing machine halts on the input  $string_n$ . We say that a language  $A$  is Turing reducible to a language  $B$ , and we write  $A \leq_T B$ , if there is an oracle Turing machine  $M$  such that  $M^B(string_n) = (\chi_A)_n$ , for all  $n \in \mathbf{N}$ . For further notation we refer to [4].

### 3. Complexity and randomness

In this section, we review some fundamentals of algorithmic information theory that we will use in this paper. We are especially concerned with self-delimiting (Chaitin/program-size) complexity and algorithmic randomness. Program-size complexity is a technical improvement of the original formulation of the descriptive complexity that was developed by Chaitin [11]; the advantage of the self-delimiting version is that it gives a precise characterization of algorithmic probability and random sequences.

Program-size complexity employs a slightly restricted model of deterministic Turing machine computation. A self-delimiting Turing machine  $M$  has a program tape, an output tape, and a work tape. Only 0's, 1's and blanks can ever appear on a tape. The program tape and the output tape are infinite to the right, while the worktape is infinite in both directions. Each tape has a scanning head. The program and output tape heads cannot move left, but the worktape head can move in both directions. The program tape is read-only, the output tape is write-only, and the worktape is read/write.

A self-delimiting Turing machine  $M$  starts in the initial state with a program  $x \in \Sigma^*$  on its program tape, the output tape blank, and the worktape blank. The left-most cell of the program tape is blank and the program tape head initially scans this cell. The program  $x$  lies immediately to the right of this cell and the rest of the program tape is blank. The output tape head initially scans the left-most cell of the output tape.

During each cycle of operation the machine reads the content of the scanned program tape cell and of the scanned worktape cell; it may halt, move the read head of the program tape one cell to the right, write a 0, a 1, or a blank on the scanned worktape cell, move the read/write head of the worktape one cell to the left or to the right, and write a 0 or a 1 on the scanned output tape cell and move the write head of the output tape one cell to the right. The machine changes state: the action performed and the next state are both functions of the present state and the contents of the two cells being scanned by the program tape head and by the worktape head.

If, after finitely many steps,  $M$  halts with the program tape head scanning the last bit of  $x$ , then the computation is a success, and we write  $M(x) < \infty$ ; the output of the computation is the string  $M(x) \in \Sigma^*$  that has been written on the output tape. Otherwise, the computation is a failure, we write  $M(x) = \infty$ , and there is no output.

In view of the above definition, a successful computation must end with the program tape head scanning the last bit of the program. Since the program tape head is read-only and cannot move left, this implies that for every self-delimiting Turing machine  $M$  the program set

$$PROG_M = \{x \in \Sigma^* \mid M(x) < \infty\}$$

is an *instantaneous code*, i.e., a set of strings with the property that no string in it is a proper prefix of another. Conversely, every prefix-free r.e. set of words is the domain of some self-delimiting Turing machine. It follows by Kraft's inequality that, for every self-delimiting Turing machine  $M$ ,

$$\Omega_M = \sum_{x \in PROG_M} 2^{-|x|} \leq 1.$$

The number  $\Omega_M$  is called the halting probability of  $M$ .

**Definition 3.1.** Let  $M$  be a self-delimiting Turing machine. The *program-size complexity* of the string  $x \in \Sigma^*$  (relatively to  $M$ ) is  $H_M(x) = \min\{|y| \mid y \in \Sigma^*, M(y) = x\}$ , where  $\min \emptyset = \infty$ .

It was shown by Chaitin [11] (see [4]) that there is a self-delimiting Turing machine  $U$  that is *universal*, in the sense that, for every self-delimiting Turing machine  $M$ , there is a constant  $c_M$  (depending upon  $M$ ) with the following property: if  $M(x) < \infty$ , then there is an  $x' \in \Sigma^*$  such that  $U(x') = M(x)$  and  $|x'| \leq |x| + c_M$ . Clearly, every universal self-delimiting machine produces every string. We denote by  $x^*$  the *canonical program* of  $x$ , i.e.,  $x^* = \min\{y \in \Sigma^* \mid U(y) = x\}$ , where the minimum is taken according to the quasi-lexicographical order. For two universal self-delimiting machines  $U$  and  $V$ , we see  $H_U(x) = H_V(x) + O(1)$ . The halting probability  $\Omega_U$  of a universal self-delimiting machine  $U$  is called *Chaitin  $\Omega$  number*; for more about  $\Omega_U$  see [2, 9, 7]. In the rest of the paper, unless stated otherwise, we will use a fixed universal self-delimiting machine  $U$  and will omit the subscript  $U$  in  $H_U(x)$  and  $\Omega_U$ . We will also abuse our notation

by identifying the real number  $\Omega$  with the infinite binary sequence which corresponds to  $\Omega$  (i.e., the infinite<sup>2</sup> binary expansion of  $\Omega$  without “0.”).

In the study of algorithmic information theory, we are often required to construct a self-delimiting Turing machine which satisfies certain properties. The following extension ([11]; see also, [5]) of Kraft’s inequality is very useful for this purpose:

**Theorem 3.2** (Kraft–Chaitin). *Given a recursive list of “requirements”  $\langle n_i, s_i \rangle$  ( $i \geq 0, s_i \in \Sigma^*, n_i \in \mathbf{N}$ ) such that  $\sum_i 2^{-n_i} \leq 1$ , we can effectively construct a self-delimiting Turing machine  $M$  and a recursive one-to-one enumeration  $x_0, x_1, x_2, \dots$  of words  $x_i$  of length  $n_i$  such that  $M(x_i) = s_i$  for all  $i$  and  $M(x) = \infty$  if  $x \notin \{x_i \mid i \in \mathbf{N}\}$ .*

Note that the halting probability of the machine  $M$  constructed in Theorem 3.2 is  $\Omega_M = \sum_i 2^{-n_i}$ .

We conclude this section with a brief discussion of (algorithmically) random infinite binary sequences.<sup>3</sup> Random sequences were originally defined by Martin-Löf [22] using constructive measure theory. Complexity-theoretic characterizations of random sequences have been obtained by Chaitin [11] (see also [21, 24]).

We use Chaitin’s [11] characterization: an infinite sequence  $\mathbf{x}$  is *random* if there is a constant  $c$  such that  $H(\mathbf{x}(n)) > n - c$ , for every integer  $n > 0$ . A slightly different characterization is contained in the next theorem. Martin-Löf’s definition is based on randomness tests. A Martin-Löf test is an r.e. set  $A \subseteq \Sigma^*$  satisfying the following measure-theoretical condition:

$$\mu(A_i \Sigma^\omega) \leq 2^{-i},$$

for all  $i \in \mathbf{N}$ .<sup>4</sup> Here  $\mu$  denotes the usual product measure on  $\Sigma^\omega$ , given by  $\mu(\{w\} \Sigma^\omega) = 2^{-|w|}$ , for  $w \in \Sigma^*$ .

**Theorem 3.3** (Chaitin [13]). *Let  $\mathbf{x} \in \Sigma^\omega$ . The following statements are equivalent:*

1. *The sequence  $\mathbf{x}$  is random.*
2. *We have:  $\lim_{n \rightarrow \infty} H(\mathbf{x}(n)) - n = \infty$ .*
3. *For every Martin-Löf test  $A$ ,  $\mathbf{x} \notin \bigcap_{i \geq 0} (A_i \Sigma^\omega)$ .*

**Theorem 3.4** (Chaitin [11]). *For every universal self-delimiting machine  $U$ , the halting probability  $\Omega_U$  is random.*

**Proof.** Let  $f$  be a recursive one-to-one function which enumerates  $PROG_U$ , the domain of  $U$ . Let  $\omega_k = \sum_{j=0}^k 2^{-|f(j)|}$ . Clearly,  $(\omega_k)$  is an increasing sequence of rationals converging to  $\Omega_U$ . Consider the binary expansion of  $\Omega_U = 0.\Omega_0\Omega_1 \dots$ .

We define a self-delimiting Turing machine  $M$  as follows: on input  $x \in \Sigma^*$  compute  $y = U(x)$  and the smallest number (if it exists)  $t$  with  $\omega_t \geq 0.y$ . Let  $M(x)$  be the first

<sup>2</sup> This expansion is unique since by Theorem 3.4,  $\Omega$  is random and, hence, irrational.

<sup>3</sup> The interested reader is referred to [4, 32] for more details.

<sup>4</sup> See [4] for a detailed motivation.

(in quasi-lexicographical order) word not belonging to the set  $\{U(f(0)), U(f(1)), \dots, U(f(t))\}$  if both  $y$  and  $t$  exist, and  $M(x) = \infty$  if  $U(x) = \infty$  or  $t$  does not exist.

If  $x \in \text{PROG}_M$  and  $x'$  is a word with  $U(x) = U(x')$ , then  $M(x) = M(x')$ . Applying this to an arbitrary  $x \in \text{PROG}_M$  and the canonical program  $x' = (U(x))^*$  of  $U(x)$  yields

$$H_M(M(x)) \leq |x'| = H_U(U(x)). \tag{1}$$

Furthermore, by the universality of  $U$  there is a constant  $c > 0$  with

$$H_U(M(x)) \leq H_M(M(x)) + c \tag{2}$$

for all  $x \in \text{PROG}_M$ . Now, fix a number  $n$  and assume that  $x$  is a word with  $U(x) = \Omega_0\Omega_1 \cdots \Omega_{n-1}$ . Then  $M(x) < \infty$ . Let  $t$  be the smallest number (computed in the second step of  $M$ ) with  $\omega_t \geq 0.\Omega_0\Omega_1 \cdots \Omega_{n-1}$ . We have

$$0.\Omega_0\Omega_1 \cdots \Omega_{n-1} \leq \omega_t < \omega_t + \sum_{s=t+1}^{\infty} 2^{-|f(s)|} = \Omega_U \leq 0.\Omega_0\Omega_1 \cdots \Omega_{n-1} + 2^{-n}.$$

Hence,  $\sum_{s=t+1}^{\infty} 2^{-|f(s)|} \leq 2^{-n}$ . This implies  $|f(s)| \geq n$ , for every  $s \geq t + 1$ . From the construction of  $M$  we conclude that  $H_U(M(x)) \geq n$ . Using (2) and (1) we obtain

$$\begin{aligned} n &\leq H_U(M(x)) \\ &\leq H_M(M(x)) + c \\ &\leq H_U(U(x)) + c \\ &= H_U(\Omega_0\Omega_1 \cdots \Omega_{n-1}) + c, \end{aligned}$$

which proves that the sequence  $\Omega_0\Omega_1 \cdots$  is random.  $\square$

#### 4. R.E. reals and domination

It is the aim of this section to compare the information contents of r.e. reals. A real  $\alpha$  is called *r.e.* if there is a recursive, increasing sequence of rationals which converges to  $\alpha$ .<sup>5</sup> We start with several characterizations of r.e.reals.

For a prefix-free set  $A \subseteq \Sigma^*$  we define a real number by

$$2^{-A} = \sum_{x \in A} 2^{-|x|},$$

which, due to Kraft's inequality, lies in the interval  $[0, 1]$ . For a set  $X \subseteq \mathbb{N}$  we define the number

$$2^{-X-1} = \sum_{n \in X} 2^{-n-1}.$$

This number also lies in the interval  $[0, 1]$ . If we disregard all finite sets  $X$ , which lead to rational numbers  $2^{-X-1}$ , we get a bijection  $X \mapsto 2^{-X-1}$  between the class of infinite

<sup>5</sup> Note that the property of being r.e. depends only on the fractional part of the real number.

subsets of  $\mathbf{N}$  and the real numbers in the interval  $(0, 1]$ . If  $0.y$  is the binary expansion of a real  $\alpha$  with infinitely many ones, then  $\alpha = 2^{-X_\alpha - 1}$  where  $X_\alpha = \{i \mid y_i = 1\}$ . Clearly, if  $X_\alpha$  is r.e., then the number  $2^{-X_\alpha - 1}$  is r.e., but the converse is not true as the Chaitin  $\Omega$  numbers show. We characterize r.e. reals  $\alpha$  in terms of prefix-free r.e. sets of strings<sup>6</sup> and in terms of the sets  $X_\alpha$ .

**Theorem 4.1.** *For a real  $\alpha \in (0, 1]$  the following conditions are equivalent:*

1. *The number  $\alpha$  is r.e.*
2. *There is a recursive, non-decreasing sequence of rationals  $(a_n)$  which converges to  $\alpha$ .*
3. *The set  $\{p \in \mathbf{Q} \mid p < \alpha\}$  of rationals less than  $\alpha$  is r.e.*
4. *There is an infinite prefix-free r.e. set  $A \subseteq \Sigma^*$  with  $\alpha = 2^{-A}$ .*
5. *There is an infinite prefix-free recursive set  $A \subseteq \Sigma^*$  with  $\alpha = 2^{-A}$ .*
6. *There is a total recursive function  $f : \mathbf{N}^2 \rightarrow \{0, 1\}$  such that*
  - (a) *If for some  $k, n$  we have  $f(k, n) = 1$  and  $f(k, n + 1) = 0$  then there is an  $l < k$  with  $f(l, n) = 0$  and  $f(l, n + 1) = 1$ .*
  - (b) *We have:  $k \in X_\alpha \Leftrightarrow \lim_{n \rightarrow \infty} f(k, n) = 1$ .*

**Proof.** It is obvious that conditions 1, 2 and 3 are equivalent that 4 implies 3, and 5 implies 4.

“1  $\Rightarrow$  5”: Let  $(a_j)$  be an increasing recursive sequence of rationals with limit  $\alpha$ . We can assume that  $0 < a_j < \alpha \leq 1$ , for all  $j$ . Using the recursive sequence  $(a_j)$  of rationals one can construct a non-decreasing recursive sequence  $(n_i)$  of positive integers and an increasing recursive sequence  $(k_j)$  of non-negative integers such that  $\sum_{i=0}^{k_j} 2^{-n_i} < a_j < 2^{-j} + \sum_{i=0}^{k_j} 2^{-n_i}$  for all  $j$ . Obviously  $\sum_{i=0}^{\infty} 2^{-n_i} = \alpha$ . By the Kraft–Chaitin Theorem (Theorem 3.2) there are a one-to-one recursive sequence  $(x_i)$  of words with  $|x_i| = n_i$ , for all  $i$ , and a self-delimiting Turing machine whose domain  $A$  is the set  $\{x_i \mid i \in \mathbf{N}\}$ . The set  $A$  is recursive because the sequence  $(|x_i|)$  of the lengths of the  $x_i$  is non-decreasing. We obtain  $\alpha = 2^{-A}$ .

“6  $\Rightarrow$  2”: We write  $f_{k,n}$  for  $f(k, n)$ . We claim that (a) implies

$$0.f_{0,n}f_{1,n} \dots f_{m,n} \leq 0.f_{0,n+1}f_{1,n+1} \dots f_{m,n+1}, \quad (3)$$

for all  $m, n$ . Assume that (3) is not true for some  $m$  and some  $n$ . Fix this number  $n$  and choose  $m$  minimal such that (3) is not true. Then, because of  $0.f_{0,n}f_{1,n} \dots f_{m-1,n} \leq 0.f_{0,n+1}f_{1,n+1} \dots f_{m-1,n+1}$  we must have  $f_{m,n} = 1$  and  $f_{m,n+1} = 0$ . By (a) there is a number  $l < m$  with  $f_{l,n} = 0$  and  $f_{l,n+1} = 1$ . Using  $0.f_{0,n}f_{1,n} \dots f_{l-1,n} \leq 0.f_{0,n+1}f_{1,n+1} \dots f_{l-1,n+1}$  we obtain

$$\begin{aligned} 0.f_{0,n}f_{1,n} \dots f_{m,n} &= 0.f_{0,n}f_{1,n} \dots f_{l-1,n} 0 f_{l+1,n} \dots f_{m,n} \\ &\leq 0.f_{0,n}f_{1,n} \dots f_{l-1,n} 1 \\ &\leq 0.f_{0,n+1}f_{1,n+1} \dots f_{l-1,n+1} 1 \end{aligned}$$

<sup>6</sup> Note that the prefix-free r.e. sets  $A \subseteq \Sigma^*$  are exactly the domains of self-delimiting Turing machines.

$$\begin{aligned} &\leq 0 \cdot f_{0,n+1} f_{1,n+1} \dots f_{l-1,n+1} 1 f_{l+1,n+1} \dots f_{m,n+1} \\ &= 0 \cdot f_{0,n+1} f_{1,n+1} \dots f_{m,n+1}. \end{aligned}$$

Contradiction! Thus, (3) is true for all  $m, n$ .

Define a recursive sequence  $(a_n)$  of rationals by  $a_n = 0 \cdot f_{0,n} f_{1,n} \dots f_{n,n}$ . Then, by (3),  $a_n \leq a_{n+1}$ , for all  $n$ . Let  $0 \cdot \mathbf{y} = 0 \cdot y_0 y_1 y_2 \dots$  be the binary expansion of  $\alpha$  which contains infinitely many ones. The assumption (a) implies that for each  $k$  the sequence  $f(k, 0), f(k, 1), f(k, 2), \dots$  changes its value only finitely many times (proof by induction over  $k$ ). Hence the limit  $\lim_{n \rightarrow \infty} f(k, n)$  exists. By (b), for each number  $L$  there is a number  $N_L$  with  $y_k = f_{k,n}$  for all  $k \leq L$  and  $n \geq N_L$ . Hence,  $|a_n - \alpha| \leq 2^{-L}$  for all  $n \geq \max\{L, N_L\}$ . We conclude  $\lim_{n \rightarrow \infty} a_n = \alpha$ . Hence,  $(a_n)$  is a non-decreasing recursive sequence of rationals converging to  $\alpha$ .

“1  $\Rightarrow$  6”: Let  $(a_n)$  be an increasing recursive sequence of rationals with limit  $\alpha$ . Again we can assume that  $0 < a_n < \alpha \leq 1$ , for all  $n$ . Define  $f$  such that  $0 \cdot f_{0,n} f_{1,n} f_{2,n} \dots$  is the binary expansion of  $a_k$  containing infinitely many ones, for each  $k$ . Then  $f$  is recursive. From  $a_n < a_{n+1}$  it follows that  $f$  satisfies (a). The equivalence  $k \in X_\alpha \Leftrightarrow \lim_{n \rightarrow \infty} f(k, n) = 1$  follows from  $\lim_{n \rightarrow \infty} a_n = \alpha$  and from  $a_n < \alpha$  for all  $n$ .  $\square$

In order to compare the information contents of r.e. reals, Solovay [30] has introduced the following definition.

**Definition 4.2** (Solovay [30], Chaitin [12]). The real  $\alpha$  is said to *dominate* the real  $\beta$  if there are a partial recursive function  $f: \mathbf{Q} \overset{\circ}{\rightarrow} \mathbf{Q}$  and a constant  $c > 0$  with the property that if  $p$  is a rational number less than  $\alpha$ , then  $f(p)$  is (defined and) less than  $\beta$ , and it satisfies the inequality

$$c(\alpha - p) \geq \beta - f(p).$$

In this case we write  $\alpha \geq_{dom} \beta$  or  $\beta \leq_{dom} \alpha$ .

Roughly speaking, a real  $\alpha$  dominates a real  $\beta$  if from any good approximation to  $\alpha$  from below (say, from a rational number  $p < \alpha$  with  $\alpha - p < 2^{-n}$ ) one can effectively obtain a good approximation to  $\beta$  from below (a rational number  $f(p) < \beta$  with  $\beta - f(p) < 2^{-n+\text{constant}}$ ). For r.e. reals this can also be expressed as follows.

**Lemma 4.3.** *An r.e. real  $\alpha$  dominates an r.e. real  $\beta$  if and only if there are recursive, increasing (or non-decreasing) sequences  $(a_i)$  and  $(b_i)$  of rationals and a constant  $c$  with  $\lim_{n \rightarrow \infty} a_n = \alpha$ ,  $\lim_{n \rightarrow \infty} b_n = \beta$ , and  $c(\alpha - a_n) \geq \beta - b_n$ , for all  $n$ .*

**Proof.** First, we assume that  $\alpha$  dominates  $\beta$ . Let  $(a_n)$  and  $(\tilde{b}_n)$  be increasing, recursive sequence of rationals converging to  $\alpha$  and  $\beta$ , respectively. Since  $\alpha$  dominates  $\beta$  there are a constant  $c > 0$  and an increasing, total recursive function  $g: \mathbf{N} \rightarrow \mathbf{N}$  with  $c(\alpha - a_n) \geq \beta - \tilde{b}_{g(n)}$ , for all  $n$ . Set  $b_n = \tilde{b}_{g(n)}$ .

On the other hand, assume now that  $(a_n)$  and  $(b_n)$  are recursive, non-decreasing sequences converging to  $\alpha$  and to  $\beta$ , respectively, and that  $c > 0$  is a rational constant

such that  $c(\alpha - a_n) \geq \beta - b_n$ , for all  $n$ . The sequences  $(\tilde{a}_n)$  and  $(\tilde{b}_n)$  defined by  $\tilde{a}_n = a_n - 2^{-n}$  and  $\tilde{b}_n = b_n - c2^{-n}$  are recursive, increasing, converge to  $\alpha$  and to  $\beta$ , respectively, and satisfy  $c(\alpha - \tilde{a}_n) \geq \beta - \tilde{b}_n$ , for all  $n$ . We define a partial recursive function  $f: \mathcal{Q} \xrightarrow{\circ} \mathcal{Q}$  as follows. Given  $p \in \mathcal{Q}$ , compute the smallest  $i$  such that  $\tilde{a}_i \geq p$ . If such an  $i$  has been found, set  $f(p) = \tilde{b}_i$ . If  $p < \alpha$ , then  $f(p)$  is defined and is smaller than  $\beta$ . It is clear that this function  $f$  shows  $\beta \leq_{dom} \alpha$ .  $\square$

Next, we prove a few results which will be useful in discussing the structure of r.e. reals under  $\leq_{dom}$ .

**Lemma 4.4.** *Let  $\alpha, \beta$  and  $\gamma$  be r.e. reals. Then the following conditions hold:*

1. *The relation  $\geq_{dom}$  is reflexive and transitive.*
2. *For every  $\alpha, \beta$  one has  $\alpha + \beta \geq_{dom} \alpha$ .*
3. *If  $\gamma \geq_{dom} \alpha$  and  $\gamma \geq_{dom} \beta$ , then  $\gamma \geq_{dom} \alpha + \beta$ .*
4. *For every non-negative  $\alpha$  and positive  $\beta$  one has  $\alpha \cdot \beta \geq_{dom} \alpha$ .*
5. *If  $\alpha$  and  $\beta$  are non-negative, and  $\gamma \geq_{dom} \alpha$  and  $\gamma \geq_{dom} \beta$ , then  $\gamma \geq_{dom} \alpha \cdot \beta$ .*

**Proof.** 1. This is straightforward from the definition.

2. For each rational number  $p < \alpha + \beta$ , we can compute two rational numbers  $p_1, p_2$  such that  $p_1 < \alpha, p_2 < \beta$  and  $p_1 + p_2 \geq p$  because  $\alpha$  and  $\beta$  are r.e. reals. Now  $\alpha + \beta - p \geq \alpha + \beta - p_1 - p_2 > \alpha - p_1$ . Hence  $\alpha + \beta \geq_{dom} \alpha$ .

3. Let  $c$  be a constant such that for each rational number  $p < \gamma$  we can find – in an effective manner – two rational numbers  $p_1 < \alpha$  and  $p_2 < \beta$  satisfying  $c(\gamma - p) \geq \alpha - p_1$  and  $c(\gamma - p) \geq \beta - p_2$ . Then  $2c(\gamma - p) \geq \alpha - p_1 + \beta - p_2 = \alpha + \beta - (p_1 + p_2)$ .

4. The assertion is clear for  $\alpha = 0$ . Let us assume that  $\alpha > 0$ . Given a rational  $p < \alpha\beta$  we can compute two positive rationals  $p_1 < \alpha$  and  $p_2 < \beta$  such that  $p_1 p_2 \geq p$ . For  $c = 1/\beta$  we obtain

$$c(\alpha\beta - p) \geq c(\alpha\beta - p_1 p_2) \geq c(\alpha\beta - p_1\beta) = \alpha - p_1.$$

5. It follows immediately from Lemma 4.3 that all r.e. reals dominate 0. Therefore the assertion is true if  $\alpha = 0$  or  $\beta = 0$ . Assume that  $\alpha > 0$  and  $\beta > 0$ , and that  $c$  is a constant such that, given a rational  $p < \gamma$ , we can find rationals  $p_1 < \alpha$  and  $p_2 < \beta$  satisfying  $c(\gamma - p) \geq \alpha - p_1$  and  $c(\gamma - p) \geq \beta - p_2$ . We can assume that  $p_1$  and  $p_2$  are positive. With  $\tilde{c} = c \cdot (\alpha + \beta)$  we obtain

$$\begin{aligned} \alpha\beta - p_1 p_2 &= \alpha(\beta - p_2) + p_2(\alpha - p_1) \\ &\leq (\alpha + p_2)c(\gamma - p) \\ &\leq (\alpha + \beta)c(\gamma - p) \\ &= \tilde{c}(\gamma - p). \quad \square \end{aligned}$$

**Corollary 4.5.** *The sum of a random r.e. real and an r.e. real is a random r.e. real. The product of a positive random r.e. real with a positive r.e. real is a random r.e. real.*

**Proof.** This follows from Lemma 4.4 and Theorem 4.9.  $\square$

**Corollary 4.6.** *The class of random r.e. reals is closed under addition. The class of positive random r.e. reals is closed under multiplication.*

The last corollary contrasts with the fact that addition and multiplication do not preserve randomness. For example, if  $\alpha$  is a random number, then  $1 - \alpha$  is random as well, but  $\alpha + (1 - \alpha) = 1$  is not random.

For two reals  $\alpha$  and  $\beta$ ,  $\alpha =_{dom} \beta$  denotes the conjunction  $\alpha \geq_{dom} \beta$  and  $\beta \geq_{dom} \alpha$ . For a real  $\alpha$ , let  $[\alpha] = \{\beta \in \mathbf{R} \mid \alpha =_{dom} \beta\}$ ;  $\mathbf{R}_{r.e.} = \{[\alpha] \mid \alpha \text{ is an r.e. real}\}$ . A real number  $\alpha$  is called *recursive* if there exists a recursive sequence  $(a_n)$  of rationals with  $|\alpha - a_n| \leq 2^{-n}$  for all  $n$ .

**Theorem 4.7.** *The structure  $\langle \mathbf{R}_{r.e.}; \leq_{dom} \rangle$  is an upper semilattice. It has a least element which is the  $=_{dom}$ -equivalence class containing exactly all recursive real numbers.*

Later (Theorem 6.6) we shall see that  $\langle \mathbf{R}_{r.e.}; \leq_{dom} \rangle$  also has a greatest element, which is the equivalence class containing exactly all Chaitin  $\Omega$  numbers.

**Proof.** Proof of Theorem 4.7. By Lemma 4.4 the structure  $\langle \mathbf{R}_{r.e.}; \leq_{dom} \rangle$  is an upper semilattice. Let  $\alpha$  be a recursive real. It is easy to see that there exists an increasing recursive sequence  $(a_n)$  of rationals with  $|\alpha - a_n| \leq 2^{-n}$ . Clearly, if  $\alpha$  dominates an r.e. real  $\beta$ , then also  $\beta$  must be recursive. Now let  $\beta$  be an r.e. real and  $(b_n)$  be an increasing recursive sequence of rationals converging to  $\beta$ . We define an increasing recursive sequence  $\tilde{a}_n$  of rationals by  $\tilde{a}_n = a_{g(n)}$  where  $g: \mathbf{N} \rightarrow \mathbf{N}$  is the total recursive function defined by  $g(-1) = -1$  and  $g(n) = \min\{m \mid m > g(n-1) \text{ and } 2^{-m} \leq b_{n+1} - b_n\}$  for all  $n \in \mathbf{N}$ . Then  $(\tilde{a}_n)$  tends to  $\alpha$ , and we see  $\beta - b_n > \alpha - \tilde{a}_n$  for all  $n \in \mathbf{N}$ . Hence,  $\beta$  dominates  $\alpha$ .  $\square$

We conclude this section with a result by Solovay on the relationship between the domination relation and the program-size complexity. First we prove a lemma.

**Lemma 4.8.** *For every  $c \in \mathbf{N}$  there is a positive integer  $N_c$  such that for every  $n \in \mathbf{N}$  and all strings  $x, y \in \Sigma^n$  with  $|0.x - 0.y| \leq c \cdot 2^{-n}$  we have*

$$|H(y) - H(x)| \leq N_c.$$

**Proof.** For  $n \geq 1$  and two strings  $x, y \in \Sigma^n$  with  $|0.x - 0.y| \leq c \cdot 2^{-n}$ , one can compute  $y$  if one knows the canonical program  $x^*$  of  $x$  and the integer  $2^n \cdot (0.x - 0.y) \in [-c, c]$ . Consequently, there is a constant  $N_c > 0$  depending only on  $c$  such that  $H(y) \leq H(x) + N_c$ , for all  $n \geq 1$ , and all  $x, y \in \Sigma^n$  with  $|0.x - 0.y| \leq c \cdot 2^{-n}$ . By symmetry, this is the assertion.  $\square$

**Theorem 4.9** (Solovay [30]). *Let  $\mathbf{x}, \mathbf{y} \in \Sigma^\omega$  be two infinite binary sequences such that both  $0.\mathbf{x}$  and  $0.\mathbf{y}$  are r.e. reals and  $0.\mathbf{x} \geq_{dom} 0.\mathbf{y}$ . Then*

$$H(\mathbf{y}(n)) \leq H(\mathbf{x}(n)) + O(1).$$

**Proof.** In view of the fact that  $0.\mathbf{x} \geq_{dom} 0.\mathbf{y}$ , there is a constant  $c \in \mathbf{N}$  such that, for every  $n \in \mathbf{N}$ , given  $\mathbf{x}(n)$ , we can find, in an effective manner, a rational  $p_n < 0.\mathbf{y}$  satisfying

$$\frac{2c}{2^{n+1}} \geq c \left( 0.\mathbf{x} - 0.\mathbf{x}(n) - \frac{1}{2^{n+1}} \right) \geq 0.\mathbf{y} - p_n > 0.$$

Let  $z_{p_n}$  be the first  $n + 1$  digits of the binary expansion of  $p_n$ . Then

$$0 \leq 0.\mathbf{y}(n) - 0.z_{p_n} \leq \frac{2c + 1}{2^{n+1}}.$$

Hence, by Lemma 4.8,

$$H(\mathbf{y}(n)) \leq H(z_{p_n}) + O(1) \leq H(\mathbf{x}(n)) + O(1). \quad \square$$

## 5. More about domination

In this section we compare the domination relation with Turing reducibility and characterize it in terms of certain reducibilities on r.e. sets.

For every infinite sequence  $\mathbf{x} \in \Sigma^\omega$  such that  $0.\mathbf{x}$  is an r.e. real, let  $A_{\mathbf{x}} = \{v \in \Sigma^* \mid 0.v \leq 0.\mathbf{x}\}$  and  $A_{\mathbf{x}}^\# = \{\text{string}_n \mid x_n = 1\}$ . Then, obviously,  $A_{\mathbf{x}}$  is an r.e. set which is Turing equivalent to  $A_{\mathbf{x}}^\#$ .<sup>7</sup> In the following, we establish the relationship between domination and Turing reducibility.

**Lemma 5.1.** *Let  $\mathbf{x}, \mathbf{y} \in \Sigma^\omega$  be two infinite binary sequences such that both  $0.\mathbf{x}$  and  $0.\mathbf{y}$  are r.e. reals and  $0.\mathbf{x} \geq_{dom} 0.\mathbf{y}$ . Then  $A_{\mathbf{y}} \leq_T A_{\mathbf{x}}$ .*

**Proof.** Without loss of generality, we may assume that

$$\mathbf{x}, \mathbf{y} \notin \{x0000 \dots, x1111 \dots \mid x \in \Sigma^*\}. \quad (4)$$

Let  $f: \Sigma^* \xrightarrow{o} \Sigma^*$  be a partial recursive function and  $c \in \mathbf{N}$  a constant satisfying the following inequality for all  $n > 0$ :

$$0 < 0.\mathbf{y} - 0.f(\mathbf{x}(n-1)) \leq \frac{c}{2^n}.$$

Given a string  $z$  we wish to decide whether  $z \in A_{\mathbf{y}}$ . Using the oracle  $A_{\mathbf{x}}^\#$  we compute the least  $i \geq 0$  such that either

$$0.f(\mathbf{x}(i-1)) \geq 0.z \quad \text{or} \quad 0.z - 0.f(\mathbf{x}(i-1)) > \frac{c}{2^i}.$$

<sup>7</sup> Note that  $A_{\mathbf{x}}^\#$  is not necessarily an r.e. set.

Such an  $i$  must exist in view of  $\mathbf{y} \notin \{x0000 \cdots, x1111 \cdots \mid x \in \Sigma^*\}$ . Finally, if  $0.f(\mathbf{x}(i-1)) \geq 0.z$ , then  $z \in A_{\mathbf{y}}$ ; otherwise  $z \notin A_{\mathbf{y}}$ .  $\square$

Does the converse of Lemma 5.1 hold true? A negative answer will be given in Corollary 6.12.

Let  $\langle RE; \leq_T \rangle$  denote the upper semi-lattice structure of the class of r.e. sets under the Turing reducibility.

**Definition 5.2.** A strong homomorphism from a partially ordered set  $(X, \leq)$  to another partially ordered set  $(Y, \leq)$  is a mapping  $h: X \rightarrow Y$  such that

1. For all  $x, x' \in X$ , if  $x \leq x'$ , then  $h(x) \leq h(x')$ .
2. For all  $y, y' \in Y$ , if  $y \leq y'$ , then there exist  $x, x'$  in  $X$  such that  $x \leq x'$  and  $h(x) = y$ ,  $h(x') = y'$ .

**Theorem 5.3.** There is a strong homomorphism from  $\langle \mathbf{R}_{r.e.}; \leq_{dom} \rangle$  onto  $\langle RE; \leq_T \rangle$ .

**Proof.** By Lemma 4.4 the structure  $\langle \mathbf{R}_{r.e.}; \leq_{dom} \rangle$  is an upper semi-lattice. Every  $=_{dom}$ -equivalence class of r.e. reals contains an r.e. real of the form  $0.\mathbf{x}$ . Lemma 5.1 shows that by  $0.\mathbf{x} \mapsto A_{\mathbf{x}}$  one defines a mapping from  $\langle \mathbf{R}_{r.e.}; \leq_{dom} \rangle$  to  $\langle RE; \leq_T \rangle$ , which satisfies the first condition in the definition of a strong homomorphism. We have to show that this mapping satisfies also the second condition. Let  $B, C \subseteq \Sigma^*$  be two r.e. sets with  $C \leq_T B$ . We have to show that there are two r.e. reals  $0.\mathbf{x}$  and  $0.\mathbf{y}$  with the following three properties: (I)  $0.\mathbf{x}$  dominates  $0.\mathbf{y}$ , (II)  $A_{\mathbf{x}}$  is Turing equivalent to  $B$ , and (III)  $A_{\mathbf{y}}$  is Turing equivalent to  $C$ .

We can assume that the sets  $B$  and  $C$  are infinite and have the form  $B = \{string_n \mid n \in \tilde{B}\}$  and  $C = \{string_n \mid n \in \tilde{C}\}$  where  $\tilde{B}$  is an r.e. set of odd natural numbers and  $\tilde{C}$  is an r.e. set of even natural numbers. Then the set  $D = B \cup C$  is Turing equivalent to  $B$ . We define two sequences  $\mathbf{x}, \mathbf{y} \in \Sigma^\omega$  by  $\mathbf{x} = \chi_D$  and  $\mathbf{y} = \chi_C$ . The real numbers  $0.\mathbf{x}$  and  $0.\mathbf{y}$  are r.e. They have the properties (II) and (III) because  $A_{\mathbf{x}}$  is Turing equivalent to  $A_{\mathbf{x}}^\# = D$ , which is Turing equivalent to  $B$ , and  $A_{\mathbf{y}}$  is Turing equivalent to  $A_{\mathbf{y}}^\# = C$ . It is left to show that  $0.\mathbf{x}$  dominates  $0.\mathbf{y}$ . Let

$$b_0, b_1, b_2, \dots \quad \text{and} \quad c_0, c_1, c_2, \dots$$

be one-to-one recursive enumerations of  $\tilde{B}$  and of  $\tilde{C}$ , respectively. The rational sequences

$$\left( \sum_{i=0}^n (2^{-b_i} + 2^{-c_i}) \right)_{n \geq 0} \quad \text{and} \quad \left( \sum_{i=0}^n 2^{-c_i} \right)_{n \geq 0}$$

are increasing, recursive, converge to  $0.\mathbf{x}$  and to  $0.\mathbf{y}$ , respectively, and satisfy the inequality

$$0.\mathbf{x} - \sum_{i=0}^n (2^{-b_i} + 2^{-c_i}) \geq 0.\mathbf{y} - \sum_{i=0}^n 2^{-c_i}.$$

Hence, by Lemma 4.3, the number  $0.\mathbf{x}$  dominates  $0.\mathbf{y}$ .  $\square$

We continue with the characterization of the domination relation between r.e. real numbers in terms of prefix-free r.e. sets of words. We consider only infinite prefix-free r.e. sets. By *R.E.* we denote the class of all infinite prefix-free r.e. subsets of  $\Sigma^*$ . First, we consider a relation between r.e. sets which is very close to the domination relation, but will turn out to be not equivalent.

**Definition 5.4.** Let  $A, B \in R.E.$  The set  $A$  *strongly simulates*  $B$  (shortly,  $B \leq_{ss} A$ ) if there is a partial recursive function  $f: \Sigma^* \xrightarrow{o} \Sigma^*$  which satisfies the following conditions:

1.  $A = \text{dom}(f)$  and  $B = f(A)$ ,
2. there is a constant  $c > 0$  such that  $|x| \leq |f(x)| + c$ , for all  $x \in A$ .

If  $A \leq_{ss} B$  and  $B \leq_{ss} A$ , then we say that  $A$  and  $B$  are  $\sim_{ss}$ -equivalent.

The following lemma follows immediately from the definition.

**Lemma 5.5.** *The relation  $\leq_{ss}$  is reflexive and transitive.*

Hence, the relation  $\leq_{ss}$  defines a partially ordered set  $\langle R.E._{ss}; \leq_{ss} \rangle$  where  $R.E._{ss}$  is the set of  $\sim_{ss}$ -equivalence classes of *R.E.* Our next goal is to see how the strong simulation relation  $\leq_{ss}$  and  $\leq_{dom}$  are related.

**Lemma 5.6.** *If  $A, B$  are infinite prefix-free r.e. sets and  $B \leq_{ss} A$ , then  $2^{-A}$  dominates  $2^{-B}$ .*

**Proof.** Let  $(x_i)$  be a one-to-one recursive enumeration of  $A$ . Let  $f$  be a function and  $c > 0$  be a constant as in Definition 5.4. For each  $n$  and each  $y \in B \setminus \{f(x_0), \dots, f(x_n)\}$  there is a word  $x \in A \setminus \{x_0, \dots, x_n\}$  with  $y = f(x)$  and  $|x| \leq |f(x)| + c$ . Hence,

$$\begin{aligned} 2^{-B} - 2^{-\{f(x_0), \dots, f(x_n)\}} &= 2^{-(B \setminus \{f(x_0), \dots, f(x_n)\})} \\ &\leq 2^c \cdot 2^{-(A \setminus \{x_0, \dots, x_n\})} \\ &= 2^c \cdot (2^{-A} - 2^{-\{x_0, \dots, x_n\}}). \end{aligned}$$

We conclude that  $2^{-A}$  dominates  $2^{-B}$ .  $\square$

The next result shows that in some sense the converse implication in Lemma 5.6 is true as well. It will also be important in the following section.

**Theorem 5.7.** *Let  $\alpha$  be an r.e. real in the interval  $(0, 1]$ , and  $B$  be an infinite prefix-free r.e. set. If  $\alpha$  dominates  $2^{-B}$ , then there is an infinite prefix-free r.e. set  $A$  with  $\alpha = 2^{-A}$  and  $B \leq_{ss} A$ .*

**Proof.** We assume that  $\alpha$  dominates  $2^{-B}$  and wish to construct an infinite prefix-free r.e. set  $A$  with  $\alpha = 2^{-A}$ . Let  $(y_i)$  be a one-to-one recursive enumeration of  $B$  and  $(a_n)$

be an increasing recursive sequence of positive rationals converging to  $\alpha$ . In view of the domination property of  $\alpha$ , there are an increasing, total recursive function  $f : \mathbf{N} \rightarrow \mathbf{N}$  and a constant  $c \in \mathbf{N}$  such that, for each  $n \in \mathbf{N}$ ,

$$2^c \cdot (\alpha - a_n) \geq 2^{-B} - \sum_{i=0}^{f(n)} 2^{-|y_i|}. \quad (5)$$

Without loss of generality, we may assume that

$$a_0 > \sum_{i=0}^{f(0)} 2^{-|y_i| - c} \quad (6)$$

(otherwise we may take a large enough  $c$ ). We construct a recursive sequence  $(n_i)_{i \geq 0}$  of numbers and a recursive double sequence  $(m_{i,j})_{i,j \geq 0}$  of elements in  $\mathbf{N} \cup \{\infty\}$ . These numbers  $n_i$  and the numbers  $m_{i,j} \neq \infty$  will be the lengths of the words in the set  $A$  which we wish to construct. The numbers  $n_i$  serve in order to guarantee that  $B \leq_{ss} A$ . The numbers  $m_{i,j}$  are used “to fill” the set  $A$  up in order to get exactly  $\alpha = 2^{-A}$ . This will follow directly from Eq. (7) below.

*Construction of  $(n_i)$ :* We define  $n_i = |y_i| + c$ , for all  $i$ .

*Beginning of construction of  $(m_{i,j})$ .*

*Stage 0:* Let  $m_{i,j} = \infty$ , for all  $i < f(0)$  and  $j \in \mathbf{N}$ , and define positive integers  $(m_{f(0),j})_{j \geq 0}$  recursively in such a way that

$$\sum_{j=0}^{\infty} 2^{-m_{f(0),j}} = a_0 - \sum_{i=0}^{f(0)} 2^{-n_i}.$$

*Stage  $s$  ( $s \geq 1$ ):* If

$$a_s \leq \sum_{i=0}^{f(s)} 2^{-n_i} + \sum_{i=0}^{f(s-1)} \sum_{j=0}^{\infty} 2^{-m_{i,j}},$$

then let  $m_{i,j} = \infty$ , for all  $i$  with  $f(s-1) < i \leq f(s)$  and  $j \in \mathbf{N}$ . Otherwise, let  $m_{i,j} = \infty$ , for all  $i$  with  $f(s-1) < i < f(s)$  and  $j \in \mathbf{N}$ , and let positive integers  $(m_{f(s),j})_{j \geq 0}$  be recursively defined in such a way that

$$\sum_{j=0}^{\infty} 2^{-m_{f(s),j}} = a_s - \left( \sum_{i=0}^{f(s)} 2^{-n_i} + \sum_{i=0}^{f(s-1)} \sum_{j=0}^{\infty} 2^{-m_{i,j}} \right).$$

*End of construction of  $(m_{i,j})$ .*

First, we prove the following equation:

$$\alpha = \sum_{i=0}^{\infty} \left( 2^{-n_i} + \sum_{j=0}^{\infty} 2^{-m_{i,j}} \right). \quad (7)$$

For the proof, we distinguish the following two cases:

*Case 1:* There are infinitely many stages  $s$  such that  $a_s = \sum_{i=0}^{f(s)} (2^{-n_i} + \sum_{j=0}^{\infty} 2^{-m_{i,j}})$ . For this case, it is straightforward that Eq. (7) holds.

*Case 2:* The inequality  $a_s < \sum_{i=0}^{f(s)} (2^{-n_i} + \sum_{j=0}^{\infty} 2^{-m_{i,j}})$  holds true for almost all  $s \in \mathbf{N}$ . On the one hand,

$$\alpha = \lim_{s \rightarrow \infty} a_s \leq \sum_{i=0}^{\infty} \left( 2^{-n_i} + \sum_{j=0}^{\infty} 2^{-m_{i,j}} \right). \quad (8)$$

For the inverse estimate, we define  $s_0$  to be the largest stage such that  $a_{s_0} = \sum_{i=0}^{f(s_0)} (2^{-n_i} + \sum_{j=0}^{\infty} 2^{-m_{i,j}})$ . Such a stage  $s_0$  exists because of (6) and the construction. By (5) we have

$$\alpha - a_{s_0} \geq \sum_{i=f(s_0)+1}^{\infty} 2^{-|y_i|-c}.$$

Hence, by the construction,

$$\alpha \geq \sum_{i=0}^{\infty} \left( 2^{-n_i} + \sum_{j=0}^{\infty} 2^{-m_{i,j}} \right). \quad (9)$$

By combining (8) and (9) we obtain equality (7) also in this case.

Let  $h: \mathbf{N} \rightarrow \{(i, j) \in \mathbf{N}^2 \mid m_{i,j} \neq \infty\}$  be a recursive bijection (note that by construction the set  $\{(i, j) \in \mathbf{N}^2 \mid m_{i,j} \neq \infty\}$  is infinite) and define a recursive sequence  $(m'_i)$  of numbers by  $m'_i = m_{h(i)}$ . Using this sequence we define  $(n'_i)$  by  $n'_{2i} = n_i$  and  $n'_{2i+1} = m'_i$ . By Theorem 3.2 and (7), combined with  $0 < \alpha \leq 1$ , we can construct a one-to-one recursive sequence  $(x_i)$  of words with  $|x_i| = n'_i$  such that the set  $\{x_i \mid i \in \mathbf{N}\}$  is prefix-free. We set  $A = \{x_i \mid i \in \mathbf{N}\}$  and, using (7), obtain

$$2^{-A} = \sum_{i=0}^{\infty} 2^{-n'_i} = \sum_{i=0}^{\infty} 2^{-n_i} + \sum_{i=0}^{\infty} 2^{-m'_i} = \alpha.$$

Finally we define a recursive function  $g: A \rightarrow B$  by  $g(x_{2i}) = y_i$  and such that  $|g(x_{2i+1})| \geq |x_{2i+1}|$ , for all  $i$ . This is possible because  $B$  is infinite. Obviously,  $g(A) = B$ , and  $|x| \leq |g(x)| + c$ , for all  $x \in A$ . This shows  $B \leq_{ss} A$ .  $\square$

**Theorem 5.8.** *The mapping from  $\langle R.E._{ss}; \leq_{ss} \rangle$  to  $\langle \mathbf{R}.e.; \leq_{dom} \rangle$  induced by  $A \mapsto 2^{-A}$  for  $A \in R.E.$  is a strong homomorphism.*

**Proof.** By Lemma 5.6 and Theorem 5.7.  $\square$

The next result shows that this mapping cannot be one-to-one.

**Theorem 5.9.** *There exist infinite prefix-free r.e. sets  $A$  and  $B$  with  $2^{-A} = 2^{-B} = 1$  but  $A \not\leq_{ss} B$  and  $B \not\leq_{ss} A$ .*

**Proof.** We define two sequences  $(n_i)$  and  $(m_i)$  of natural numbers by

$$n_0 = 0, \quad m_i = 2^{n_i} \quad \text{and} \quad n_{i+1} = 2^{m_i}$$

for all  $i$ . Let  $E_i$  be the set of all words of length  $n_i + 1$  with prefix  $0^i1$ , and let  $G_i$  be the set of all words of length  $m_i + 1$  with prefix  $0^i1$ . Then  $|E_i| = 2^{n_i - i}$  and  $|G_i| = 2^{m_i - i}$ . Define  $A = \bigcup_i E_i$  and  $B = \bigcup_i G_i$ . Both sets  $A$  and  $B$  are obviously recursive and prefix-free and satisfy  $2^{-A} = 2^{-B} = 1$ . We have to show that neither  $A$  strongly simulates  $B$  nor  $B$  strongly simulates  $A$ . If  $A$  would strongly simulate  $B$  there would be a surjective mapping from  $A$  to  $B$  satisfying the second condition in Definition 5.4, that is a mapping which does not map long words to short words. We show that this is impossible. Namely,  $A$  contains at most  $\sum_{j=0}^i 2^{n_j - j} \leq 2^{n_i}$  words of length less than  $n_{i+1} + 1 = 2^{n_i} + 1$  while  $B$  contains  $2^{m_i - i} = 2^{2^{n_i} - i}$  words of length  $m_i + 1 = 2^{n_i} + 1$ . For large  $n_i$  — and the sequence  $(n_i)$  is unbounded — this contradicts  $B \leq_{ss} A$ . On the other hand,  $A$  contains  $2^{n_{i+1} - i - 1} = 2^{2^{m_i} - i - 1}$  words of length  $n_{i+1} + 1 = 2^{m_i} + 1$  while  $B$  contains at most  $\sum_{j=0}^i 2^{m_j - j} \leq 2^{m_i}$  words of length less than  $m_{i+1} + 1 = 2^{m_i} + 1$ . This rules out the relation  $A \leq_{ss} B$ .  $\square$

However, by relaxing the strong simulation relation one can characterize the domination relation by a simulation relation between prefix-free r.e. sets. A sequence  $E_0, E_1, E_2, \dots$  of finite sets in  $\Sigma^*$  is called a *strong array* [27] if there is a total recursive function  $g$  such that with respect to a standard bijection  $D$  from  $\mathbf{N}$  onto the set of all finite subsets of  $\Sigma^*$  we have  $E_i = D_{g(i)}$  for all  $i$ .

**Definition 5.10.** An *effective, finite partition* of an infinite, r.e. set  $A$  is a strong array  $E_0, E_1, E_2, \dots$  of finite, pairwise disjoint sets with  $\bigcup_{i=0}^{\infty} E_i = A$ .

An example of an effective, finite partition is the partition whose equivalence classes contain only one element: if  $a_0, a_1, \dots$  is a one-to-one recursive enumeration of  $A$  one sets  $E_i = \{a_i\}$

**Definition 5.11.** Let  $A$  and  $B$  be infinite, prefix-free, r.e. sets. We say that  $A$  *simulates*  $B$  if there are two effective, finite partitions  $(E_i)$  of  $A$  and  $(G_i)$  of  $B$ , respectively, and a constant  $c > 0$  such that for all  $i$ :

$$c \cdot (2^{-E_i}) \geq 2^{-G_i}.$$

We are ready to characterize the  $\leq_{dom}$ -relation in terms of the simulation relation between sets. We remark that the following theorem is true also if the definition of an effective finite partition is changed so that all sets  $E_i$  must be nonempty.

**Theorem 5.12.** Let  $A, B \subseteq \Sigma^*$  be infinite prefix-free r.e. sets. Then  $A$  simulates  $B$  if and only if  $2^{-A}$  dominates  $2^{-B}$ .

**Proof.** Assume that  $A$  simulates  $B$ . Let  $E_0, E_1, E_2, \dots$  be an effective finite partition of  $A$ , and  $G_0, G_1, G_2, \dots$  be a corresponding effective finite partition of  $B$ , and  $c > 0$  an appropriate constant. The rational sequences

$$\left( \sum_{i \leq n} 2^{-E_i} \right)_{n \geq 0} \quad \text{and} \quad \left( \sum_{i \leq n} 2^{-G_i} \right)_{n \geq 0}$$

are recursive, non-decreasing, and converge to  $2^{-A}$  and to  $2^{-B}$ , respectively. Furthermore we have

$$2^{-B} - \sum_{i \leq n} 2^{-G_i} = \sum_{i > n} 2^{-G_i} \leq c \cdot \left( \sum_{i > n} 2^{-E_i} \right) = c \cdot \left( 2^{-A} - \sum_{i \leq n} 2^{-E_i} \right).$$

This shows that  $2^{-A}$  dominates  $2^{-B}$ .

Now assume that  $2^{-A}$  dominates  $2^{-B}$ . That is, there are a rational constant  $c > 0$  and a partial recursive function  $f: \mathbf{Q} \overset{\circ}{\rightarrow} \mathbf{Q}$  such that for all rationals  $q < 2^{-A}$  the number  $f(q)$  is defined, smaller than  $2^{-B}$  and satisfies the inequality  $c(2^{-A} - q) \geq 2^{-B} - f(q)$ . Since we can increase  $c$  we can assume that actually  $c \cdot 2^{-A} > 2^{-B}$  and  $c(2^{-A} - q) > 2^{-B} - f(q)$ , for all rationals  $q < 2^{-A}$ . Let

$$x_0, x_1, x_2, \dots \quad \text{and} \quad y_0, y_1, y_2, \dots$$

be one-to-one recursive enumerations of  $A$  and  $B$ , respectively. Using  $f$  we see that there is a total recursive, increasing function  $g: \mathbf{N} \rightarrow \mathbf{N}$  satisfying the inequality

$$c \cdot \left( 2^{-A} - \sum_{i \leq m} 2^{-|x_i|} \right) > 2^{-B} - \sum_{i \leq g(m)} 2^{-|y_i|}$$

for all  $m$ . We define a total recursive, increasing function  $h: \mathbf{N} \rightarrow \mathbf{N}$ , where we also define  $h(-1) = -1$ , by

$$h(n+1) = \min \left\{ k > h(n) \mid c \cdot \left( \sum_{h(n) < i \leq k} 2^{-|x_i|} \right) \geq \sum_{g(h(n)) < i \leq g(k)} 2^{-|y_i|} \right\}$$

for all  $n \geq -1$  (where we assume  $g(-1) = -1$ ). The function  $h$  is well defined since for each  $m \geq -1$  we have

$$c \cdot \left( \sum_{m < i} 2^{-|x_i|} \right) > \sum_{g(m) < i} 2^{-|y_i|}.$$

We set

$$E_i = \{x_{h(i-1)+1}, \dots, x_{h(i)}\} \quad \text{and} \quad G_i = \{y_{g(h(i-1))+1}, \dots, y_{g(h(i))}\}.$$

Then the sequence  $(E_i)$  is an effective finite partition of  $A$ , the sequence  $(G_i)$  is an effective finite partition of  $B$ , and we have

$$c \cdot 2^{-E_i} = c \cdot \sum_{h(i-1) < j \leq h(i)} 2^{-|x_j|} \geq \sum_{gh(i-1) < j \leq gh(i)} 2^{-|y_j|} = 2^{-G_i},$$

which shows that  $A$  simulates  $B$ .  $\square$

## 6. Random R.E. reals and $\Omega$ -like reals

In this section, we study random r.e. reals and especially  $\Omega$ -like reals, which were introduced by Solovay [30]. Chaitin [12] has given a slightly different definition. We

show that Chaitin  $\Omega$  numbers, Solovay's  $\Omega$ -like reals and Chaitin's  $\Omega$ -like reals are all the same. Then we answer the question raised after Lemma 5.1. Furthermore, we give an elementary construction of a random number  $\alpha$  in  $\mathcal{A}_2$  such that neither  $\alpha$  nor  $1 - \alpha$  is an r.e. real. Finally we address the question whether  $\Omega$  is also maximally useful if one wishes to compute not only an approximation of an r.e. real but the digits of its binary representation. We start with Chaitin's definition of  $\Omega$ -like reals.

**Definition 6.1** (Chaitin [12]). An r.e. real  $\alpha$  is called  $\Omega$ -like if it dominates all r.e. reals.

Solovay's original manuscript [30] contains the following definition.

**Definition 6.2** (Solovay [30]). A recursive, increasing, and converging sequence  $(a_i)$  of rationals is called *universal* if for every recursive, increasing and converging sequence  $(b_i)$  of rationals there exists a number  $c > 0$  such that

$$c \cdot (\alpha - a_n) \geq \beta - b_n$$

for all  $n$ , where  $\alpha = \lim_{n \rightarrow \infty} a_n$  and  $\beta = \lim_{n \rightarrow \infty} b_n$ .

Solovay called a real  $\alpha$   $\Omega$ -like if it is the limit of a universal recursive, increasing sequence of rationals. We shall see that both definitions are equivalent. One implication is very easy.

**Lemma 6.3.** *If a real  $\alpha$  is the limit of a universal recursive, increasing sequence of rationals, then it is  $\Omega$ -like.*

**Proof.** This follows immediately from Theorem 4.1 and Lemma 4.3.  $\square$

By modifying slightly the proof of Solovay [30] we obtain the following:

**Theorem 6.4.** *Let  $U$  be a universal self-delimiting machine. Every recursive, increasing sequence of rationals converging to  $\Omega_U$  is universal.*

**Proof.** Let  $(a_n)$  be an increasing, recursive sequence of rationals with limit  $\Omega_U$ , and let  $(b_n)$  be an increasing, recursive, converging sequence of rationals. Set  $\beta = \lim_{n \rightarrow \infty} b_n$ . We have to show that there is a constant  $c > 0$  with  $c(\Omega_U - a_n) \geq \beta - b_n$  for all  $n$ . Without loss of generality, we may assume that  $0 < b_n < \beta < 1$ , for all  $n \in \mathbf{N}$ .

Let  $(x_i)$  be a one-to-one, recursive enumeration of  $PROG_U$ , and  $\Omega_{U,n} = \sum_{i=0}^n 2^{-|x_i|}$ . We define a total recursive, increasing function  $g: \mathbf{N} \rightarrow \mathbf{N}$ , where we also define  $g(-1) = -1$ , by

$$g(n) = \min\{j > g(n-1) \mid \Omega_{U,j} \geq a_n\}.$$

The sequence  $(\Omega_{U,g(n)})$  is an increasing, recursive sequence with limit  $\Omega_U$ . In view of the inequality

$$\Omega_U - a_n \geq \Omega_U - \Omega_{U,g(n)}.$$

it is sufficient to prove that there is a constant  $c > 0$  with  $c(\Omega_U - \Omega_{U,g(n)}) \geq \beta - b_n$  for all  $n$ .

For each  $i \in \mathbf{N}$ , let  $y_i$  be the first string (with respect to the quasi-lexicographical ordering) which is not in the set  $\{U(x_j) \mid j \leq g(i)\} \cup \{y_j \mid j < i\}$ . Furthermore, put  $n_i = \lceil -\log(b_{i+1} - b_i) \rceil + 1$ . Since  $\sum_{i=0}^{\infty} 2^{-n_i} \leq \beta - b_0 < 1$ , by Theorem 3.2 we can construct a self-delimiting Turing machine  $M$  such that, for every  $i \in \mathbf{N}$ , there is a string  $u_i \in \Sigma^{n_i}$  satisfying  $M(u_i) = y_i$ . Hence, there is a constant  $c_M$  such that  $H_U(y_i) \leq n_i + c_M$ . In view of the choice of  $y_i$ , there is a string  $x'_i \in \text{PROG}_U \setminus \{x_j \mid j \leq g(i)\}$  such that  $|x'_i| \leq n_i + c_M$  and  $U(x'_i) = y_i$ . For different  $i$  and  $j$  we have  $y_i \neq y_j$ , whence  $x'_i \neq x'_j$ . We obtain

$$\begin{aligned} \Omega_U - \Omega_{U,g(n)} &= \sum_{i=g(n)+1}^{\infty} 2^{-|x'_i|} \\ &\geq \sum_{i=n}^{\infty} 2^{-|x'_i|} \\ &\geq \sum_{i=n}^{\infty} 2^{-n_i - c_M} \\ &\geq 2^{-c_M - 1} \sum_{i=n}^{\infty} (b_{i+1} - b_i) \\ &= 2^{-c_M - 1} (\beta - b_n), \end{aligned}$$

which proves the assertion.  $\square$

Thus, every Chaitin  $\Omega$  number is  $\Omega$ -like in Solovay's sense. The converse of Theorem 6.4 holds true even for  $\Omega$ -like numbers in Chaitin's sense.

**Theorem 6.5.** *Let  $0 < \alpha < 1$  be an  $\Omega$ -like real. Then there exists a universal self-delimiting machine  $U$  such that  $\Omega_U = \alpha$ .*

**Proof.** Let  $V$  be a universal self-delimiting machine. Since  $\alpha$  is  $\Omega$ -like it dominates  $2^{-\text{PROG}_V}$ . By Theorem 5.7 there exist a prefix-free r.e. set  $A$  with  $2^{-A} = \alpha$ , a recursive function  $f : A \rightarrow \text{PROG}_V$  with  $A = \text{dom}(f)$  and  $f(A) = \text{PROG}_V$ , and a constant  $c > 0$  with  $|x| \leq |f(x)| + c$ , for all  $x \in A$ . We define a self-delimiting machine  $U$  by  $U(x) = V(f(x))$ . The universality of  $V$  implies that also  $U$  is universal. We have  $\alpha = 2^{-A} = 2^{-\text{PROG}_U} = \Omega_U$ .  $\square$

The following theorem summarizes our description of  $\Omega$ -like numbers.

**Theorem 6.6.** *Let  $0 < \alpha < 1$  be an r.e. real. The following conditions are equivalent:*

1. *For some universal self-delimiting Turing machine  $U$ ,  $\alpha = \Omega_U$ .*
2. *The real  $\alpha$  is  $\Omega$ -like.*
3. *There exists a universal recursive, increasing sequence of rationals converging to  $\alpha$ .*
4. *Every recursive, increasing sequence of rationals with limit  $\alpha$  is universal.*

**Proof.** This follows from Lemma 6.3, Theorems 6.4, and 6.5.  $\square$

We obtain the following addendum to Theorem 4.7.

**Corollary 6.7.** *The structure  $\langle \mathbf{R}_{r.e.}; \leq_{dom} \rangle$  has a greatest element which is the  $=_{dom}$ -equivalence class containing exactly all Chaitin  $\Omega$  numbers.*

The following result was proved by Solovay [30] for  $\Omega$ -like numbers.

**Corollary 6.8.** *Let  $U$  and  $V$  be two universal self-delimiting Turing machines. Then  $H(\Omega_U(n)) = H(\Omega_V(n)) + O(1)$ , for all  $n \in \mathbf{N}$ .*

**Proof.** This follows from Theorems 4.9 and 6.6.

In analogy with Corollary 4.5 we obtain the following.

**Corollary 6.9.** *The fractional part of the sum of an  $\Omega$  number and an r.e. real is an  $\Omega$  number. The fractional part of the product of an  $\Omega$  number with a positive r.e. real is an  $\Omega$  number. Especially, the fractional parts of the sum and product of two  $\Omega$  numbers are again  $\Omega$  numbers.*

**Proof.** This follows from Lemma 4.4 and Theorem 6.6.  $\square$

**Corollary 6.10** (Solovay [30]). *Every  $\Omega$ -like real is random.*

**Proof.** This follows from Theorems 3.4 and 6.5.  $\square$

**Corollary 6.11.** *The real  $0.\chi_K$  is not  $\Omega$  like.*

**Proof.** It is well known that  $\chi_K$  is not random, whence the corollary follows from Corollary 6.10.  $\square$

Now we can answer the question raised after Lemma 5.1. The sets  $A_\Omega$  and  $A_{\chi_K}$  are defined as before Lemma 5.1. For sets  $A, B \subseteq \Sigma^*$  let  $A \sim_T B$  denote the conjunction  $A \leq_T B$  and  $B \leq_T A$ .

**Corollary 6.12.** *The following statements hold:*

1.  $0.\chi_K \not\leq_{dom} \Omega$ ,
2.  $A_\Omega \sim_T A_{\chi_K} \sim_T K$ .

**Proof.** The first claim follows from Corollary 6.11.  $A_\Omega \leq_T K \sim_T A_{\chi_K}$  is clear and  $A_{\chi_K} \leq_T A_\Omega$  follows from Lemma 5.1.  $\square$

Let  $\Delta_2$  be the class of sets which are recursive in  $K$ . Then all  $\Omega$  like reals<sup>8</sup> are in  $\Delta_2$ . Now one may ask whether there exists a random real in  $\Delta_2$  which is not in the set  $\{\alpha, 1 - \alpha \mid \alpha \text{ is } \Omega\text{-like}\}$ ? The answer to this question is positive.

<sup>8</sup>Note that here we identify a real  $0.x$  with the set  $A_x^\#$ , that is, we identify sets of numbers and their characteristic sequences.

**Proposition 6.13.** *There is a random sequence  $\mathbf{y}$  with  $A_{\mathbf{y}}^{\#} \in \Delta_2$  such that neither  $0.\mathbf{y}$  nor  $1 - 0.\mathbf{y}$  is an r.e. real.*

In fact, Kucera [20] (see also [17]) observed that  $0'$  is the only r.e. degree which contains random reals. Therefore, any random real in the set  $\{\alpha, 1 - \alpha \mid \alpha \text{ is r.e.}\}$  is in  $0'$ . On the other hand, Kucera [20] also observed that there is a random real  $0.\mathbf{y}$  of low degree (use the fact that there is a universal randomness test and the Low Basis Theorem by Jockusch and Soare [27]). This random real is in  $\Delta_2$ , but it cannot be in  $0'$ , hence, neither  $0.\mathbf{y}$  nor  $1 - 0.\mathbf{y}$  can be an r.e. real. In the following we give a completely elementary construction of such a random real  $\mathbf{y}$ .

**Proof.** Elementary proof. Let  $\mathbf{x} = x_0x_1x_2\dots$  be an infinite binary sequence such that  $0.\mathbf{x}$  is  $\Omega$  like. We define an infinite binary sequence  $\mathbf{y} = y_0y_1y_2\dots$  by letting

$$y_i = \begin{cases} x_i & \text{if } i \leq 1, \\ x_{i+3^n} & \text{if } 3^n < i \leq 2 \cdot 3^n, \\ x_{i-3^n} & \text{if } 2 \cdot 3^n < i \leq 3^{n+1}. \end{cases}$$

The sequence  $\mathbf{y}$  is obtained by recursively re-ordering the digits of the sequence  $\mathbf{x}$ . Hence, also  $\mathbf{y}$  is a random sequence in  $\Delta_2$ . Next, we show that neither  $0.\mathbf{y}$  nor  $1 - 0.\mathbf{y}$  is an r.e. real. In fact, we show more:

$$0.\mathbf{x} \not\geq_{dom} 0.\mathbf{y} \quad \text{and} \quad 0.\mathbf{x} \not\geq_{dom} 1 - 0.\mathbf{y}. \quad (10)$$

By symmetry, it suffices to show that  $0.\mathbf{x}$  does not dominate  $0.\mathbf{y}$ . For the sake of a contradiction, assume that  $0.\mathbf{x} \geq_{dom} 0.\mathbf{y}$ . Then, by Theorem 4.9,

$$H(\mathbf{y}(2 \cdot 3^n)) \leq H(\mathbf{x}(2 \cdot 3^n)) + O(1),$$

and hence, by the definition of  $\mathbf{y}$  we obtain

$$H(\mathbf{x}(3^{n+1})) \leq H(\mathbf{y}(3^{n+1})) + O(1) \leq H(\mathbf{x}(2 \cdot 3^n)) + O(1),$$

for all  $n \in \mathbf{N}$ . That is,

$$H(\mathbf{x}(3^{n+1})) \leq 2 \cdot 3^n + H(\text{string}_{2 \cdot 3^n}) + O(1).$$

Since  $\lim_{n \rightarrow \infty} (3^{n+1} - 2 \cdot 3^n - H(\text{string}_{2 \cdot 3^n})) = \infty$  the sequence  $\mathbf{x}$  is not random by Theorem 3.3. This contradicts the fact that  $0.\mathbf{x}$  is  $\Omega$  like. We have proved (10). By Definition 6.1 we conclude that neither  $0.\mathbf{y}$  nor  $1 - 0.\mathbf{y}$  is an r.e. real.  $\square$

In a sense, compared with a non- $\Omega$  like r.e. real, an  $\Omega$  like real number either contains more information or at least its information is structured in a more useful way because we can find a good approximation from below to any r.e. real from a good approximation from below to any fixed  $\Omega$  like real. Sometimes we wish to compute not just an arbitrary approximation (say, of precision  $2^{-n}$ ) from below to an r.e. real, instead, we wish to compute a special approximation, namely the first  $n$

digits of its binary expansion. Is the information in  $\Omega$  organized in such a way as to guarantee that for any r.e. real  $\alpha$  there exists a total recursive function  $g: \mathbf{N} \rightarrow \mathbf{N}$  (depending upon  $\alpha$ ) such that from the first  $g(n)$  digits of  $\Omega$  we can actually compute the first  $n$  digits of  $\alpha$ ? We show that the answer to this question is negative if one demands that the computation is done by a total recursive function.

For two infinite sequences  $\mathbf{x}, \mathbf{y} \in \Sigma^\omega$  we write  $0.\mathbf{x} \leq_{tt} 0.\mathbf{y}$  in case  $A_{\mathbf{x}}^\# \leq_{tt} A_{\mathbf{y}}^\#$ .<sup>9</sup> It is easy to see that this can also be expressed as follows:  $0.\mathbf{x} \leq_{tt} 0.\mathbf{y}$  if and only if there are two total recursive functions  $g: \mathbf{N} \rightarrow \mathbf{N}$  and  $F: \Sigma^* \rightarrow \Sigma^*$  with  $\mathbf{x}(n) = F(\mathbf{y}(g(n)))$  for all  $n$ . This preorder  $\leq_{tt}$  has a maximum among the r.e. reals, but this maximum is not  $\Omega$ , as no random r.e. real is maximal.

**Theorem 6.14.** *The following statements hold:*

1. For every r.e. real  $\alpha$ ,  $\alpha \leq_{tt} 0.\chi_K$ .
2.  $0.\chi_K \not\leq_{tt} \Omega$ .

**Proof.** For the first assertion observe that for an arbitrary r.e. real  $0.\mathbf{x}$  the set  $A_{\mathbf{x}}$  is r.e., whence  $A_{\mathbf{x}} \leq_1 K$  (i.e. there is a recursive one-to-one function  $g$  with  $A_{\mathbf{x}} = g^{-1}(K)$ ). Since  $A_{\mathbf{x}}^\# \leq_{tt} A_{\mathbf{x}}$  is obvious we obtain  $A_{\mathbf{x}}^\# \leq_{tt} K$ . The second assertion follows from the following result by Bennett [1] (proved indirectly in Juedes et al. [16]) stating that

*for every language  $A \subseteq \Sigma^*$  with  $K \leq_{tt} A$  the sequence  $\chi_A$  is not random*

and from the fact that  $\Omega$  is random (Theorem 3.4).  $\square$

We remark that a direct proof of the cited fact by Bennett has been given by Calude and Nies [8], who also prove that  $\Omega$  is wtt-complete (for the definition of wtt-reduction the reader is referred to Soare [27]). This last fact shows that for any r.e. real  $0.\mathbf{x}$  there exist a total recursive function  $g: \mathbf{N} \rightarrow \mathbf{N}$  and a partial recursive function  $F: \Sigma^* \overset{o}{\rightarrow} \Sigma^*$  with  $\mathbf{x}(n) = F(\Omega(g(n)))$  for all  $n$  (use again  $A_{\mathbf{x}}^\# \leq_{tt} A_{\mathbf{x}}$ ).

## 7. Open problems

We close our paper with some open problems and comments on some of them.

1. Does there exist a random r.e. real which is not  $\Omega$ -like?

Comment. Kucera [20] (see also [17]) has observed that  $0'$  is the only r.e. degree which contains random sets (where we identify a set with its characteristic sequence). But Corollary 6.12 shows that  $0'$  splits into different  $=_{dom}$ -equivalence classes.

Added on 1 April 1999: Recently Slaman [25] has shown that every r.e. random real is  $\Omega$ -like. Hence, by Theorem 6.6, r.e. random reals coincide with  $\Omega$  numbers. This

<sup>9</sup> Let  $D$  be a total standard notation of all finite sets of words in  $\Sigma^*$ . A language  $A$  is said to be truth-table reducible to a language  $B$  (in that case we write  $A \leq_{tt} B$ ), if there are two total recursive functions  $f: \Sigma^* \rightarrow \mathbf{N}$  and  $g: \Sigma^* \rightarrow \Sigma^*$  such that  $x \in A$  if and only if  $\chi_B(f(x)) \in D_{g(x)}$  (compare [27]).

makes it interesting to analyze the world of all r.e. reals by asking how “close” an r.e. real is to the class of random r.e. reals, which are simply the Chaitin  $\Omega$  numbers, the  $\leq_{dom}$ -greatest  $=_{dom}$ -class of r.e. reals.

2. Let  $A$  be a universal Martin-Löf test. Is  $\alpha = \sum_n \mu(A_n \Sigma^\omega)$   $\Omega$ -like?  
Added on 1 April 1999: Slaman [26] has answered this question in the affirmative: he proved that the measure of any section  $A_n$  of a universal Martin-Löf test  $A$ ,  $\mu(A_n \Sigma^\omega)$ , is  $\Omega$ -like.
3. Further study the first-order theory of  $\langle \mathbf{R}_{r.e.}; \leq_{dom} \rangle$ .

### Acknowledgements

The authors thank Gregory Chaitin and Richard Shore for useful comments.

### References

- [1] C.H. Bennett, Logical depth and physical complexity, in: R. Herken (Ed.), *The Universal Turing Machine, A Half-Century Survey*, Oxford University Press, Oxford, 1988, pp. 227–258.
- [2] C.H. Bennett, M. Gardner, The random number omega bids fair to hold the mysteries of the universe, *Scientific Amer.* 241 (1979) 20–34.
- [3] D.S. Bridges, F. Richman, *Varieties of Constructive Mathematics*, Cambridge University Press, Cambridge, 1987.
- [4] C. Calude, *Information and randomness. An Algorithmic Perspective*, Springer, Berlin, 1994.
- [5] C. Calude C. Grozea, Kraft-Chaitin inequality revisited, *J. UCS* 5 (1996) 306–310.
- [6] C.S. Calude, P. Hertling, B. Khossainov, Y. Wang, Recursively enumerable reals and Chaitin  $\Omega$  numbers, in: M. Morvan et al. (Eds.), *Proceedings of the 15th Symposium on Theoretical Aspects of Computer Science (Paris)*, Springer, Berlin, 1998, pp. 596–606.
- [7] C. Calude, F.W. Meyerstein, Is the universe lawful?, *Chaos, Solitons Fractals* (1999), to appear.
- [8] C. Calude, A. Nies, Chaitin  $\Omega$  numbers and strong reducibilities, *J. UCS* 3 (1997) 1161–1166.
- [9] C. Calude, A. Salomaa, Algorithmically coding the universe, in: G. Rozenberg, A. Salomaa (Eds.), *Developments in Language Theory*, World Scientific, Singapore, 1994, pp. 472–492.
- [10] G.J. Chaitin, On the length of programs for computing finite binary sequences, *J. Assoc. Comput. Mach.* 13 (1966) 547–569 (Reprinted in: *Information, Randomness and Incompleteness, Papers on Algorithmic Information Theory* (2nd Edition, 1990) World Scientific, Singapore, 1987, pp. 219–244).
- [11] G.J. Chaitin, A theory of program size formally identical to information theory, *J. Assoc. Comput. Mach.* 22 (1975) 329–340 (Reprinted in: *Information, Randomness and Incompleteness, Papers on Algorithmic Information Theory* (2nd Edition, 1990) World Scientific, Singapore, 1987, pp. 113–128).
- [12] G.J. Chaitin, Algorithmic information theory, *IBM J. Res. Develop.* 21 (1977) 350–359, 496 (Reprinted in: *Information, Randomness and Incompleteness, Papers on Algorithmic Information Theory* (2nd Edition, 1990) World Scientific, Singapore, 1987, pp. 44–58).
- [13] G.J. Chaitin, *Algorithmic Information Theory*, Cambridge University Press, Cambridge, 1987.
- [14] G.J. Chaitin, *Information, Randomness and Incompleteness, Papers on Algorithmic Information Theory* (2nd Edition, 1990) World Scientific, Singapore, 1987.
- [15] G.J. Chaitin, *The Limits of Mathematics*, Springer, Singapore, 1997.
- [16] D. Juedes, J. Lathrop, J. Lutz, Computational depth and reducibility, *Theoret. Comput. Sci.* 132 (1994) 37–70.
- [17] S. Kautz, *Degrees of Random Sets*, Ph.D. Thesis, Cornell University, Ithaca, 1991.
- [18] Ker-I. Ko, *Complexity Theory of Real Functions*, Birkhäuser, Boston, 1991.
- [19] A.N. Kolmogorov, Three approaches for defining the concept of information quantity, *Problems Inform. Transmission* 1 (1965) 3–11.

- [20] A. Kucera. Measure,  $\Pi_1^0$  classes and complete extensions of PA, in: H.D. Ebbinghaus, G.H. Müller, G.E. Sacks (Eds.), Recursion Theory Week, Oberwolfach, 1984, Lecture Notes in Mathematics. 1141, Springer, Berlin, 1985, pp. 245–259.
- [21] L.A. Levin, On the notion of a random sequence, Soviet Math. Dokl. 14 (1973) 1413–1416.
- [22] P. Martin-Löf, The definition of random sequences, Inform. Control 9 (1966) 602–619.
- [23] G. Rozenberg, A. Salomaa, Cornerstones of Undecidability, Prentice-Hall, Englewood Cliffs, NJ, 1994.
- [24] C.P. Schnorr, Process complexity and effective random tests, J. Comput. System Sci. 7 (1973) 376–388.
- [25] T.A. Slaman, Random Implies  $\Omega$ -Like, Manuscript, 14 December 1998, 2 pp.
- [26] T.A. Slaman, Recursive Enumerability and Randomness, Manuscript, 11 January 1999, 5 pp.
- [27] R.I. Soare, Recursively Enumerable Sets and Degrees, Springer, Berlin, 1987.
- [28] R.I. Soare, Computability and recursion, Bull. Symbolic Logic 2 (1996) 284–321.
- [29] R.J. Solomonoff, A formal theory of inductive inference, Parts 1 and 2, Inform. and Control 7 (1964) 1–22, 224–254.
- [30] R. Solovay, Draft of a paper (or series of papers) on Chaitin’s work ... done for the most part during the period of Sept.–Dec. 1974, unpublished manuscript, IBM Thomas J. Watson Research Center, Yorktown Heights, New York, May 1975, 215 pp.
- [31] R. Solovay, On random r.e. sets, in: A.I. Arruda, N.C.A. Da Costa, R. Chuaqui (Eds.), Non-Classical Logics, Model Theory and Computability, North-Holland, Amsterdam, 1977, pp. 283–307.
- [32] Y. Wang, Randomness and Complexity. Ph.D. Thesis, Universität Heidelberg, Germany, 1996.
- [33] K. Weihrauch, Computability, Springer, Berlin, 1987.