1 Calude - Information and Randomness book

Questions :

1. what is a Chaitin computer? OK
2. what is null-free data ? OK
3. what is $U_\lambda, M_\lambda, C_\lambda$? OK
4. why is $\mathrm{dom}(U_\lambda)$ c.e. ? OK
5. what is H_M, H_U? OK

{1} In this book, the empty string is λ !! Also, $\log n := \lfloor \log_2(n+1) \rfloor$. $p|q$ means p divides q. {2} We denote by $\mathrm{string}_{\mathrm{Q}}(n)$ the n-th element in the quasi-lexicographical ordering of $A_Q^* := \{0, \dots, Q-1\}^*$. We denote $A_Q^+ := A_Q^* \backslash \{\lambda\}$. When it is clear, we write string instead of $\mathrm{string}_{\mathrm{Q}}$. Note that $|\mathrm{string}_{\mathrm{Q}}(n)| := \lfloor \log_Q(n(Q-1)+1) \rfloor$. Prefix-order : $x <_p y$ indicates that there exists $z \in \{0,1\}^*$ s.t. $y = xz$. Concatenation of x and y is denoted by xy, for two sets S and T, define $ST := \{xy : x \in S, y \in T\}$. {3} $A_Q := \{0, 1, \dots, Q-1\}$. $(n)_Q$ is the bases Q representation of n (watch out: $\mathrm{string}_{\mathrm{Q}}(n) \neq (n)_Q$). A_Q^ω is the set of infinite sequences of A_Q. Elements of A_Q^ω are written in boldface, i.e. $\mathbf{x} \in A_Q^\omega$. $\mathbf{x}(n) := x_1 \dots x_n$. We define, for $S \subseteq A_Q^*$, $SA_Q^\omega := \{\mathbf{x} \in A_Q^\omega : \mathbf{x}(n) \in S \textit{ for some } n \geq 1\}$, $xA_Q^\omega := \{x\}A_Q^\omega$. Important: $f \overset{+}{\prec} g$ means $f \leq g + O(1)$. If $f \overset{+}{\prec} g$ and $g \overset{+}{\prec} f$, we write $f \simeq g$. We write $\varphi : X \overset{o}{\to} Y$ for partial functions, and $\varphi : X \to Y$ for total functions. The range of a function is denoted $\mathrm{range}(\varphi) := \{\varphi(x) : x \in \mathrm{dom}(\varphi)\}$. Two partial functions φ, f are equal if $\mathrm{dom}(\varphi) = \mathrm{dom}(f)$, and $\varphi(x) = f(x)$ for all $x \in \mathrm{dom}(\varphi)$.

1.1 Computability theory

He reviews basis topics in computability theory.

1.2 Definitions of Kolmogorov complexity

Fix a universal computer ψ and a universal Chaitin computer U.

Definition 1. {36} *(Kolmogorov-Chaitin absolute complexity) Let φ be a computer. We define the partial function $K_\varphi : A_Q^* \overset{o}{\to} \mathcal{N}$, as*

$$K_\varphi := \min\left\{|u| : u \in A_Q^*, \varphi(u, \lambda) = x\right\}. \tag{1}$$

We put $K(x) := K_\psi(x)$.

Definition 2. {36} *(Chaitin self-delimiting absolute complexity) Let C be a Chaitin computer. We define the partial function $H_C : A_Q^* \xrightarrow{o} \mathcal{N}$, as*

$$H_C := \min\left\{|u| : u \in A_Q^*, \varphi(u, \lambda) = x\right\}. \tag{2}$$

We put $H(x) := H_U(x)$.

Definition 3. {37} *The canonical program defined with respect to the Chaitin universal computer U is*

$$x^* = \min\left\{u \in A_Q^* : U(u, \lambda) = x\right\}, \tag{3}$$

where the minimum is taken with respect to the shortlex (quasilexicographical) ordering.

{37} Thermodynamic cost ???

Lemma 1. *$K(x) \leq K_\varphi + c_\varphi$, $H(x) \leq H_C(x) + c_C$, for all $x \in A_Q^*$.*

Definition 4. *Let $f : X \times Y \to S$ be a function. $f_x := f(\cdot, x)$ is called the section of f at x.*

Lemma 2.

1.3 Answers to the questions

1.3.1 Question 1: what is a Chaitin computer?

Definition 5. {35} *(Chaitin computer) A computer is a p.c. function $\varphi : A^* \times A^* \to A^*$. A Chaitin computer is computer C such that for every $v \in A^*$,* $\mathrm{dom}(C(\cdot, v))$ *is prefix-free.*

For specifications on how a prefix-free turing machine can be defined explicitely, see pages {35 – 36} ! However, it it unclear how these machines can receive multiple inputs.

Definition 6. {36} *(Universal Chaitin computer) A (Chaitin) computer ψ is universal if for each (Chaitin) computer φ, there is a constant c (depending on ψ, φ) with the following property. If $\varphi(x, v) < \infty$, there exists x' such that $\psi(x', v) = \varphi(x, v)$ and $|x'| \leq |x| + c$.*

Remark: in Li (2008), this corresponds (almost) to the definition of additively optimal self-delimiting universal computable function.

Theorem 1. {36} *(Existence of universal Chaitin computer) There (effectively) exists a (Chaitin) universal computer.*

1.3.2 Question 2: what is null-free data?

It just means that we compute the probability of halting with no advice, i.e. the probability of halting of $x \mapsto U(\lambda, x)$.

1.3.3 Question 3: what are $U_\lambda, M_\lambda, C_\lambda$?

The subscriopt λ denotes the section of the functions U, M, C, that are functions from $A_Q^* \times A_Q^*$. Hence $U_\lambda := U(\lambda, \cdot)$.

I guess that U is the fixed universal Chaitin computer, C is a Chaitin computer, and for M, on page {80} it seems to be also a Chaitin computer.

1.3.4 Question 4: why is $\mathrm{dom}(U_\lambda)$ c.e. ?

I am stupid, it is just the definition of c.e. sets.

1.3.5 Question 5: what is H_M, H_U?

H_M, H_U are according to the definition of Chaitin self-delimiting absolute complexity.

1.4 Proof that Ω_U is random!

Let

$$\Omega_U := \sum_{u \in \mathrm{dom}(U)_\lambda} Q^{-|u|}. \tag{4}$$

In the book, they take $\mathbf{r}_q(\Omega_U) = \Omega_1\Omega_2\ldots$ to be the "non-terminating Q-ary expansion" of Ω_U, which in my own words stands for the lazy Q-expansion. The Chaitin theorem asserts that $\mathbf{r}_q(\Omega_U)$ is random.

Theorem 2. $\mathbf{r}_q(\Omega_U)$ *is random.*

We decompose it in three lemmas. Fix an injective computable function $f : \mathcal{N} \to \mathrm{dom}(U)$ (f exists because $\mathrm{dom}(U)$ is computably enumerable by definition), and the sequence

$$\omega_k := \sum_{i=1}^{k} Q^{-|f(i)|},\ \forall k \in \mathcal{N}. \tag{5}$$

Obviously, $\lim_{k\to\infty} \omega_k = \Omega_U$.

Lemma 3. *Let $n, k \in \mathcal{N}$, such that $\omega_k \geq 0.\Omega_1\Omega_2\ldots\Omega_n$. Then,*

$$|f(i)| \geq n,\ \forall i \geq k+1. \tag{6}$$

Proof. Let $n, k \in \mathcal{N}$, such that $\omega_k \geq 0.\Omega_1\Omega_2\ldots\Omega_n$. Note that

$$\lim_{i\to\infty} \omega_i = \omega_k + \sum_{i=k+1}^{\infty} Q^{-|f(i)|} = \Omega_U \leq 0.\Omega_1\Omega_2\ldots\Omega_n + Q^{-n}. \tag{7}$$

Then,

$$\sum_{i=k+1}^{\infty} Q^{-|f(i)|} \leq 0.\Omega_1\Omega_2\ldots\Omega_n + Q^{-n} - \omega_k \leq Q^{-n}. \tag{8}$$

Therefore, no term in the sum $\sum_{i=k+1}^{\infty} Q^{-|f(i)|}$ exceeds Q^{-n}, i.e. $|f(i)| \geq n,\ \forall i \geq k+1$. □

Lemma 4. *Let $n, k \in \mathcal{N}$, such that $\omega_k \geq 0.\Omega_1\Omega_2\ldots\Omega_n$, and let $x \in A_Q^*$, and suppose that $x \notin \{U(f(1)), U(f(2)), \ldots, U(f(k))\}$. Then,*

$$H_U(x) \geq n. \tag{9}$$

Proof. First note that

$$H_U(x) := \min\{|p| : U(p) = x\} \tag{10}$$

$$\stackrel{(a)}{=} \min\{|f(i)| : U(f(i)) = x\} \tag{11}$$

$$\stackrel{(b)}{=} \min\{|f(i)| : U(f(i)) = x, i \geq k+1\}, \tag{12}$$

where (a) is because f enumerates $dom(U)$, and
(b) is because $x \notin \{U(f(1)), U(f(2)), \ldots, U(f(k))\}$. By previous Lemma, $|f(i)| \geq n$ for all $i \geq k+1$, so

$$H_U(x) = \min\{|f(i)| : U(f(i)) = x, i \geq k+1\} \geq n. \tag{13}$$

□

We next define a computable function that builds such an x, computably from $\Omega_1\Omega_2\ldots\Omega_n$.

1. enumerate $k = 1, 2, \ldots$ until $\omega_k \geq 0.\Omega_1\Omega_2\ldots\Omega_n$ (it will stop as $\lim_{k\to\infty} \omega_k = \Omega_U$)
2. Compute $U(f(1))$, $U(f(2))$, $\ldots$, $U(f(n))$
3. Choose x as not belonging to $\{U(f(1)), U(f(2)), \ldots, U(f(k))\}$, let say take x to be the quasi-lexicographically smallest word not belonging to $\{U(f(1)), U(f(2)), \ldots, U(f(k))\}$.

Lemma 5. *As the procedure above is computable, we deduce that $H_U(\Omega_1\Omega_2\ldots\Omega_n) \geq H_U(x) + O(1)$. The theorem directly follows.*

1.5 Base in variance of randomness

So now, we have proven that there is at least one random real number, in every base $Q \in \mathcal{N}$. Now, is this randomness a base invariant, for $Q \in \mathcal{N}$?

{240} First, the author acknowleges that he makes the choice of confining himself to natural positional representations.

{240} The author says that it must be intuitively true, as changing from a base to another should know "prefer" some digits to another, and hence not destroy randomness, and second, that if randomness was destroyed, then there would be no inverse (computable) base transform. The whole problem, as the author says, is that there is no continuous computable transform that carries a

number from some base to another (but for β-expansions there is (I guess, by the one I have defined) !)

{241} The author announces the theorem (invariance of randomness through base representation), and proceeds to the proof. He defines the *value* v_Q similarly as equivalent to my δ_Q. He the defines $\mathbf{r}_Q$ as being the inverse of v_Q on $\mathcal{I} = (0,1)\backslash\mathcal{Q}$.

For the proof, he basically defines a function Γ to convert a sequence in base $Q+1$ to a seqeunce in base Q, that is computable and "almost" injective. I thinl that there is also something related to prefix-freeness of that function.

2 Hertling - Randomness spaces

References