# Topics in Randomness

Karthik Ravishankar

September 21, 2022

## 1 Lecture 1

The main notions are Kolmogorav complexity and Martin Lof Randomness.
**Kolmogorov complexity**: This measures the information content or complexity of a finite binary string. $C(\sigma)$ is the legnth of the shortest binary description of $\sigma$.
**Martin Lof Randomness**: An infinite binary sequence $X \in 2^\omega$ is random if it is in no effective measure zero set (typical sequences are random).

How are these notions related? The idea is that random sequences should have incompressible initial segments.This is seen by the fact that For almost all $X \in 2^\omega$, $\exists c \exists^\infty n$ such that $C(X|_n) \geq n - c$ and this implies $X$ is $ML - random$. (Miller 2005, NST 2006) An $X$ as above $\iff$ $X$ is $ML - random$ relative to $0'$ - $(2random)$.
Levin(73) and Chaitin(75) used modified forms of Kolmogrov complexity to characterize randomness. Let $K : 2^{<\omega} \to \omega$ be prefix - free complexity, then by (Schnorr 75) : $X$ is ML-random $\iff$ $\exists c \forall n K(X|_n) \geq n - c$.
Schnorr(71) characterized ML-randomness in terms of certain (semi computable) betting games to formalize the fact that Random reals are 'unpredictable'.
Partial Randomness/Hausdorff dimension : Lutz(2000/2003) effectivized Hausdorff dimension. Now the effective Hausdorff dimension of a singleton need not be 0. Mayordomo (2002) shoed that $dim(X) = liminf_n K(X|_n)/n = liminf_n C(X|n)/n$. So $ML-random \implies dim(X) = 1$. In Lutz and Lutz 2018, they gave the point to set principle: $dim_H(E) = min_{Z \in 2^\omega} sup_{X \in E} dim^Z(X)$ for any $E \subset 2^\omega$. This has applications to geometric measure theory (Lutz, Lutz, Don Stall...).

# 2 Lecture 2

**References:** i) Computability and Randomness - Nies 2009
ii) Algorithmic Randomness and Complexity - Downey and Hirschfeldt 2010

## 2.1 Kolmogorov Complexity

**Definition:** Let $M : 2^{<\omega} \to 2^{<\omega}$ be any partial function. Then $C_M(\sigma) = min\{|\tau : M(\tau) = \sigma\}$ or $\infty$.
Let $\{M_k\}_{k\in\omega}$ be an effective listing of all partial computable functions $2^{<\omega} \to 2^{<\omega}$.
Then we define a partial computable $V : 2^{<\omega} \to 2^{<\omega}$ by $V(0^k1\sigma) = M_k(\sigma)$. This is our universal machine and compresses as well as any other machine (upto a constant).
**Definition:** $C(\sigma) = C_V(\sigma)$ for $V$ as above. This is called the Kolmogorov complexity of $\sigma$.
If $M : 2^{<\omega} \to 2^{<\omega}$ is any partial computable function, then $C(\sigma) \leq^+ C_M(\sigma)$ i.e. there is at most a constant blow up in complexity and this constant is independent of $\sigma$. If $\hat{V}$ is another universal machine then $C(\sigma) =^+ C_{\hat{V}}(\sigma)$. We also have $C(\sigma) \leq^+ |\sigma|$ as the identity function is partial computable.
If $h$ is partial computable, then $C(h(\sigma)) \leq^+ C(\sigma)$. We always have incompressible strings :$\forall n \exists \sigma \in 2^n$ such that $C(\sigma) \geq n$.
$C(n) =^+ C(0^n) \leq^+ log_2(n+1)$. Here we are identifying $\sigma \in 2^{<\omega}$ with the natural number $n \in \omega$ if $1\sigma$ is the binary expansion of $n+1$.
$C$ is not computable but there is a computable function approximating it from above (and so $0'$ computable).

**Intuition**: We want random sequences to be incompressible. But no sequence $X \in 2^\omega$ has the property that $C(X|_n) \geq^+ n$ as we see below.
**Lemma**: If $|\tau| = \sigma$ i.e $\sigma$ is the string representing the number $|\tau|$ then $C(\sigma\tau) \leq^+ |\tau|$, here $|\tau|$ is a number..
Proof: Let $M$ be the machine which takes in $\tau$ and outputs $\sigma\tau$ where $\sigma = |\tau|$. Then $C(\sigma\tau) \leq^+ C_M(\sigma\tau) = |\tau|$.
**Theorem:** If $X \in 2^\omega$ then $\exists^\infty n C(X|_n) \leq^+ n - log(n)$.
Proof: For $k \in \omega$, let $\sigma = X|_k$ and $n = k + \sigma$ (where we are treating $\sigma$ as the number it codes) and $\sigma\tau = X|_n$. This means that $|\tau| = n - k = \sigma$. So $C(\sigma\tau) \leq^+ |\tau|$.
Now $k = log(\sigma)$ (treating $\sigma$ as a number) and so $k =^+ log(n)$ and so we're done.

Another consequence is as follows:
**Theorem**: It is not always the case that $C(\sigma\tau) \leq^+ C(\sigma) + C(\tau)$.
Proof: Fix $k \in \omega$. Take a string $\mu$ such that $|\mu| \geq 2^{k+1} + k$ ($\mu$ is long enough) and $C(\mu) \geq |\mu|$. Let $\sigma = \mu|_{k+\mu|_k}$ and let $\tau$ be the rest of $\mu$ i.e. $\sigma\tau = \mu$.
Then $C(\sigma) \leq^+ |\sigma| - k$ (as in the previous theorem), and so $C(\sigma) + C(\tau) \leq^+ |\sigma| = k + |\tau| = |\mu| - k \leq C(\mu) - k = C(\sigma\tau) - k$.

The problem in all this is that we are using the length of an input to code extra bits of information. In other words program length can underestimate 'information content'.

# 3 Lecture 3

Last time we saw that for any sequence in $2^\omega$ there are infinitely many initial segments which are compressible by upto a factor of $log(n)$.
Possible fixes to this: i) We could require monotonicity: Restrict to $M$ such that $\sigma \prec \tau \implies M(\sigma) \prec M(\tau)$ if both halt. But this isn't a very useful direction to pursue. Levin defined a monotone complexity using a more permissive model.
ii) We will restrict to machines $M$ which have prefix free domains, that is $\sigma, \tau \in dom(M) \implies \sigma \not\prec \tau$. We say $M, dom(M)$ are prefix -free.
Chaitin thought in terms of self delimiting Turing machines where $M(\tau) = \sigma$ if the machine has read exactly $\tau$ off the input tape before halting with output $\sigma$. This is clearly prefix free (by uniqueness of the run), and it is easy to see that any prefix - free $M$ can be given by a self delimiting machine- the machine starts doing all possible computations and checks whether it agrees with $\tau$.
Intuition behind prefix free machines: Length of the program (input) is intrinsic to the program and doesn't provide extra information.
We can effectively list the prefix free partial computable functions. Using this effective listing, we can define a universal machine as before: $U(0^k1\sigma) = M_k(\sigma)$.
Note that this is prefix free- If two strings are comparable, they must be input to the same prefix free machine and so cannot be comparable!
**Definition:** The prefix-free complexity of $\sigma$ denoted by $K(\sigma) = C_U(\sigma) = min\{|\tau| : U(\tau) = \sigma\}$.
We have $K(\sigma) \leq^+ |\sigma| + K(|\sigma|)$.
Proof: Define $M$ to be $M(\eta\sigma) = \sigma$ if $n = |\sigma|$ and $U(\eta) = n$. This is prefix free and shows $K(\sigma) \leq^+ K_M(\sigma) = |\sigma| + K(|\sigma|)$.
We can give a weaker bound of $K(\sigma) \leq^+ 2|\sigma|$ (To get rid of the $K$ in on the right hand side) above. To get this bound, just repeat digits and use 01 as a delimitter.
We can get $K(\sigma) \leq^+ |\sigma| + log|\sigma| + 2loglog|\sigma|...$
Now we finally have subadditivity:
$K(\sigma\tau) \leq^+ K(\sigma) + K(\tau)$.
Proof: Define $M$ to be $M(\tau_0\tau_1) = U(\tau_0)U(\tau_1)$ if both converge. We are using prefix free ness of $U$ here to make this well defined
$K$ is not computable but is approximable from above. $0'$ computes $K$.
**(Krafts Inequality)**: If $D \subset 2^{<\omega}$ is prefix-free, then $\sum_{\sigma \in D} 2^{-|\sigma|} \leq 1$.
Let $[D] = \cup_{\sigma \in D}[\sigma]$. Since $D$ is prefix free $\sigma, \tau \in D$ with $\sigma \neq \tau \implies [\sigma] \cap [\tau] = \emptyset$.
Therefore $\mu([D]) = \mu(\cup[\sigma]) = \sum_\sigma \mu[\sigma] = \sum_{\sigma \in D} 2^{-|\sigma|}$ and we know $\mu[D] \leq 1$.
As a corollary we get $\sum_{\sigma \in 2^{<\omega}} 2^{-K(\sigma)} \leq 1$.

# 4 Lecture 4

**Definition:** $X \in 2^\omega$ is $1-$ random if $K(X|_n) \geq^+ n$.
In fact we later show that $lim\ K(X|_n) - n \to \infty$ when $X$ is $1-$ random.
**Proposition:** Almost all $X \in 2^\omega$ are $1-$ random.
Proof: Let $S_c = \{\sigma \in 2^{<\omega} : K(\sigma) \leq |\sigma| - c\}$ and $U_c = [S_c] = \{X \in 2^\omega : \exists n K(X|_n) \leq n - c\}$. Note that $X$ is not $1-$random $\iff X \in \cap_{c\in\omega} U_c$.
But $\mu(U_c) = \mu([S_c]) \leq \sum_{\sigma\in S_c} \mu([\sigma]) = \sum_{\sigma\in S_c} 2^{-|\sigma|} \leq \sum_{\sigma\in S_c} 2^{-K(\sigma)-c} \leq 2^{-c} \sum_{\sigma\in 2^{<\omega}} 2^{-K(\sigma)} \leq 2^{-c}$.. Hence $\mu(\cap U_c) = 0$.

Recall: If $S \subset 2^{<\omega}$ is a *c.e.* set then $[S]$ is a $\Sigma^0_1$ class and $2^\omega - [S]$ is a $\Pi^0_1$ class.
**Definition**: A Martin Lof test is an effective sequence of $\Sigma^0_1$ classes (effective open sets) $\{V_n\}_{n\in\omega}$ such that $\mu(V_n) \leq 2^{-n}$. We say $X \in 2^\omega$ passes $\{V_n\}_n$ if $X \notin \cap V_n$.
$X \in 2^\omega$ is Martin Lof random if it passes all $ML-$ tests.
$ML-$ random $\implies$ $1-$ random. Every $ML-$ test gives us a measure $0, G_\delta$ set of non $ML-$ randoms. There are only countably many $ML-$ tests. Almost every $X \in 2^\omega$ is $ML-$ random.
**Aside**: Every measure 0 set $E \subset 2^\omega$ is covered by open sets of arbitrarily small measure. So $E \subset \cap_{n\in\omega} V_n$ for a Martin - Lof test $\{V_n\}$ relative to some oracle $Z$ (which basically codes the strings generating each $V_n$.)
$E \subset 2^\omega$ has non zero outer measure $\iff \forall Z$ there is a $Z - ML$ random $X \in E$.
Getting back to Prefix free complexity, the Kraft inequality has an effective converse.
**Theorem:** Let $\{d_i\}_{i\in\omega}$ be a sequence of natural numbers such that $\sum_{i\in\omega} 2^{-d_i} \leq 1$. Then there is a prefix free sequence $\{\sigma_i\}_{i\in\omega}$ such that $|\sigma_i| = d_i$. We can compute $\sigma_i$ from $d_0, ..., d_i$.
Proof: At stage $n$ we have determined $\sigma_0, ..., \sigma_{n-1}$. Let the terminating binary expansion of $1 - \sum_{i<n} 2^{-d_i} = x_0.x_1x_2...x_m$. Inductively we will have strings with $|\tau_j| = j$ for each $x_j \neq 0$ such that $\{\sigma_i\}_{i<n} \cup \{\tau_j\}_{x_j\neq 0}$ is prefix free.
Now if $x_{d_n} \neq 0$ let $\sigma_n = \tau_{d_n}$. Otherwise let $k < d_n$ be greatest such that $x_k \neq 0$. Such a $k$ will always exist by the weight condition. Then let $\sigma_n = \tau_k \frown 0^{k-d_n}$, and we add $\tau_k 1, \tau_k 01, ..., \tau_k 0^{k-d_n-1}1$ for the next stage.
**Corollary (Kraft Chaitin/Machine existence theorem)** Given an effective list of requests $< d_i, \tau_i >$ with $\sum 2^{-d_i} \leq 1$ then there is a prefix free machine $M$ such that $\forall i \exists \sigma_i$ such that $|\sigma_i| = d_i$ and $M(\sigma_i) = \tau_i$.
$K(\tau_i) \leq^+ d_i$. If we only have $\sum 2^{-d_i} < \infty$ then $K(\tau_i) \leq^+ d_i$. Such sets of requests are called bounded request sets.

# 5 Lecture 5

**Theorem:** $X$ is $1-$ random $\iff$ $x$ is $ML-$ random.
Proof: The backward direction is done- we constructed a $ML$ test above which prevents compressibility of initial segments.
For the forward direction, assume that $X$ is not $ML$ random. There is an $ML$ test $\{V_n\}_{n\in\omega}$ such that $X \in \cap V_n$. Let $\{S_n\}$ be an effective list of *c.e.* sets of strings such that $[S_n] = V_n$. WLOG we may assume that $S_n$ is prefix free (Just don't put a prefix, instead put a subset of the prefix which covers the same set as the prefix would). We define the request set $W = \{< |\sigma| - n, \sigma >: \sigma \in S_{2n}\}$. Then this is a bounded request set:
$\sum_{<d,\sigma>\in W} 2^{-d} \leq \sum_{n\in\omega}\sum_{\sigma\in S_{2n}} 2^{-|\sigma|+n} = \sum_{n\in\omega} 2^n \sum_{\sigma\in S_{2n}} 2^{-|\sigma|} = \sum_n 2^n \mu(V_{2n}) \leq \sum_n 2^n 2^{-2n} < \infty$ So $\sigma \in S_{2n} \implies K(\sigma) \leq^+ |\sigma| - n$. But $\forall n \exists k$ we have $X|_k \in S_{2n}$. So $X$ is not $1-$ random.
**Corollary:** There is a universal $ML-$ test, that is a test $\{U_n\}_n$ such that $\cap_n U_n$ is eactly the non $ML-$ randoms.
**Corollary:** i) The set of $ML-$ randoms is $\Sigma^0_2$.
ii) $2^\omega - U_1$ is a nonempty $\Pi^0_1$ class containing only $ML-$ randoms.
iii) There is a (super) low $ML-$ random.
iv) The leftmost point in $2^\omega - U_1$ is left - c.e ML -random. (computably approximable from below).

**Definition:** If $M$ is a prefix free machine taking binary strings to binary strings, then $\Omega_M = \mu([dom(M)]) = \sum_{\sigma\in dom(M)} 2^{-|\sigma|}$ is the halting probability of $M$.
Chaitin's $\Omega$ is $\Omega = \Omega_U$.
**Theorem:** $\Omega$ is a left c.e. $ML$ random.
Proof: Let $U_t$ be the stage $t$ approximation to $U$. Assume $U_t$ contains strings of length at most $t$. Let $\Omega_t = \mu([domU_t])$. Then $\{\Omega_t\}$ is a non decreasing computable sequence of rationals such that $\Omega = lim\Omega_t$.
Define a partial computable $g : 2^{<\omega} \to 2^{<\omega}$ as follows: On input $x$ of length $n$ wait for $t$ such that $0.x \leq \Omega_t \leq 0.x + 2^{-n}$. Then output the least element $y$ not in the range of $U_t$.
If $X = \Omega|_n$ then such a $t$ exists. By stage $t$ all $U-$ programs of length $\leq n$ have halted. So $K(y) > n$ where $y = g(\Omega|_n)$.
Therefore $K(\Sigma|_n) \geq^+ K(g(\Omega|_n)) > n$.
Other left c.e. $ML-$ randoms: $\sum_n 2^{-K(n)}$, $\mu(U_1)$. In general $\mu(V)$ where $V$ is a $\Sigma^0_1$ class and $2^\omega - V$ is non empty and contains noly $ML$-randoms.
**Theorem:** $K$ is the least (w.r.t $\leq^+$) function $D : 2^{<\omega} \to 2^{<\omega}$ computable from above and having $\sum 2^{-D(\sigma)} < \infty$.
Proof: $W = \{< D(\sigma) + k, \sigma >: \sigma \in 2^{<\omega}, k \in \omega\}$ is a bounded request set: $\sum_{<d,\sigma>\in W} 2^{-d} = \sum_{k\in\omega}\sum_{\sigma\in 2^{<\omega}} 2^{-D(\sigma)-k} = \sum_{k\in\omega} 2^{-k} \sum_{\sigma\in 2^{<\omega}} 2^{-D(\sigma)} = 2\sum_{\sigma\in 2^{<\omega}} 2^{-D(\sigma)}$. Therefore $K(\sigma) \leq^+ D(\sigma)$.

# 6 Lecture 6

For any prefix free machine $M$ let $P_M(\sigma) = \mu[M^{-1}(\sigma)]$.
**Coding Theorem:** For any prefix free machine $M$, $P_M(\sigma) \leq^* 2^{-K(\sigma)}$.
$P_U(\sigma) =^* 2^{-K(\sigma)}$ where $U$ is the universal machine and $\leq^*$ is '$\leq$ upto multiplicative constant'.
**Corollary**: $\exists c \forall \sigma$, $\sigma$ has at most $c$ shortest $U-$ descriptions.
Proof: Let $D(\sigma) = ciel(-logP_M(\sigma))$. Note that $D$ is computable approximable from above and $D(\sigma) \geq -logP_M(\sigma) \leq D(\sigma) - 1$. So $2^{-D(\sigma)} \leq P_M(\sigma) \leq 2^{-D(\sigma)+1}$. So $\sum_\sigma$ of LHS $\leq \sum_\sigma P_M(\sigma) \leq 1$. Thus $2^{-K(\sigma)} \geq^* 2^{-D(\sigma)} \geq^* P_M(\sigma)$. Since $P_U(\sigma) \geq 2^{-K(\sigma)}$ the second statement follows.
**Counting Theorem:** There is a $c \in \omega$ such that:
i) $\forall d, n, |\{\sigma \in 2^n : K(\sigma) \leq n + K(n) - d\}| < 2^c 2^{n-d}$.
ii) $\forall b, n, |\{\sigma \in 2^n : K(\sigma) \leq K(n) + b\}| < 2^c 2^b$.

Remark: a) Most strings have complexity close$^+$ to the upper bound
b) $A \in 2^\omega$ is $K-$ trivial if $K(A|_n) \leq^+ K(n)$.
Solovay showed that $K-$ trivial $\not\Longrightarrow$ computable. But computable $\Longrightarrow$ $K-$ trivial..$C-$ trivial $\Longrightarrow$ computable. By $ii)$ above, at most $2^c 2^b$ $K-$ trivials with constant $b$. So only countable many $K-$ trivials. In fact all are $\Delta^0_2$. ($0'$ computes it since $K \leq_T 0'$ and we have a $0'$ computable tree with only isolated paths - since tree is bounded width).
c)The counting theorem is not tight.

Proof (Counting Theorem): Let $M$ be the prefix free machine $M(\tau) = |U(\tau)|$. By the coding theorem $\exists c, \forall n P_M(n) < 2^c 2^{-K(n)}$. Let $S_{n,d} = S = \{\sigma \in 2^n : K(\sigma) \leq |\sigma| + K(|\sigma|) - d\}$. We have $P_M(n) \geq |S| 2^{-n-K(n)+d}$. So $|S| 2^{-n-K(n)+d} < 2^c 2^{-K(n)}$ so $|S| < 2^c 2^{n-d}$.

**Definition (Martingales)** : Let $B(\sigma)$ be the capital remaining after betting on $|\sigma|$ bits and seeing $\sigma$. $B(\sigma) = \frac{B(\sigma 0) + B(\sigma 1)}{2}$.

# 7 Lecture 7

Betting on a binary string bit by bit. Start with $B(\lambda)$ 'dollars'. After betting along $\sigma$ we have $B(\sigma)$. If we bet $\gamma$ on 0, then $B(\sigma 0) = B(\sigma 1) = B(\sigma) + \lambda + B(\sigma) - \lambda = 2B(\sigma)$.
**Definition(Martingales)** $B : 2^{<\omega} \to \mathbb{R}^{\geq 0}$ is a martingale if
$\forall \sigma, B(\sigma) = \frac{B(\sigma 0)+B(\sigma 1)}{2}$
B succeeds on $X \in 2^\omega$ if $limsup B(X|_n) = \infty$. Requiring $liminf B(X|_n)$ gives the same notion although rate of convergence may change.
Example: $B_\tau(\sigma)$ bets $2^{|\sigma|}$ when $\sigma \prec \tau$ and $2^{|\tau|}$ if $\tau \prec \sigma$ and 0 otherwise. This martingale fails for all $X \in 2^\omega$.
**Definition** : A supermartingale is a generalization of a martingale where we replace the equality by the inequality $S(\sigma 0) + S(\sigma 1) \leq 2S(\sigma)$.
**Proposition** For each supermatingale $S$ there is a martingale $B$ with the same start capital, such that $\forall \sigma B(\sigma) \geq S(\sigma)$.
Proof: Send extra capital to the left.
**Proposition**: A weighted sum of (super)martingales is a (super) martingale as long as the start capital is finite.
**(Kolmogrov's Inequality)**: If $S$ is a supermartingale and $W \subset 2^{<\omega}$ is prefix free, then $\sum_{\sigma \in W} 2^{-|\sigma|} S(\sigma) \leq S(\lambda)$.
Proof: WLOG assume $W$ is finite. We prove by induction on the length $n$ of the longest string in $W$. Clearn for $n = 0$, let $W_0 = \{\sigma : 0\sigma \in W\}$ and $W_1 = \{\sigma : 1\sigma \in W\}$. Then $S(\lambda) \geq 1/2(S(0)+S(1)) \geq 1/2(\sum_{\sigma \in W_0} 2^{-|\sigma|} S(0\sigma) + \sum_{\sigma \in W_1} 2^{-|\sigma|} S(1\sigma)) = \sum_{\sigma \in W} 2^{-|\sigma|} S(\sigma)$.
**Definition**: A supermartingale $S$ is (left) c.e. if $S(\sigma)$ is left c.e. (a limit of a computable non decreasing sequence of rationals) uniformly in $\sigma$. (also called c.e. or lower semicomputable).
**Corollary**: For a supermartingale $S$, $\mu\{Z \in 2^\omega : \exists n S(Z|_n) \geq b\} \leq S(\lambda)/b$.
Proof: Let $W$ be the prefix free set of minimal strings $\sigma$ such that $S(\sigma) \geq b$, then $\mu(W) = \sum_{\sigma \in W} 2^{-|\sigma|}$. By Kolmogrov $\sum_{\sigma \in W} 2^{-|\sigma|} b \leq \sum_{\sigma \in W} 2^{-|\sigma|} S(\sigma) \leq S(\lambda)$.
**Proposition:** The follow are equivalent for $A \in 2^\omega$.
i) No c.e. supermartingale succeeds on $A$
ii) No c.e. martingale succeeds on $A$
iii) $\sum 2^{n-K(A|_n)} < \infty$
iv) $limK(A|_n) - n = \infty$.
v) $K(A|_n) \geq^+ n$
vi) $A$ is $ML$ random.
Proof: *vi)* $\implies$ *i)* - Given a supermartingale $S$ with $S(\lambda) \leq 1$, define $V_n = \{Z \in 2^\omega : \exists m S(Z|_m) > 2^n\}$. Then $\{V_n\}_{n \in \omega}$ is a $ML$ test. IF $S$ succeeds on $A$, then $A \in \cap V_n$.
*ii)* $\implies$ *iii)* - Define $M(\sigma) = \sum_{\tau \prec \neq \sigma} 2^{|\tau|-K(\tau)} + \sum_{\sigma \prec \tau} 2^{|\sigma|-K(\tau)} = \sum_{\tau \in \sigma} 2^{-K(\tau)} B_\tau(\sigma)$. $M(\lambda) = \sum 2^{-K(\tau)} \leq 1$. By *ii* $M$ does not succeed on $A$. So there is a $b$ such that $M(A|_m) < b$ for all $m$, but $\sum_0^m 2^{n-K(A|_n)} \leq M(A|_m) < b \forall m$.