Part 3: Randomness extraction, asymptotic Hamming distance, and the LIL

Bjørn Kjos-Hanssen
Cameron Freer

Conference on game-theoretical probability and related topics
2012

Definition

A set X is immune if for each $N \in \mathfrak{C}$, $N \not\subseteq X$. If $\omega \setminus X$ is immune then X is co-immune. If X is both immune and co-immune then X is bi-immune.

Definition

A set X is stochastically bi-immune if for each set $N \in \mathfrak{C}$, $X \upharpoonright N$ satisfies the strong law of large numbers, i.e.,

$$\lim_{n \to \infty} \frac{|X \cap N \cap n|}{|N \cap n|} = \frac{1}{2}.$$

Definition

A set X is immune if for each $N \in \mathfrak{C}$, $N \not\subseteq X$. If $\omega \setminus X$ is immune then X is co-immune. If X is both immune and co-immune then X is bi-immune.

Definition

A set X is stochastically bi-immune if for each set $N \in \mathfrak{C}$, $X \upharpoonright N$ satisfies the strong law of large numbers, i.e.,

$$\lim_{n\to\infty} \frac{|X \cap N \cap n|}{|N \cap n|} = \frac{1}{2}.$$

Could also be called: *weakly Mises-Wald-Church stochastic*

Definition

A sequence $X \in 2^\omega$ is *Mises-Wald-Church stochastic* if no partial computable monotonic selection rule can select a *biased subsequence* of X, i.e., a subsequence where the relative frequencies of 0s and 1s do not converge to $1/2$.

Hamming distance $d(\sigma, \tau)$ is given by

$$d(\sigma, \tau) = |\{n : \sigma(n) \neq \tau(n)\}| .$$

Let the collection of all infinite computable sets be denoted by $\mathfrak{C}$. Let $p : \omega \to \omega$. For $X, Y \in 2^\omega$ and $N \in \mathfrak{C}$ we write

$$\begin{aligned} X \sim_{p,N} Y &\iff (\forall^\infty n \in N) \quad (d(X \upharpoonright n, Y \upharpoonright n) \leqslant p(n)). \\ X \sim_p Y &\iff X \sim_{p,\omega} Y. \\ X \asymp_p Y &\iff X \sim_{p,L} Y \quad (\exists L \in \mathfrak{C}). \end{aligned}$$

Easy to understand randomness extraction in terms of $\asymp_p$.
Seems hard in terms of $\sim_p$.

Let $\mathcal{A}$ and $\mathcal{B}$ with $\mathbb{P}(\mathcal{A}) = \mathbb{P}(\mathcal{B}) = 1$ be given by

$$\mathcal{A} = \{X : X \text{ is weakly 3-random}\},$$
$$\mathcal{B} = \{X : X \text{ is stochastically bi-immune}\}.$$

Theorem

Let $p : \omega \to \omega$ be any computable function such that $p(n) = \omega^*(\sqrt{n})$. Let Φ be a Turing reduction. Then

$$(\forall X \in \mathcal{A})(\exists Y \asymp_p X)(\Phi^Y \notin \mathcal{B}).$$

Two cases: Φ maps almost every random to a random, or not.

Question

Why did you obtain results for $\asymp_p$ but not for $\sim_p$? Lack of problem-solving... or a valid reason?

Theorem (Law of the iterated logarithm, Khintchine 1924)

Let $X = (X_0, X_1, \ldots)$ *be a random variable on* 2^ω *having the fair-coin distribution. Let* $S_n = \sum_{k=0}^{n-1} X_k = d(X \upharpoonright n, \varnothing \upharpoonright n)$. *Then with probability one,*

$$\limsup_{n\to\infty} \frac{S_n - \frac{n}{2}}{\varphi(n)\sqrt{n}} = 1,$$

where $\varphi(n) = \sqrt{\frac{1}{2}\log\log n}$.

Theorem (Law of the iterated logarithm, Khintchine 1924)

Let $X = (X_0, X_1, \ldots)$ be a random variable on 2^ω having the fair-coin distribution. Let $S_n = \sum_{k=0}^{n-1} X_k = d(X \restriction n, \varnothing \restriction n)$. Then with probability one,

$$\limsup_{n\to\infty} \frac{S_n - \frac{n}{2}}{\varphi(n)\sqrt{n}} = 1,$$

where $\varphi(n) = \sqrt{\frac{1}{2}\log\log n}$.

- The standard deviation of S_n is simply $\sqrt{n}$, so why the strange $\varphi(n)$?

Theorem (Law of the iterated logarithm, Khintchine 1924)

Let $X = (X_0, X_1, \ldots)$ be a random variable on 2^ω having the fair-coin distribution. Let $S_n = \sum_{k=0}^{n-1} X_k = d(X \restriction n, \varnothing \restriction n)$. Then with probability one,

$$\limsup_{n\to\infty} \frac{S_n - \frac{n}{2}}{\varphi(n)\sqrt{n}} = 1,$$

where $\varphi(n) = \sqrt{\frac{1}{2}\log\log n}$.

- The standard deviation of S_n is simply $\sqrt{n}$, so why the strange $\varphi(n)$?
- Michel Weber (1990): can replace φ by arbitrarily slow-growing function if we take $\limsup_{n\in N}$ for sparse set N.

Theorem (Law of the iterated logarithm for subsequences, Michel Weber 1990)

Let $N = \{\nu_1 < \nu_2 < \cdots\} \subseteq \omega$ *and let* $\{Y_n\}$ *be an i.i.d. sequence with* $\mathbb{E}(Y_n) = 0$ *and* $\mathbb{E}(Y_n^2) = 1$. *Let* $S_n = Y_1 + \cdots + Y_n$. *Let*

$$p_n = \left|\{m \leqslant n : N \cap (2^{m-1}, 2^m] \neq \varnothing\}\right|,$$

$$\mathcal{L}(k) = \ln p_n \quad \textit{if} \quad k \in (2^{n-1}, 2^n].$$

Then we have

$$\limsup_{j \to \infty} \frac{S_{\nu_j}}{\sqrt{2\nu_j \mathcal{L}(\nu_j)}} = 1 \quad a.s.$$

For $N = \omega$ we get the usual law of the iterated logarithm.
For sparse sets N, the function $\mathcal{L}(\nu_j)$ is an arbitrarily slow-growing function, so the dominator is standard deviation ($\sqrt{\nu_j}$) times a small factor.

Theorem

If X is Kurtz random relative to A and $S_n := d(X \upharpoonright n, A \upharpoonright n)$ then

$$\limsup_{n\to\infty} \frac{S_n - \frac{n}{2}}{\varphi(n)\sqrt{n}} \geqslant 1.$$

Theorem (K, 2007)

A has non-DNR Turing degree
$\Longrightarrow$ *each Martin-Löf random set X is Kurtz random relative to A.*

(Deeper but less useful here: the converse also holds; Greenberg and J. Miller, 2009.)

Corollary

$A \asymp_p X$*, where* p *is computable,* X *is Martin-Löf random, and*
$\mathbb{P}(\{Y : Y \asymp_p X\}) = 0$
$\Longrightarrow$ *A has DNR degree.*

The end