Randomness Conservation over Algorithms

Samuel Epstein
samepst@bu.edu
Boston University

May 7, 2014

Abstract

Current discrete randomness and information conservation inequalities are over total recursive functions, i.e. restricted to deterministic processing. This restriction implies that an algorithm can break algorithmic randomness conservation inequalities. We address this issue by proving tight bounds of randomness and information conservation with respect to recursively enumerable transformations, i.e. processing by algorithms. We also show conservation of randomness of finite strings with respect to enumerable distributions, i.e. semicomputable semi-measures.

1 Introduction

A finite string $x$ is typical of a computable probability measure $p$ if the length of its shortest description with respect to a prefixless universal algorithm, $K(x) \in \mathbb{N}$, is close to the length of its $p$ code, $[-\log p(x)]$. $K(x)$ is the Kolmogorov complexity of $x$. Such $p$-typical elements $x$ have a low deficiency of randomness, $d_p(x) = [-\log p(x)] - K(x)$. Atypical elements $x$ have extra regularity that allows them to be compressed to length $K(x) \ll [-\log p(x)]$. The algorithmic joint information of individual finite strings $x$ and $y$ is $I(x:y) = K(x) + K(y) - K(x,y)$, the difference between the length of the shortest separate descriptions of $x$, $y$ and the length of the shortest joint description of $x$, $y$. Strings are independent if they have low mutual information.

It has been shown that this definition of information is robust, i.e. invariant to processing by total functions $A$ over finite strings [Lev74]. Such deterministic functions cannot create an increase, $(I(A(x):y) - I(x:y))$, in the mutual information of strings $x$ and $y$ by more than a constant factor, dependent on $A$. Randomness is also conserved over total recursive functions, where $d_{Ap}(A(x))$ is not much more than $d_p(x)$. The measure $(Ap)(y) = \sum_{A(z)=y} p(z)$ is the image of $p$ under $A$.

However randomness is not conserved over the set of limit computable functions $B$ over finite strings, i.e. functions computed by possibly non-halting algorithms. There exists a simple limit computable function $B$, a probability measure $p$, and a string $x$ such that (1) $x$ is $p$-typical and (2) $B(x)$ not $(Bp)$-typical (see theorem 2). Thus randomness conservation inequalities do not hold with respect to $B$ and $x$. This article shows only exotic strings $x$ break information and randomness conservation inequalities over limit computable functions. We use $I(x;H) = K(x) - K(x|H)$, to denote the amount of information the halting sequence $H$ has about $x$. A string $x$ is called exotic if $I(x;H)$ is large. We prove randomness and information conservation inequalities over non-exotic strings and limit computable functions.
In addition, this article uses notions of rarity over enumerable distributions. Enumerably distributable measures are semi-measures, nonnegative functions \( p \) over strings such that \( \sum_{x \neq \perp} p(x) \leq 1 \). The images of measures under partial functions are semi-measures. This article also shows randomness and information conservation of infinite binary strings. This article contains continuous results limited to specialized definitions of information and rarity that are amenable to natural extensions of the proofs in Sections 4 and 5.

2 Conventions

Let \( \mathbb{R}, \mathbb{Q}, \mathbb{N}, \Sigma, \Sigma^*, \Sigma^\infty \) be the set of reals, rationals, natural numbers, bits, finite strings, and infinite binary sequences. \( \Sigma^* \sqcup \Sigma^\infty \) is the length of string \( x \). \( \alpha \leq \| x \| \) represents the first \( n \) bits of \( \alpha \in \Sigma^\infty \), and \( \alpha \geq \| x \| \) represents the remaining bits of \( \alpha \). We say \( x \sqsubseteq y \) if \( x \in \Sigma^* \) is a prefix of \( y \in \Sigma^\infty \). \( \langle x \rangle \in \Sigma^* \) is a self-delimiting representation of \( x \in \Sigma^* \). We use \( O_{a_1, \ldots, a_k}(X) \) to denote any quantity bounded in magnitude by \( CX \) where \( C \in \mathbb{N} \) is dependent on parameters \( a_1, \ldots, a_k \). Let \( [Z] = 1 \) if statement \( Z \) is true, and \( [Z] = 0 \), otherwise. Let \( U_y \) be a fixed universal prefixless algorithm with auxiliary input \( y \in \Sigma^\infty \) and \( K(x|y) = \min \|p|: U_y(p) = x \) \).

Function \( p : \Sigma^* \to \mathbb{R}_{\geq 0} \) is a semi-measure if \( \sum_{x \neq \perp} p(x) \leq 1 \). \( p \) is also a measure if \( \sum_{x \neq \perp} p(x) = 1 \). A nonnegative function \( f \) is semicomputable if the subgraph \( \{ (x, q) : f(x) > q \in \mathbb{Q} \} \) is enumerable. \( f \) is \( \alpha \)-semicomputable if \( f \) is semicomputable over \( U_\alpha \). For a fixed enumeration of semicomputable semi-measures, \( \{ p_n \} \ni p, K(p|y) = \min_{p_n = p} K(n|y) \). The function \( m(x|y) \) is a majorant of \( \alpha \)-semicomputable semi-measure relativized to \( y \in \Sigma^\infty \).

By the coding lemma \( K(x|y) = -\log m(x|y) \pm O(1) \). Function \( f : \Sigma^* \to \Sigma^* \) is a partial recursive function if it can be computed by a Turing machine \( T \). In particular, \( f(x) = \perp \) if \( T \) halts without output or \( T \) does not halt. A function \( B : \Sigma^* \to \Sigma^* \) is limit computable if there is a Turing machine \( T \) such that if \( B(x) \neq \perp \) then machine \( T \), when given input \( x \), will at some point, print \( B(x) \) to the output tape and make no further changes to the output (and then either halt or never halt). Note that if \( B(x) = \perp \) then such \( T \) will eventually output nothing (\( \perp \)) when given input \( x \), and (may) either halt or not halt). For a fixed enumeration \( \{ B_n \} \ni B \) of limit computable functions over strings, \( K(B) = \min_{B_n = B} K(n) \). The halting sequence, \( \mathcal{H} \), is the characteristic sequence of the domain of \( U \). Chaitin’s halting probability is defined by \( \Omega = \sum_{x \neq \perp} m(x) \). The deficiency of randomness of \( x \in \Sigma^* \) with respect to an arbitrary semi-measure \( p \), relative to \( y \in \Sigma^\infty \), is \( d_p(x|y) = [-\log p(x)] - K(x|y) \). For semi-measure \( p \), we say nonnegative function \( t \) is a \( p \)-test, if \( \sum_{x \neq \perp} p(x) t(x) \leq 1 \).

3 Related Work

This work is resultant from my trip to Montpellier with Alexander Shen and P´eter Gács. Kolmogorov complexity was introduced independently in [Kol65, Sol64, Cha75]. For a detailed history of Algorithmic Information Theory, we refer to [LV08], [Lev74] introduced laws of information non-growth over deterministic functions and later revisited in [Lev84]. The definition of \( \Gamma^\infty(\alpha; \mathcal{H}) \) and theorem 5 relies on modified arguments of Section 2 in [Lev84]. An extension of rarity to semi-measures can be found in the recent work of [Lev12] and also can seen in the work of [Lev84], [Gacs13] contains an extended survey of randomness conservation inequalities and also describes properties of the rarity term \( D \) used in this article.
4 Randomness Conservation

The central trick of the article is using the fact that $2^\mathcal{I}(x; \mathcal{H})$ is a majorant $\mathcal{H}$-semicomputable, $m$-test. This enables proof techniques centered around the creation of $m$-tests $t$. For any computable measure $p$, the function $t_p(x) = m(x)/p(x)$ is a majorant (up to a multiplicative constant) semicomputable $p$-test. For more information about universal semicomputable tests, see [Gacs13]. Proposition 1 follows from $I(x; \mathcal{H}) = \log m(x|\mathcal{H})/m(x) + O(1) = d_m(x|\mathcal{H}) + O(1)$, and from the fact that $m$ is computable from $\mathcal{H}$.

**Proposition 1.** $I(x; \mathcal{H}) = d_m(x|\mathcal{H}) + O(1)$.

Theorem 1 extends finite randomness conservation inequalities to limit computable functions $B$ and discrete semicomputable $m$-measure $p$. For convenience we define $d_p(\perp) = 0$. Randomness is conserved for all strings that are non-exotic, i.e. have low mutual information with the halting sequence. The proof follows from the definition of an $m$-test $t$ such that $\log t(x) = d_{B_p}(B(x)) - d_p(x) + O_{B,p}(1)$. Theorem 2 shows the tightness of theorem 1, and represents a generalization of the example used in the introduction. The proof of theorem 2, leverages arguments in the proof of theorem 7, adapted to the case of finite strings [BHPS13].

**Theorem 1.** For limit computable function $B : \Sigma^* \rightarrow \Sigma^{*\infty}$ and semicomputable $m$-measure $p$, for all $x \in \Sigma^*$, $d_{B_p}(B(x)) < d_p(x) + I(x; \mathcal{H}) + O_{B,p}(1)$.

**Proof.** We use the $\mathcal{H}$-semicomputable $m$-test $t$, where $t(x) = m(B(x)p(x))/(m(x)Bp(B(x)))$. Since $t$ is computable in the limit, it is $\mathcal{H}$-computable, with $K(t|\mathcal{H}) = O_{B,p}(1)$. Also $t$ is an $m$-test with $\sum_x m(x)t(x) = \sum_x m(B(x)p(x)/Bp(B(x)) = \sum_{y \in \text{Range}(B)} m(y) \sum_{x:B(x)=y} p(x)/Bp(y) \leq \sum_y m(y) \leq 1$. So $d_{B_p}(B(x)) - d_p(x) < \log t(x) + O(1) < d_m(x|\mathcal{H}) + K(t|\mathcal{H}) < I(x; \mathcal{H}) + O_{B,p}(1)$.

**Theorem 2.** For all $b, c \in \mathbb{N}$, there exists limit computable function $B$, measure $p$, and string $x$ such that $K(B, p) = O(\log bc)$, $d_{B_p}(B(x)) = b + c + O(\log bc)$, $d_p(x) = b + O(\log bc)$, and $I(x; \mathcal{H}) = c + O(\log bc)$.

**Proof.** Let $n = b + c$ and $\Omega_{\leq c}$ be a string representing the first $c$ bits of $\Omega$. So $\Omega_{\leq c}$ is a random string and can be identified with a $c$-bit number that is enumerable from below. Let $\preccurlyeq$ be a partial order over finite strings where if $x, y \in \Sigma^n$, then $x \preccurlyeq y$ iff the $n$ bit number associated with $x$ is smaller than the $n$-bit number associated with $y$.

Let $B(x) = \perp$ if $\|x\| \neq n$. Otherwise $B(x) = x$ if $x_{>b} \preccurlyeq \Omega_{c}$, $B(x) = x_{<b}$ if $x_{>b} = \Omega_{c}$, or $B(x) = \perp$ if $\Omega_{c} < x_{>b}$. $B$ can be enumerated by a non-halting Turing machine. Let $x = 0^b\Omega_{c}$. $x$ has deficiency $b + O(\log bc)$ with respect to the uniform measure over $n$-bit strings $p(x) = \|x\| = n|2^{-n}$.

This is because $d_p(x) = [-\log p(x)] - K(x) = b + c - K(\Omega_{c}) + O(\log(bc)) + b + O(\log(bc))$. $B(x)$ has a greater randomness deficiency with respect to the probability measure $Bp$. This is because $d_{B_p}(B(x)) = d_{B_p}(0^b) = [-\log Bp(0^b)] - K(0^b) = b + c - O(\log(bc))$. In addition, $\Omega_{c}$ is simple relative to $\mathcal{H}$ and $c$, since $\Omega$ can be computed to any degree of precision by an algorithm with access $\mathcal{H}$. Thus $K(\Omega_{c}|\mathcal{H}) = O(\log c)$ implies $I(x; \mathcal{H}) = K(0^b\Omega_{c}) - K(0^b\Omega_{c}|\mathcal{H}) = c + O(\log(bc))$. $\square$
5 Information Conservation

We prove information nongrowth over limit computable functions. Theorem 3 shows conservation of the symmetric information $I(x:y)$ and theorem 4 shows conservation of asymmetric information $I(x;H)$ between $x$ and the halting sequence.

Theorem 3.
For $x, y \in \Sigma^*$ and limit computable function $B$, $I(B(x):y) < I(x:y) + I(x,y;H) + O_B(1)$.

Proof. We define the function $s : \Sigma^* \rightarrow \Sigma^*$ where $s(x) = cm(f(x)|H)(m(x)/m(f(x)))$ when $f(x) \neq \bot$, and $s(x) = 0$ otherwise. $c$ is a constant to be determined later. The function $s$ is a semimeasure by the following reasoning. Since $m$ is a majorant semi-computable semi-measure, $m(y) > \sum_{x:f(x)=y} m(x)/O_f(1)$. So $\sum_{x} s(x) = c \sum_{y} \sum_{x:f(x)=y} m(y)|H|m(x)/m(y) < O_f(1)c \sum_{y} m(y)|H| \leq 1$, for proper choice of $c$ solely dependent on $f$. Since $s$ is computable relative to $H$, we have that $\log s(x) < \log m(x)|H| + K(s) + O(1)$. So $I(f(x);H) < I(x;H) + O_f(1)$.

Theorem 4. For partial recursive function $f$ and all $x \in \Sigma^*$, $I(f(x);H) < I(x;H) + O_f(1)$.

Proof. Let $P$ be an enumeration of all semicomputable continuous semi-measures, $M(x) = \sum_{i=1}^2 t_{-i}P_i(x)$. Semicomputable functions $f : \Sigma^* \rightarrow \mathbb{R}_{\geq 0}$ are defined with respect to their elementary functions $f^G : \Sigma^* \rightarrow \mathbb{R}_{\geq 0}$, with $f(\alpha) = \sup_{\beta \subseteq \alpha} f^G(\beta)$. Such $f$ is semicomputable if its elementary function $f^G$ is semicomputable. Let $f^G$ be a fixed enumeration such elementary functions and let $K(f) = \min_{f^G \supseteq f} K(n)$. For continuous semi-measure $Q$, we say semicomputable $t$ is a $Q$-test if $Q(|t(\alpha) > 2^m|) < 2^{-m}$ for all $m \in \mathbb{N}$. The domain of such $t$ is extended to finite strings $x$, with $t(x) = \min_{\alpha \subseteq x} t(\alpha)$.

The function $\llcorner$-sup is the supremum under the partial order of $\subseteq$ on $\Sigma^{\infty*}$. A function $\nu : \Sigma^* \rightarrow \Sigma^*$ is monotone iff for all $p, q \in \Sigma^*$, $\nu(p) \subseteq \nu(pq)$. Then monotone function $B : \Sigma^{\infty*} \rightarrow \Sigma^{\infty*}$ denotes the unique extension of $\nu$, where $B(p) \overset{def}{=} \llcorner$-sup $\{\nu(p_{\leq n}) : n \leq ||p||, n \in \mathbb{N}\}$ for all $p \in \Sigma^{\infty*}$. We say $\nu$ is a recursive monotone function if there is a Turing machine $T$ with a write only output tape such that
\( \nu(x) \) is equal to the output of \( T \) on input \( x \). For \( x \in \Sigma^* \), we say \( D^{-1}(x) = D \subseteq \Sigma^* \) is the prefix-free set of finite strings \( y \) such that \( \nu(y^-) \subseteq x \sqsupseteq \nu(y) \).

Let \( T_{M^*} \) be an enumeration of all \( H \)-semicomputable \( M \)-tests. The information that \( H \) has about \( \alpha \in \Sigma^* \) is defined to be the logarithm of a weighted sum of such tests, with \( \Gamma^\infty(\alpha;H) = \log \sum_{i \in T_{M^*}} m(i|H)t_i(\alpha) \). Note however that \( 2^{\Gamma^\infty(\alpha;H)} \) is not necessarily an \( M \)-test, since \( M \) is superadditive. This is a major difference from the finite case, where \( 2^{H(x;H)} \) is an \( m \)-test. The domain of \( \Gamma^\infty(\alpha;H) \) is extended to \( \Sigma^* \) with \( \Gamma^\infty(x;H) = \inf_{x \subseteq \alpha \subseteq \Sigma^*} \Gamma^\infty(\alpha;H) \) for all \( x \in \Sigma^* \). Theorem 5 represents the continuous variant of theorem 4. The theorem shows the asymmetric information term \( \Gamma^\infty \) has nongrowth properties with respect to recursive monotone transformations.

**Theorem 5.** For recursive monotone function \( B : \Sigma^* \rightarrow \Sigma^* \) and all \( \alpha \in \Sigma^* \), \( \Gamma^\infty(B(\alpha);H) < \Gamma^\infty(\alpha;H) + O_B(1) \).

**Proof.** Let \( \mu(x) = M(B^{-1}(x)) \). \( \mu \) is a semi-measure because \( \mu(\bot) \leq 1 \) and \( \mu(x0) + \mu(x1) = M(B^{-1}(x0)) + M(B^{-1}(x1)) \leq M(B^{-1}(x)) = \mu(x) \). \( \mu \) is semicomputable because \( M \) is semicomputable and \( B^{-1}(x) \) is enumerable. Since \( M \) is a majorant semicomputable semi-measure, there exists \( c \) solely dependent on \( B \) with \( \mu(x) \leq cM(x) \). So for any open set \( U \), \( \mu(U) < cM(U) \).

For all \( t \in T_{M^*} \) and \( m \in \mathbb{N} \), let \( S \) be a set of finite strings representing the maximal binary intervals of \( \{ \alpha : t(\alpha) > 2^m \} \). So \( 2^{-m} > M(S) \geq \mu(S)/c \). So \( c2^{-m} > \mu(S) = M(B^{-1}(S)) \geq M(\{ \alpha : B_t(\alpha) > 2^m \}) \), where \( B_t(\alpha) = \min_{\beta \supseteq B(\alpha)} t(\beta) \). So \( B_t(\alpha)/c \in T_{M^*} \) is an \( M \)-test. \( B_t \) is \( H \)-computable because \( t \) and \( B \) are \( H \)-semicomputable, with \( K(B_t|H) < K(t|H) + O_B(1) \). So this implies the inequality \( \Gamma^\infty(B(\alpha);H) = \log \sum_{i \in T_{M^*}} m(i|H)t_i(B(\alpha)) = \log \sup_{B \in T_{M^*}} m(B_t|H)B_t(\alpha) + O_B(1) = \log \sum_{i \in T_{M^*}} m(i|H)t_i(B(\alpha)) + O_B(1) = \Gamma^\infty(\alpha;H) + O_B(1) \). \( \square \)

For continuous measures and finite strings \( x \), we define the following finite deficiency function \( D_P(x) = \log \max_{y \subseteq x} (M(y)/P(y)) \). Its extension to infinite strings \( \alpha \in \Sigma^\infty \) is denoted by \( D_P(\alpha) = \sup_n D_P(\alpha_{\leq n}) \). \( D_P \) is a \( P \)-test, with for all \( m \in \mathbb{N} \), \( P(\{ \alpha : D_P(\alpha) > 2^m \}) \leq 2^{-m} \). \( D \) is also a probability bounded ML test [Gacs13]. For continuous semi-measures \( P \), \( D_P(\alpha) = \sup_n D_P(\alpha_{\leq n}) \) is the largest, non-increasing on \( P \), semicontinuous on \( \alpha \), of \( D \). This term \( D \) is admittedly not a definitive definition of randomness with respect to a continuous (semi)measure. However proving properties about \( D \) could have utility in future applications. Theorem 6 follows using the same general proof technique as theorem 1, with the construction of a \( M \)-test, \( t \). Theorem 7 shows tightness of theorem 6 (on a finite/infinite level).

**Theorem 6.** For recursive monotone function \( B : \Sigma^* \rightarrow \Sigma^* \) and continuous semicomputable semi-measure \( P \), for all \( \alpha \in \Sigma^* \), \( D_{BP}(B(\alpha)) < D_P(\alpha) + \Gamma^\infty(\alpha;H) + O_B, P(1) \).

**Proof.** We the semicontinuous function \( t(\alpha) = \sup_n P(\alpha_{\leq n})M(B(\alpha_{\leq n}))(M(\alpha_{\leq n})BP(B(\alpha_{\leq n}))) \). \( t(\alpha) \) is a \( M \)-test. Indeed, let \( m \in \mathbb{N} \) and \( S = \{ \alpha : t(\alpha) > 2^m \} \). So \( M(S) \leq 2^{-m} \sum_{x \in S} P(x)M(B(x))/BP(B(x)) \leq 2^{-m} \sum_{y \in B(S)} M(y) \sum_{x, y \in B} P(x)/BP(y) = 2^{-m} M(B(S)) \leq 2^{-m} \). Since \( t \) is computable in the limit, \( t \) is \( H \)-semicomputable, with \( K(t|H) = O_B(1) \). Since \( t \in T_{M^*} \) is a \( M \)-test, \( D_{BP}(B(\alpha)) - D_P(\alpha) < \log t(\alpha) < \Gamma^\infty(\alpha;H) + K(t|H) < \Gamma^\infty(\alpha;H) + O_B, P(1) \). \( \square \)

**Theorem 7 ([BHPS13]).** There exists limit computable \( B : \Sigma^* \rightarrow \Sigma^* \), continuous measure \( P \), and infinite sequence \( \alpha \in \Sigma^* \), where \( D_P(\alpha) < \infty \), \( D_{BP}(B(\alpha)) = \infty \), and \( I(\alpha;H) = \infty \).
7 Acknowledgements

I would like to thank Laurent Bienvenu, Péter Gács, Wolfgang Merkle, Joseph Miller, Chris Porter, Paul Shafer, and Alexander Shen for insightful discussions and reference material.

References

[BHPS13] L. Bienvenu, R. Hölzl, C. Porter, and P. Shafer. Randomness and Semi-measures. In Preparation, 2013.

[Cha75] G. J. Chaitin. A Theory of Program Size Formally Identical to Information Theory. Journal of the ACM, 22(3):329–340, 1975.

[Gacs13] Peter Gács. Lecture notes on descriptional complexity and randomness, 1989-2013.

[Kol65] A. N. Kolmogorov. Three approaches to the quantitative definition of information. Problems in Information Transmission, 1:1–7, 1965.

[Lev74] L. A. Levin. Laws of Information Conservation (Non-growth) and Aspects of the Foundations of Probability Theory. Problemy Peredachi Informatsii, 10(3):206–210, 1974.

[Lev84] L. A. Levin. Randomness conservation inequalities; information and independence in mathematical theories. Information and Control, 61(1):15–37, 1984.

[Lev12] L.A. Levin. Rarity for semimeasures. In Foundations of Computer Science (FOCS), 2012 IEEE 53rd Annual Symposium on, 2012.

[LV08] M. Li and P. Vitányi. An Introduction to Kolmogorov Complexity and Its Applications. Springer Publishing Company, Incorporated, 3 edition, 2008.

[Sol64] R. J. Solomonoff. A Formal Theory of Inductive Inference, Part 1. Information and Control, 7:1–22, 1964.