

# Finite-precision Intrinsic Randomness and Source Resolvability

Yossef Steinberg and Sergio Verdú

C3I Center, George Mason Univ., Fairfax, VA 22030 and Dept. of EE, Princeton Univ., Princeton, NJ 08544, USA

## I. INTRODUCTION AND DEFINITIONS

Random number generators are important devices in randomized algorithms, Monte-Carlo methods, and in simulation studies of random systems. A random number generator is usually modeled as a random source emitting independent, equally likely random bits. In practice, the random source one has at hand can deviate from this idealized model, and the random number generator operates by applying a deterministic mapping on the output of the (nonideal) random source. The deterministic mapping is chosen so that the resulting process approximates – in some sense – a sequence of independent, equally likely random bits. A prime measure of the intrinsic randomness of a given source  $X$  is the maximal rate at which random bits can be extracted from  $X$  by suitably mapping its output. This maximal rate depends on the statistics of the source  $X$  and on the sense of approximation. In [1] it is shown that the maximal rate at which arbitrarily accurate approximations of pure random bits can be extracted from  $X$  equals its inf entropy rate,  $\underline{H}(X)$ . The measures of accuracy with respect to which this result was shown to hold are the variational distance, the  $\bar{d}$  distance and normalized divergence.

In problems like randomized algorithms, or Monte-Carlo simulations, an arbitrarily accurate approximation of pure random bits may be more than what we need, and a controlled deviation from pure random bits can be tolerated. In such cases, one may wish to increase the rate of generation of random bits at the expense of a coarser approximation of the desired fair coin flip distributions. In this work we study the problem of finite-precision random bit generation, where the accuracy measure is the variational distance. The results presented here extend part of the results in [1] and also provide a nice counterpart to the finite-precision source resolvability problem that was studied in detail in [2].

Throughout,  $X$  is a random source with finite alphabet  $A$ , and logarithms have base 2. We start with a few definitions. Definition 1 [1]  $R$  is a  $D$ -achievable intrinsic randomness rate of  $X$  if there exists a sequence of deterministic mappings  $\phi_n : A^n \rightarrow \{0, 1\}^r$  such that for all  $\gamma > 0$  and sufficiently large  $n$ ,

$$\frac{r}{n} > R - \gamma$$

and

$$d_v(\phi_n(X^n), B^r) \leq D$$

where  $B^r$  stands for an equiprobable distribution over  $\{0, 1\}^r$  and  $d_v(\cdot, \cdot)$  is the variational distance between distributions.

**Definition 2** The *finite-precision intrinsic randomness rate* of  $X$  is defined as the supremum of the  $D$ -achievable intrinsic randomness rates of  $X$  and is denoted by  $U_v(D, X)$ .

Note that  $U_v(2, X) = \infty$  for every source  $X$ . The next definition deals with the relevant information theoretic function.

**Definition 3** The *variational inf rate-distortion function* of  $X$ ,  $\underline{R}_v(D)$ , is defined as the supremum over all real numbers

$h$  satisfying

$$\limsup_{n \rightarrow \infty} P_X^n \left( \frac{1}{n} \log \frac{1}{P_{X^n}(X^n)} < h \right) \leq \frac{D}{2}.$$

Thus,  $\underline{R}_v(D)$  is the largest real number  $h$  such that the mass of the entropy density to the left of  $h$  does not exceed  $D/2$ , asymptotically. Note that for every source  $\underline{R}_v(0)$  equals the inf entropy-rate of the source,  $\underline{H}(X)$ , and  $\underline{R}_v(2) = \infty$ .

## II. RESULTS

### Theorem 1

$$U_v(D, X) = \underline{R}_v(D).$$

The next corollary is an easy consequence of Definition 3 and Theorem 1: it implies that if  $X$  is information stable, one cannot increase the asymptotic rate of production of random bits by increasing their deviation (w.r.t. variational distance) from ideal fair coin flips. This result has a nice counterpart in the finite-precision source resolvability problem: it is shown in [2] that if  $X$  is information stable, then its variational finite-precision resolvability  $S_v(D, X)$  is independent of  $D$  in the region  $0 < D < 2$ .

**Corollary 1** If  $X$  is information stable, then for  $0 < D < 2$

$$\underline{R}_v(D) = U_v(D, X) = H(X).$$

In [2] the variational finite-precision source resolvability was characterized as the infimum of the sup information rate over an appropriate class of channels — the corresponding sup rate-distortion function. The nice duality between the problems of finite-precision source resolvability and finite-precision bit generation, and Corollary 1, leads one to suspect that the variational finite-precision source resolvability (and hence also the sup rate-distortion function) as defined in [2] admits a simpler characterization – such as that in Definition 3. This is indeed the case, as one can see from the following theorem.

### Theorem 2

$$\begin{aligned} S_v(D, X) &= \bar{R}_v(D) \\ &= \inf \left\{ h : \limsup_{n \rightarrow \infty} P_{X^n} \left( \frac{1}{n} \log \frac{1}{P_{X^n}(X^n)} > h \right) \leq \frac{D}{2} \right\}. \end{aligned}$$

Thus, the variational sup rate-distortion function as defined in [2] is also equal to the smallest real number  $h$  such that the mass of the entropy density to the right of  $h$  does not exceed  $D/2$ , asymptotically.

## REFERENCES

- [1] S. Vembu, S. Verdú, “Generating Random Bits from an Arbitrary Source: Fundamental Limits,” submitted.
- [2] Y. Steinberg, S. Verdú, “Coarse Approximations of Source Statistics and Rate-Distortion Theory,” submitted.