Variable-Length Extractors

Hongchao Zhou
Department of Electrical Engineering
California Institute of Technology
Pasadena, CA 91125
Email: hzhou@caltech.edu

Jehoshua Bruck
Department of Electrical Engineering
California Institute of Technology
Pasadena, CA 91125
Email: bruck@caltech.edu

***Abstract*—The topic of generating random bits from imperfect random sources was studied extensively. Existing work provides solutions that are based on the concept of a fixed-length extractor; namely, an algorithm that gets a fixed number of random bits from a source and generates random bits. Typically, the number of random bits extracted using fixed-length extractors is upper-bounded by the min-entropy. However, based on Shannon's theory, the information theoretic limit for randomness extraction is the source's entropy - that is typically strictly larger than the min-entropy. In this paper, we consider a scenario where the source is a weak stochastic process and the output sequence is required to be ϵ-close to the uniform distribution on $\{0,1\}^m$, where m is a prescribed value. We introduce a new class of extractors with a variable input-length and fixed output-length. Our variable-length extractors have two important properties: (i) they approach the information theoretic upper bound on efficiency (entropy of the source) while the extracted bits are random in the sense of statistical difference; and (ii) they minimize the expected number of symbols read from the source in order to reach a prescribed number of random bits.**

I. Introduction

The topic of generating random bits from imperfect random sources, as required by many applications [7], has been extensively studied. Existing work can be classified into two main categories, namely, generating truly random bits from ideal sources or extracting almost-random bits from non-ideal sources. The work in the first category dates back to von Neumann [14], who first considered the problem of simulating unbiased coins by using a biased coin with unknown probability. The optimal algorithms were later derived by Elias [3] and Peres [9]. In 1986, Blum [1] studied the problem of generating random bits from a correlated source, specifically, he considered finite Markov chains. Recently, we generalized Blum's method and proposed the first known algorithm that runs in expected linear time and achieves the information-theoretic upper bound on efficiency [15], namely, the expected number of random bits generated is asymptotically equal to the entropy of source.

Extracting randomness from non-ideal sources has been an active research topic in the last two decades. In 1990, Zuckerman introduced a general model of weak random sources, called k-sources, namely whose min-entropy is at least k. It was shown that given a source on $\{0,1\}^n$ with min-entropy $k < n$, it is impossible to devise a single function that extracts even one bit of randomness. This observation led to the introduction of seeded extractors, which using a small number of additional truly random bits as the seed (catalyst). When simulating a probabilistic algorithm, one can simply eliminate the requirement of truly random bits by enumerating all the possible strings for the seed and taking a majority vote on the final results. There are a variety of very efficient constructions of seeded extractors, summarized in [2], [8], [12]. On the other hand, people study seedless extractors for some specific classes of random sources, including independent sources [10], bit-fixing sources [5], and samplable sources [6]. Almost all known constructions of seeded or seedless extractors have fixed input length and fixed output length, hence, we call them fixed-length extractors. For many weak random sources, the maximal number of random bits extracted based on a fixed-length construction is upper bounded by the source's min-entropy. However, Shannon's theory tells us that the information theoretic limit for randomness extraction is the source's entropy, which is larger than the min-entropy. The concept of min-entropy and entropy are defined as follows.

Definition 1. *Given a random source X on $\{0,1\}^n$, the min-entropy of X is defined as*

$$H_{\min}(X) = \min_{x \in \{0,1\}^n} \log \frac{1}{P[X = x]}.$$

The entropy of X is defined as

$$H(X) = \sum_{x \in \{0,1\}^n} P[X = x] \log \frac{1}{P[X = x]}.$$

Example 2. *Let X be a random variable such that $P[X = 0] = 0.9$ and $P[X = 1] = 0.1$, then $H_{\min}(X) = 0.152$ and $H(X) = 0.469$. In this case, the entropy of X is about three times its min-entropy.* □

In this paper, we focus on the notion and constructions of variable-length extractors, namely, extractors with variable input-length and fixed output-length. Here, we would like to fix the output length because the demand of random bits is application-dependent and usually fixed. The input length can be variable because many natural sources for randomness extraction are stochastic processes, like those based on noise signals and quantum effects. So our goal is to extract a required number of random bits in the sense of statistical difference while minimizing the expected input cost – measured by the entropy of the input sequence (whose length may not be

fixed). Hence, we define the efficiency η of an extractor as the asymptotic ratio between its output length and the entropy of its input sequence, which is upper bounded by 1.

Given a general source $\mathcal{R}$, we use β to indicate the minimum distance between $\mathcal{R}$ and an ideal source (such as general stationary ergodic processes). We prove that the efficiency of a variable-length extractor can reach $\eta \geq 1 - \beta$. For instance, consider an independent source $x_1x_2x_3...$ such that $P[x_i = 1] \in [0.9, 0.91]$, it has $\beta \leq 0.0315$. For this source, our variable-length extractor can generate random bits with efficiency at least 0.9685 that is very close to the upper bound 1. In comparison, the efficiency of a fixed-length extractor is at most 0.3117. In general, proposed variable-length extractors have two benefits: (i) they are generalizations of algorithms for ideal sources to address general noisy sources; and (ii) they bridge the gap between min-entropy and entropy on efficiency.

The remainder of this paper is organized as follows. Section II presents background and related results. Section III, Section IV and Section V present and analyze different constructions for variable-length extractors. Due to space limitation, we omit some of the proofs.

II. Preliminaries

A. Statistical Difference

Statistical Difference is used in computer science to measure the difference between two distributions. Let X and Y be two random sequences with range $\{0,1\}^m$, then the statistical difference between X and Y is defined as

$$\|X - Y\| = \max_{T:\{0,1\}^m \to \{0,1\}} |P[T(X) = 1] - P[T(Y) = 1]|$$

over a boolean function T. We say that X and Y are ϵ-close if $\|X - Y\| \leq \epsilon$. In this paper, we want to extract m almost-random bits such that they are ϵ-close to the uniform distribution U_m on $\{0,1\}^m$ with specified small $\epsilon > 0$.

B. Fixed-length Extractors

Extraction of randomness from a weak random source with min-entropy $k < n$, where n is the input length is an active research area. Seeded-extractors are introduced to extract randomness from a single source by using a small number additional truly random bits [8], [12]. A seeded extractor is a function

$$E : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$$

such that for every distribution X on $\{0,1\}^n$ with $H_{\min}(X) \geq k$, the distribution $E(X, U_d)$ is ϵ-close to the uniform distribution U_m. Here, d is the seed length, and we call such an extractor as (k, ϵ) extractor. There are a lot of works focusing on the constructions of seeded-extractors. A standard application of the probabilistic method [11] shows that there exists a seeded-extractor which can extract asymptotically $H_{\min}(X)$ random bits with $\log(n - H_{\min}(X))$ additional truly random bits. Recently, Guruswami, Umans and Vadhan [4] provided an explicit construction of seeded-extractors, whose efficiency is very close to the bound obtained based on the probabilistic method. Their main result is described as follows:

Lemma 3. *[4] For every constant $\alpha > 0$, and all positive integers n, k and all $\epsilon > 0$, there is an explicit construction of a (k, ϵ) extractor $E : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ with $d \leq \log n + O(\log(k/\epsilon))$ and $m \geq (1 - \alpha)k$.*

C. Variable-length Extractors

A seeded variable-length extractor is a function

$$V_E : S_p \times \{0,1\}^d \to \{0,1\}^m$$

such that given a real source $\mathcal{R}$, the output sequence is ϵ-close to the uniform distribution U_m. Here, S_p, the set of input sequences, is a prefix-free code, namely, for any sequence $y \in \{0,1\}^\infty$, there is exactly one sequence $x \in S_p$ such that x is a prefix of y. The general procedure of extracting randomness by using variable-length extractors can be divided into two steps:

1) First, we read bits from the source $\mathcal{R}$ one by one until the current input sequence x is in S_p. In this case, we construct a function

$$V : S_p \to \{0,1\}^n$$

to map the current input sequence into a binary sequence of length n. As a result, we get a random sequence Z with length n and min-entropy k, where k is determined by the selection of S_p and V.

2) Second, by applying a seeded extractor

$$E : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$$

to the random sequence Z, we can extract m almost-random bits that are ϵ-close to U_m.

We can see that the construction of a variable-length extractor is a cascade of a function V and a seeded extractor E, namely,

$$V_E = E \bigotimes V.$$

Note that our requirement is to extract m almost-random bits that are ϵ-close to U_m. According to the constructions of seeded extractors, see Lemma 3, the value of k can be predetermined by m and ϵ. So the key of constructing variable-length extractors is to find the input set S_p and the function V such that the min-entropy of the random sequence Z is at least k and the expected length of the elements in S_p is minimized.

For some specific types of sources, including independent sources and samplable sources, by applying the ideas in [10] and [6] we can remove the requirement of the seed without degrading the asymptotic performance. As a result, we have seedless variable-length extractors. For example, if $\mathcal{R}$ is an independent source, we can first apply the method in [10] to extract d random bits from the first $\Theta(\log \frac{m}{\epsilon})$ bits, and then use them as the seed of a seeded variable-length extractor to extract randomness from the other bits. Due to space limitation, in this paper we mainly focus on seeded constructions of variable-length extractors.

D. Model Approximation

The main idea of constructing variable-length extractors is base on model approximation, namely, given a real source $\mathcal{R}$, we use a simple model $\mathcal{M}$ to approximate it and then based on which we construct the input set S_p. The performance of the resulting variable-length extractor strongly depends on the difference between $\mathcal{R}$ and $\mathcal{M}$. Although there are some existing ways such as normalized Kullback-Leibler divergence to measure the difference between two sources, certain difficulties exist in using them in variable-length extractors. In this paper, we use $\beta_t(\mathcal{R}, \mathcal{M})$ to measure the distance between the source $\mathcal{R}$ and the model $\mathcal{M}$, defined by

$$\beta_t(\mathcal{R}, \mathcal{M}) = \max_{|x| \geq t, x \in \{0,1\}^*} \frac{\log_2 \frac{P_{\mathcal{R}}(x)}{P_{\mathcal{M}}(x)}}{\log_2 \frac{1}{P_{\mathcal{M}}(x)}},$$

where t is a constant, $P_{\mathcal{R}}(x)$ is the probability of generating x from $\mathcal{R}$ when the sequence length is $|x|$, $P_{\mathcal{M}}(x)$ is the probability of generating x from $\mathcal{M}$ when the sequence length is $|x|$, and the term $\log_2 \frac{1}{P_{\mathcal{M}}(x)}$ is used for normalization. Then

$$0 \leq \beta_t(\mathcal{R}, \mathcal{M}) \leq 1$$

for any source $\mathcal{R}$ and model $\mathcal{M}$. Typically, we are interested in those sources $\mathcal{R}$ such that we can find a simple model $\mathcal{M}$ to make $\beta_t(\mathcal{R}, \mathcal{M})$ small. In our applications, we only care about those input sequences in S_p, so we consider

$$\beta(\mathcal{R}, \mathcal{M}) = \beta_{\min_{x \in S_p} |x|}(\mathcal{R}, \mathcal{M}),$$

namely, only the sequences which reach a certain length.

Example 4. *Let $x_1 x_2 ... \in \{0,1\}^*$ be a sequence generated from an indepedent source $\mathcal{R}$ such that*

$$\forall i \geq 1, P[x_i = 1] \in [0.8, 0.82].$$

If we let $\mathcal{M}$ be a biased coin with probability 0.8132, then

$$\beta_t(\mathcal{R}, \mathcal{M}) = \beta(\mathcal{R}, \mathcal{M})$$
$$\leq \max\left(\frac{\log_2 \frac{0.2}{0.1868}}{\log_2 \frac{1}{0.1868}}, \frac{\log_2 \frac{0.82}{0.8132}}{\log_2 \frac{1}{0.8132}}\right) = 0.0405, \forall t \geq 1$$

□

E. Efficiency

To consider the performance of a construction, we are interested in the expected input cost (we ignore the seed length d because it is very small and it can be treated as fixed in our constructions), so we define its efficiency as

$$\eta = \lim_{m \to \infty} \frac{m}{H_{\mathcal{R}}(X_m)}$$

such that the output sequence is ϵ-close to the uniform distribution U_m on $\{0,1\}^m$ with $\epsilon_{m \to \infty} = 0$, where m is the output length and $H_{\mathcal{R}}(X_m)$ is the entropy of the input sequence X_m.

According to Shannon's theory, it is easy to get the upper bound of η.

Lemma 5. *For any construction of variable-length extractors with $d = o(m)$, its efficiency $\eta \leq 1$.*

If $\mathcal{R}$ is a stationary ergodic process, we can define its entropy rate as

$$h(\mathcal{R}) = \lim_{l \to \infty} \frac{H(X^l)}{l},$$

where X^l is a random sequence of length l generated from the source $\mathcal{R}$. In this case, the entropy of the input sequence is proportional to the expected input length.

Lemma 6. *Given a stationary ergodic source $\mathcal{R}$, let X_m be the input sequence of a variable-length extractor with output length m. Then*

$$\lim_{m \to \infty} \frac{H_{\mathcal{R}}(X_m)}{E_{\mathcal{R}}[|X_m|]} = h(\mathcal{R}),$$

where $E_{\mathcal{R}}[|X_m|]$ is the expected input length.

III. Construction Based on Specified Models

In this section, we consider those sources which can be approximated by a specified model $\mathcal{M}$. Here, we say a model $\mathcal{M}$ is specified if its distribution is known, i.e., $P_{\mathcal{M}}(x)$ can be easily calculated for any $x \in \{0,1\}^*$. Note that this model $\mathcal{M}$ is not necessary to be stationary or ergodic. For instance, $\mathcal{M}$ can be an independent process $z_1 z_2 ... \in \{0,1\}^*$ such that

$$\forall i \geq 1, P_{\mathcal{M}}(z_i = 1) = \frac{1 + sin(i/10)}{2}.$$

Our goal is to extract randomness from an imperfect random source $\mathcal{R}$. The problem is that we don't know the exact distribution of $\mathcal{R}$, but we know that it can be approximated by a specified model $\mathcal{M}$. So we can use the distribution of $\mathcal{M}$ to estimate the distribution of $\mathcal{R}$. As a result, we have the following procedure to extract m almost-random bits.

Construction 7. *Assume the real source is $\mathcal{R}$, and there exists a specified model $\mathcal{M}$ such that $\beta(\mathcal{R}, \mathcal{M}) \leq \beta$ for a constant β.*

1) *Read input bits one by one from $\mathcal{R}$ until we get an input sequence $x \in \{0,1\}^*$ such that*

$$\log_2 \frac{1}{P_{\mathcal{M}}(x)} \geq \frac{k}{1 - \beta}.$$

2) *Let n be the maximum length of all the possible input sequences, then*

$$n = \arg\min_l \{l \in \mathbb{N} | \forall y \in \{0,1\}^l, \log_2 \frac{1}{P_{\mathcal{M}}(y)} \geq \frac{k}{1 - \beta}\}.$$

If $|x| < n$, we extend the length of x to n by adding $n - |x|$ trivial zeros at the end. Since x is randomly generated, from the above procedure we get a random sequence Z of length n.

3) *Applying a (k, ϵ) extractor to Z yields a binary sequence of length m that is ϵ-close to U_m.* □

The following example is provided for comparing this construction with fixed-length constructions.

Example 8. *Let $\mathcal{M}$ be a biased coin with probability 0.8 (of being 1). If $k = 2$ and $\beta = 0$, then we can get the input set*

$$S_p = \{0, 10, 110, 1110, 11110, 111110, 1111110, 1111111\}.$$

In this case, the expected input length is strictly smaller than 7. For fixed-length constructions, to get a random sequence with min-entropy at least 2, we have to read 7 input bits independent of the context. It is less efficient than the former method. □

Theorem 9. *Construction 7 generates a random sequence of length m that is ϵ-close to U_m if there exists a (k, ϵ) extractor with input length n and output length m.*

Proof: According to the definition of $\beta(\mathcal{R}, \mathcal{M})$, for all $x \in S_p$,

$$\frac{\log_2 \frac{P_{\mathcal{R}}(x)}{P_{\mathcal{M}}(x)}}{\log_2 \frac{1}{P_M(x)}} \leq \beta.$$

Based on the construction, for all $x \in S_p$

$$\log_2 \frac{1}{P_{\mathcal{M}}(x)} \geq \frac{k}{1-\beta}.$$

The two inequalities above yield

$$\log_2 \frac{1}{P_{\mathcal{R}}(x)} \geq k$$

for all $x \in S_p$. Since the mapping from S_p to the assignments of Z is one-to-one, the min-entropy keeps unchanged under this mapping, hence, the min-entropy of Z is at least k. Furthermore, we get the conclusion in the theorem. ■

Theorem 10. *Given a real source $\mathcal{R}$ such that there exists a specified model $\mathcal{M}$ with $\beta(\mathcal{R}, \mathcal{M}) \leq \beta$, then the efficiency of Construction 7 is*

$$1 - \beta \leq \eta \leq 1.$$

Proof: We only need to show that $\eta \geq 1 - \beta$. According to Lemma 3, as $m \to \infty$, to make $\epsilon \to 0$, we have

$$\lim_{m\to\infty} \frac{k}{m} = 1.$$

Now, let's consider the number of elements in S_p, namely, $|S_p|$. To calculate $|S_p|$, we let

$$S'_p = \{x[1 : |x| - 1] | x \in S_p\},$$

then for all $y \in S'_p$, $\log_2 \frac{1}{P_M(y)} \leq \frac{k}{1-\beta}$. Hence,

$$\log_2 |S'_p| \leq \frac{k}{1-\beta}.$$

It is easy to see that $|S_p| \leq 2|S'_p|$, so

$$\log_2 |S_p| \leq \frac{k}{1-\beta} + 1.$$

Let X_m be the input sequence, then

$$\lim_{k\to\infty} \frac{H_{\mathcal{R}}(X_m)}{k} \leq \lim_{k\to\infty} \frac{\log_2 |S_p|}{k} \leq \frac{1}{1-\beta},$$

Finally, it yields

$$\eta = \lim_{m\to\infty} \frac{m}{H_{\mathcal{R}}(X_m)} \geq 1 - \beta.$$

This completes the proof. ■

We see that the gap β on efficiency in the above theorem is introduced by the difference between the source $\mathcal{R}$ and the specified model $\mathcal{M}$. In some sense, it reflects the *model uncertainty* of the real source $\mathcal{R}$.

IV. Construction Based on Biased-Coin Models

In this section, we use a general ideal model such as a biased coin or a Markov chain to approximate the real source $\mathcal{R}$. Here, we don't care about the specific parameters of the ideal model. The reason is, in some cases, the source $\mathcal{R}$ is very close to an ideal source but we cannot (or don't want to) estimate the parameters accurately. As a result, we introduce a construction by exploring the characters of biased coins or Markov chains. For simplicity, we only discuss the case that the ideal model is a biased coin, and the same idea can be generalized when the ideal model is a Markov chain. Let $\mathcal{G}_{b.c.}$ denote the set consisting of all the models of biased coins with different probabilities, then the following procedure is provided to extract m almost-random bits.

Construction 11. *Assume the real source is $\mathcal{R}$ such that $\min_{M\in\mathcal{G}_{b.c.}} \beta(\mathcal{R}, M) \leq \beta$ for a constant β.*

1) *Read input bits one by one from $\mathcal{R}$ until we get an input sequence $x \in \{0, 1\}^*$ such that*

$$\log_2 \binom{k_0 + k_1}{\max(1, \min(k_0, k_1))} \geq \frac{k}{1-\beta},$$

where k_0 is the number of zeros in x and k_1 is the number of ones in x.

2) *Since the input sequence x can be very long, we map it into a sequence z of fixed length n such that*

$$z = [I_{(k_0 \geq k_1)}, \min(k_0, k_1), r(x)],$$

where $I_{(k_0\geq k_1)} = 1$ if and only if $k_0 \geq k_1$, and $r(x)$ is the rank of x among all the permutations of x with respect to the lexicographic order. Since x is randomly generated, the above procedure leads us to a random sequence Z of length n.

3) *Applying a (k, ϵ) extractor to Z yields a random sequence of length m that is ϵ-close to U_m.* □

Let $\mathbf{1}^a$ denote the all-one vector of length a, then we get the following result.

Theorem 12. *Construction 11 generates a random sequence of length m that is ϵ-close to U_m if $P_{\mathcal{R}}(\mathbf{1}^a) \leq 2^{-k}, P_{\mathcal{R}}(\mathbf{0}^a) \leq 2^{-k}$ for $a = 2^{\lfloor \frac{k}{1-\beta} \rfloor}$ and there exists a (k, ϵ) extractor with input length n and output length m.*

Theorem 13. *Given a real source $\mathcal{R}$ such that $\min_{M\in\mathcal{G}_{b.c.}} \beta(\mathcal{R}, M) \leq \beta$. If there exists a model $M \in \mathcal{G}_{b.c.}$ with probability $p \leq \frac{1}{2}$ of being 1 or 0 such that $p > \sqrt{\beta(\mathcal{R}, M) \log_2 \frac{1}{p} \frac{\ln 2}{2}}$, then the efficiency of Construction 11 is*

$$1 - \beta \leq \eta \leq 1.$$

V. Construction Based on Stationary Ergodic Models

In this section, we consider imperfect sources that are approximately stationary and ergodic. In [13], Visweswariah, Kulkarni and Verdú showed that optimal variable-length source codes asymptotically achieve optimal variable-length random bits generation in the sense of normalized divergence. Although their work only focused on ideal stationary ergodic processes and generates 'weaker' random bits, it motivates us to combine universal compression with fixed-length extractors for efficiently generating random bits from noisy stochastic processes. In this section, we will first introduce Lempel-Ziv code and then present its application in constructing variable-length extractors.

Lempel-Ziv code is a universal data compression scheme introduced by Ziv and Lempel [16], which is simple to implement and can achieve the asymptotically optimal rate for stationary ergodic sources. The idea of Lempel-Ziv code is to parse the source sequence into strings that haven't appear so far, as demonstrated by the following example.

Example 14. *Assume the input is* 010111001110000..., *then we parse it as strings*

$$0, 1, 01, 11, 00, 111, 000, ...$$

where each string is the shortest string that never appear before. That means all its prefixes have occurred earlier.

Let $c(n)$ be the number of strings obtained by parsing a sequence of length n. For each string, we describe its location with $\log c(n)$ bits. Given a string of length l, it can described by (1) the location of its prefix of length $l-1$, and (2) its last bit. Hence, the code for the above sequence is

$$(000, 0), (000, 1), (001, 1), (010, 1), (001, 0), (100, 1), (101, 0), ...$$

□

Typically, Lempel-Ziv is applied to an input sequence of fixed-length. Here, we are interested in Lempel-Ziv code with fixed output-length and variable input-length. As a result, we can apply a single fixed-length extractor to the output of Lempel-Ziv code for extracting randomness. In our algorithm, we read raw bits one by one from an imperfect source until the length of the output of a Lempel-Ziv code reaches a certain length. In another word, the number of strings after parsing is a predetermined number c. For example, if the source is 1011010100010... and $c = 4$, then after reading 6 bits, we can parse them into $1, 0, 11, 01$. Now, we get an output sequence $(000, 1), (000, 0), (001, 1), (010, 1)$, which can be used as the input of a fixed-length extractor. We call this Lempel-Ziv code as a variable-length Lempel-Ziv code, based on which we have the following construction to extract m almost-random bits.

Construction 15. *Assume the real source is $\mathcal{R}$ and there exists a stationary ergodic process M such that $\beta(\mathcal{R}, M) \leq \beta$.*

1) *Read input bits one by one based on the variable-length Lempel-Ziv code until we get an output sequence Z whose length reaches $n = \frac{k}{1-\beta}(1+\varepsilon)$, where $\varepsilon \to 0$ as $k \to 0$.*
2) *Applying a (k, ϵ) extractor to Z yields a random sequence of length m that is ϵ-close to U_m.* □

It can be proved that the min-entropy of Z approaches k as $k \to \infty$ and $\varepsilon \to 0$, so that we can continue to apply a fixed-length extractor to 'purify' the sequence.

Theorem 16. *When $k \to \infty$ and $\varepsilon \to 0$, Construction* 15 *generates a random sequence of length m that is ϵ-close to U_m if there exists a (k, ϵ) extractor with input length n and output length m.*

Theorem 17. *Given a real source $\mathcal{R}$ such that there exists a stationary ergodic process M with $\beta(\mathcal{R}, \mathcal{M}) \leq \beta$, then the efficiency of Construction* 15 *is*

$$1 - \beta \leq \eta \leq 1.$$

In the above theorem, the gap β represents how far the source $\mathcal{R}$ is from an ideal source. Also from Theorem 10, we see that the efficiency loss in randomness (distance from 1) stems from the quality of the model or the distance of the source from an ideal source.

References

[1] M. Blum, "Independent unbiased coin flips from a correlated biased source: - a finite state Markov chain", *Combinatorica*, vol. 6, pp. 97-108, 1986.

[2] Z. Dvir and A. Wigderson. "Kakeya sets, new mergers and older extractors", *In Processings of IEEE Symposium on Foundations of Computer Science (FOCS)*, 2008.

[3] P. Elias, "The efficient construction of an unbiased random sequence", *Ann. Math. Statist.*, vol. 43, pp. 865-870, 1972.

[4] V. Guruswami, C. Umans, and S. Vadhan. "Unbalanced expanders and randomness extractors from parvaresh-vardy codes", *In Proceedings of IEEE Conference on Computational Complexity (CCC)*, pp. 96-108, 2007.

[5] J. Kamp and D. Zuckerman, "Deterministic extractors for bit-fixing sources and exposure-resilient cryptography", *SIAM Journal on Computing*, 36:1231-1247, 2006.

[6] J. Kamp, A. Rao, S. Vadhan and D. Zuckerman, "Deterministic extractors for small-space sources", *Journal of Computer and System Sciences*, vol. 77, pp. 191-220, 2011.

[7] R. Motwani and P. Rgahavan. *Randomized Algorithms*, Combridge University press, 1995.

[8] N. Nisan, "Extracting randomness: how and why: a survey", *In Proceedings of IEEE Conference on Computational Complexity (CCC)*, pp. 44-58, 1996.

[9] Y. Peres, "Iterating von Neumann's procedure for extracting random bits", *Ann. Statist.*, vol. 20, pp. 590-597, 1992.

[10] A. Rao, "Randomness extractors for independent sources and applications", Ph.D. Thesis, Department of Computer Science, University of Texas at Austin, 2007.

[11] J. Radhakrishnan and A. Ta-Shma. "Bounds for dispersers, extractors, and depth-two supperconcentrators", *SIAM Journal on Discrete Mathmatics*, 13(1): 2-24, 2000.

[12] R. Shaltiel, "Recent developments in explicit constructions of extractors", *BULLETIN-European Association For Theoretical Computer Science*, vol. 77, pp. 67-95, 2002.

[13] K. Visweswariah, S.R. Kulkarni and S. Verdú, "Source codes as random number generators", *IEEE Trans. on Information Theory*, vol. 44, no. 2, pp. 462-471, 1998.

[14] J. von Neumann, "Various techniques used in connection with random digits", *Appl. Math. Ser.*, Notes by G. E. Forstyle, Nat. Bur. Stand., vol. 12, pp. 36-38, 1951.

[15] H. Zhou and J. Bruck, "Efficiently generating random bits from finite state markov chains", *To appear in IEEE Trans. on Information Theory*, DOI 10.1109/TIT.2011.2175698, 2011.

[16] J. Ziv and A. Lempel. "Compression of individual squences by varaible rate coding", *IEEE Trans. on Information Theory*, vol. 24, pp. 530-536, 1978.