Efficient Simulations by a Biased Coin

Ryuhei Uehara
Center for Information Science, Tokyo Woman's Christian University,
Zempukuji, Suginami-Ku, Tokyo 167, Japan, uehara@twcu.ac.jp

Key words: Probabilistic Turing machines, randomized algorithms, biased coins.

1 Introduction

The existence of a random coin has been extensively assumed for applications such as randomizing algorithms, cryptographic protocols, and stochastic simulation experiments. The available sources of randomness are sometimes physical devices, such as Zener diodes, and Geiger counters. The sample mean of the devices as an estimate of the bias of a random coin is always rational. Thus, in this paper, *bias* is a rational number between 0 and $\frac{1}{2}$. (We note that in order to determine the irrationality of the mean of a random variable is investigated by Cover [1].)

A *probabilistic Turing machine* (PTM) is a Turing machine with distinguished states called coin-tossing states. For formal definitions of a PTM, see [3]. In general, it is assumed that a PTM has a fair coin. This is led by the following results: Santos showed that there is no important difference between a PTM with a fair coin and a PTM with a biased coin for the language recognition [8, Theorem 5.1]. Moreover, any biased coin can simulate another biased coin in a constant expected time. This follows from that any biased coin can simulate a fair coin in a constant expected time ([7, 4, 9]), and vice versa ([6]).

The interchangeability of the simulation among coins is measured only by the *expected* time of computation. However, it is necessary to terminate in bounded time on some applications such as realtime operations, and synchronous machines. In this paper, we consider the computation which will always terminates in *bounded* time, as opposed to *expected* time. Feldman, et al. [2] compared these models and they noticed that there is a conceptual difference between these two kinds of measures. We will show that the conceptual difference breaks the interchangeability of the coins. We say that a PTM *efficiently* computes when it always terminates in bounded time. We consider a PTM with a biased coin which efficiently simulates biased coins. A *coin of bias* p, denoted by $\mathcal{C}_p$, is a coin such that an outcome of the coin-tossing is "$\mathcal{H}$" with probability p, and "$\mathcal{T}$" with probability $1-p$. Let $\mathcal{S}_p$ be the set of biases efficiently simulated by a PTM with $\mathcal{C}_p$. The main theorem in this paper is the following:

Theorem 1 *(i) The set $\mathcal{S}_{\frac{1}{2}}$ is equal to the set of the biases in finite figures on the binary system,*

(ii) the set $\mathcal{S}_{\frac{1}{3}}$ is equal to the set of the biases in finite figures on the ternary system, and

(iii) the set $\mathcal{S}_{\frac{b}{a}}$ in reduced form with $a > 3$, is properly contained in the set of the biases in finite figures on the a-ary system.

In this sense, $\mathcal{C}_{\frac{1}{2}}$ and $\mathcal{C}_{\frac{1}{3}}$ are more expressive coins than the others.

Then, oppositely, how many least coins which efficiently simulate the set of the biases in finite figures on the a-ary system when $a > 3$? The answer is only *two*, which is stated in the last section. Feldman, et al. [2] investigated a fair n-sided die, which is efficiently simulated by a PTM with a rationally biased coin. We will compare coins and dice in the last section.

2 Preliminaries

An efficient simulation by a PTM with $\mathcal{C}_p$, is associated with a binary tree in a natural way. (For formal definitions of a *binary tree*, *internal nodes*, *edges*, *sons*, *leaves*, and a *root*, see [5].) Thus we define an *efficient algorithm* $\mathcal{A}_p$, representing an efficient simulation by a PTM with $\mathcal{C}_p$, by a finite binary tree such that;

(i) each internal node, representing a coin-tossing, has two edges to its sons,

(ii) one of the two edges above is labeled p, and the other is labeled $1-p$, and

(iii) each leaf is labeled "$\mathcal{H}$" or "$\mathcal{T}$".

The *depth of a leaf* (or the *depth of an internal node*) is the number of the edges of the path from the leaf (or the internal node, respectively) to the root. The *depth of an efficient algorithm* is the maximal depth of its leaves. The *probability of a leaf* is defined by the product of all labels on the path from the leaf to the root. An efficient algorithm $\mathcal{A}_p$ *simulates* $\mathcal{C}_q$, if the sum of all probabilities of the leaves of $\mathcal{A}_p$ labeled "$\mathcal{H}$" is equal to q. We write $\mathcal{C}_p \to \mathcal{C}_q$ if there is an efficient algorithm $\mathcal{A}_p$ simulating $\mathcal{C}_q$, and by $\mathcal{C}_p \not\to \mathcal{C}_q$ otherwise. An efficient algorithm is called a *complete efficient algorithm* if the depths of all leaves are equal to each other. Note that for each efficient algorithm of depth k, there exists a complete efficient algorithm of depth k, simulating the same coin.

As mentioned in Introduction, we only consider rational numbers as biases. The rational numbers consist of the finite decimals and the recurring decimals. For a finite decimal p on the a-ary system, we denote p by $(0.p_1p_2\cdots p_k)_a$, where $k > 0$, $0 < i \leq k$, $0 \leq p_i < a$ and $p_k \neq 0$, and $p = p_1a^{-1} + p_2a^{-2} + \cdots + p_ia^{-i} + \cdots + p_ka^{-k}$. The number of figures of p on the a-ary system is denoted by $|p|_{(a)}$ (equal to k, in the case above). For a recurring decimal q on the a-ary system, $|q|_{(a)}$ is defined as an infinity. Note that for a rational number p, it depends on a whether $|p|_{(a)}$ is finite or not (e.g. $\frac{1}{2} = (0.1)_2 = (0.11\cdots)_3$).

3 Proof of Main Theorem

First, we show that for every integer a greater than 1 and b with $0 < b \leq \frac{a}{2}$, $\mathcal{C}_{\frac{b}{a}} \to \mathcal{C}_p$ implies that p is a finite decimal on the a-ary system. This is a sufficient condition of Theorem 1.

Lemma 2 *For every $\mathcal{C}_p$ simulated by an efficient algorithm $\mathcal{A}_{\frac{b}{a}}$ of depth k, $|p|_{(a)}$ is bounded by k.*

Proof. For an efficient algorithm $\mathcal{A}_{\frac{b}{a}}$ of depth k, the denominator of the probability of a leaf is a^i with $0 < i \leq k$. Since p is the sum of these probabilities, it is a fraction of denominator a^k. This implies the lemma. ∎

Next we show necessary conditions of Theorem 1 for each case (i), (ii), and (iii). We now show a technical lemma in order to prove the claim for $a = 3$. In this lemma, we consider a PTM with many coins:

Lemma 3 *Let a_1 and a_2 be integers with $2 \leq a_1 \leq a_2$. Then for any i with $0 < i < a_1 a_2$, there exists a PTM M with $\mathcal{C}_{\frac{1}{a_1}}, \mathcal{C}_{\frac{1}{a_2}}, \mathcal{C}_{\frac{2}{a_2}}, \cdots, \mathcal{C}_{\frac{(a_2-1)}{a_2}}$ such that M efficiently simulates $\mathcal{C}_{\frac{i}{a_1 a_2}}$.*

Proof. We constructs an efficient algorithm which simulates $\mathcal{C}_{\frac{i}{a_1 a_2}}$ by using three of the coins. Without loss of generality, we can assume that $0 < i < \lfloor \frac{a_1 a_2}{2} \rfloor$. Let i_1 and i_2 be integers such that $i_2 = i \bmod (a_1 - 1)$ and $i_1 = \lfloor \frac{i}{a_1 - 1} \rfloor$. We note that $i = i_1(a_1 - 1) + i_2$ holds. Since $(a_1 - 1)(a_2 - 1) + (a_2 - 1) = a_1(a_2 - 1) \geq \frac{a_1 a_2}{2} \geq i$, we can assume that $0 \leq i_1, i_2 \leq a_2 - 1$. For these i_1 and i_2, we construct an efficient algorithm as follows:

1. Toss $\mathcal{C}_{\frac{1}{a_1}}$;
2. if outcome is "$\mathcal{H}$" then toss $\mathcal{C}_{\frac{i_2}{a_2}}$ else toss $\mathcal{C}_{\frac{i_1}{a_2}}$;
3. if outcome is "$\mathcal{H}$" then output "$\mathcal{H}$" else output "$\mathcal{T}$".

The efficient algorithm outputs "$\mathcal{H}$" with probability equal to $\frac{1}{a_1}\frac{i_2}{a_2} + \frac{a_1 - 1}{a_1}\frac{i_1}{a_2} = \frac{i_2}{a_1 a_2} + \frac{i_1(a_1-1)}{a_1 a_2} = \frac{i}{a_1 a_2}$. ∎

Next we show necessary condition of Theorem 1-(ii).

Lemma 4 *For every $\mathcal{C}_p$ such that $|p|_{(3)}$ is finite, $\mathcal{C}_{\frac{1}{3}} \to \mathcal{C}_p$ holds.*

Proof. Let $|p|_{(3)} = k$ and $p = \frac{c}{3^k}$ where $0 \leq c \leq 3^k$. We show by induction for k. Since it is clear when $k = 1$, suppose $k > 1$. By letting $a = 3$, and $b = 3^k$, inductive hypothesis satisfies the conditions of Lemma 3. Thus Lemma 3 implies the lemma. ∎

As same as Lemma 4, we can show it for $\mathcal{C}_{\frac{1}{2}}$, which is a necessary condition of Theorem 1-(i). We note that it has been shown in [6] how to construct a tree algorithm with $\mathcal{C}_{\frac{1}{2}}$, which *optimally* simulates any given rational bias. For every rational bias, the expected value of the times of the coin-tossing of the algorithm is at most 2. Although the algorithm does not terminate for some biases, it efficiently simulates any rational bias in finite figures on the binary system. This also gives a necessary condition of Theorem 1-(i).

Finally we show necessary condition of Theorem 1-(iii).

Lemma 5 *Let a and b be positive integers such that a and b are relatively prime, $a > 3$, and $0 < b < \frac{a}{2}$. Then there exists a rational number p such that $|p|_{(a)}$ is finite and $\mathcal{C}_{\frac{b}{a}} \not\to \mathcal{C}_p$ holds.*

Proof. Since $a > 3$, there exists an integer c such that $0 < c \leq \frac{a}{2}$ and $c \neq b$. (Note that a and c may not be relatively prime.) To prove the lemma, assume $\mathcal{C}_{\frac{b}{a}} \to \mathcal{C}_{\frac{c}{a}}$ and derive a contradiction. Then there would exist a complete efficient algorithm $\mathcal{A}_{\frac{b}{a}}$ simulating $\mathcal{C}_{\frac{c}{a}}$. Let k be the depth of $\mathcal{A}_{\frac{b}{a}}$. Then for each integer i with $0 \leq i \leq k$, it would have $\binom{i}{k}$ leaves of probability equal to $\left(\frac{b}{a}\right)^{k-i}\left(\frac{a-b}{a}\right)^{i} = \frac{(a-b)^i b^{k-i}}{a^k}$. Hence every leaf has a probability being a multiple of $\frac{a-b}{a^k}$ (we say that x is a *multiple* of y if $x = wy$ for some integer w), except one leaf with probability equal to $\frac{b^k}{a^k}$. Let H be the set of the leaves labeled "$\mathcal{H}$", and T be the set of the leaves labeled "$\mathcal{T}$". Then one of H and T only contains leaves of probabilities being multiples of $\frac{a-b}{a^k}$. Thus one of $\frac{c}{a}(= \sum_{j \in H}(\text{probability of } j))$ and $\frac{a-c}{a}(= \sum_{j \in T}(\text{probability of } j))$ is a multiple of

$\frac{a-b}{a^k}$. Consequently, one of the following holds for some positive integer d_1 and d_2: $\frac{c}{a} = d_1\frac{a-b}{a^k}$, or $\frac{a-c}{a} = d_2\frac{a-b}{a^k}$. If the former holds, $a^{k-1}c = d_1(a-b)$. If a and b are relatively prime, so are a and $(a-b)$. Hence $c = d_1'(a-b)$ for some positive integer d_1', contradicting $c \leq \frac{a}{2} < a-b$. If the latter holds, $a^{k-1}(a-c) = d_2(a-b)$. Since a and $(a-b)$ are relatively prime, $a-c = d_2'(a-b)$, or $c = a - d_2'(a-b)$ for some positive integer d_2'. Since $\frac{a}{2} < a-b$, $d_2' = 1$, consequently, $b = c$, contradicting $c \neq b$. Thus $\mathcal{C}_{\frac{b}{a}} \not\to \mathcal{C}_{\frac{c}{a}}$ holds. ∎

4 Concluding Remarks

Feldman, et al. [2] investigated a fair n-sided die efficiently simulated by a PTM with a rationally biased coin. A fair n-sided die and a set $\{\mathcal{C}_{\frac{i}{n}} \mid 0 < i < n\}$ of coins are interchangeable for a random algorithm which randomly selects one of two choices with probability of denominator n. (Notice that n-sided die can be regarded as $\mathcal{C}_{\frac{i}{n}}$ for any i by properly relabeling each side.) A PTM with a rationally biased coin can efficiently simulate a fair n-sided die if and only if n is a power of 2 (and then the PTM has $\mathcal{C}_{\frac{1}{2}}$) as shown in [2]. On the other hand, Theorem 1 also can be stated as follows: A PTM with a rationally biased coin can efficiently simulate $\mathcal{C}_{\frac{i}{n}}$ for every integer i with $0 < i < n$, if and only if n is a power of 2 or a power of 3. In this sense, a set $\{\mathcal{C}_{\frac{i}{n}} \mid 0 < i < n\}$ of coins is more useful than a fair n-sided die when n is a power of 3, since the PTM with $\mathcal{C}_{\frac{1}{3}}$ can efficiently simulate it.

Theorem 1 shows that a PTM with $\mathcal{C}_{\frac{b}{a}}$ in reduced form with $a > 3$ can only efficiently simulate the subset of the biases in finite figures on the a-ary system. Then, oppositely, how many least coins which efficiently simulate the set of the biases in finite figures on the a-ary system? By observing Lemma 5, it is likely to be equal to $\lfloor \frac{a}{2} \rfloor$, which is given by the set $\{\mathcal{C}_{\frac{1}{a}}, \mathcal{C}_{\frac{2}{a}}, \cdots, \mathcal{C}_{\frac{\lfloor a/2 \rfloor}{a}}\}$. (In the fact, Lemma 3 shows its sufficiency.) However, the answer is only *two*, which is $\mathcal{C}_{\frac{1}{a}}$ and $\mathcal{C}_{\frac{1}{2}}$. A PTM with $\mathcal{C}_{\frac{1}{a}}$ and $\mathcal{C}_{\frac{1}{2}}$ can efficiently simulate $\mathcal{C}_{\frac{1}{a^k}}$ for any k by tossing $\mathcal{C}_{\frac{1}{a}}$ k times. Theorem 1 in [2] showed that a fair coin and $\mathcal{C}_{\frac{1}{a^k}}$ can efficiently simulate a^k-sided die. As noticed above, a^k-sided die can be regarded as $\mathcal{C}_{\frac{i}{a^k}}$ for any i with $0 < i < a^k$.

References

[1] T.M. Cover. ON DETERMINING THE IRRATIONALITY OF THE MEAN OF A RANDOM VARIABLE. *The Annals of Statistics*, 1(5):862–871, 1973.

[2] D. Feldman, R. Impagliazzo, M. Naor, N. Nisan, S. Rudich, and A. Shamir. On Dice and Coins: Models of Computation for Random Generation. *Information and Computation*, 104:159–174, 1993.

[3] J. Gill. Computational Complexity of Probabilistic Turing Machines. *SIAM J. Comput.*, 6(4):675–695, Dec. 1977.

[4] W. Hoeffding and G. Simons. Unbiased Coin Tossing with a Biased Coin. *The Annals of Mathematical Statistics*, 41(2):341–352, 1970.

[5] J.E. Hopcroft and J.D. Ullman. *Introduction to Automata Theory, Languages, and Computation.* Addison-Wesley Publishing Company, 1979.

[6] D.E. Knuth and A.C. Yao. The complexity of nonuniform random number generation. In J.F.Traub, editor, *Algorithms and Complexity, New Directions and Results*, pages 357–428. Academic, New York, 1976.

[7] J. von Neumann. Various techniques used in connection with random digits. Notes by G.E.Forsythe. National Bureau of Standards. *Applied Math Series*, 12:36–38, 1951. Reprinted in von Neumann's Collected Works 5 (Pergamon Press, 1963), 768–770.

[8] E.S. Santos. Computability by Probabilistic Turing Machines. *Transactions of the American Mathematical Society*, 159:165–184, Sep. 1971.

[9] Q.F. Stout and B. Warren. Tree Algorithms for Unbiased Coin Tossing with a Biased Coin. *The Annals of Probability*, 12(1):212–222, 1984.