Chapter 3

Efficient Simulations by a Biased Coin

3.1 Sets efficiently simulated

The following theorem is the main theorem in this chapter.

Theorem 3.1 (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.

We first show that for every integer a greater than 1 and b with $0 < b \leq \frac{a}{2}$, $\mathcal{C}_{\frac{b}{a}} \rightarrow \mathcal{C}_p$ implies that p is a finite decimal on the a-ary system. This is a sufficient condition of Theorem 3.1.

Lemma 3.2 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 3.1 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 3.3 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 3.1(ii).

Lemma 3.4 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 $0 \le c \le 3^k$. 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 3.3. Thus Lemma 3.3 implies the lemma. ∎

As same as Lemma 3.4, we can show it for $\mathcal{C}_{\frac{1}{2}}$, which is a necessary condition of Theorem 3.1(i). We note that it has been shown in [KY76] 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 3.1(i). Finally we show necessary condition of Theorem 3.1(iii).

Lemma 3.5 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 $0 < c \le \frac{a}{2}$ and $c \ne b$. (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 $0 \le i \le k$, 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 $c \le \frac{a}{2} < a-b$. 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 $c \ne b$. Thus $\mathcal{C}_{\frac{b}{a}} \not\to \mathcal{C}_{\frac{c}{a}}$ holds. ∎

3.2 Relations between biased coins and a fair n-sided die

Feldman *et al.* [FIN+93] 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 [FIN+93]. On the other hand,

Theorem 3.1 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 3.1 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 3.5, 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 3.3 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. This is proved as follows: Theorem 1 in [FIN+93] 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 $0 < i < a^k$.