<table>
<thead>
<tr>
<th>Title</th>
<th>Simulating Fair Dice with a Small Set of Rationally Biased Coins</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Itoh, Toshiya; Mochiduki, Takahiro</td>
</tr>
<tr>
<td>Citation</td>
<td>数理解析研究所講究録 (1994), 871: 130-137</td>
</tr>
<tr>
<td>Issue Date</td>
<td>1994-05</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/84045">http://hdl.handle.net/2433/84045</a></td>
</tr>
<tr>
<td>Type</td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td>Textversion</td>
<td>publisher</td>
</tr>
</tbody>
</table>
Simulating Fair Dice with a Small Set of Rationally Biased Coins

東京工業大学総合理工学研究科 伊東 利哉 (Toshiya Itoh)
東京工業大学総合理工学研究科 望月 賢裕 (Takahiro Mochiduki)

1 Introduction

1.1 Background and Motivation

A problem of simulating fair dice with coins is initiated by Feldman et al [Fetal]. Informally, the problem can be defined as follows: Let \( n \geq 2 \) be an integer. Given a set of \( m \geq 1 \) (biased or unbiased) coins, output with equal probability \( 1, 2, \ldots, n \) in a short time by flipping the (biased or unbiased) coins. Such a task is sometimes very crucial in choosing with equal probability an element from a finite but large set, e.g., interactive proof systems [BM], [GM], program checking [BK], self-testing/correcting [BLR], public-key cryptosystems [E], public key distribution schemes [DH], etc. Feldman et al [Fetal], however, showed that if only an unbiased coin is allowed to be flipped, then for any integer \( n \geq 3 \) (not a power of 2), there does not exist any algorithm that always terminates to simulate a fair \( n \)-sided die. This implies that an even a fair \( 3 \)-sided die cannot be simulated only with an unbiased coin. Then for any integer \( n \geq 2 \), we allow in our model of computation to flip biased coins to efficiently simulate a fair \( n \)-sided die (The formal model of computation will be defined in subsection 2.1).

In this model of computation, Feldman et al [Fetal] showed that for any integer \( n \geq 2 \), there exists an efficient algorithm that simulates a fair \( n \)-sided die with an unbiased coin and a coin of bias \( 1/n \) within \( \lceil 2 \log n \rceil + 1 \) coin flips. This implies that for any integer \( n \geq 2 \), \( \lceil 2 \log n \rceil + 1 \) coin flips are sufficient to efficiently simulate a fair \( n \)-sided die. Then our first question is

- **Question 1**: When sufficiently many coins are allowed to be flipped, how many coin flips are necessary to efficiently simulate a fair \( n \)-sided die for any integer \( n \geq 2 \)?

In addition, Feldman et al [Fetal] showed that for any integer \( n \geq 2 \), there exists an efficient algorithm that simulates a fair \( n \)-sided die within \( \lceil 3 \log n \rceil \) coin flips with a single coin of bias \( p_n \), where \( p_n \) is an appropriate algebraic number. This algorithm flips only a single coin of bias \( p_n \), however, it flips the coin of bias \( p_n \) more times than the algorithm above with an unbiased coin and a coin of bias \( 1/n \) does. Then our second question is

- **Question 2**: For any integer \( n \geq 2 \), how many coins are sufficient to efficiently simulate a fair \( n \)-sided die with minimum coin flips?

To efficiently simulate a fair \( n \)-sided die with minimum coin flips for any integer \( n \geq 2 \), the number of coins necessary to do it would be very large. Then our final question is

- **Question 3**: For any integer \( n \geq 2 \), how many coins are necessary to efficiently simulate a fair \( n \)-sided die with minimum coin flips?

In this paper, we carefully analyze the model of computation for simulating dice with coins and provide total or partial solutions to the questions above.

1.2 Results

In this paper, we first show as a solution to Question 1 that for any integer \( n \geq 2 \), if a fair \( n \)-sided die can be simulated within \( d \) coin flips of any set of \( m \geq 1 \) coins, then \( d \geq \lceil \log n \rceil \) (see Theorem 3.1). It is trivial that for any integer \( n \geq 2 \), \( 2^{\lceil \log n \rceil} - 1 \) coins are sufficient to simulate a fair \( n \)-sided die within \( \lceil \log n \rceil \) coin flips, because we have \( 2^{\lceil \log n \rceil} - 1 \) chances to flip different coins to simulate a
fair $n$-sided die within $\lceil \log n \rceil$ coin flips. As a nontrivial solution to Question 2, we show that for any integer $n \geq 2$, there exists an efficient algorithm that simulates a fair $n$-sided die with a set of $H(n)$ rational coins within $\lceil \log n \rceil$ coin flips, where $H(n)$ is the number 1's of the binary representation of an integer $n$ (see Theorem 3.2). This is a nontrivial upper bound on the number of coins, i.e., for any integer $n \geq 2$, a set of $H(n) \leq \lceil \log n \rceil$ rational coins is sufficient to simulate a fair $n$-sided die within $\lceil \log n \rceil$ coin flips.

As we will exemplify in section 4, there exists an integer $n \geq 2$ for which a set of $m < H(n)$ rational coins can simulate a fair $n$-sided within $\lceil \log n \rceil$ coin flips. Thus for every integer $n \geq 2$, a set of $H(n)$ rational coins is not necessary to simulate a fair $n$-sided die within $\lceil \log n \rceil$ coin flips. Then we show as a partial solution to Question 3 that for any integer $n = 2^d - 1$ ($d \geq 3$), a set of $d = H(n)$ rational coins is unique and sufficient to simulate a fair $n$-sided die within $\lceil \log n \rceil$ coin flips (see Theorem 4.3). This implies that for any integer $n = 2^d - 1$ ($d \geq 3$), irrational coins are of no use to simulate a fair $n$-sided die within $\lceil \log n \rceil$ coin flips.

2 Preliminaries

2.1 The Model of Computation

A coin $c$ is said to be of bias $p$ ($0 \leq p \leq 1$) if (upon request) it outputs either heads or tails with probability $p$ for tails. We say that $c$ is a $p$-coin if it is of bias $p$ ($0 \leq p \leq 1$). Note that for any bias $p$ ($0 \leq p \leq 1$), we can transform $p$-coins to $(1-p)$-coins with no additional coin flips by regarding heads as tails and vice versa and that for bias $p = 0, 1$, we can simulate the same process without flipping such coins. Then we assume without loss of generality that $0 < p \leq 1/2$ for any bias $p$. We also assume that for any bias $p$ ($0 < p \leq 1/2$), the outputs of coins of bias $p$ are (statistically) independent. We refer to a coin $c$ of bias $p$ ($0 \leq p < 1/2$) as a rational coin if $p$ is rational. A sequence of $d \geq 1$ coin flips can be viewed as a binary number of length $d \geq 1$ by assigning the value 1 to heads and the value 0 to tails.

Here we use $C = \{p_1, p_2, \ldots, p_m\}$ to denote a set of $m \geq 1$ coins in which the $i$-th $(1 \leq i \leq m)$ coin is of bias $p_i$ ($0 \leq p_i \leq 1/2$). Here we assume that the outputs of a $p_i$-coin and a $p_j$-coin are (statistically) independent for each $i, j$ ($1 \leq i < j \leq m$). For any integer $n \geq 2$, an $n$-sided die $d_n$ is said to be fair if (upon request) it outputs one of $1, 2, \ldots, n$ with equal probability, i.e., for each $i$ ($1 \leq i \leq n$), it outputs $i$ with probability $1/n$. A fair coin is a fair 2-sided die.

To simulate an $n$-sided die with a set of coins $C = \{p_1, p_2, \ldots, p_m\}$ within $d \geq 1$ coin flips, here we consider the following model of computation. Let $T$ be a finite full binary decision tree of depth $d \geq 1$. At every node of $T$, we assume that its right branch is labeled with head (or 1) and its left branch is labeled with tail (or 0). Then $T$ has $2^d$ leaves and each leaf $\ell$ of $T$ is assumed to be numbered from left to right with $0, 1, \ldots, 2^d - 1$. We first assign some $p_i$-coin in $C$ ($1 \leq i \leq m$) to each node of $T$.

Here we refer to this process as node assignment of $T$.

Then we recursively label each node of $T$ with $(a, b) \in \{0, 1\}^* \times \{0, 1\}$ as follows: The root $r$ of $T$ is labeled with $(\epsilon, 1)$, where $\epsilon$ is a null string. When some $p_i$-coin in $C$ ($1 \leq i \leq m$) is assigned to the root $r$ of $T$, its right son is labeled with $(1, 1 - p_i)$ and its left son is labeled with $(0, p_i)$. Now assume that an internal node $v$ of $T$ is labeled with $(s, w) \in \{0, 1\}^* \times (0, 1)$ and that some $p_i$-coin in $C$ ($1 \leq i \leq m$) is assigned to the node $v$ of $T$. Then its right son is labeled with $(s||1, w \times (1 - p_i))$ and its left son is labeled with $(s||0, w \times p_i)$, where $a||b$ denotes the concatenation of strings $a, b \in \{0, 1\}^*$. Finally, each leaf $\ell$ ($0 \leq \ell < 2^d$) of $T$ is labeled with $(s_\ell, w_\ell) \in \{0, 1\}^d \times (0, 1)$. Here we note that for each $\ell$ ($0 \leq \ell < 2^d$), $s_\ell = \bin(\ell)$, where $\bin(\ell)$ denotes the binary representation of an integer $\ell$.

We then determine a mapping from each leaf $\ell$ ($0 \leq \ell < 2^d$) of $T$ to the $k$-th ($1 \leq k \leq n$) side of the $n$-sided die, i.e., $f : \{0, 1, \ldots, 2^n - 1\} \mapsto \{1, 2, \ldots, n\}$. For each $k$ ($1 \leq k \leq n$), the weight $W_k$ of the $k$-th side of the $n$-sided die is defined to be

$$W_k = \sum_{\ell \in \ell^{-1}(k)} w_\ell,$$  \hspace{1cm} (1)
where each leaf \( \ell \) \((0 \leq \ell < 2^d)\) of \( T \) is assumed to be labeled with \((s_\ell, w_\ell) \in \{0,1\}^d \times \{0,1\}\). We refer to this process as \emph{leaf assignment} of \( T \).

We say that a set of \( m \) coins \( C = \{p_1, p_2, \ldots, p_m\} \) simulates a \emph{fair \( n \)-sided die} within \( d \geq 1 \) coin flips if there exist node/leaf assignment of a finite full binary decision tree \( T \) of depth \( d \geq 1 \) such that \( W_k = 1/n \) for each \( k \) \((1 \leq k \leq n)\), and we say that a fair \( n \)-sided die can be simulated within \( d \geq 1 \) coin flips of \( m \geq 1 \) coins if there exists a set of \( m \) coins \( C = \{p_1, p_2, \ldots, p_m\} \) that simulates a fair \( n \)-sided die within \( d \geq 1 \) coin flips.

### 2.2 Known Results

On the model of computation in subsection 2.1, Feldman et al. [Fetal] showed the following:

**Theorem 2.1** [Fetal]: For any integer \( n \geq 2 \), a fair \( n \)-sided die can be simulated with a set of 2 rational coins \( C_n = \{1/n, 1/2\} \) within \([2 \log n] + 1\) coin flips.

**Theorem 2.2** [Fetal]: For any integer \( n \geq 2 \) (not a power of 2), it is impossible to efficiently simulate a fair \( n \)-sided die only with a single rational coin.

**Theorem 2.3** [Fetal]: For any integer \( n \geq 2 \), a fair \( n \)-sided die can be simulated only with a single irrational coin within \([3 \log n]\) coin flips.

### 3 Simulating a Die with Minimum Coin Flips

Feldman et al. [Fetal] showed that for any integer \( n \geq 2 \), \([2 \log n] + 1\) coin flips are sufficient to simulate a fair \( n \)-sided die with a set of 2 rational coins \( C = \{1/n, 1/2\} \) (see Theorem 2.1).

In this section, we first show a lower bound on the number of coin flips to simulate a fair \( n \)-sided die with any fixed set of coins (Theorem 3.1). Then we show that for any integer \( n \geq 2 \), a fair \( n \)-sided die can be simulated with minimum coin flips of a set of \( H(n) \) rational coins, where \( H(n) \) is the number of 1's of the binary representation of \( n \geq 2 \) (Theorem 3.2).

Recall the model of computation (see subsection 2.1) to simulate an \( n \)-sided die with a set of coins \( C = \{p_1, p_2, \ldots, p_m\} \) within \( d \geq 1 \) coin flips. Then the finite full binary decision tree \( T \) of depth \( d \geq 1 \) has \( 2^d \) leaves. When \( 2^d < n \), it is impossible to simulate a fair \( n \)-sided die with any set of coins within \( d \geq 1 \) coin flips even if any node/leaf assignment of \( T \) are used. Thus it follows that \( 2^d \geq n \) and then we have the following theorem:

**Theorem 3.1**: For any integer \( n \geq 2 \) and any integer \( m \geq 1 \), if a fair \( n \)-sided die can be simulated within \( d \geq 1 \) coin flips of any set of \( m \geq 1 \) coins, then \( d \geq \lceil \log n \rceil \).

In the rest of this section, we will focus on showing the theorems that guarantees to simulate a fair \( n \)-sided die for any \( n \geq 2 \) with a small set of coins \( C \) within \([\log n]\) coin flips.

**Theorem 3.2**: For any integer \( n \geq 2 \), a fair \( n \)-sided die can be simulated with a set of \( H(n) \) rational coins \( C_n = \{p_1, \ldots, p_{H(n)} \} \) within \([\log n]\) coin flips, where \( H(n) \) denotes the number of 1's of the binary representation of an integer \( n \geq 2 \).

**Proof**: Let \( n = 2^e N \), where \( N \) is odd and \( e \geq 0 \). We first note that within \( e = [\log 2^e] \) coin flips, a fair \( 2^e \)-sided die can be simulated with a coin of bias 1/2 as follows:

1. define a finite full binary decision tree \( T_{2^e} \) of depth \( e \) by assigning a coin of bias 1/2 to each node of \( T_{2^e} \);
2. map each leaf \( \ell \) \((0 \leq \ell < 2^e)\) of \( T_{2^e} \) to the \((\ell + 1)\)-th side of a \( 2^e \)-sided die.

It is obvious that this simulates a fair \( 2^e \)-sided die with a coin of bias 1/2 within \( e \) coin flips.

Let \( C_N = \{p_1, \ldots, p_{H(N)} \} \) be any set of \( H(N) \) rational coins. Here we assume that a fair \( N \)-sided die can be simulated with the set of \( H(N) \) rational coins \( C_N \) within \([\log N]\) coin flips. Then we can simulate a fair \( n \)-sided die with the set of \( H(n) \) rational coins \( C_N \) as follows:
(1) simulate a fair $2^e$-sided die with a coin of bias $1/2$ within $e = \lceil \log 2^e \rceil$ coin flips;
(2) simulate a fair $N$-sided die with $C_N = \{p_1, \ldots, p_{H(N)-1}, 1/2\}$ within $\lceil \log N \rceil$ coin flips;
(3) when the outcome of a fair $2^e$-sided die is $i$ ($1 \leq i \leq 2^e$) and the outcome of a fair $N$-sided die is $j$ ($1 \leq j \leq N$), output $t = N(i-1) + j$.

Then this process simulates a fair $n$-sided die with a set of coins $C_n = \{p_1, \ldots, p_{H(N)-1}, 1/2\}$ within $\lceil \log N \rceil + e$ coin flips. We note that $H(n) = H(2^e N) = H(N)$ and $\lceil \log n \rceil = \lceil \log 2^e N \rceil = \lceil \log N \rceil + e$ for $n = 2^e N$. Thus it suffices to show that for any odd integer $n \geq 2$, a fair $N$-sided die can be simulated with $C_N = \{p_1, \ldots, p_{H(N)-1}, 1/2\}$ within $\lceil \log N \rceil$ coin flips.

Let $N = 2^{e_1} + 2^{e_2} + \cdots + 2^{e_i}$ be an odd integer, where $0 = e_1 < e_2 < \cdots < e_m$. Then $H(N) = m$ and $\lceil \log N \rceil = e_m + 1$. Define $N_i$ to be $N_i = 2^{e_{m-i}} + 2^{e_{m-i-1}} + \cdots + 2^{e_1}$ for each $i$ ($0 \leq i \leq m-1$). For a set of $m \geq 1$ coins $C_N = \{p_1, p_2, \ldots, p_m\}$, let $p_i = N_i/N_{i-1}$ for each $i$ ($1 \leq i \leq m-1$) and let $p_m = 1/2$. Let $T_N$ be a finite full binary decision tree of depth $\lceil \log N \rceil$. We first recursively define node assignment of $T_N$ as follows:

(1) assign a $p_1$-coin to the root $r$ of $T_N$;
(2) at the node of $T_N$ to which a $p_i$-coin ($1 \leq i \leq m-1$) is assigned, assign a $p_{i+1}$-coin to its left son and assign a $p_m$-coin to its right son;
(3) at the node of $T_N$ to which a $p_m$-coin is assigned, assign a $p_m$-coin to its both sons.

Define $m$ groups of a set of leaves $\ell$ ($0 \leq \ell < 2^{e_m+1} - 1$) of $T_N$ to be

\[
G_1 = \{ \ell \mid 0 \leq \ell < 2^{e_m+2} \};
G_i = \{ \ell \mid 2^{e_m-m+i} \leq \ell < 2^{e_m-m+i+1} \} \quad (2 \leq i \leq m).
\]

Note that $|G_1| = 2^{e_m-m+2}$ and $|G_i| = 2^{e_m-m+i}$ ($2 \leq i \leq m$), where $|A|$ denotes the cardinality of a finite set $A$. For each $G_i$ ($2 \leq i \leq m$), define $2^{e_i}$ blocks $B_{ij}$ ($1 \leq j \leq 2^{e_i}$) of $G_i$ to be

\[
B_{ij} = \{ \ell \in G_i \mid 2^{e_m-m+i} + (j-1) \cdot 2^{e_m-e_i-m+i} \leq \ell < 2^{e_m-m+i} + j \cdot 2^{e_m-e_i-m+i} \}.
\]

Note that for each $i$ ($2 \leq i \leq m$) and each $j$ ($1 \leq j \leq 2^{e_i}$), $|B_{ij}| = 2^{e_m-e_i-m+i}$. We then define leaf assignment $f : \{0, 1, \ldots, 2^{e_m+1} - 1\} \mapsto \{1, 2, \ldots, N\}$ of $T_N$ to be

\[
f(\ell) = \begin{cases} 1 & \ell \in G_1 \\ j + \sum_{h=1}^{\lceil \log n \rceil} 2^{e_h} & \ell \in B_{ij} \quad (2 \leq i \leq m) \end{cases}
\]

It is not difficult to show that $W_k = 1/N$ for each $k$ ($1 \leq k \leq N$). Thus a fair $n$-sided die can be simulated with a set of rational coins $C_n = \{p_1, p_2, \ldots, p_{H(n)}\}$ within $\lceil \log n \rceil$ coin flips for any (not necessarily odd) integer $n \geq 2$.

4 A Lower Bound on the Number of Coins

In section 3, we have shown that for any integer $n \geq 2$, a set of $H(n)$ rational coins is sufficient to simulate a fair $n$-sided die with minimum (i.e., $\lceil \log n \rceil$) coin flips (see Theorems 3.1 and 3.2). In this section, we consider the following question:

- **Question**: For any integer $n \geq 2$, is a set of $H(n)$ rational coins necessary to simulate a fair $n$-sided die with minimum (i.e., $\lceil \log n \rceil$) coin flips?

It is obvious that the answer to the question above is no. Let us look at the example below.

Let $n = 343 = 7^3$. Then $H(343) = 6$ and $\lceil \log 343 \rceil = 9$. It follows from Theorem 3.2 that a fair 7-sided die can be simulated with a set of coins $C_7 = \{3/7, 1/3, 1/2\}$ within 3 coin flips, because $H(7) = \lceil \log 7 \rceil = 3$. Then within 9 $= \lceil \log 343 \rceil$ coin flips, a fair 343-sided die can be simulated with a set of coins $C_7 = \{3/7, 1/3, 1/2\}$ by simulating each fair 7-sided die 3 times.
This implies that a set of $H(n)$ rational coins is not necessary to simulate a fair $n$-sided die within $[\log n]$ coin flips for some integer $n \geq 2$. In the following (see Theorem 4.3), however, we show that there exists a set of integers $S$ such that for every $n \in S$, a set of $H(n)$ rational coins is necessary to simulate a fair $n$-sided die within $[\log n]$ coin flips.

Now let us begin with simple cases: $n = 2^d$ ($d \geq 1$) and $n = 3$. In Lemma 4.1, we show that for any integer $n = 2^d$ ($d \geq 1$), only a fair coin can simulate a fair $n$-sided die within $d = [\log n]$ coin flips and in Lemma 4.2, we show that for $n = 3$, either a set of 2 rational coins or a set of 2 irrational coins is necessary to simulate a fair 3-sided die within $2 = [\log 3]$ coin flips.

**Lemma 4.1:** For any integer $n = 2^d$ ($d \geq 1$), only a coin of bias $1/2$ can simulate a fair $n$-sided die within $d = [\log n]$ coin flips.

From Theorem 2.2, it follows that it is impossible to simulate a fair 3-sided die with a single rational coin. Then Theorem 3.2 implies that if any irrational coin is not allowed to be flipped, then a set of 2 rational coins is necessary and sufficient to simulate a fair 3-sided die within $2 = [\log 3]$ coin flips. From Theorem 2.3, however, it could be possible to simulate a fair 3-sided die with a single irrational coin within $2 = [\log 3]$ coin flips.

The following lemma shows that a set of 2 coins is necessary to simulate a fair 3-sided die within $2 = [\log 3]$ coin flips even if any irrational coin is flipped.

**Lemma 4.2:** For $n = 3$, either a set of 2 rational coins $C_3 = \{p_1, p_2\}$ or a set of 2 irrational coins $C_3 = \{p'_1, p'_2\}$ is necessary to simulate a fair 3-sided die with $2 = [\log 3]$ coin flips.

Now we are ready to show that for any integer $n = 2^d - 1$ ($d \geq 3$), a set of $d = H(n)$ rational coins $C_n = \{p_1, p_2, \ldots, p_d\}$ is necessary to simulate a fair $n$-sided die within $d = [\log n]$ coin flips. Indeed, we show in the following a stronger result, i.e., for any integer $n = 2^d - 1$ ($d \geq 3$), a set of $d = H(n)$ rational coins $C_n = \{p_1, p_2, \ldots, p_d\}$ is necessary and unique to simulate a fair $n$-sided die within $d = [\log n]$ coin flips.

**Theorem 4.3:** Let $S = \{n \mid n = 2^d - 1 \ (d \geq 3)\}$. Then for every $n \in S$, a set of $d = H(n)$ rational coins $C_n = \{p_1, p_2, \ldots, p_d\}$ is necessary and unique to simulate a fair $n$-sided die within $[\log n]$ coin flips, where $p_i = (2^{d-i} - 1)/(2^{d-i+1} - 1)$ ($1 \leq i \leq d - 1$) and $p_d = 1/2$.

**Proof:** Since $n = 2^d - 1$ ($d \geq 3$) for any $n \in S$, $H(n) = d \geq 3$ and $[\log n] = d \geq 3$. Let $T_n$ be a finite full binary decision tree of depth $d = [\log n] \geq 3$. Then $T_n$ has $2^d = n + 1$ leaves. Now we assume that each leaf $\ell$ of $T_n$ is numbered from left to right with $0, 1, 2, \ldots, 2^d - 1$ and is labeled with $(s_\ell, w_\ell) \in \{0, 1\}^d \times \{0, 1\}$, where $s_\ell = \text{bin}(\ell)$ for each $\ell$ ($0 \leq \ell < 2^d$). It is enough to consider a set of $d \geq 3$ coins, because Theorem 3.2 guarantees that a set of $d = H(n)$ rational coins $C_n = \{p_1, p_2, \ldots, p_d\}$, where $p_i = (2^{d-i} - 1)/(2^{d-i+1} - 1)$ for each $i$ ($1 \leq i \leq d - 1$) and $p_d = 1/2$, is sufficient to simulate a fair $n$-sided die within $d = [\log n]$ coin flips.

Let $C_n = \{q_1, q_2, \ldots, q_d\}$ be a set of valid coins in which $0 < q_i \leq 1/2$ ($1 \leq i \leq d$). Even if any node/leaf assignment of $T_n$ is used to simulate a fair $n$-sided die within $d = [\log n]$ coin flips, leaf assignment $f : \{0, 1, \ldots, 2^d - 1\} \mapsto \{1, 2, \ldots, n\}$ of $T_n$ must satisfy that

1. there exists a single side $k_0$ ($1 \leq k_0 \leq n$) of a fair $n$-sided die such that $|f^{-1}(k_0)| = 2$;
2. $|f^{-1}(k)| = 1$ for any side $k$ ($1 \leq k \leq n$) but $k = k_0$ of a fair $n$-sided die,

because $2^{[\log n]} - n = 2^d - (2^d - 1) = 1$. Let $\alpha, \beta$ ($0 \leq \alpha < \beta < 2^d$) be a pair of leaves of $T_n$ such that $f(\alpha) = f(\beta) = k_0$ and $w_\alpha + w_\beta = 1/n$. Here we refer such leaves $\alpha, \beta$ of $T_n$ as merging leaves of $T_n$. Then $0 < w_\alpha, w_\beta < 1/n$ and $w_\ell = 1/n$ for any leaf $\ell$ ($0 \leq \ell < 2^d$) but $\ell = \alpha, \beta$.

Now let us consider the path $P_n$ of length $d = [\log n]$ in $T_n$ from the root of $T_n$ to the merging leaf $0$. Here we assume that each node on $P_n$ is numbered from the root to the (merging) leaf 0 with $v_1, v_2, \ldots, v_d$ and that for each $j$ ($1 \leq j \leq d$), a coin $q_j \in C_n$ ($0 < q_j \leq 1/2$) is assigned to $v_j$. Recall that $2^d > n$ and $0 < q_j \leq 1/2$ ($1 \leq i \leq d$). Then for a leaf 0 of $T_n$,

$$w_0 = q_1 \times q_2 \times \cdots \times q_d \leq \left(\frac{1}{2}\right)^d < \frac{1}{n},$$
where \( q_{ij} \in \tilde{C}_{n} \) for each \( j \) \((1 \leq j \leq d)\). This implies that \( \alpha = 0 \). Then the following two cases are possible: (C1) \( 1 \leq \beta < 2^{d-1} \), and (C2) \( 2^{d-1} \leq \beta < 2^{d} \).

We then show by induction on \( d \geq 3 \) that for every \( n \in S \), a set of \( d = H(n) \) rational coins \( C_{n} = \{ p_{1}, p_{2}, \ldots, p_{d} \} \), where \( p_{i} = (2^{d-i} - 1)/(2^{d-i+1} - 1) \) \((1 \leq i \leq d)\) and \( p_{d} = 1/2 \), is necessary and unique to simulate a fair \( n \)-sided die with \( d = \lceil \log n \rceil \) coin flips.

(Base Stage: \( d = 3 \)). Since \( d = 3 \), \( n = 7 = 2^{3} - 1 \). Let \( T_{7} \) be a finite full binary decision tree of depth \( 3 = \lceil \log 7 \rceil \). Let \( \tilde{C}_{7} = \{ q_{1}, q_{2}, q_{3} \} \) be a set of 3 \(( \text{rational or irrational} \)\) coins in which \( 0 < q_{1}, q_{2}, q_{3} \leq 1/2 \).

Recall that a leaf \( 0 \) of \( T_{7} \) is one of two merging leaves of \( T_{7} \).

In the case of (C1), it follows that \( 1 \leq \beta \leq 3 \) and thus \( w_{\ell} = 1/7 \) for each \( \ell \) \((4 \leq \ell \leq 7)\). It is obvious that \( 1 - q_{i} = w_{3} + w_{6} + w_{7} \). Then \( q_{i} = 3/7 \). This implies that the left half subtree \( T_{7}^{L} \) of \( T_{7} \) simulates a fair 3-sided die within 2 coin flips and the right half subtree \( T_{7}^{R} \) of \( T_{7} \) simulates a fair 4-sided die within 2 coin flips. Then Lemma 4.2 guarantees that on \( T_{7}^{L} \), either a set of 2 rational coins \( C_{3} = \{ p_{1}, p_{2} \} \) or a set of 2 irrational coins \( C_{3}' = \{ p_{1}', p_{2}' \} \) is necessary to simulate a fair 3-sided die within 2 \[= \lceil \log 3 \rceil \] coin flips and Lemma 4.1 guarantees that on \( T_{7}^{R} \), only a coin of bias \( 1/2 \) can simulate a fair 4-sided die within 2 \[= \lceil \log 4 \rceil \] coin flips. If a set of 2 irrational coins \( C_{3}' = \{ p_{1}', p_{2}' \} \) is flipped on \( T_{7}^{L} \), then a set of 4 coins \( C = \{ 3/7, 1/2, p_{1}'p_{2}' \} \) is flipped on \( T_{7} \). This contradicts the assumption that a set of 3 coins \( \tilde{C}_{7} = \{ q_{1}, q_{2}, q_{3} \} \) is flipped on \( T_{7} \). Then it follows that a set of 2 irrational coins \( C_{3}' = \{ 1/3, 1/2 \} \) must be flipped on \( T_{7}^{L} \). Thus in the case of (C1), a set of 3 rational coins \( C_{7} = \{ 3/7, 1/3, 1/2 \} \) is necessary and unique to simulate a fair 7-sided die within \( 3 = \lceil \log 7 \rceil \) coin flips.

In the case of (C2), it follows that \( 4 \leq \beta \leq 7 \). Then we have \( w_{0} = 1\times q_{1} \times q_{2} \times q_{3} < 1/7, w_{1} = w_{2} = w_{3} = 1/7 \), and \( w_{\ell} = 1/7 \) for each \( \ell \) \((4 \leq \ell \leq 7)\) but \( \ell = \beta \). Thus

\[
q_{i_{1}} = w_{0} + w_{1} + w_{2} + w_{3} = w_{0} + 3/7; \\
q_{i_{1}} \times q_{i_{2}} = w_{0} + w_{1} = w_{0} + 1/7; \\
q_{i_{1}} \times q_{i_{2}} \times q_{i_{3}} = w_{0} = w_{0}.
\]

Then for each \( j \) \((1 \leq j \leq 3)\), \( q_{ij} \in \tilde{C}_{7} \) \((0 < q_{ij} \leq 1/2)\) is given by

\[
q_{i_{1}} = w_{0} + 3/7; \\
q_{i_{2}} = \frac{w_{0} + 1/7}{w_{0} + 3/7}; \\
q_{i_{3}} = \frac{w_{0}}{w_{0} + 1/7}.
\]  \[(2)\]

We first show by contradiction that \( q_{ij} \neq q_{ik} \) for each \( j, k \) \((1 \leq j < k \leq 3)\). To do this, we consider the following three cases: (D1) \( q_{ij} = q_{ik} \); (D2) \( q_{ij} = q_{ik}' \); and (D3) \( q_{ij} = q_{ik} \). In the case of (D1), \( w_{0} \) must satisfy that \( w_{0}^{2} = (1/7) \cdot w_{0} + 2/49 = 0 \). In this case, however, \( w_{0} \) cannot be real and this contradicts the assumption that \( 0 < q_{i} \leq 1/2 \). In the case of (D2), \( w_{0} = 1/7 \). Then \( q_{i} = 4/7 \), however, this contradicts the assumption that \( 0 < q_{i} \leq 1/2 \). In the case of (D3), \( w_{0} \) must satisfy that \( w_{0}^{2} = (3/7) \cdot w_{0} + 3/49 = 0 \). In this case, however, \( w_{0} \) cannot be real and this contradicts the assumption that \( 0 < q_{i} \leq 1/2 \). Thus \( q_{ij} \neq q_{ik} \) for each \( j, k \) \((1 \leq j < k \leq 3)\). Then it follows that in the case of (C2), a set of 3 \(= H(7) \) coins \( \tilde{C}_{7} = \{ q_{1}, q_{2}, q_{3} \} \) is necessary to simulate a fair 7-sided die within \( 3 = \lceil \log 7 \rceil \) coin flips.

We then show that in the case of (C2), \( \tilde{C}_{7} \) is unique, i.e., \( \tilde{C}_{7} = C_{7} = \{ 3/7, 1/3, 1/2 \} \). Let \( u \) be the parent of leaves 2 and 3 of \( T_{7} \). Assume that \( u \) is labeled with \((0,1) \in \{ 0,1 \}^{2} \times \{ 0,1 \} \) and a \( q_{r} \)-coin \((1 \leq i \leq 3)\) is assigned to \( u \). Since \( w_{2} = w \times q_{i}, w_{3} = w \times (1 - q_{i}), \) and \( w_{2} = w_{3}, \) we have \( q_{i} = 1/2 \). Thus one of the coins in \( \tilde{C}_{7} = \{ q_{1}, q_{2}, q_{3} \} \) must be of bias \( 1/2 \).

Since \( q_{j} \neq q_{ik} \) \((1 \leq j < k \leq 3)\), there must exist some \( j \) \((1 \leq j \leq 3)\) such that \( q_{ij} = 1/2 \). From equation (2), it follows that if either \( q_{ij} = 1/2 \) or \( q_{ik} = 1/2 \), then \( w_{0} = 1/7 \) and thus \( q_{i} = 4/7 \). This contradicts the assumption that \( 0 < q_{i} \leq 1/2 \). Thus \( q_{i} = 1/2 \) and we have \( w_{0} = 1/14 \) from equation (2). Then it follows from equation (2) that \( q_{ij} = 1/2, q_{ik} = 1/2, q_{ik} = 1/2 \), and \( q_{ik} = 1/2 \). This implies that in the case of (C2), a set of 3 rational coins \( C_{7} = \{ 3/7, 1/3, 1/2 \} \) is necessary and unique to simulate a fair 7-sided die within \( 3 = \lceil \log 7 \rceil \) coin flips.

Thus it follows that a set of 3 \(= H(7) \) rational coins \( C_{7} = \{ 3/7, 1/3, 1/2 \} \) is necessary and unique to simulate a fair 7-sided die within \( 3 = \lceil \log 7 \rceil \) coin flips.

(Induction Stage: \( d > 3 \)). Let \( d \geq 3 \). Assume that for \( n = 2^{d - 1} - 1 \in S \), a set of \( d = H(n) \) rational coins \( C_{n} = \{ p_{1}, p_{2}, \ldots, p_{d} \} \), where \( p_{i} = (2^{d-i} - 1)/(2^{d-i+1} - 1) \) \((1 \leq i \leq d-1)\) and \( p_{d} = 1/2 \), is
necessary and unique to simulate a fair n-sided die within d = \lceil \log n \rceil coin flips. Here we define \( N \in S \) to be \( N = 2^{d+1} - 1 \). Let \( T_N \) be a finite full binary decision tree of depth \( d+1 = \lceil \log N \rceil + 1 \) and let \( C_N = \{q_1, q_2, \ldots, q_{d+1}\} \) be a set of \( d+1 \) (rational or irrational) coins in which \( 0 < q_i \leq 1/2 \) for each \( i \) (\( 1 \leq i \leq d+1 \)). Recall that a leaf 0 of \( T_N \) is one of two merging leaves of \( T_N \).

In the following, we show that a set of \( d+1 = H(N) \) rational coins \( C_N = \{p_1^N, p_2^N, \ldots, p_{d+1}^N\} \), where \( p_i^N = (2^{d-i+1} - 1)/(2^{d-i+1} - 1) \) for each \( i \) (\( 1 \leq i \leq d \)) and \( p_{d+1}^N = 1/2 \), is necessary and unique to simulate a fair \( N \)-sided die within \( d+1 = \lceil \log N \rceil \) coin flips.

In the case of (C1), it follows that \( 1 \leq \beta < 2^{d} \) and thus \( w_\ell = 1/N \) for each \( \ell \) (\( 2^{d} \leq \ell < 2^{d+1} \)). It is obvious that \( 1 - q_i = w_0 + \frac{2^{d} - 2^{d+1-j} + 1}{2^{d+1}-1} = 2^{d}/N \). Then \( q_i = (2^{d} - 1)/(2^{d+1} - 1) \). This implies that the left half subtree \( T_N^L \) of \( T_N \) simulates a fair \( n \)-sided die within \( d = \lceil \log N \rceil - 1 \) coin flips and the right half subtree \( T_N^R \) of \( T_N \) simulates a fair \( 2^{d} \)-sided die within \( d = \lceil \log N \rceil - 1 \) coin flips. Then Lemma 4.1 guarantees that on \( T_N^R \), only a coin of bias 1/2 can simulate a fair \( 2^{d} \)-sided die within \( d = \lceil \log N \rceil \) coin flips. Thus in the case of (C1), a set of \( d = H(N) \) rational coins \( C_N = \{p_1^N, p_2^N, \ldots, p_{d+1}^N\} \) is necessary and unique to simulate a fair \( N \)-sided die within \( d = \lceil \log N \rceil \) coin flips.

In the case of (C2), it follows that \( 2^{d} \leq \beta < 2^{d+1} \). Then we have \( w_\ell = q_{i_1} \times q_{i_2} \times \cdots \times q_{i_{d+1}} < 1/N \) and \( w_\ell = 1/N \) for each \( \ell \) (\( 1 \leq \ell < 2^{d} \)). Then for each \( j \) (\( 1 \leq j \leq d+1 \)),

\[
\prod_{k=1}^{j} q_{i_k} = \sum_{0 \leq \ell < 2^{d+1-j}} w_\ell = w_0 + \sum_{1 \leq \ell < 2^{d+1-j}} w_\ell = w_0 + \frac{2^{d+1-j} - 1}{N}.
\]

Then for each \( j \) (\( 1 \leq j \leq d+1 \)), \( q_{i_j} \in \tilde{C}_N \) \((0 < q_{i_j} \leq 1/2)\) is given by

\[
q_{i_j} = w_0 + \frac{2^{d} - 1}{N} = w_0 + \frac{2^{d} - 1}{2^{d+1} - 1};
\]

\[
q_{i_j} = \frac{w_0 + \frac{2^{d+1-j} - 1}{2^{d+1} - 1}}{w_0 + \frac{2^{d+1-j} - 1}{2^{d+1} - 1}}.
\]

We first show by contradiction that \( q_{i_j} \neq q_{i_\ell} \) for each \( j \) (\( 2 \leq j \leq d+1 \)). Assume that there exists some \( j \) (\( 2 \leq j \leq d+1 \)) such that \( q_{i_j} = q_{i_\ell} \). Then from equations (3) and (4),

\[
\frac{w_0 + \frac{2^{d} - 2^{d+1-j} + 1}{2^{d+1} - 1}}{w_0 + \frac{2^{d} - 2^{d+1-j} + 1}{2^{d+1} - 1}} = \frac{w_0 + \frac{2^{d} - 2^{d+1-j} + 1}{2^{d+1} - 1}}{w_0 + \frac{2^{d} - 2^{d+1-j} + 1}{2^{d+1} - 1}}.
\]

From the equation above, it follows that for some \( j \) (\( 2 \leq j \leq d+1 \)),

\[
\frac{w_0 + \frac{2^{d} - 2^{d+1-j} + 1}{2^{d+1} - 1}}{w_0 + \frac{2^{d} - 2^{d+1-j} + 1}{2^{d+1} - 1}} = \frac{w_0 + \frac{2^{d} - 2^{d+1-j} + 1}{2^{d+1} - 1}}{w_0 + \frac{2^{d} - 2^{d+1-j} + 1}{2^{d+1} - 1}}.
\]

From the assumption that \( 0 < q_{i_j} \leq 1/2 \), it follows that \( 0 < w_0 \leq 1/(2N) \). Then we show that \( \nu_j, v_j \not \in (0, 1/(2N)) \), for any \( j \) (\( 2 \leq j \leq d+1 \)), where \( \nu_j, v_j \) are the solutions of equation (5). For each \( j \) (\( 2 \leq j \leq d+1 \)), define a polynomial \( f_j(x) \) of degree 2 to be

\[
f_j(x) = x^2 - \frac{2^{d} - 2^{d+2-j} + 1}{2^{d+1} - 1} \cdot x + \frac{2^{d} - 2^{d+1-j}}{(2^{d+1} - 1)^2}.
\]

Let \( x_j \) (\( 2 \leq j \leq d+1 \)) be a value that gives the minimum of \( f_j(x) \). Then

\[
x_j = \frac{2^{d} - 2^{d+2-j} + 1}{2 \cdot (2^{d+1} - 1)} = \frac{2^{d} - 2^{d+2-j} + 1}{2N},
\]
and thus we have $x_j = 1/(2N)$ and $x_i > 1/(2N)$ for each $j$ ($3 \leq j \leq d+1$). It is easy to show that for each $j$ ($2 \leq j \leq d+1$), $f_j(1/(2N)) = 1/(4N) > 0$. It follows that $\mu_j, \nu_j \notin (0, 1/(2N))$ for any $j$ ($2 \leq j \leq d+1$), where $\mu_j, \nu_j$ are the solutions of $f_j(x) = 0$. This implies that for all $j$ ($2 \leq j \leq d+1$) such that $q_i = q_i$, then $q_i \notin (0, 1/2)$ and this contradicts the assumption that $0 < q_i \leq 1/2$. Thus $q_i \neq q_i$ for each $j$ ($2 \leq j \leq d+1$).

We then show by contradiction that $q_{i_j} \neq q_{i_k}$ for each $j, k$ ($2 \leq j < k \leq d+1$). To do this, we assume that $q_{i_j} = q_{i_k}$ for some $j, k$ ($2 \leq j < k \leq d+1$). Then $w_0$ must satisfy that

$$w_0 + \frac{2^{d+1-j} - 1}{2^{d+1} - 1} = w_0 + \frac{2^{d+1-k} - 1}{2^{d+1} - 1},$$

and we have $w_0 = 1/N$. It follows that $q_{i_j} = 2^d/N = 2^d/(2^{d+1} - 1) > 1/2$. This contradicts the assumption that $0 < q_i \leq 1/2$. Thus $q_{i_j} \neq q_{i_k}$ for each $j, k$ ($2 \leq j < k \leq d+1$).

From the result that $q_{i_1} \neq q_{i_k}$ ($2 \leq j \leq d+1$) and the result that $q_{i_j} \neq q_{i_k}$ ($2 \leq j < k \leq d+1$), it follows that in the case of (C2), a set of $d+1 = H(N)$ coins $\tilde{C}_N = \{q_{i_1}, q_{i_2}, \ldots, q_{i_{d+1}}\}$ is necessary to simulate a fair $N$-sided die within $d+1 = \lceil \log N \rceil$ coin flips.

We finally show that in the case of (C2), $\tilde{C}_N = C_N = \{p_{i_1}^N, p_{i_2}^N, \ldots, p_{i_{d+1}}^N\}$. Let $u$ be the parent of leaves 2 and 3 of $T_N$. Here we assume that $u$ is labeled with $0^{d-1}1, w \in \{0, 1\}^d$ and a $q_i$-coin ($1 \leq i \leq d+1$) is assigned to $u$. Since $w_2 = w \times q_1$, $w_3 = w \times (1 - q_1)$, and $w_N = w_N$, we have $q_1 = 1/2$.

Thus one of the coins in $\tilde{C}_N = \{q_{i_1}, q_{i_2}, \ldots, q_{i_{d+1}}\}$ must be of bias $1/2$.

Since $q_{i_j} \neq q_{i_k}$ for each $j, k$ ($1 \leq j < k \leq d+1$), there must exist some $j$ ($1 \leq j \leq d+1$) such that $q_{i_j} = 1/2$. From equation (4), it follows that for each $j$ ($2 \leq j \leq d+1$), if $q_{i_j} = 1/2$, then $w_0 = 1/N$ and $q_{i_j} = 2^d/N = 2^d/(2^{d+1} - 1) > 1/2$. This contradicts the assumption that $0 < q_i \leq 1/2$. Thus $q_{i_j} = 1/2$ and we have $w_0 = 1/(2N)$ from equation (3). Then it follows from equation (4) that $q_{i_j} = (2^{d-j+2} - 1)/(2^{d-j+3} - 1) = p_{i_j}^N$ for each $j$ ($2 \leq j \leq d+1$). This implies that in the case of (C2), a set of $d+1 = H(N)$ rational coins $C_N = \{p_{i_1}^N, p_{i_2}^N, \ldots, p_{i_{d+1}}^N\}$, where $p_{i_j}^N = (2^{d-j+3} - 1)/(2^{d-j+2} - 1)$ for each $i$ ($1 \leq i \leq d$) and $p_{i_{d+1}}^N = 1/2$, is necessary and unique to simulate a fair $N$-sided die within $d+1 = \lceil \log N \rceil$ coin flips.

Thus it follows that a set of $d+1 = H(N)$ rational coins $C_N = \{p_{i_1}^N, p_{i_2}^N, \ldots, p_{i_{d+1}}^N\}$, where $p_{i_j}^N = (2^{d-j+3} - 1)/(2^{d-j+2} - 1)$ for each $i$ ($1 \leq i \leq d$) and $p_{i_{d+1}}^N = 1/2$, is necessary and unique to simulate a fair $N$-sided die within $d+1 = \lceil \log N \rceil$ coin flips. \hfill \Box

References


