Report No. TWCU-M-0002

A New Proof for the Monte Carlo Constructibility of $\log\log n$

Ryuhei Uehara
Center for Information Science,
uehara@twcu.ac.jp

Abstract

The Monte Carlo constructibility of $\log\log n$ has proved by Karpinski and Verbeek ([KV87]). They proposed an algorithm, and proved the constructibility by applying a statistical result in [Fel57] to the algorithm. We give a new algorithm, and prove the constructibility by analyzing the algorithm.

1 Introduction

One of the important subjects in the theory of computational complexity is the computation with the small space (see [RCH91] for a comprehensive reference). It is known that no monotone unbounded function below $\log n$ is fully space constructible by deterministic Turing machines [FL75, AM76] or nondeterministic Turing machines [Gef90]. Interestingly, Karpinski and Verbeek showed that $\log\log n$ is fully space constructible by a probabilistic Turing machine with bounded error probability [KV87]. More precisely, they defined Monte Carlo Turing machines as probabilistic Turing machines with bounded error probability equal to $\frac{1}{4}$, and proved that $\log\log n$ is fully space constructible by a Monte Carlo Turing machine, or $\log\log n$ is fully Monte Carlo constructible. They proposed an algorithm computing some function without extra space. They used a statistical result in [Fel57], and proved the function computed by this algorithm is $\log n$. We give a new algorithm. We analyze this algorithm, and prove the function computed by this algorithm is $\log n$.

2 Preliminaries

We assume a standard Turing machine model. For formal definitions of deterministic Turing machines (DTMs) and nondeterministic Turing machines (NTMs), see [HU79]. A *probabilistic Turing machine* (PTM) is a Turing machine with distinguished states called coin-tossing states. For each coin-tossing state, a finite control unit of the PTM specifies two possible next states. The computation of the PTM is deterministic except that in coin-tossing states, when the machine tosses a fair coin to choose one of the possible two next states. We denote by $\Pr\{\mathcal{M}(x) = y\}$ the probability that an $\mathcal{M}$ of PTM produces an output y for an input x.

For an $\mathcal{M}$ of PTM, $\mathcal{M}$ *computes* a partial function f defined as follows: For all x, if there is some y such that $\Pr\{\mathcal{M}(x) = y\} > \frac{1}{2}$, then $f(x) = y$; otherwise, $f(x)$ is undefined. Formal definitions of PTMs are given in [Gil77, JDG88] and are omitted here.

A *Monte Carlo Turing machine* (MTM), introduced by Karpinski and Verbeek in [KV87], is defined by a probabilistic Turing machine computing a partial function f defined as follows: For all x, if there is some y such that $\Pr\{\mathcal{M}(x) = y\} > \frac{3}{4}$, then $f(x) = y$; otherwise, $f(x)$ is undefined. In other words, A Monte Carlo Turing machine is a probabilistic Turing machine with bounded error probability equal to $\frac{1}{4}$. We denote by $\mathrm{MSPACE}(S(n))$ the class of all partial functions computed by MTMs whose work spaces are bounded above by $S(n)$. In addition, $\mathrm{M}^{\mathrm{T}}\mathrm{SPACE}(S(n))$ denotes the class of all partial functions computed by MTMs which always halt. A function $f : \mathbf{N} \to \mathbf{N}$ is called *Monte Carlo constructible* (MC-constructible) if there is an $\mathcal{M}$ of MTM with space bound $f(n)$ for which for all n there exists some x, $|\,x\,| = n$, such that $\mathcal{M}$ computes $f(n)$. If $\mathcal{M}$ satisfies the condition above for $x = 0^n$, then f is called *fully MC-constructible*. The notions of MC^{T}-constructibility and full MC^{T}-constructibility will corresponds to the class of the MTMs which always terminate.

We denote an outcome of coin-tossing by a symbol $\mathcal{H}$ or $\mathcal{T}$. In any ordered sequence of the outcomes of coin-tossing, each maximal subsequence of the outcomes of the same symbol is called a *run*. A run, which consists of a symbol $\mathcal{H}$ (or $\mathcal{T}$), is called a *$\mathcal{H}$-run* (or a *$\mathcal{T}$-run*, respectively).

For a *real* number r and function $f(x)$, $\sum_{i=r}^{\infty} f(i)$ denotes $\lim_{k\to\infty}(f(r)+f(r+1)+f(r+2)+\cdots+f(r+k))$. For a real number r, $[r]$ denotes the closest integer to r, $\lfloor r \rfloor$ denotes the largest integer not greater than r, and $\lceil r \rceil$ denotes the integer $\lfloor r \rfloor + 1$. (Note that when r is an integer, $\lceil r \rceil = r + 1$. This notation is useful since $\lceil \log a \rceil$ space is required to represent an integer a.)

We denote by $\ln n$ the natural logarithm and by $\log n$ the binary logarithm. Let e be the base of the natural logarithm (≈ 2.718) and γ be the Eular's constant, i.e., $\gamma = \lim_{n\to\infty}(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \ln n) \approx 0.577$. Let $\Gamma(z)$ be the gamma function defined by $\Gamma(z) = \int_0^\infty e^{-t}t^{z-1}dt$, and $\psi(z)$ be the psi function defined by $\psi(z) = \frac{d}{dz}\ln\Gamma(z)$.

3 New Proof for Monte Carlo constructibility of $\log\log n$

We will prove the following theorem:

Theorem 1 $\log n \in \mathrm{M}^{\mathrm{T}}\mathrm{SPACE}(\log\log n)$.

In order to prove Theorem 1, we will construct an MTM computing $[\log n]$ without extra space for every input of length n. Since this MTM uses exactly $\lceil \log \lceil \log n \rceil \rceil$ space representing $\log n$, and always terminates, $\log \log n$ is fully MC^{T}-constructible.

We first construct an $\mathcal{M}$ of PTM which, on the input 0^n, operates as follows: While generating a run n times, $\mathcal{M}$ records in binary the maximal length of the runs. Note that n is the number of the runs to be generated rather than the number of coin-tossing. We show that $\mathcal{M}$ witnesses that $\log n \in \mathrm{M}^{\mathrm{T}}\mathrm{SPACE}(\log \log n)$. Let L_n be the random variable taking the maximal length of n runs as its value. Let μ_{Ln} be the expected value of L_n, and σ^2_{Ln} be the variance of L_n. The following Lemma 1 is crucial to the proof.

Lemma 1 *For all positive integers l_1, l_2, and n,*

$$\Pr\{l_1 \leq L_n \leq l_2\} = \left(1 - \left(\frac{1}{2}\right)^{l_2}\right)^n - \left(1 - \left(\frac{1}{2}\right)^{l_1}\right)^n.$$

In particular, for all positive integers l and n,

$$\Pr\{L_n = l\} = \left(1 - \left(\frac{1}{2}\right)^{l}\right)^n - \left(1 - \left(\frac{1}{2}\right)^{l-1}\right)^n.$$

Proof. When $\mathcal{M}$ generates the first run, the length of the first run is equal to l with probability $2 \cdot \left(\frac{1}{2}\right)^{l+1} = \left(\frac{1}{2}\right)^l$ since the first subsequence of the outcomes of the coin-tossing is one of the two subsequences, $\mathcal{H}^l\mathcal{T}$ or $\mathcal{T}^l\mathcal{H}$. When $\mathcal{M}$ generates the other runs, the length of one of the runs is equal to l with probability $\left(\frac{1}{2}\right)^l$ since the subsequence of the outcomes of the coin-tossing is $\mathcal{H}^l\mathcal{T}$ or $\mathcal{T}^l\mathcal{H}$, whose first symbol is decided by the last run. Therefore when $\mathcal{M}$ generates a run, the length of a run is equal to l with probability $\left(\frac{1}{2}\right)^l$, and the length of a run is less than or equal to l with probability $\sum_{i=1}^{l}\left(\frac{1}{2}\right)^l = 1 - \left(\frac{1}{2}\right)^l$. Since $\mathcal{M}$ independently generates a run n times, we obtain $\Pr\{L_n \leq l\} = \left(1 - \left(\frac{1}{2}\right)^l\right)^n$. This implies the lemma. ∎

Now we consider the expected value μ_{Ln} and the variance σ^2_{Ln} to show Theorem 1. To analyze μ_{Ln} and σ^2_{Ln}, the following Lemma 2 and Lemma 3 are useful:

Lemma 2 $\int_0^\infty e^{-t} \ln t \, dt = -\gamma (\approx -0.5772)$, *and* $\int_0^\infty e^{-t} (\ln t)^2 dt = \gamma^2 (\approx 0.3332)$.

Proof. For the gamma function and the psi function, $\frac{d^n}{dz^n}\Gamma(z) = \int_0^\infty e^{-t} t^{z-1} (\ln t)^n dt = (\psi(z))^n \Gamma(z)$ ([MUH60]). On the other hand, $\Gamma(1) = 1$, and $\psi(1) = -\gamma \approx -0.5772$. By letting $z = 1$, we have the lemma. ∎

Lemma 3 *For $0 < p < 1$,*

$$1 - p = \left(1 - \frac{p}{1}\right)^1 < \left(1 - \frac{p}{2}\right)^2 < \cdots < \left(1 - \frac{p}{n}\right)^n < \left(1 - \frac{p}{n+1}\right)^{n+1} < \cdots < e^{-p} <$$

$$\cdots < \left(1 - \frac{p}{n+1}\right)^n < \left(1 - \frac{p}{n}\right)^{n-1} < \cdots < \left(1 - \frac{p}{3}\right)^2 < \left(1 - \frac{p}{2}\right)^1 = 1 - \frac{p}{2}.$$

Proof. Let $a_n(p) = \left(1 - \frac{p}{n}\right)^n$ and $b_n(p) = \left(1 - \frac{p}{n+1}\right)^n$. It is easy to check that $a_1(p) < e^{-p} < b_1(p)$ and $\lim_{n\to\infty} a_n(p) = \lim_{n\to\infty} b_n(p) = e^{-p}$. Hence it is sufficient to show that $a_{n-1}(p) < a_n(p)$ and $b_{n-1}(p) > b_n(p)$ for all $n > 1$. Since $\frac{c_1 + c_2 + \cdots + c_n}{n} \geq \sqrt[n]{c_1 c_2 \cdots c_n}$ for all $c_i \geq 0$ and $n \geq 1$,

$$\begin{aligned}
\frac{a_{n-1}(p)}{a_n(p)} &= \left(\frac{n}{n-p}\right)^n \left(\frac{n-1-p}{n-1}\right)^{n-1} \leq \left(\frac{\frac{n^2}{n-p} + n - 1 - p}{2n-1}\right)^{2n-1} \\
&= \left(1 - \frac{p(n-1)}{2n^2 - (1+p)n + p^2}\right)^{2n-1} < 1.
\end{aligned}$$

Also, since $\frac{n+d}{m+d} > \frac{n}{m}$ holds for $m > n > 0$ and $d > 0$,

$$\frac{b_{n-1}(p)}{b_n(p)} = \left(\frac{n-p}{n}\right)^{n-1}\left(\frac{n+1}{n+1-p}\right)^{n} > \left(\frac{n-p}{n}\right)^{n-1}\left(\frac{n}{n-p}\right)^{n} = \frac{n}{n-p} > 1.$$

■

We are now ready to show the key lemma for proving Theorem 1.

Lemma 4 *For large n, there exist two constants c_1 and c_2 such that $\mu_{Ln} = \log n + c_1$, where $-0.17 < c_1 < 0.83$, and $\sigma^2_{Ln} = c_2$, where $(0 <) c_2 < 5.44$.*

Proof. First, we consider the expected value μ_{Ln}. By definition,

$$\mu_{Ln} = \sum_{l=0}^{\infty} \Pr\{L_n = l\} \cdot l = \sum_{l=0}^{\infty} \left(\left(1 - \left(\frac{1}{2}\right)^{l}\right)^{n} - \left(1 - \left(\frac{1}{2}\right)^{l-1}\right)^{n}\right) \cdot l.$$

By letting $l = \log(n-1) + c$, we obtain

$$\begin{aligned}
\mu_{Ln} &= \sum_{c=-\log(n-1)}^{\infty} (\log(n-1)+c)\left(\left(1 - \left(\frac{1}{2}\right)^{c}\left(\frac{1}{n-1}\right)\right)^{n} - \left(\left(1 - \left(\frac{1}{2}\right)^{c-1}\left(\frac{1}{n-1}\right)\right)^{n}\right)\right) \\
&= \sum_{c=-\log(n-1)}^{\infty} (\log(n-1)+c)\int_{c-1}^{c} \ln 2 \left(\frac{1}{2}\right)^{x}\left(1 - \left(\frac{1}{2}\right)^{x}\left(\frac{1}{n-1}\right)\right)^{n-1} dx \\
&< \sum_{c=-\log(n-1)}^{\infty} (\log(n-1)+c)\int_{c-1}^{c} \ln 2 \left(\frac{1}{2}\right)^{x} e^{-\left(\frac{1}{2}\right)^{x}} dx \quad \text{(by Lemma 3)} \\
&< \log(n-1)\int_{-\log(n-1)-1}^{\infty} \ln 2 \left(\frac{1}{2}\right)^{x} e^{-\left(\frac{1}{2}\right)^{x}} dx + \int_{-\log(n-1)-1}^{\infty} \ln 2 \left(\frac{1}{2}\right)^{x} x e^{-\left(\frac{1}{2}\right)^{x}} dx \\
&\quad \text{(by the property of integral)} \\
&< \left(1 - e^{-2(n-1)}\right)\log(n-1) - \frac{1}{\ln 2}\int_{0}^{2(n-1)} e^{-t}\ln t\, dt \quad (\text{where } t = \left(\tfrac{1}{2}\right)^{x}) \\
&< \left(1 - e^{-2(n-1)}\right)\log(n-1) + \frac{\psi(1)\Gamma(1)}{\ln 2} \quad \text{(by Lemma 2)} \\
&< \log n + \frac{\gamma}{\ln 2}.
\end{aligned}$$

On the other hand, letting $l = \log n + d$, then we have

$$\begin{aligned}
\mu_{Ln} &= \sum_{d=-\log n}^{\infty} (\log n + d)\left(\left(1 - \left(\frac{1}{2}\right)^{d}\left(\frac{1}{n}\right)\right)^{n} - \left(1 - \left(\frac{1}{2}\right)^{d-1}\left(\frac{1}{n}\right)\right)^{n}\right) \\
&= \sum_{d=-\log n}^{\infty} (\log n + d)\int_{d-1}^{d} \ln 2 \left(\frac{1}{2}\right)^{x}\left(1 - \left(\frac{1}{2}\right)^{x}\left(\frac{1}{n}\right)\right)^{n-1} dx \\
&> \sum_{d=-\log n}^{\infty} (\log n + d)\int_{d-1}^{d} \ln 2 \left(\frac{1}{2}\right)^{x} e^{-\left(\frac{1}{2}\right)^{x}} dx \quad \text{(by Lemma 3)} \\
&> (\log n - 1)\int_{-1-\log n}^{\infty} \ln 2 \left(\frac{1}{2}\right)^{x} e^{-\left(\frac{1}{2}\right)^{x}} dx + \int_{-1-\log n}^{\infty} \ln 2 \left(\frac{1}{2}\right)^{x} x e^{-\left(\frac{1}{2}\right)^{x}} dx \\
&\quad \text{(by the property of integral)} \\
&= (1 - e^{-2n})(\log n - 1) - \frac{1}{\ln 2}\int_{0}^{2n} e^{-t}\ln t\, dt \quad (\text{where } t = \left(\tfrac{1}{2}\right)^{x}) \\
&> (1 - e^{-2n})\log n - 1 + \frac{\gamma}{\ln 2} \quad \text{(by Lemma 2).}
\end{aligned}$$

Thus for all n, $\mu_{Ln} - \log n < 0.83$, and for large n, $\mu_{Ln} - \log n > -0.17$.

Secondly, we consider the variance σ^2_{Ln}. By definition,

$$\sigma^2_{Ln} = \sum_{l=0}^{\infty} \Pr\{L_n = l\} \cdot (l - \mu_{Ln})^2 = \sum_{l=0}^{\infty} \left(\left(1 - \left(\frac{1}{2}\right)^l\right)^n - \left(1 - \left(\frac{1}{2}\right)^{l-1}\right)^n \right) \cdot (l - \mu_{Ln})^2 .$$

Letting $l = \log(n-1) + c$ and $\mu_{Ln} = \log n + c_1$, then we have

$$\begin{aligned}
\sigma^2_{Ln} &= \sum_{c=-log(n-1)}^{\infty} (\log(n-1) + c - \log n - c_1)^2 \left(\left(1 - \left(\frac{1}{2}\right)^c \frac{1}{n-1}\right)^n - \left(1 - \left(\frac{1}{2}\right)^{c-1} \frac{1}{n-1}\right)^n \right) \\
&< \sum_{c=-log(n-1)}^{\infty} (c - 1 - c_1)^2 \int_{c-1}^{c} \ln 2 \left(\frac{1}{2}\right)^x e^{-\left(\frac{1}{2}\right)^x} dx \\
&< \int_{-\log(n-1)-1}^{\infty} \ln 2 \left(x^2 - 2(1+c_1)x + (1+c_1)^2\right) \left(\frac{1}{2}\right)^x e^{-\left(\frac{1}{2}\right)^x} dx \\
&\quad \text{(by the property of integral)} \\
&= \int_0^{2(n-1)} \left(\left(\frac{1}{\ln 2}\right)^2 (\ln t)^2 - \frac{2(1+c_1)}{\ln 2} \ln t + (1+c_1)^2 \right) e^{-t} dt \quad \text{(by Lemma 3)} \\
&< \left(\frac{\gamma}{\ln 2}\right)^2 + \frac{2\gamma}{\ln 2}(1+c_1) + (1+c_1)^2 < 5.44 \quad \text{(by Lemma 2).}
\end{aligned}$$

∎

Proof of Theorem 1. Let $\mathcal{M}^k$ be a PTM which simulates $\mathcal{M}$ k times and records the average over the k numbers recorded by $\mathcal{M}$ in the k simulations. Lemma 4 and the basic facts from statistics show that the variance of the number recorded by $\mathcal{M}^k$ is equal to $\frac{c_2}{k}$. Hence, there exists a constant k_0 such that for all $k > k_0$, $\mathcal{M}^k$ computes $[\log n + c_1]$ with probability greater than $\frac{3}{4}$. Therefore there exists an $\mathcal{M}$ of MTM computing $[\log n]$ with no extra space since the finite states can correct the constant error. Thus $\log n \in \mathrm{MSPACE}(\log\log n)$.

Although $\mathcal{M}$ terminates with probability 1, $\mathcal{M}$ does not always halt. To complete the proof, we consider an $\mathcal{M}'$ of PTM operates in the same way as $\mathcal{M}$ does except coin-tossing steps. In the computation of $\mathcal{M}'$, let l be the length of the current run. In each coin-tossing step, $\mathcal{M}'$ moves the input tape head right l times, moves the input tape head left l times, and checks whether the input tape head arrives at the end of the input tape. If the input tape head arrives at the end of the input tape on both sides, $\mathcal{M}'$ halts and rejects, since the length of the current run is at least $\frac{n}{2}$. It is clear that $\mathcal{M}'$ always halts, and records the same number as $\mathcal{M}$ does when $\mathcal{M}'$ accepts. Thus $\log n \in \mathrm{M^T SPACE}(\log\log n)$. ∎

References

[AM76] H. Alt and K. Mehlhorn. Lower bounds for the space complexity of context-free recognition. *Proceedings, Int. Colloq. Automate Lang. & Programm. '76*, pages 338–351, 1976.

[Fel57] William Feller. *An Introduction to Probability Theory and Its Applications*, volume 1. John Wiley & Sons, Inc., second edition, 1957.

[FL75] A.R. Freedman and R.E. Ladner. Space bounds for processing counterless inputs. *Journal of Computer and System Sciences*, 11:118–128, 1975.

[Fre81] Rusins Freivalds. Probabilistic two-way machines. In *Proceedings, Math. Found. Comput. Sci. '81*, pages 33–45, New York/Berlin, 1981. Lecture Notes in Computer Science Vol. 118, Springer-Verlag.

[Gef90] Viliam Geffert. Nondeterministic computation in sublogarithmic space and space constructibility. In *Proceedings, 17th Int. Colloq. Automata, Languages and Programming*, pages 111–124. Lecture Notes in Computer Science Vol. 443, Springer-Verlag, 1990.

[Gil77] John Gill. Computational complexity of probabilistic turing machines. *SIAM J. Comput.*, 6(4):675–695, Dec. 1977.

[HU79] John E. Hopcroft and Jeffrey D. Ullman. *Introduction to Automata Theory, Languages, and Computation.* Addison-Wesley Publishing Company, 1979.

[JDG88] J.L.Balcázar, J. Díaz, and J Gabarró. *Structural Complexity I.* Springer-Verlag, 1988.

[KV87] Marek Karpinski and Rutger Verbeek. On the monte carlo space constructible functions and separation results for probabilistic complexity classes. *Information and Computation*, 75:178–189, 1987.

[MUH60] Shigeichi Moriguchi, Kanehisa Udagawa, and Shin Hitotsumatsu. *Mathematical Formulas*, volume III Special Functions. Iwanami, 1960. (In Japanese).

[RCH91] Desh Ranjan, Richard Chang, and Juris Hartmanis. Space bounded computations: review and new separation results. *Theoretical Computer Science 80*, pages 289–302, 1991.

[Sze89] Andrzej Szepietowski. Some notes on strong and weak $\log\log n$ space complexity. *Information Processing Letters*, 33:109–112, Nov. 1989.