Computability versus Exact Computability of Martingales*

Jack H. Lutz
Department of Computer Science
Iowa State University
Ames, IA 50011, USA
lutz@cs.iastate.edu

Abstract

This note gives a simple example of a polynomial time computable martingale that has rational values but is not exactly computable.

Keywords: Computability, computational complexity, martingales, real-valued functions

1 Introduction

This note concerns the computability and complexity of real-valued functions on discrete domains. Such functions arise most commonly as martingales (or supermartingales, or gales, or systems of such) in the theories of algorithmic randomness, resource-bounded measure, and effective fractal dimensions [5, 11, 9, 12, 7, 8, 6]. To be concrete, we thus restrict attention to the computability and complexity of a *martingale*, which is a nonnegative real-valued function $d : \{0,1\}^* \to [0,\infty)$ satisfying the condition

$$d(w) = \frac{d(w0) + d(w1)}{2} \tag{1}$$

for all $w \in \{0,1\}^*$. It will be clear, however, that our central observation holds generally for real-valued functions on discrete domains.

A martingale $d : \{0,1\}^* \to [0,\infty)$ is *computable* if there is a computable, rational-valued function $\hat{d} : \mathbb{N} \times \{0,1\}^* \to \mathbb{Q}$ such that, for all $r \in \mathbb{N}$ and $w \in \{0,1\}^*$,

$$|\hat{d}(r,w) - d(w)| \leq 2^{-r}. \tag{2}$$

That is, given an input w for d and a precision parameter r, $\hat{d}$ gives a rational approximation of $d(w)$ with an error no greater than 2^{-r}. Moreover, $\hat{d}$ is computable in the discrete sense that there is a Turing machine that, given the inputs r and w in some specified format, halts after finitely many computation steps, having printed the rational number $\hat{d}(r,w)$ (numerator, denominator, and sign bit) in some specified output format.

It is straightforward to impose complexity bounds on the above definition. For example, a martingale $d : \{0,1\}^* \to [0,\infty)$ is *polynomial time computable* if there is a function $\hat{d} : \mathbb{N} \times \{0,1\}^* \to \mathbb{Q}$ satisfying (2) and having the property that $\hat{d}(r,w)$ is computable in time polynomial in $r + |w|$.

*This research was supported in part by National Science Foundation grants 9988483 and 0344187.

These definitions of computability and complexity are essentially due to Grzegorczyk [1, 2]. (See also [4, 13].) Aside from being computationally realistic, they are useful because martingales often arise naturally as infinite sums whose values need not be rational. On the other hand, it is sometimes convenient to work with martingales that can be computed exactly, i.e., without the approximation (2). A martingale $d : \{0,1\}^* \to [0,\infty)$ is thus *exactly computable* if it is rational-valued (i.e., $d : \{0,1\}^* \to \mathbb{Q} \cap [0,\infty)$) and computable in the discrete sense that there is a Turing machine that, on input $w \in \{0,1\}^*$, outputs the rational number $d(w)$ after finitely many computation steps. Similarly, d is *exactly polynomial time computable* if d is rational-valued and there is a Turing machine that outputs the rational number $d(w)$ in time polynomial in $|w|$.

The Exact Computation Lemma, proven independently in [3, 10], says that for every computable (respectively, polynomial time computable) martingale d, there is an exactly computable (respectively, exactly polynomial time computable) martingale d' that is "as good as" d in the technical sense that d' succeeds on every sequence on which d succeeds. (A martingale d *succeeds* on an infinite binary sequence S if the values $d(w)$, for prefixes w of S, are unbounded.) Many theorems have now been proven using this lemma.

At first glance, it is natural to believe that the Exact Computation Lemma is only needed when the martingale d has irrational values. For example, it is natural to conjecture that a computable martingale whose values are all rational must already be exactly computable. Indeed, we have encountered several researchers who have implicitly or explicitly assumed the truth of this natural conjecture.

The purpose of this note is to clarify this issue by explicitly refuting this conjecture. Specifically, we give a simple example of a polynomial-time computable martingale that is rational-valued but not exactly computable in any amount of time.

2 The Example

Let $M_0, M_1, M_2, \ldots$ be a standard enumeration of Turing machines, and let $t(n)$ denote the number of steps that M_n executes on input n. Assume that the initial state of a Turing machine is never a halting state, so that $t(n)$ is strictly positive. It is well known that the *halting problem*

$$K = \{n \in \mathbb{N} \mid t(n) < \infty\}$$

is undecidable. Define the martingale $d : \{0,1\}^* \to [0,\infty)$ by

$$d(w) = \prod_{n=0}^{|w|-1} (1 + (-1)^{w[n]} 2^{-t(n)}) \tag{3}$$

for all $w \in \{0,1\}^*$, where $w[n]$ is the n^{th} bit of w ($0 \leq n < |w|$) and $2^{-\infty} = 0$. Since $d(w0) = (1+2^{-t(|w|)})d(w)$ and $d(w1) = (1-2^{t(|w|)})d(w)$, it is clear that (1) holds for all $w \in \{0,1\}^*$, i.e., d is a martingale. An exact computation of d would solve the halting problem (i.e., $n \in K \Leftrightarrow d(0^n) < d(0^{n+1})$), so d is not exactly computable.

To see that d is polynomial-time computable, define $\theta : \mathbb{N}^3 \to \mathbb{Q}$ and $\hat{d} : \mathbb{N} \times \{0,1\}^* \to \mathbb{Q}$ by

$$\theta(r,l,n) = \begin{cases} 2^{-t(n)} & \text{if } t(n) \leq r + 2l + 1 \\ 0 & \text{if } t(n) > r + 2l + 1 \end{cases}$$

and

$$\hat{d}(r,w) = \prod_{n=0}^{|w|-1} (1 + (-1)^{w[n]}\theta(r,|w|,n))$$

for all $r, l, n \in \mathbb{N}$ and $w \in \{0,1\}^*$. It is clear that $\theta(r,l,n)$ can be computed in time polynomial in $r+l+n$, whence $\hat{d}(r,w)$ can be computed in time polynomial in $r+|w|$.

For all $r \in \mathbb{N}$ and $w \in \{0,1\}^*$, we have

$$\left|\ln \frac{\hat{d}(r,w)}{d(w)}\right| \leq \sum_{n=0}^{|w|-1} \delta(r,w,n), \tag{4}$$

where we write

$$\delta(r,w,n) = \left|\ln(1 + (-1)^{w[n]}\theta(r,|w|,n)) - \ln(1 + (-1)^{w[n]}2^{-t(n)})\right|.$$

Our definition of θ and (3) ensure that

$$\delta(r,w,n) \leq \left|\ln(1 + (-1)^{w[n]}2^{-(r+2|w|+2)})\right| \tag{5}$$

for all $r \in \mathbb{N}$, $w \in \{0,1\}^*$, and $0 \leq n < |w|$. Using the inequality $x - x^2 \leq \ln(1+x) \leq x$ (valid for all $x \geq -\frac{1}{2}$ by elementary calculus) with $x = \pm 2^{-(r+|w|+2)}$, (5) implies that

$$\delta(r,w,n) \leq |x| + x^2 < 2|x| = 2^{-(r+|w|+1)}$$

for all $r \in \mathbb{N}$, $w \in \{0,1\}^*$, and $0 \leq n < |w|$. It follows by (4) that, for all $r \in \mathbb{N}$ and $w \in \{0,1\}^*$,

$$\left|\ln \frac{\hat{d}(r,w)}{d(w)}\right| \leq |w|2^{-(r+2|w|+1)} < \epsilon(r,|w|),$$

where we write $\epsilon(r,l) = 2^{-(r+l+1)}$. This implies that

$$e^{-\epsilon(r,|w|)}d(w) \leq \hat{d}(r,w) \leq e^{\epsilon(r,|w|)}d(w) \tag{6}$$

for all $r \in \mathbb{N}$ and $w \in \{0,1\}^*$. Using the inequalities $e^{-\epsilon} \geq 1 - \epsilon$ and $e^{\epsilon} \leq 1 + 2\epsilon$ (valid for all $\epsilon \in [0,1)$ by elementary calculus), (6) tells us that

$$\begin{aligned}\hat{d}(r,w) &> (1 - \epsilon(r,|w|))d(w) \\ &\geq d(w) - \epsilon(r,|w|)2^{|w|} \\ &= d(w) - 2^{-(r+1)}\end{aligned}$$

and

$$\begin{aligned}\hat{d}(r,w) &< (1 + 2\epsilon(r,|w|))d(w) \\ &\leq d(w) + 2\epsilon(r,|w|)2^{|w|} \\ &= d(w) + 2^{-r},\end{aligned}$$

whence

$$|\hat{d}(r,w) - d(w)| < 2^{-r}$$

for all $r \in \mathbb{N}$ and $w \in \{0,1\}^*$. Thus $\hat{d}$ testifies that d is polynomial-time computable.

Acknowledgment. I thank Anthony Finkelstein and IFIP Working Group 2.9 for their warm hospitality while this note was written.

References

[1] Andrzej Grzegorczyk. Computable functionals. *Fundamenta Mathematicae*, 42:168–202, 1955.

[2] Andrzej Grzegorczyk. On the definitions of computable real continuous functions. *Fundamenta Mathematicae*, 44:61–71, 1957.

[3] D. W. Juedes and J. H. Lutz. Weak completeness in E and E_2. *Theoretical Computer Science*, 143(1):149–158, 1995.

[4] K. Ko. *Complexity Theory of Real Functions*. Birkhäuser, Boston, 1991.

[5] M. Li and P. M. B. Vitányi. *An Introduction to Kolmogorov Complexity and its Applications*. Springer-Verlag, Berlin, 1997. Second Edition.

[6] J. H. Lutz. Effective fractal dimensions. *Mathematical Logic Quarterly*. To appear.

[7] J. H. Lutz. The quantitative structure of exponential time. In L. A. Hemaspaandra and A. L. Selman, editors, *Complexity Theory Retrospective II*, pages 225–254. Springer-Verlag, 1997.

[8] J. H. Lutz. Resource-bounded measure. In *Proceedings of the 13th IEEE Conference on Computational Complexity*, pages 236–248, 1998.

[9] P. Martin-Löf. The definition of random sequences. *Information and Control*, 9:602–619, 1966.

[10] E. Mayordomo. *Contributions to the study of resource-bounded measure*. PhD thesis, Universitat Politècnica de Catalunya, 1994.

[11] C. P. Schnorr. *Zufälligkeit und Wahrscheinlichkeit*. Springer-Verlag, Berlin, 1971.

[12] M. van Lambalgen. *Random Sequences*. PhD thesis, Department of Mathematics, University of Amsterdam, 1987.

[13] Klaus Weihrauch. *Computable Analysis. An Introduction*. Springer-Verlag, 2000.