석 사 학 위 논 문
Master's Thesis

# 브라운 운동을 포함한 연속적 객체 확률추출의 계산가능성

# Random Sampling of Continuous Objects: Can we Computably Generate Brownian Motions?

2020

이 현 우 (李 炫 遇 Lee, Hyunwoo)

한 국 과 학 기 술 원

Korea Advanced Institute of Science and Technology

석 사 학 위 논 문

# 브라운 운동을 포함한 연속적 객체 확률추출의 계산가능성

2020

이 현 우

한 국 과 학 기 술 원

전산학부

# 브라운 운동을 포함한 연속적 객체 확률추출의 계산가능성

이 현 우

위 논문은 한국과학기술원 석사학위논문으로
학위논문 심사위원회의 심사를 통과하였음

2019년 12월 11일

| | | |
|---|---|---|
| 심사위원장 | Martin Ziegler | (인) |
| 심 사 위 원 | Svetlana Selivanova | (인) |
| 심 사 위 원 | Paul Jung | (인) |

# Random Sampling of Continuous Objects: Can we Computably Generate Brownian Motions?

Hyunwoo Lee

Advisor: Martin Ziegler

A dissertation submitted to the faculty of
Korea Advanced Institute of Science and Technology in
partial fulfillment of the requirements for the degree of
Master of Science in Computer Science

Daejeon, Korea
December 11, 2019

Approved by

Martin Ziegler
Professor of School of Computing

The study was conducted in accordance with Code of Research Ethics[1].

[1] Declaration of Ethical Conduct in Research: I, as a graduate student of Korea Advanced Institute of Science and Technology, hereby declare that I have not committed any act that may damage the credibility of my research. This includes, but is not limited to, falsification, thesis written by someone else, distortion of research findings, and plagiarism. I confirm that my thesis contains honest conclusions based on my own careful research under the guidance of my advisor.

MCS 20183477

이현우. 브라운 운동을 포함한 연속적 객체 확률추출의 계산가능성. 전산학부 . 2020년. 17+iii 쪽. 지도교수: 지글러마틴. (영문 논문)
Hyunwoo Lee. Random Sampling of Continuous Objects: Can we Computably Generate Brownian Motions?. School of Computing . 2020. 17+iii pages. Advisor: Martin Ziegler. (Text in English)

**초 록**

확률화는 많은 실용적인 상황에서 다양한 알고리즘의 복잡도를 낮출수 있는 강력한 도구이다. 하지만 이러한 알고리즘을 구현하는데에 있어서는 주어진 확률분포로 부터 확률추출의 과정이 필수적이다. 본 논문에서는 연속 확률분포로부터의 확률추출을 연속적 데이터에 대한 계산을 다루기 위한 체계인 유형-2 계산이론의 관점에서 형식화하였다. 첫번째로 우리는 제 2 가산 $T_0$ 공간위의 확률측도는 단지 칸토어 공간 위의 일반적인 확률 측도의 전진측도에 불과하다는 것을 발견하였다. 이는 Simpson 과 Schröder 의 2006년 결과의 확장이다.

본 논문의 두번째 결과는 브라운 운동을 $f(0) = 0$ 를 만족하는 연속함수 $f : [0, 1] \to \mathbb{R}$ 들의 공간위에 주어진 확률측도로 생각하는 것으로부터 시작한다. 우리는 이러한 측도가 확률추출 가능한 조건을 규명하였다. 이 측도가 확률추출 가능하다는 것이 해당하는 함수들의 연속률의 모임으로부터 확률추출이 가능하다는 것과 동치임을 증명하였다

**핵 심 낱 말** 계산 해석학, 유형-2 계산이론, 확률추출, 확률론, 확률변수, 위너 확률과정, 브라운 운동

**Abstract**

Randomization is a very powerful tool which can reduce the complexity of a lot of algorithms in practice. However, to implement a randomized algorithm, sampling procedure from the fixed probability distribution is essential. In this paper, we formalized the sampling procedure from continuous probability distribution in the sense of Type-2 Theory of Effectivity which is theoretical framework to handle the computation over continuous data. We first show that every Borel probability measure on second countable $T_0$ spaces is just a push-forward measure of Canonical probability measure on Cantor Space. This is the extension of the result by Simpson and Schröder, 2006.

Second result is concerned with Brownian motion as the probability measure on the space of continuous function $f : [0, 1] \to \mathbb{R}$ with $f(0) = 0$. We figure out the condition when such a measure can be sampled. This measure can be sampled if and only if its family of modulus of continuity can be sampled.

**Keywords** Computable Analysis, Type-2 Theory of Effectivity, Random Sampling, Probability Theory, Random Variable, Wiener Process, Brownian motion

# Contents

# List of Tables

# List of Figures

# Chapter 1. Introduction

In mathematics, especially in real analysis or measure theory, 'measure' on the space $S$ is mapping from its $\sigma$-algebra to positive reals. If the measure of whole space $S$ equals to 1, we call such measure a probability measure or just probability. And we can define two different types of computability of measure. Think about the case of rolling a dice. The probability distribution of each face of dice can be regarded as a (uniform) probability measure on $\{1, 2, 3, 4, 5, 6\}$. It is so trivial that there exists a computable function that can give the probability of a given subset of $\{1, 2, 3, 4, 5, 6\}$. In other words, we can say that this program computes the measure as the function from its $\sigma$- algebra to $\mathbb{R}$. Traditionally, computability of measure is defined as the computability of such function [3]. It is known that these kinds of computability of measure are equivalent to the computability of integration over such measure. However, building the algorithm, or making a program which generates the number from 1 to 6 with given probability distribution is a completely different problem. This procedure is also known as sampling. We will call measure is *samplable* if such a program exists.

So far, several authors have already researched about the computational aspect of measure or probability. Weihrauch suggested the standard representation of set of every measures on real interval $[0, 1]$ in [14]. Müller extended this result to the standard representation of Random Variable [9]. In [11], Schröder found the Admissible representation for probability measure.

In the above papers, computability of measure is commonly treated as the first type of computability. However, we want to focus on the second type of computability, i.e. *samplability* of probability measure. In many probabilistic algorithms such as Random Knapsack [1] or Monte Carlo integration [5], the sampling procedure is implicitly or explicitly included. Several authors already studied the sampling procedure over discrete data [13]. However, even though sampling procedure on more general spaces is very widely used in the numerical algorithm such as Walk on Sphere methods [2], there is only few research about sampling over continuous data in the sense of computable analysis. So, in this paper, we try to formalize the concept and notion of sampling procedure.

## 1.1 Overview

In Chapter 2, we're considering the question of how to represent Borel probability measures. It is known that on the spaces with a very weak condition, every Borel probability distribution can be represented by the distribution of an infinite sequence of coin flips with adaptively biased coins. We extend this result by theorem 2.3.2 and show that every Borel probability distribution on such space can be represented by *fair* coin flips. Also, based on such representation, we suggest the definition 2.4.1 which can formalize the random sampling in a highly rigorous sense.

Chapter 3 approaches the notion of probabilistic computation using the concept of a random variable. Unlike function, a random variable has a bit different concept of computability and convergence. Definition 3.1.1 and 3.1.2 shows it. We figure out that there exists a relationship between them of a random variable which is very similar to the usual function and function sequence.

Finally, we discuss the question of whether we can sample the Brownian motion, which is a well-known probability distribution on space of continuous function, in Chapter 4. We provide the algorithm to sample the Brownian motion. And based on this algorithm, characterize the samplability of Brownian motion. At last, we show why some well-known sequence which converges to Brownian motion doesn't imply the samplability of Brownian motion.

## 1.2 Preliminaries

In this section, we will give a brief introduction about computation over continuous data. In the traditional theory of computation, a natural number is represented as a finite binary string. Similarly, it is not difficult to show that we can represent rationals as a finite binary string. However, if the set we want to represent is bigger than the set of natural numbers, i.e. uncountable, then finite binary string is not enough. Because there are only countably many finite binary strings. That's why we use infinite binary string to handle continuous data such as reals.

Cantor space $\mathcal{C}$ is set of every infinite binary string. For any fixed finite binary string $w$, $w\mathcal{C}$ is the set of every infinite binary string which starts with $w$. For any $n \in \mathbb{N}$, $\bigcup_{w\in\{0,1\}^n} w\mathcal{C} = \mathcal{C}$ holds. And if $w \neq w'$ and $|w| = |w'|$, $w\mathcal{C} \cap w'\mathcal{C} = \emptyset$. So, it is very natural that we give the probability measure $\gamma$ on $\mathcal{C}$ s.t. $\gamma(w\mathcal{C}) = 1/2^{|w|}$. Such $\gamma$ is often called *Canonical probability measure.*

The type-2 Turing machine is a variant of the Turing machine which allows infinite input and output. So, unlike ordinary one, type-2 TM may not halt. The theory of computation with type-2 TM is often called TTE(Type-2 theory of Effectivity).

**Definition 1.2.1.** *1. An infinite binary string $w \in \mathcal{C}$ is computable if there exists type-2 TM which produce $w$ without any input.*

*2. An partial function $F :\subseteq \mathcal{C} \to \mathcal{C}$ is computable if there exists type-2 TM which produce $F(p)$ for every input string $p \in \mathrm{dom}(F)$.*

If we want to handle the mathematical object more than just string, we need to *represent* them by a string.

**Definition 1.2.2.** *[15, §2.3]*

1. *A* notation *of countable set $A$ is partial surjective mapping $\alpha : \{0,1\}^* \to A$.*

2. *A* representation *of set $X$ is partial surjective mapping $\delta : \mathcal{C} \to X$. For $x \in X$, $\delta^{-1}(x)$ is said to be* name *of $x$ w.r.t. $\delta$.*

**Definition 1.2.3.** *[15, §3] Let $\delta_X$ and $\delta_Y$ be representation of set $X$ and $Y$, respectively. Let $f :\subseteq X \to Y$ be partial function. $F :\subseteq \mathcal{C} \to \mathcal{C}$ is said to be $(\delta_X, \delta_Y) - realizer$ if $f \circ \delta_X = \delta_Y \circ F$.*

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle \delta_X}\uparrow & & \uparrow{\scriptstyle \delta_Y} \\ \mathcal{C} & \xrightarrow{F} & \mathcal{C} \end{array}$$

So, the realizer is string function $F$ which makes above diagram commutes. We say partial function $f :\subseteq X \to Y$ is $(\delta_X, \delta_Y) - computable$ if there exists computable $(\delta_X, \delta_Y) - realizer$. We can also apply this definition when one of $X$ or $Y$ is countable set and one of $\delta_X$ or $\delta_Y$ is notation.

Consider separable metric space $S$ with dense subset $A$. For every element $s \in S$, there exists Cauchy sequence consists of an element of $A$ which converges to $s$. And this fact yields the natural representation of metric space.

**Definition 1.2.4.** *[15, §8.1]*

1. *A tuple $(S, d, A, \alpha)$ is computable metric space if $(S, d)$ is separable metric space and $A$ is dense subset of $S$ and $\alpha$ is notation of $A$, where* $\mathrm{dom}(\alpha)$ *is computably enumerable and $d|_{A\times A}$ is $(\alpha, \alpha, \rho)$-computable.*

2. *A* Cauchy representation *$\delta$ of $S$ is defined as belows*

$$\delta(p) = s \Longleftrightarrow \exists w_1, w_2, \cdots \in \mathrm{dom}(\alpha) \text{ s.t.} \begin{cases} \alpha(w_i) = s_i \\ d(\alpha(w_i), \alpha(w_j)) < 2^i \text{ for } i < k \\ \lim_{i\to\infty} s_i = s \\ p \text{ is computable concatenation of } w_i \end{cases}$$

# Chapter 2. Probability Measure and Samplability

## 2.1 Sampling and Pushforward Measure

**Definition 2.1.1.** *Let $(X, \mathcal{A})$ and $(Y, \mathcal{B})$ be measure space with measure $\mu$ and $\nu$, and $F \subseteq: X \to Y$ be measurable partial mapping. $\nu$ is pushforward measure of $\mu$ w.r.t. $F$ if $\mu(F^{-1}[V]) = \nu(V)$ for every $v \in \mathcal{B}$. In this case, we call $F$ realizes $\nu$ on $\mu$ and write $\nu \preccurlyeq \mu$.*

Think about the case of rolling dice as in Chapter 1. Suppose that we roll 12-sided dice. This situation can be modelled as uniform probability measure $\mu$ on $\{1, 2, \cdots, 11, 12\}$. And define function $F : \{1, 2, \cdots, 11, 12\} \to \{1, 2, 3, 4, 5, 6\}$ as $F(x) = \lceil \frac{x}{2} \rceil$. Let $\nu$ be an uniform measure on $\{1, 2, 3, 4, 5, 6\}$. One can check that $F$ realizes $\nu$ on $\mu$.

Intuitionally, the above situation means that we can simulate the situation of rolling 6-sided dice using 12-sided dice and function $F$. Generally speaking, if we can simulate the random sampling from the set $X$ with $\mu$ and $\nu \preccurlyeq \mu$, we also can simulate the random sampling from $Y$ with $\nu$.

Note that realizability of measure is transitive, i.e. if $\lambda$ is realized on $\mu$ and $\mu$ is realized on $\nu$, then $\lambda$ is realized on $\nu$.

**Example 2.1.2.** *a) Let $\lambda$ be Lebesgues measure on $[0, 1]$. Then binary representation $\rho_{\mathrm{b}} := b \mapsto \sum_{i \geq 0} b_i 2^{-i-1}$ realizes $\lambda$ on* Canonical probability measure.

*b) Consider the standard Gaussian probability distribution $\mu$. $G : (0, 1) \ni t \mapsto \Phi^{-1}(t) \in \mathbb{R}$ realizes $\mu$ on $\lambda$, where $\Phi$ is cumulative distribution function of Gaussian probability measure.*

*c) Consider the Dirac delta measure $\delta_r$ for some $r \in (0, 1)$. Constant function $H : [0, 1] \mapsto \{r\}$ realizes $\delta_r$ on $\lambda$.*

*d) The Cantor measure on $[0, 1]$ is realized on $([0, 1], \lambda)$ by inverse of Cantor-Vitali function.*

The realizer of measure is commonly considered as a $(\theta_<, \rho_<)$-realizer. However, note that our notion of the realizer of measure is quite different from the traditional one.

## 2.2 Realizer of Measure on Reals

We know that a modern computer can generate a single bit with fair probability. It means we can simulate the sampling from $\mathcal{C}$ with a canonical probability measure. So, if the measure $\mu$ on set $X$ can be realized on $\gamma$, it's reasonable to say we can simulate the sampling from $X$ with $\mu$. So, the next question will be this. "Which kinds of measure can be realized on $\gamma$?".

Let's start with a simple case, $X = \mathbb{R}$. For the probability measure $\mu$ on $\mathbb{R}$, we can naturally define the cumulative distribution function $F : \mathbb{R} \to [0, 1]$ defined as $\mathbb{R} \ni s \mapsto \mu\big((-\infty, s]\big) \in [0, 1]$. This function is known to be upper semi-continuous function. But it does not need to be bijective unless it's strictly increasing. So there exist some subtle points to define its inverse.

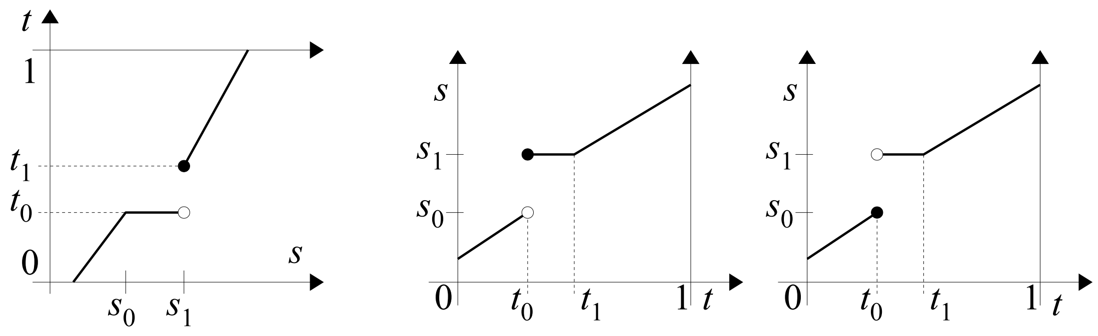


Figure 2.1: Example cumulative distribution function with upper/lower semi-inverse

Look at the leftmost graph in the above figure. If we want to define the inverse of such function, what will be the value of its inverse at $t_0$? There will be multiple inverses. And we pick 2 of them as followings.

**Definition 2.2.1.** *Let $\mu$ be Borel probability measure. The function defined below is said to be upper and lower* semi-inverse *of the cumulative distribution function of $\mu$.*

$$
\begin{aligned}
F^{\mu}_{>} : (0,1) \ni t &\mapsto \inf\left\{s \in \mathbb{R} \,\middle|\, \mu\big((-\infty, s)\big) > t\right\} = \min\left\{s \,\middle|\, \mu\big((-\infty, s]\big) > t\right\} \\
&= \sup\left\{s \in \mathbb{R} \,\middle|\, \mu\big((-\infty, s]\big) \le t\right\} \\
F^{\mu}_{<} : (0,1) \ni t &\mapsto \max\left\{s \in \mathbb{R} \,\middle|\, \mu\big((-\infty, s)\big) < t\right\} = \sup\left\{s \,\middle|\, \mu\big((-\infty, s]\big) < t\right\} \\
&= \sup\left\{s \,\middle|\, \mu\big((s, \infty)\big) > 1 - t\right\}
\end{aligned}
$$

Why do we need to define such a concept? Because it is deeply related to the realizer of measure on the real line by the following fact.

**Fact 2.2.2.** *[10, §2.5] $F^{\mu}_{>}$ and $F^{\mu}_{<}$ both realizes $\mu$ on $\lambda$, where $\lambda$ is lebesgue measure on* $[0,1]$.

## 2.3 Realizer of Measure on Topological Spaces

But what if our target space $X$ is not $\mathbb{R}$? For the topological spaces equipped with Borel $\sigma$-algebra and Borel probability measure, Simpson and Shröder establishes the following.

**Fact 2.3.1.** *[12, Proposition 13.] Let $X$ be second countable $T_0$ space with Borel probability measure $\mu$. Then there exists Borel probability measure $\bar{\gamma}$ on $\mathcal{C}$ s.t. $\mu$ has continuous partial realizer over $\gamma$.*

Note that the measure $\bar{\gamma}$ in the above theorem is not *Canonical probability measure*. However, we show that measure $\mu$ on the above theorem can be realized by canonical 'fair' one. This is our first main result.

**Theorem 2.3.2.** *Every Borel probability measure $\bar{\gamma}$ on Cantor space $\mathcal{C}$ admits a continuous partial realizer over the 'fair' measure $(\mathcal{C}, \gamma)$. The realizer is defined on $\mathcal{C}$ with the exception of at most countably many points.*

Before starting the proof, let's consider following approach. Consider Borel measure $\bar{\mu}$ on $\mathbb{R}$ and realizer $F : (\mathbb{R}, \bar{\mu}) \to (\mathcal{C}, \bar{\gamma})$. Then by Fact 2.2.2, $\bar{\mu}$ can be realized on $\lambda$. By inverse of $\rho_{\mathrm{b}}$, $\lambda$ can be realized on $\gamma$. So, $\bar{\gamma}$ can be realized on $\gamma$. However, construction of such realizer $F$ is not an easy problem. Instead, we use more direct approach to construct realizer.

*Proof.* For each open interval $I = (a, b) \subseteq [0, 1]$ consider the set $\mathcal{C}_I = \rho_{\mathrm{b}}^{-1}[I] \subseteq \mathcal{C}$ of measure $\gamma(\mathcal{C}_I) = \lambda(I)$. Note that $\mathcal{C}_{I\cup J} = \mathcal{C}_I \cup \mathcal{C}_J$ and $\mathcal{C}_{I\cap J} = \mathcal{C}_I \cap \mathcal{C}_J$. Fix $n \in \mathbb{N}$ and equip $\{0, 1\}^n$ with the total lexicographical order; and consider the disjoint open intervals

$$I_{\vec{0}} = \big(0, \bar{\gamma}(\vec{0} \circ \mathcal{C})\big) \quad \text{as well as} \quad I_{\vec{w}} = \Big(\sum\nolimits_{\vec{v}<\vec{w}} \bar{\gamma}(\vec{v} \circ \mathcal{C}), \sum\nolimits_{\vec{v}\leq\vec{w}} \bar{\gamma}(\vec{v} \circ \mathcal{C})\Big)$$

of lengths $\lambda(I_{\vec{w}}) = \bar{\gamma}(\vec{w} \circ \mathcal{C})$ for each $\vec{w} \in \{0, 1\}^n \setminus \vec{0}$. Since $\bar{\gamma}$ is a Borel probability measure on $\mathcal{C}$, these lengths add up to $\sum_{\vec{w}} \bar{\gamma}(\vec{w} \circ \mathcal{C}) = 1$. Also note that $I_{\vec{w}\,0}, I_{\vec{w}\,1} \subseteq I_{\vec{w}}$ are disjoint with lengths $\lambda(I_{\vec{w}\,0}) + \lambda(I_{\vec{w}\,1}) = \lambda(I_{\vec{w}})$; and that $I_{\vec{w}}$ may be empty in case $\bar{\gamma}(\vec{w} \circ \mathcal{C}) = 0$. Finally abbreviate

$$\mathcal{C}_{\vec{w}} := \mathcal{C}_{I_{\vec{w}}} \quad \text{and} \quad F_n :\subseteq \mathcal{C} \to \{0, 1\}^n, \quad F_n\big|_{\mathcal{C}_{\vec{w}}} :\equiv \vec{w}$$

so that $F_n$ is defined except for at finitely many arguments (namely the binary encodings of the real interval endpoints) with $F_n^{-1}(\vec{w}) = \mathcal{C}_{\vec{w}}$ of measure $\gamma\big(F_n^{-1}(\vec{w})\big) = \bar{\gamma}\big(\mathcal{C}_{\vec{w}}\big)$. Since $F_{n+1}(\bar{u}) \in F_n(\bar{u}) \circ \{0, 1\}$, $F(\bar{u}) := \lim_n F_n(\bar{u}) \in \mathcal{C}$ is well-defined (except for at countably many arguments) and continuous with $F^{-1}[\vec{w}\,\mathcal{C}] = \mathcal{C}_{\vec{w}}$ for every $\vec{w} \in \{0, 1\}^*$. Hence $\gamma \circ F^{-1}$ coincides with $\bar{\gamma}$ on the basic clopen subsets of $\mathcal{C}$ and, being Borel measures, also on all Borel subsets. □

Fact 2.3.1 said that arbitrary Borel probability measure $\mu$ is realized on $\bar{\gamma}$, and theorem 2.3.2 said that $\bar{\gamma}$ can be realized on $\gamma$. By transitivity of realizer, $\mu$ can be realized on $\gamma$.

**Corollary 2.3.2.1.** *Let $X$ be second countable $T_0$ space with Borel probability measure $\mu$. Then $\mu$ has continuous partial realizer over $\gamma$ defined everywhere except countably many points.*

This is more powerful result than Lemma 2.2.2.

## 2.4 Samplability via Realizer

Now we know that some kinds of measure always can be realized on $\gamma$. But to simulate the random sampling, we need one more thing. The computability of such realizer. With computability notion, we can finally define the samplability of some measure.

**Definition 2.4.1.** *Fix a Borel probability measure $\mu$ on $X$ and a representation $\xi :\subseteq \mathcal{C} \twoheadrightarrow X$. A $\xi$-*realizer *of $\mu$ is a mapping $G :\subseteq \mathcal{C} \to \mathrm{dom}(\xi)$ such that $\xi \circ G :\subseteq \mathcal{C} \to X$ is a realizer of $\mu$ (over the 'fair' measure) in the above sense. Call $\mu$ $\xi$-*samplable *if it has a computable $\xi$-realizer.*

Note that the realizer we defined above is different from the traditional meaning of the realizer of measure. (The realizer of measure as the function from $\sigma$-algebra to reals.) Here are some examples and properties of samplable measures.

**Example 2.4.2.** *a) Lebesgue measure on $[0, 1]$ is $I$-samplable. Where $I$ is identity function.*

*b) If $\mu$ is $\xi$-samplable and if $\xi \preccurlyeq \xi'$ holds, then $\mu$ is also $\xi'$-samplable.*

*c) In particular the Lebesgues measure on $[0, 1]$ is $\rho$-samplable for the admissible representation $\rho$* [15, Theorem 4.1.13.7].

*d) The Dirac distribution $\delta_r$ is $\rho$-samplable iff $r$ is $\rho$-computable.*

According to Theorem 2.2.2, semi-inverse of cumulative distribution function realizes the corresponding probability measure on Lebesgue measure. Now, we can move on to the next phase.

**Lemma 2.4.3.** *Fix a Borel probability measure $\mu$ on $\mathbb{R}$ with cumulative distribution function $F$ and lower and upper semi-inverse $F^{\mu}_{<}$ and $F^{\mu}_{>}$. Then $\mu$ is $\rho_{<}$-samplable (resp, $\rho_{>}$-samplable) if $F^{\mu}_{<}$ is $(\rho_b, \rho_<)$-computable(resp, $F^{\mu}_{>}$ is $(\rho_b, \rho_>)$-computable).*

*Proof.*

$$\begin{array}{ccc} dom(\rho_<) & \xrightarrow{\rho_<} & (\mathbb{R}, \mu) \\ {\scriptstyle G}\uparrow & & \uparrow{\scriptstyle F^{\mu}_{<}} \\ \mathcal{C} & \xrightarrow{\rho_b} & (0, 1) \end{array}$$

If $F^{\mu}_{<}$ is $(\rho_b, \rho_<)$-computable, then there exists computable function $G$ which makes above diagram commutes. It means $\rho_< \circ G = F^{\mu}_{<} \circ \rho_b$. Because $\rho_{\mathrm{b}}$ realizes $\lambda$ on $\gamma$ and $F^{\mu}_{<}$ realizes $\mu$ on $\lambda$, by transitivity of realizer, $F^{\mu}_{<} \circ \rho_b$ realizes $\mu$ over $\gamma$. It means $\rho_< \circ G$ realizes $\mu$ over $\gamma$. So, $G$ is computable realizer of $\mu$ and then $\mu$ is samplable. □

# Chapter 3. Convergence and Computability of Random Variable

## 3.1 Classic Definition of Convergence of Random Variable

Let $(S, d)$ be metric space and $\Omega$ be measure space with Borel probability measure $\mathcal{P}$. Let $X : \Omega \to S$ be a random variable. The following is a classic definition of almost sure convergence of random variable.

**Definition 3.1.1.** *The sequence of random variable $X_n$ converges to $X$ almost surely if*

$$\exists A \subseteq \Omega, \forall \omega \in A, \forall m \in \mathbb{N}, \exists N \in \mathbb{N}, (n \geq N \implies (X_n(w), X(w)) < 2^{-m}) \ \& \ \mathcal{P}(A) = 1$$

However, in the above definition, one can check that $N$ depends on each single element $\omega$ in $A$. In some sense, we can say that it's not uniform convergence. The definition below is the uniform version of almost sure convergence.

**Definition 3.1.2.** *The sequence of random variable $X_n$ converges to $X$* uniformly almost surely *if*

$$\exists A \subseteq \Omega, \forall m \in \mathbb{N}, \exists N \in \mathbb{N}, \forall w \in A, (n \geq N \implies d(X_n(w), X(w)) < 2^{-m}) \ \& \ \mathcal{P}(A) = 1$$

In this definition, $N$ only depends on $m$. We can define the function which maps $m$ to the smallest such $N$. It's called *modulus of uniform almost sure convergence.*

## 3.2 Computability of Random Variable and Convergence

Bosselhoff presents various kinds of notions about probabilistic computability in his paper[4]. In this section, we'll show the relationship between such a concept of computability and convergence.

Let $(S, d, \alpha)$ be computable metric space with Cauchy representation $\delta_S$. Let $\Omega$ be measure space equipped with probability measure $\mathcal{P}$ and representation $\delta$.

**Definition 3.2.1.** *[4] The random variable $X : \Omega \to S$ is almost surely computable if*

$$\exists A \subseteq \Omega, \mathcal{P}(A) = 1 \ \& \ X|_A \text{ is } (\delta|^{\alpha}, \delta_S)\text{-computable.}$$

And we prove that this concept is deeply related to uniform almost sure convergence explained above.

**Theorem 3.2.2.** *The followings are equivalent*

1. *The random variable $X : \Omega \to S$ is almost surely computable.*
2. *There exists the computable sequence of almost surely computable random variable $X_i : \Omega \to S$ s.t. $X_i$ uniformly almost surely converges to $X$ with computable modulus of convergence.*

*Proof.* ($1 \implies 2$) Define sequence $(X_i)$ as $X_i = X$ for every $i \in \mathbb{N}$. Then it trivially holds.
($2 \implies 1$) Let $A_i$ be measure 1 set which makes $X_i$ be computable, and $A'$ be measure 1 set which makes $X_i$ be uniformly almost surely converges to $X$. Let $A = (\cap_{i=1}^{\infty} A_i) \cap A'$. Then $X_i$ is computable on $A$, and $X_i$ converges to $X$ on $A$.

However, $A$ is also measure 1 set. For all $i \in \mathbb{N}$, $\mathcal{P}(\overline{A_i}) = 0$ and $\mathcal{P}(\overline{A'}) = 0$. By countable subadditivity of measure, $\mathcal{P}(\cup \overline{A_i} \cup \overline{A'}) \leq \sum \mathcal{P}(\overline{A_i}) + \mathcal{P}(\overline{A'}) = 0$. So $\mathcal{P}(\cup \overline{A_i} \cup \overline{A'}) = \mathcal{P}(\overline{A}) = 0$ and $\mathcal{P}(A) = 1$.

Now we'll show that if a computable sequence of computable function $Y_i : A \to S$ uniformly converges to $Y$ with a computable modulus of convergence, then $Y$ is also computable. Note that this implies our original claim.

Let $\mu$ be modulus of convergence. For any $x \in A$ and $n \in \mathbb{N}$, because $\{Y_i\}$ is computable sequence, we can compute $Y_{\mu(n)}$. By definition of modulus of convergence, $\sup_{t \in A} d(Y_{\mu(n)}(t), Y(t)) < 2^{-n}$. So, $d(Y_{\mu(n)}(x), Y(x)) < 2^{-n}$. It means we can construct the computable Cauchy sequence which converges to $Y(x)$, i.e. we can compute the $\delta_s$-name of $Y(x)$. For any $x$, it's possible to construct such sequence, and it's the algorithm which computes the function $Y$ with respect to $\delta$ and $\delta_S$. □

## 3.3 Computability of Random Variable and Samplability

Let's recall the definition of the realizer of measure. Because it is measurable mapping, we can view realizer as a random variable and realized measure as an induced measure. Also, we can define the samplability of the random variable itself instead of measure.

**Definition 3.3.1.** *Let $X$ be random variable with support set $S$ and $\mu$ is measure on $S$ induced by $X$. If $\mu$ is samplable, we call $X$ is samplable.*

Think about Random Variable whose sample space is Cantor space. One can check that such Random Variable is exactly the realizer of measure induced by itself. Then the following very naturally holds.

**Lemma 3.3.2.** *Let $X$ be random variable whose sample space is $\mathcal{C}$. Then $X$ is samplable iff $X$ is almost surely computable.*

# Chapter 4. Samplability of Brownian motion

1-dimensional *Brownian Motion*, or *Wiener Process*, or *Wiener measure* is a probability measure on the space $X := \mathcal{C}[0,1]$ of continuous functions $W : [0,1] \to \mathbb{R}$, which satisfies followings.

i) $W(0) = 0$ almost surely.

ii) For every $0 \le r < s < t \le 1, W(t) - W(s)$ is independent of $W(r)$.

iii) $W(t) - W(s)$ is Gaussian normally distributed with mean 0 and variance $|t - s|$.

Our question is, whether this probability measure is $[\rho \to \rho]$-samplable in the sense of Definition 2.4.1. As in [15, §6.1], the $[\rho \to \rho]$-name of function $f \in \mathcal{C}[0,1]$ contains two kinds of information, (I) its values $f(a/2^n)$ on dyadic rationals and (II) a binary modulus of continuity *moc* of $f$.

## 4.1 Algorithm to Sample the Brownian motion

**Definition 4.1.1.** *For a uniform continuous function $f : (A,d) \to (B,e)$, where $(A,d)$ and $(B,e)$ are both metric space, a binary modulus of continuity* moc $: \mathbb{N} \to \mathbb{N}$ *of $f$ is a function which satisfies the followings.*

$$d(x,y) < 2^{-moc(n)} \implies e(f(x), f(y)) < 2^{-n}$$

*Similarly, modulus of continuity $\omega : \mathbb{R}_{\ge 0} \to \mathbb{R}_{\ge 0}$ is a function which satisfies the followings.*

$$e(f(x), f(y)) \le \omega(d(x,y))$$

Note that a function has a (computable) modulus of continuity iff it has (computable) binary modulus of continuity.

**Remark 4.1.2.** *a) The standard Gaussian cumulative distribution function is increasing, so its inverse is well defined. And also, it's $(\rho,\rho)$-computable. By lemma 2.4.3, Gaussian measure is $\rho$-samplable.*

*b) Combining property i) and iii) of Brownian motion, we can sample the value of the function $W \in \mathcal{C}[0,1]$ on every dyadic rational. However, by this method, we cannot determine* moc *with finite time. For any modulus of continuity function, there must be a small but positive probability that the value of $W$ on non-dyadic number violates the* moc*. See figure 4.1.*

*c) Conversely, guessing modulus of continuity $\omega$ at first. If we fix the $\omega$, we can distinguish whether the sampled value violates it or not. If the sampled value violates, drop it and sample the value again until sampled value doesn't violate sampled modulus. See figure 4.2.*

Algorithm 1 and 2 show the pseudo-code of the above algorithm. Because it's algorithm on the type-2 machine, it includes infinite loops. Algorithm 2 includes undecidable real inequality. However, we don't need to care about it. Because it fails only when $rdif = \omega(1/2^n)$ or $ldif = \omega(1/2^n)$. But for fixed $\omega$, such events occurs with probability 0. So we can sample Brownian motion with probability 1 with this algorithm.

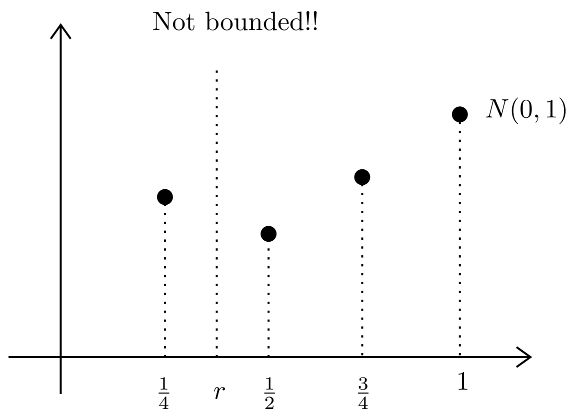


Figure 4.1: Unbounded value of function on non-dyadic point

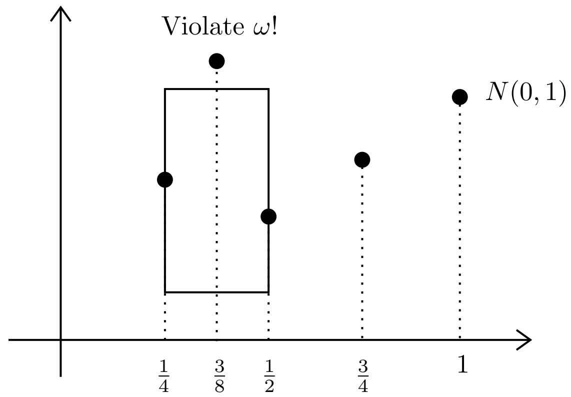


Figure 4.2: Bound of valid sampled value with $\omega$

**Algorithm 1** Sample the Brownian motion

Sample the modulus of continuity $\omega$
$n \leftarrow 0$
Set $W(0)$ as 0
**loop**
    $k \leftarrow 1$
    **while** $k < 2^n$ **do**
        $x \leftarrow GAUSSIAN(0, k/2^n)$
        **while** $VIOLATE(\omega, x, n, k, W)$ **do**
            $x \leftarrow GAUSSIAN(0, k/2^n)$
        **end while**
        Set $W(k/2^n)$ as $x$
        $k \leftarrow k + 2$
    **end while**
    $n \leftarrow n + 1$
**end loop**

**Algorithm 2** Check Whether sampled value violates moc

```
procedure VIOLATE(ω, x, n, k, W)
    ldif ← |W((k − 1)/2^n) − W(k/2^n)|
    rdif ← |W((k + 1)/2^n) − W(k/2^n)|
    if ldif > ω(1/2^n) or rdif > ω(1/2^n) then
        return True
    else
        return False
    end if
end procedure
```

## 4.2 Parameterized Modulus of Continuity

Algorithm 1 and 2 imply that the distribution of modulus of continuity of Brownian motion takes an important role. Indeed, there are some known results about its distribution.

**Fact 4.2.1** (Lévy's modulus of Continuity theorem). *With probability 1, following holds.*

$$\lim_{h\to 0} \sup_{|s-t|\le h} \frac{|W(s)-W(t)|}{\sqrt{2h\ln 1/h}} = 1$$

*In other words, the sample paths of Brownian Motion have modulus of continuity*

$$\omega(h) = \sqrt{2h\ln 1/h}$$

*for small $h > 0$.*

From above fact, following can be derived.

**Lemma 4.2.2.** *For every $W \in \mathcal{C}[0,1]$ (except for a subset of measure 0), there exists smallest $c \ge 1$ which makes*

$$\omega(h,c) := \begin{cases} \sqrt{2ch\ln(1/h)} & : h \le 1/ec \\ \sqrt{2\ln ec/e} + (h - 1/ec)\cdot c \cdot \ln(c)/\sqrt{2\ln ec/e} & : h \ge 1/ec \end{cases} \tag{4.1}$$

*be modulus of continuity of $W$. We denote such function $\omega$* parameterized modulus of continuity*.*

*Proof.* Fix $C > 1$. By Fact 4.2.1 it holds $\lim_{h\to 0}\sup_{|s-t|\le h} \frac{|W(s)-W(t)|}{\sqrt{2Ch\ln 1/h}} < 1$. Therefore there exists a $c = c(C) < \infty$ such that every $h \le 1/ce$ satisfies $\sup_{|s-t|\le h} \frac{|W(s)-W(t)|}{\sqrt{2Ch\ln 1/h}} < 1$, that is,

$$|s-t| \le h \quad\Rightarrow\quad |W(s)-W(t)| \;\le\; \sqrt{2Ch\ln 1/h}\ .$$

Without loss of generality $h = 1/ec$, $c = c(C)$ is increasing, and $c \ge C$: settling the first case of Equation (4.1).

Now we want to extend this result. If $\omega$ is continuous convex function, then $\omega$ satisfies subadditivity, i.e. $\forall s,t\ \omega(s+t) < \omega(s)+\omega(t)$. And if $\omega$ has subadditivity, we can easily construct the bound of value on larger domain. To make $\omega$ be convex, we choose to use linear function after the point $1/ec$. Let $\omega_c$ be function $\omega(\cdot,c)$. Then $\omega_c$ for $h \ge 1/ec$ can be extended by followings.

$$\begin{aligned}\omega_c(h) &= \omega_c\left(\frac{1}{ec}\right) + \frac{d\omega_c}{dh}\left(\frac{1}{ec}\right)\cdot\left(h - \frac{1}{ec}\right) \\ &= \sqrt{\frac{2\ln ec}{e}} + \left(h - \frac{1}{ec}\right)\cdot\frac{c\cdot\ln ec - 1}{\sqrt{\frac{2\ln ec}{e}}}\end{aligned}$$

□

Note that $c$ is determined by $W$, and $W$ is determined by an element of sample space. So $c$ is determined by an element of sample space, i.e. $c$ is the random variable. We can now state our second main result, which characterizes the samplability of the Wiener Process by the probability distribution of parameterized modulus of continuity.

**Theorem 4.2.3.** *The following are equivalent:*

- *The Wiener Process $W$ is $[\rho \to \rho]$ - samplable*
- *The random variable $c$ in Lemma 4.2.2 is samplable.*

*Proof.* As in algorithm 1, 2 and lemma 4.1, it is clear that if random variable $c$ is samplable, then modulus of continuity is also samplable and Wiener process is also samplable.

Conversely, suppose that Wiener Process $W$ is $[\rho \to \rho]$ - samplable with realizer $F : \mathcal{C} \to \mathrm{dom}([\rho \to \rho])$. Then, we can view $c$ as random variable whose sample space is also $\mathcal{C}$. By lemma 3.3.2, it's enough to show that $c$ is almost surely computable. Fix $C$ and $\bar{\mu} \in dom([\rho \to \rho])$ and let $W$ be $[\rho \to \rho](\bar{\mu})$. Because $\omega$ is computable, following mappings are also computable.

$$(C, W) \mapsto \Psi(C, W) := \max_{0 \le s,t \le 1} \omega(|s-t|, C) - |W(s) - W(t)|$$

One can check that $\Psi$ is continuous and strictly increasing to $C$ and unbounded. By definition, $c(W) = \min\{C : \Psi(C, W) \ge 0\} = \max\{C : \Psi(C, W) \le 0\}$. This mapping is defined for almost every $W$ since $\Psi$ is strictly increasing and continuous. We also can check that $c$ is upper and lower computable on its domain. So $c$ is almost surely computable. □

## 4.3 Sequence Converging to Brownian motion

There are various kinds of sequence or series which is known to be converging to Brownian motion. In section 3.3, we show that the almost sure computability of the random variable implies its samplability. And uniform almost sure convergence of computable sequence implies almost sure computability of its limit. So, it seems that we can use those mathematical facts to build the algorithm to sample the Brownian motion. Actually, some of them are very useful to informally simulate the Brownian motion. However, in this section, we will show why those convergence doesn't imply the samplability of Brownian motion at all.

The first and most famous example is called *Donsker's theorem.*

**Fact 4.3.1** (Donsker's theorem)**.** *Let $(X_i)$ be sequence of i.i.d random variable with mean 0 and variance 1. Let $S_n = \sum_{i=1}^{n} X_i$. Then, following sequence converges to Brownian motion in distribution.*

$$W^n := t \mapsto \frac{S_{\lfloor nt \rfloor}}{\sqrt{n}}$$

Although this is easy to compute and widely used in the informal simulation of Brownian motion, it doesn't give any hint about the formal samplability of Brownian motion. Because this convergence is *convergence in distribution.* It is a much weaker condition than uniform almost convergence we need. So it doesn't imply and also gives no hint about samplability.

Here's another example called levy's representation.

**Definition 4.3.2** (Schauder's hat function)**.** *Let* $\varphi_0(t) = t$ *and*

$$\varphi_{n,j}(t) = \begin{cases} 2^{(n-1)/2} \cdot (t - \frac{k-1}{2^n}) & \frac{k-1}{2^n} \le t \le \frac{k}{2^n} \\ 2^{(n-1)/2} \cdot (\frac{k+1}{2^n} - t) & \frac{k}{2^n} \le t \le \frac{k+1}{2^n} \\ 0 & \text{otherwise} \end{cases}, \qquad 0 \le k < 2j, \quad 1 \le j \le 2^{n-1}$$

$\varphi_{n,j}$ *is called* ***Schauder function*** *or* ***Schauder's hat function****.*

**Fact 4.3.3.** *[7, Thm 3.2] Let* $R_{n,j}$ *be independent standard normally distributed random variables. Then following sequence converges to the Wiener Process almost surely:*

$$W^N(t) = R_0 \cdot t + \sum_{n=1}^{N} \sum_{j=1}^{2^{n-1}} R_{n,j}\varphi_{n,j}(t) \tag{4.2}$$

However, this doesn't imply the computability of Brownian motion even though $W^N$ is the computable random variable for every $N \in \mathbb{N}$ and its convergence is *almost sure convergence*. Indeed, we can show that this convergence doesn't have the computable global modulus of convergence. The main reason is that this convergence is not uniform.

**Theorem 4.3.4.** *There is no function* $\mu : \mathbb{N} \to \mathbb{N}$ *which satisfies*

$$m > \mu(n) \implies \mathcal{P}(d(W^m, W) < 2^{-n}) = 1$$

*Proof.* Assume that there exists such function $\mu$. Fix $n \in \mathbb{N}$ and let $m = \mu(n)$. Then $\sup_{t\in[0,1]} |W^m(t) - W(t)| < 2^{-n}$. However, for some $k > m$, it's possible with positive probability that $R_{k,j}$ is arbitrarily big so that $|W_k(t) - W(t)| > 2^{-n}$ for some $t \in [0, 1]$. Because $R_{k,j}$ is gaussian random variable and not almost surely bounded. It's contradiction because $k > m$ implies that $\sup_{t\in[0,1]} |W^k(t) - W(t)| < 2^{-n}$. So, there's no such function $\mu$. □

With a similar argument, we can also prove that sequence in *Donsker's theorem* also doesn't have a global modulus of convergence.

Here's the little bit different example. Let's consider the Kolmós-Major-Tusnády approximation theorem. It says that the supremum norm between empirical process and Brownian bridges is bounded with given probability bound.

**Theorem 4.3.5.** *[8, Thm 4] Let* $X_1, X_2, \cdots$ *be a sequence of i.i.d. random variables with distribution*

$$P(X_n < t) = \begin{cases} 0 & \text{if } t < 0 \\ t & \text{if } 0 \le t \le 1 \\ 1 & \text{if } t > 1 \end{cases}$$

*Let* $F_n(t)$ *be empirical distribution function based on the sample* $X_1, X_2, \cdots, X_n$ *and let* $B_1(t), B_2(t), \cdots$ *be sequence of independent Brownian bridges. There is a version of the sequences* $F_n(t), B_n(t)$ *such that*

$$\mathcal{P}\left( \sup_{1\le k\le n} \sup_{0\le t\le 1} \left| k(F_k(t) - t) - \sum_{j=1}^{k} B_j(t) \right| > C(\log n + x)\log n \right) < ke^{-\lambda x}$$

*for all* $x$ *and* $n$*, where* $C, K, \lambda$ *are positive absolute constants.*

However, this theorem also said that there always be positive probability that finite approximation has unbounded error. It means that we cannot compute the Brownian motion with probability 1 using this approximation.

# Chapter 5. Conclusion and Future Work

In this paper, we suggest the new concept related to probabilistic computation called *samplability.* But we don't know the relationship between samplability of measure $\mu$, and traditional computability of $\mu$. It seems that sampling is much more difficult than just computing measures as a function. But we cannot find any evidence supporting it yet.

Also, we figure out the relationship between almost sure computability and almost sure convergence. However, the random variable has two more types of convergence concept, called convergence in probability and convergence in distribution. [4] proposes a computability concept called computable approximation and computability in mean. This concept is supposed to be related to the corresponding convergence concept, but not covered in this paper.

In lemma 4.2.2, we show that random variable $c$ do a key role in the sampling of the Brownian motion. However, the problem of whether $c$ is the computable random variable remains open. It means that even though we make a significant step, but still cannot figure out the samplability of Brownian motion.

# Bibliography


[1] René Beier and Berthold Vöcking. Random knapsack in expected polynomial time. *Journal of Computer and System Sciences*, 69(3):306–329, 2004.

[2] Ilia Binder and Mark Braverman. The rate of convergence of the walk on spheres algorithm. *Geometric and Functional Analysis*, 22(3):558–587, 2012.

[3] Errett Bishop and Henry Cheng. *Constructive measure theory*, volume 116. American Mathematical Soc., 1972.

[4] Volker Bosserhoff. Notions of probabilistic computability on represented spaces. *Electronic Notes in Theoretical Computer Science*, 202:137–170, 2008.

[5] Russel E Caflisch. Monte carlo and quasi-monte carlo methods. *Acta numerica*, 7:1–49, 1998.

[6] Willem L Fouché, Hyunwoo Lee, Donghyun Lim, Sewon Park, Matthias Schröder, and Martin Ziegler. Randomized computation of continuous data: Is brownian motion strongly computable? *CCC 2019: Computability, Continuity, Constructivity-from Logic to Algorithms*, page 18.

[7] Ioannis Karatzas and Steven E Shreve. Brownian motion. In *Brownian Motion and Stochastic Calculus*, pages 47–127. Springer, 1998.

[8] János Komlós, Péter Major, and Gábor Tusnády. An approximation of partial sums of independent rv'-s, and the sample df. i. *Zeitschrift für Wahrscheinlichkeitstheorie und verwandte Gebiete*, 32(1-2):111–131, 1975.

[9] Norbert Th Müller. Computability on random variables. *Theoretical Computer Science*, 219(1-2):287–299, 1999.

[10] Sidney I Resnick. *A probability path.* Springer, 2003.

[11] Matthias Schröder. Admissible representations for probability measures. *Mathematical Logic Quarterly*, 53(4-5):431–445, 2007.

[12] Matthias Schröder and Alex Simpson. Representing probability measures using probabilistic processes. *Journal of Complexity*, 22(6):768–782, 2006.

[13] Alastair J Walker. An efficient method for generating discrete random variables with general distributions. *ACM Transactions on Mathematical Software (TOMS)*, 3(3):253–256, 1977.

[14] Klaus Weihrauch. Computability on the probability measures on the borel sets of the unit interval. *Theoretical Computer Science*, 219(1-2):421–437, 1999.

[15] Klaus Weihrauch. *Computable Analysis.* Springer, Berlin, 2000.

# Acknowledgments in Korean

졸업을 앞두고 지난 석사과정을 돌이켜보면, 수많은 분의 얼굴이 눈앞에 떠오릅니다. 이 자리를 빌려 저는 그동안 이 학위논문을 완성하는 데 있어 많이 부족한 저에게 물심양면으로 도움을 주셨던 분들에게 감사 인사를 전하려 합니다.

먼저 2년간의 석사과정 동안 연구만이 아닌 외적인 부분 역시 큰 힘이 되어주시고 지지를 아끼지 않아 주셨던 마틴 지글러 교수님, 그리고 지도교수님만큼 저에게 많은 걸 가르쳐주신 박세원 씨에게 감사의 말씀을 드리고 싶습니다. 그리고 같은 연구실에서 마치 자기 일처럼 열정적으로 도움을 주신 임동현, 선동성, 박찬수, 황지만, 신승우 씨 그리고 Svetlana 박사님께도 진심으로 감사의 말씀을 전합니다. 또한, 석사과정에 함께 입학하여 많은 추억을 나눈 김영훈 학우님과 언제나 즐거운 토론을 함께 할 수 있었던 임성혁 학우님께도 정말 감사드립니다.

마지막으로 부족한 자식을 끝까지 믿어주시고 지지해주신 부모님 두 분께 감사의 말씀을 드립니다.