論文 / 著書情報
Article / Book Information

題目(和文)	計算理論と抽象代数
Title(English)	Computation Theory and Abstract Algebra
著者(和文)	湯山孝雄
Author(English)	Takao Yuyama
出典(和文)	学位:博士(理学), 学位授与機関:東京工業大学, 報告番号:甲第12303号, 授与年月日:2023年3月26日, 学位の種別:課程博士, 審査員:加藤 文元,田口 雄一郎,内藤 聡,落合 理,鈴木 正俊,鹿島 亮
Citation(English)	Degree:Doctor (Science), Conferring organization: Tokyo Institute of Technology, Report number:甲第12303号, Conferred date:2023/3/26, Degree Type:Course doctor, Examiner:,,,,,
学位種別(和文)	博士論文
Type(English)	Doctoral Thesis

Computation Theory and Abstract Algebra

by

Takao Yuyama

A Doctorial Thesis,

Submitted to the Department of Mathematics,
Tokyo Institute of Technology

December 2022

Contents

Abstract

We study several relations between computation theory and abstract algebra. The thesis comprises three chapters.

Chapter 1 is about semantics of simply-typed lambda calculus. The simple type assignment system $\lambda\!\!\rightarrow$ consists of the three rules (Id), ($\rightarrow$ I), and ($\rightarrow$ E), which lacks the rule (EQ_β). Barendregt provided a sound, but not complete, semantics for $\lambda\!\!\rightarrow$. We introduce two new semantics: term-space semantics and proper term-space semantics. We show that $\lambda\!\!\rightarrow$ is complete but not sound with respect to term-space semantics and is complete and sound with respect to proper term-space semantics. We further consider two other semantics: saturated term-space semantics and weakly saturated term-space semantics, and provide an example that illustrates the difficulty of proving the completeness of $\lambda\!\!\rightarrow$ with respect to (weakly) saturated term-space semantics.

Chapter 2 is about Hilbert's tenth problem (HTP) over subrings of the rational numbers $\mathbb{Q}$. HTP is a decision problem as to whether a given multivariate polynomial equation $f = 0$ with integer coefficients has a solution in the ring of integers $\mathbb{Z}$. In 1970, Matiyasevich proved the undecidability of HTP. Contrastingly, the undecidability of HTP over $\mathbb{Q}$ is still open. Miller proved that, for a generic subring R of $\mathbb{Q}$, the Turing degree of HTP over R determines that of HTP over $\mathbb{Q}$. We show that, conversely, the Turing degree of HTP over R for a generic subring R of $\mathbb{Q}$ almost determines that of HTP over $\mathbb{Q}$. Moreover, we characterize the undecidability of HTP over $\mathbb{Q}$ via Banach–Mazur game, which is an infinite game played by two players. In addition, we collect some consequences of the assumption that $\mathbb{Z}$ is Diophantine in $\mathbb{Q}$.

Chapter 3 is about word problems for finitely generated groups and G-automata. For a group G, a G-automaton is a finite automaton augmented with a register that contains an element of G. Such an automaton can update

the register content by multiplying an element of G and accepts an input word if it can reach a final state and the register content is the identity element of G when the entire input word is read. The word problem of a finitely generated group H is the set of words, over some fixed generating set of H, that represents the identity element of H. Elder, Kambites, and Ostheimer showed that if a finitely generated group H has a word problem accepted by a $\mathbb{Z}^n$-automaton, then H is virtually free abelian of rank at most n. However, their proof is somewhat indirect because it depends on Gromov's polynomial growth theorem. We give a new, elementary, and purely combinatorial proof to the theorem.

Acknowledgments

Firstly I gratefully acknowledge my supervisor Prof. Fumiharu Kato, who has constantly supported me and has given me many helpful comments.

I would like to acknowledge my co-researchers Ryo Kashima and Naosuke Matsuda for introducing me to problems about simply-typed lambda calculus and for fruitful discussions of the problems.

Thanks to Ryoma Sin'ya for exciting discussions of automata theory and for advice on writing papers.

Thanks to the staff and my friends at the Tokyo Institute of Technology.

Chapter 1

Term-Space Semantics and Typed Lambda Calculus

Barendregt [Bar92] gave a sound semantics of the simple type assignment system $\lambda\!\!\rightarrow$ by generalizing Tait's proof of the strong normalization theorem. In this chapter, we aim to extend the semantics so that the completeness theorem holds. This chapter is based on the author's joint paper [KMY20] with Kashima and Matsuda.

Introduction

Background

Curry [CF58] provided the type assignment system $\lambda\!\!\rightarrow$[1] which consists of the rules (Id), ($\rightarrow$ I), and ($\rightarrow$ E) in Figure 1.1. This system has long been studied as the most fundamental type assignment system. However, $\lambda\!\!\rightarrow$ lacks an important property, called the *(beta-)equality-invariance property*. That is, $\Gamma \vdash_{\lambda\!\!\rightarrow} M : \alpha$ and $M =_\beta N$ do not always imply $\Gamma \vdash_{\lambda\!\!\rightarrow} N : \alpha$. For example, $\vdash_{\lambda\!\!\rightarrow} \lambda x.x : p \rightarrow p$ and $\lambda x.x =_\beta (\lambda yx.x)(\lambda x.xx)$ but $\not\vdash_{\lambda\!\!\rightarrow} (\lambda yx.x)(\lambda x.xx) : p \rightarrow p$.

Hindley [Hin97, p. 52] discussed the lack as follows:[2]

> As noted in 2C3 this lack of equality-invariance has not hindered

[1] In [CF58], the system is called $\mathfrak{F}_1(\lambda)^\intercal$. The name $\lambda\!\!\rightarrow$ is according to Barendregt [Bar92].

[2] In Hindley [Hin83], the system $\lambda\!\!\rightarrow$ is called TA_λ.

$$\frac{}{\{x:\alpha\}\cup\Gamma\vdash x:\alpha}\ (\mathrm{Id}) \qquad \frac{\Gamma\vdash M:\alpha \quad M=_\beta N}{\Gamma\vdash N:\alpha}\ (\mathrm{EQ}_\beta)$$

$$\frac{\Gamma\vdash M:\beta}{\Gamma\setminus\{x:\alpha\}\vdash\lambda x.M:\alpha\to\beta}\ (\to \mathrm{I}) \qquad \frac{\Gamma\vdash M:\alpha\to\beta \quad \Gamma\vdash N:\alpha}{\Gamma\vdash MN:\beta}\ (\to \mathrm{E})$$

Figure 1.1: Typing rules

> TA_λ from a practical point of view, nor its descendant ML, as the main need in both systems has been simply for the subject-reduction theorem. However, on the theoretical side, equality-invariance of Types(M) seems a desirable property from the viewpoint of any of the standard λ-calculus semantics (except possibly an operational semantics): if we believe terms represent functions of some sort and equal terms represent the same function, then equal terms should have the same types.

As discussed above, we can provide a natural semantics of the system $\lambda\to+(\mathrm{EQ}_\beta)$ with lambda models (see Barendregt, Coppo, and Dezani-Ciancaglini [BCDC83], Hindley [Hin83]). Contrastingly, there are few semantical studies on $\lambda\to$. A rare example was provided by Barendregt [Bar92].[3] He provided a sound (but not complete) semantics of $\lambda\to$ by generalizing the strong normalization proof of Tait [Tai67]. Roughly speaking, in Barendregt's semantics, each type α is interpreted as the set $[\![\alpha]\!]$ of lambda terms defined as follows:

$$[\![p]\!] = \{\, M \mid M \text{ is a strongly normalizing term} \,\},$$
$$[\![\alpha\to\beta]\!] = \{\, M \mid MN\in[\![\beta]\!] \text{ for each } N\in[\![\alpha]\!] \,\}.$$

And each statement $M:\alpha$ is interpreted as $M\in[\![\alpha]\!]$.

In the same way, Ghilezan [Ghi96] provided sound semantics of the intersection type assignment system $\mathcal{D}_\leq$.

Overview

This study aims to extend Barendregt's semantics so that the completeness theorem holds. In Section 1.1, we introduce some basic concepts used in this

[3] Plotkin [Plo94] provided another semantics of $\lambda\to$.

chapter, in addition to introducing Barendregt's semantics. In Section 1.2, we provide a naive extension of Barendregt's semantics. Roughly speaking, our semantics, which we call *term-space semantics*, is obtained from Barendregt's by modifying the interpretation of type to be more flexible.[4] We show that $\lambda\!\!\rightarrow$ is complete but not sound with respect to term-space semantics. In Section 1.3, we provide new semantics by restricting term-space semantics, and demonstrate that $\lambda\!\!\rightarrow$ is sound and complete with respect to the restricted semantics. In Section 1.4, we provide some open questions.

1.1 Preliminary

1.1.1 Basic concepts

With respect to the notation and fundamental properties of lambda calculus, we refer to [Bar92] as the standard text. The following notation is according to [Bar92]: V (the set of term variables); Λ (the set of lambda terms); SN (the set of strongly normalizing lambda terms); $\mathrm{FV}(M)$ (the set of all free variables in M); $M[x := N]$ (the term obtained from M by replacing each free occurrence of x with N); $M \equiv N$ (M is α-equivalent to N); $M =_\beta N$ (M is β-equivalent to N). We equate a lambda term M with a lambda term N if M is α-equivalent to N. We assume that V is countably infinite.

1.1.2 The type assignment system $\lambda\!\!\rightarrow$

Given a countably infinite set V of type variables, then the set $\mathbb{T}$ of (simple) types is defined as follows:

$$\mathbb{T} ::= \mathbb{V} \mid (\mathbb{T} \to \mathbb{T}).$$

The metavariables p, q, and r denote type variables; α, β, and γ denote types. Parentheses may be omitted in such a way that, for example, $\alpha \to \beta \to \gamma$ denotes the type $(\alpha \to (\beta \to \gamma))$. A statement is an expression of the form $M : \alpha$ with $M \in \Lambda$ and $\alpha \in \mathbb{T}$. The type α is called the *predicate*, and the term M is called the *subject* of the statement. A *declaration* is a statement with a term variable as the subject. A basis is a *finite* set of declarations

[4] Recall, in Barendregt's semantics, that the interpretation of a type variable is fixed: $[\![p]\!] = \{\, M \mid M \text{ is a strongly normalizing term} \,\}$.

with distinct variables as subjects. If $\Gamma = \{x : \alpha, y : \beta, \dots\}$, then we write $\mathrm{dom}(\Gamma) = \{x, y, \dots\}$.

The simple type assignment system $\lambda\!\!\rightarrow$ is defined by the rules (Id), ($\rightarrow$ I) and ($\rightarrow$ E) in Figure 1.1. We write $\Gamma \vdash_{\lambda\!\!\rightarrow} M : \alpha$ if $\Gamma \vdash M : \alpha$ is derivable in $\lambda\!\!\rightarrow$.

1.1.3 Barendregt's semantics

Barendregt [Bar92] provided a sound (but not complete) semantics of $\lambda\!\!\rightarrow$ by generalizing the strong normalization proof of Tait [Tai67].

Definition 1.1.1 (Barendregt's semantics)**.** For each $\mathbb{A}, \mathbb{B} \subseteq \Lambda$, define $\mathbb{A} \to \mathbb{B} \subseteq \Lambda$ by

$$\mathbb{A} \to \mathbb{B} = \{\, M \in \Lambda \mid MN \in \mathbb{B} \text{ for every } N \in \mathbb{A} \,\}.$$

Then, for each $\alpha \in \mathbb{T}$, define $[\![\alpha]\!] \subseteq \Lambda$ as follows:

(1) $[\![p]\!] = \mathrm{SN}$,

(2) $[\![\alpha \to \beta]\!] = [\![\alpha]\!] \to [\![\beta]\!]$.

We denote the set $\{\, [\![\alpha]\!] \mid \alpha \in \mathbb{T} \,\}$ by $[\![\mathbb{T}]\!]_{\mathrm{SN}}$.

A *term valuation* is a mapping from V into Λ. Let ρ be a term valuation, and let M be a lambda term. Then we write the lambda term obtained from M by replacing each free occurrence of x by $\rho(x)$ as $[\![M]\!]_\rho$. For each statement $M : \alpha$ and each basis Γ, we write $\rho \models M : \alpha$ if $[\![M]\!]_\rho \in [\![\alpha]\!]$, and write $\rho \models \Gamma$ if $\rho \models x : \alpha$ for all $x : \alpha \in \Gamma$. Furthermore, we write $\Gamma \models M : \alpha$ if $\rho \models M : \alpha$ holds for each ρ such that $\rho \models \Gamma$.

Proposition 1.1.2 ([Bar92, Proposition 4.3.5])**.** *If* $\Gamma \vdash_{\lambda\!\!\rightarrow} M : \alpha$*, then* $\Gamma \models M : \alpha$*.*

Note 1.1.3. For each term valuation ρ, $[\![\lambda x.xx]\!]_\rho \equiv \lambda x.xx \in \mathrm{SN} = [\![p]\!]$. Hence $\models \lambda x.xx : p$. However, $\not\vdash_{\lambda\!\!\rightarrow} \lambda x.xx : p$. Therefore, $\lambda\!\!\rightarrow$ is not complete with respect to $\models$.

1.2 Term-space semantics of $\lambda\!\!\rightarrow$

In this section, we first provide a new semantics that is obtained from Barendregt's by modifying the interpretation of type to be more flexible. Then we show that $\lambda\!\!\rightarrow$ is complete but not sound with respect to the semantics.

1.2.1 Term-space semantics

Definition 1.2.1 (Term space)**.** A set $\mathcal{L} \subseteq 2^{\Lambda}$ is called a *term space* if it is closed under the operation $\to$, that is, $\mathbb{A} \in \mathcal{L}$ and $\mathbb{B} \in \mathcal{L}$ imply $\mathbb{A} \to \mathbb{B} \in \mathcal{L}$.

Definition 1.2.2 (Term-space semantics)**.** A *type valuation* on a term space $\mathcal{L}$ is a mapping from $\mathbb{V}$ into $\mathcal{L}$. For each type valuation θ on $\mathcal{L}$ and each $\alpha \in \mathbb{T}$, define $[\alpha]_\theta \in \mathcal{L}$ as follows:

$$[p]_\theta = \theta(p),$$
$$[\alpha \to \beta]_\theta = [\alpha]_\theta \to [\beta]_\theta.$$

A *term valuation* is a mapping from V into Λ. For each term valuation ρ and each lambda term M, the term obtained from M by replacing each free occurrence of x with $\rho(x)$ is written as $[M]_\rho$. Given a term valuation ρ, $\rho[x := M]$ denotes the following term valuation:

$$\rho[x := M](y) = \begin{cases} M & \text{if } y \equiv x, \\ \rho(y) & \text{if } y \not\equiv x. \end{cases}$$

Let $\mathcal{L}$ be a term space, let θ be a type valuation on $\mathcal{L}$, let ρ be a term valuation, let $M : \alpha$ be a statement, and let Γ be a basis. Then we write $\rho, \theta \Vdash M : \alpha$ if $[M]_\rho \in [\alpha]_\theta$, and write $\rho, \theta \Vdash \Gamma$ if $\rho, \theta \Vdash x : \alpha$ for each $x : \alpha \in \Gamma$. We also write $\Gamma \Vdash M : \alpha$ if $\rho, \theta \Vdash M : \alpha$ for every term space $\mathcal{L}$, every term valuation ρ, and every type valuation θ on $\mathcal{L}$ such that $\rho, \theta \Vdash \Gamma$.

Note 1.2.3. Clearly, $[\![\mathbb{T}]\!]_{\mathrm{SN}}$ is a term space. Hence term-space semantics is regarded as an extension of Barendregt's semantics naturally. Indeed, Barendregt's semantics can be obtained from ours by adopting the term space $[\![\mathbb{T}]\!]_{\mathrm{SN}}$.

1.2.2 Completeness

Here we show that $\lambda\!\to$ is complete with respect to $\Vdash$. We first prepare some definitions and lemmas.

Definition 1.2.4. A *rich basis* P is an *infinite*[5] set of declarations such that:

- for each $\alpha \in \mathbb{T}$, there exist infinitely many x such that $x : \alpha \in \mathrm{P}$.

[5]Note that a rich basis is an infinite set although a basis is a finite set.

Definition 1.2.5. For each rich basis P and each $\alpha \in \mathbb{T}$, define the set $\langle\!\langle \alpha \rangle\!\rangle_{\mathrm{P}} \subseteq \Lambda$ by

$$\langle\!\langle \alpha \rangle\!\rangle_{\mathrm{P}} = \{\, M \in \Lambda \mid \mathrm{P}' \vdash_{\lambda\to} M : \alpha \text{ for some } \mathrm{P}' \subseteq_{\mathrm{fin}} \mathrm{P} \,\}.$$[6]

We denote the set $\{\, \langle\!\langle \alpha \rangle\!\rangle_{\mathrm{P}} \mid \alpha \in \mathbb{T} \,\}$ by $\langle\!\langle \mathbb{T} \rangle\!\rangle_{\mathrm{P}}$.

Lemma 1.2.6. *Let* P *be a rich basis. Then*

$$\langle\!\langle \alpha \to \beta \rangle\!\rangle_{\mathrm{P}} = \langle\!\langle \alpha \rangle\!\rangle_{\mathrm{P}} \to \langle\!\langle \beta \rangle\!\rangle_{\mathrm{P}}.$$

Proof. The inclusion $\langle\!\langle \alpha \to \beta \rangle\!\rangle_{\mathrm{P}} \subseteq \langle\!\langle \alpha \rangle\!\rangle_{\mathrm{P}} \to \langle\!\langle \beta \rangle\!\rangle_{\mathrm{P}}$ is easy. Below, we show the inverse inclusion.

Take $M \in \langle\!\langle \alpha \rangle\!\rangle_{\mathrm{P}} \to \langle\!\langle \beta \rangle\!\rangle_{\mathrm{P}}$ arbitrarily. Because P is rich, we can take a term variable x such that $x : \alpha \in \mathrm{P}$. Since $x : \alpha \vdash_{\lambda\to} x : \alpha$, we obtain $x \in \langle\!\langle \alpha \rangle\!\rangle_{\mathrm{P}}$. Then, because $M \in \langle\!\langle \alpha \rangle\!\rangle_{\mathrm{P}} \to \langle\!\langle \beta \rangle\!\rangle_{\mathrm{P}}$, $Mx \in \langle\!\langle \beta \rangle\!\rangle_{\mathrm{P}}$. Hence $\mathrm{P}' \vdash_{\lambda\to} Mx : \beta$ for some $\mathrm{P}' \subseteq_{\mathrm{fin}} \mathrm{P}$. Then, from the generation lemma of $\lambda\to$ (see [Bar92, Proposition 3.1.8]), we obtain $\mathrm{P}' \vdash_{\lambda\to} M : \alpha \to \beta$. Therefore $M \in \langle\!\langle \alpha \to \beta \rangle\!\rangle_{\mathrm{P}}$. □

Corollary 1.2.7. *For each rich basis* P, $\langle\!\langle \mathbb{T} \rangle\!\rangle_{\mathrm{P}}$ *is a term space.*

Definition 1.2.8 (Canonical term space)**.** Let P be a rich basis. We call the term space $\langle\!\langle \mathbb{T} \rangle\!\rangle_{\mathrm{P}}$ the canonical term space associated to P.

Lemma 1.2.9. *If* $\Gamma \not\vdash_{\lambda\to} M : \alpha$*, then there exists a rich basis* $\mathrm{P} \supseteq \Gamma$ *such that* $\mathrm{P}' \not\vdash_{\lambda\to} M : \alpha$ *for each* $\mathrm{P}' \subseteq_{\mathrm{fin}} \mathrm{P}$.

Proof. Because Γ is finite, we can easily extend Γ to a rich basis P such that if $x : \alpha \in \mathrm{P}$ and $x \in \mathrm{FV}(M)$, then $x : \alpha \in \Gamma$. Then, because

$$\mathrm{FV}(M) \cap \mathrm{dom}(\Gamma) = \mathrm{FV}(M) \cap \mathrm{dom}(\mathrm{P}),$$

$\mathrm{P}' \not\vdash_{\lambda\to} M : \alpha$ for any $\mathrm{P}' \subseteq_{\mathrm{fin}} \mathrm{P}$ (see [Bar92, Proposition 3.1.7]). □

Then we proceed to the proof of completeness.

Theorem 1.2.10 (Completeness)**.** *If* $\Gamma \Vdash M : \alpha$*, then* $\Gamma \vdash_{\lambda\to} M : \alpha$.

Proof. Suppose $\Gamma \not\vdash_{\lambda\to} M : \alpha$. Consider the rich basis P given in Lemma 1.2.9. Let ρ be the term valuation such that $\rho(x) = x$, and let θ be the type valuation on the canonical term space $\langle\!\langle \mathbb{T} \rangle\!\rangle_{\mathrm{P}}$ such that $\theta(p) = \langle\!\langle p \rangle\!\rangle_{\mathrm{P}}$. Then

$$[M]_\rho \equiv M \notin \langle\!\langle \alpha \rangle\!\rangle_{\mathrm{P}} = [\alpha]_\theta.$$

Hence $\Gamma \not\Vdash M : \alpha$. □

[6] If A is a finite subset of B, then we write $A \subseteq_{\mathrm{fin}} B$.

1.2.3 Unsoundness

Note 1.2.11. Let $\mathcal{L} = 2^{\Lambda}$, $\theta(p) = \{x\}$, and $\rho(x) = x$. Then we obtain $\Vdash \not\lambda x.x : p \to p$ because

$$[\lambda x.x]_\rho \equiv \lambda x.x \notin \emptyset = [p \to p]_\theta.$$

On the other hand, $\vdash_{\lambda\to} \lambda x.x : p \to p$. Hence $\lambda\to$ is not sound with respect to $\Vdash$.

1.3 Proper term-space semantics

In the previous section, we saw that $\lambda\to$ is not sound with respect to term-space semantics. In this section, we consider the following restricted term-space semantics.

Definition 1.3.1 (Proper-term-space semantics)**.** A term space $\mathcal{L}$ is said to be *proper* if the following conditions hold:

(♯1) each set in $\mathcal{L}$ includes infinitely many term variables,

(♯2) each sets $\mathbb{A}$ and $\mathbb{B}$ in $\mathcal{L}$ satisfy the following condition: if $M[x := N] \in \mathbb{A}$, $N \in \mathbb{B}$, $M \in \mathbb{A}$ and $x \in \mathbb{B}$, then $(\lambda x.M)N \in \mathbb{A}$.

We write $\Gamma \Vdash^{\mathrm{P}} M : \alpha$ if $\rho, \theta \Vdash M : \alpha$ for each *proper* term space $\mathcal{L}$, each term valuation ρ, and each type valuation θ on $\mathcal{L}$ such that $\rho, \theta \Vdash \Gamma$.

In Sections 1.3.1 and 1.3.2, we show that $\lambda\to$ is sound and complete with respect to $\Vdash^{\mathrm{P}}$. Then, in Section 1.3.3, we consider the relation between Barendregt's semantics and proper-term-space semantics.

1.3.1 Soundness

Theorem 1.3.2 (Soundness)**.** *If* $\Gamma \vdash_{\lambda\to} M : \alpha$*, then* $\Gamma \Vdash^{\mathrm{P}} M : \alpha$*.*

Proof. By induction on the size of the derivation of $\Gamma \vdash_{\lambda\to} M : \alpha$. The only nontrivial case is when the last rule is $(\to \mathrm{I})$:

$$\frac{\Gamma \vdash M : \beta}{\Gamma \setminus \{x : \alpha\} \vdash \lambda x.M : \alpha \to \beta}\ (\to \mathrm{I}).$$

Take a proper term space $\mathcal{L}$, a type valuation θ on $\mathcal{L}$, and a term valuation ρ such that $\rho, \theta \Vdash \Gamma \setminus \{x : \alpha\}$. Let N be in $[\alpha]_\theta$. To prove $[\lambda x.M]_\rho \in [\alpha \to \beta]_\theta$, we will show $[\lambda x.M]_\rho N \in [\beta]_\theta$ below.

Because of the condition (♯1), we can take a term variable $y \in [\alpha]_\theta$ such that $y \notin \mathrm{FV}(M) \cup \mathrm{dom}(\Gamma)$. Here, we can easily check that there exists a derivation of $(\Gamma \setminus \{x : \alpha\}) \cup \{y : \alpha\} \vdash_{\lambda\to} M[x := y] : \beta$ whose size is equal to the size of the derivation of $\Gamma \vdash_{\lambda\to} M : \beta$. Since $y \notin \mathrm{dom}(\Gamma)$, $y \in [\alpha]_\theta$, and $N \in [\alpha]_\theta$, we obtain $\rho[y := y], \theta \Vdash (\Gamma \setminus \{x : \alpha\}) \cup \{y : \alpha\}$ and $\rho[y := N], \theta \Vdash (\Gamma \setminus \{x : \alpha\}) \cup \{y : \alpha\}$. Hence, by induction hypothesis, $[M[x := y]]_{\rho[y:=y]} \in [\beta]_\theta$ and $[M[x := y]]_{\rho[y:=N]} \in [\beta]_\theta$. Then, from the condition (♯2), $(\lambda y.[M[x := y]]_{\rho[y:=y]})N \in [\beta]_\theta$. Here, since $\lambda y.[M[x := y]]_{\rho[y:=y]}$ is α-equivalent to $[\lambda x.M]_\rho$, we obtain $[\lambda x.M]_\rho N \in [\beta]_\theta$. □

1.3.2 Completeness

Theorem 1.3.3 (Completeness)**.** *If* $\Gamma \Vdash^{\mathrm{P}} M : \alpha$*, then* $\Gamma \vdash_{\lambda\to} M : \alpha$*.*

Proof. We can easily check that, for each rich basis P, the canonical term space $\langle\!\langle \mathbb{T} \rangle\!\rangle_{\mathrm{P}}$ is proper. Hence, we can prove this theorem in the same way as the proof of Theorem 1.2.10. □

1.3.3 $[\![\mathbb{T}]\!]_{\mathrm{SN}}$ is proper

Let us now show that Barendregt's term space $[\![\mathbb{T}]\!]_{\mathrm{SN}}$, which is detailed in Definition 1.1.1, is proper. This fact shows that proper-term-space semantics can also be regarded as an extension of Barendregt's semantics.

Theorem 1.3.4. $[\![\mathbb{T}]\!]_{\mathrm{SN}}$ *is proper.*

Proof. Because every $[\![\alpha]\!]$ includes V (see [Bar92, Lemma 4.3.3]), $[\![\mathbb{T}]\!]_{\mathrm{SN}}$ satisfies (♯1). Furthermore, for each $\alpha, \beta \in \mathbb{T}$, $[\![\alpha]\!] \in [\![\mathbb{T}]\!]_{\mathrm{SN}}$ is saturated[7] and $[\![\beta]\!] \subseteq \mathrm{SN}$ (see [Bar92, Lemma 4.3.3]). Therefore, $M[x := N] \in [\![\alpha]\!]$ and $N \in [\![\beta]\!]$ imply $(\lambda x.M)N \in [\![\alpha]\!]$. □

[7] A subset $X \subseteq \mathrm{SN}$ is said to be *saturated* if: (a) $x\vec{R} \in X$ for each $n \geq 0$, $R_1, \ldots, R_n \in \mathrm{SN}$, and $x \in \mathrm{V}$, and (b) $M[x := N]\vec{R} \in X$ implies $(\lambda x.M)N\vec{R} \in X$, for each $n \geq 0$, $R_1, \ldots, R_n \in \mathrm{SN}$, and $Q \in \mathrm{SN}$ (see [Bar92, Definition 4.3.2])

1.4 Saturated-term-space semantics

In the previous section, we provide the restrictions (♯1) and (♯2) of term space such that the soundness theorem and the completeness theorem hold. In this section, we consider whether we can make the restrictions stronger or not. Here, recall the proof of Theorem 1.3.4. We show that Barendregt's term space $[\![\mathbb{T}]\!]_{\mathrm{SN}}$ satisfies the following condition, which is stronger than (♯2):

(♯2)$^{++}$ sets $\mathbb{A}$ and $\mathbb{B}$ in $\mathcal{L}$ each satisfy the following condition: if $M[x := N] \in \mathbb{A}$ and $N \in \mathbb{B}$, then $(\lambda x.M)N \in \mathbb{A}$.

We now consider the following two kinds of semantics.

Definition 1.4.1 (Saturated-term-space semantics)**.** A term space is said to be *saturated*, if it satisfies (♯1) and (♯2)$^{++}$. Furthermore, a term space is said to be *weakly saturated* if it satisfies (♯1) and the following condition:

(♯2)$^{+}$ sets $\mathbb{A}$ and $\mathbb{B}$ in $\mathcal{L}$ each satisfy the following condition: if $M[x := N] \in \mathbb{A}$, $N \in \mathbb{B}$, and $M \in \mathbb{A}$, then $(\lambda x.M)N \in \mathbb{A}$.

We write $\Gamma \Vdash^{\mathrm{S}} M : \alpha$ (resp., $\Gamma \Vdash^{\mathrm{W}} M : \alpha$) if $\rho, \theta \Vdash M : \alpha$ for each *saturated* (resp., *weakly saturated*) term space $\mathcal{L}$, each term valuation ρ, and each type valuation θ on $\mathcal{L}$ such that $\rho, \theta \Vdash \Gamma$.

Note 1.4.2. It is clear that every saturated term space is weakly saturated, and every weakly saturated term space is proper. Hence, $\lambda\!\!\rightarrow$ is sound with respect to both $\Vdash^{\mathrm{S}}$ and $\Vdash^{\mathrm{W}}$. Furthermore, from the proof of Theorem 1.3.4, for each $[\![\alpha]\!]$ and $[\![\beta]\!]$, $M[x := N] \in [\![\alpha]\!]$ and $N \in [\![N]\!]$ imply $(\lambda x.M)N \in [\![\alpha]\!]$. Therefore, $[\![\mathbb{T}]\!]_{\mathrm{SN}}$ is saturated (and hence it is also weakly saturated).

Here, the following questions arise naturally.

Question 1.4.3. Is $\lambda\!\!\rightarrow$ complete with respect to $\Vdash^{\mathrm{S}}$? That is, does $\Gamma \Vdash^{\mathrm{S}} M : \alpha$ imply $\Gamma \vdash_{\lambda\!\!\rightarrow} M : \alpha$?

Question 1.4.4. Is $\lambda\!\!\rightarrow$ complete with respect to $\Vdash^{\mathrm{W}}$? That is, does $\Gamma \Vdash^{\mathrm{W}} M : \alpha$ imply $\Gamma \vdash_{\lambda\!\!\rightarrow} M : \alpha$?

Unfortunately, this thesis could not solve these questions. In the following, we show that, for any rich basis P, the canonical term space $\langle\!\langle \mathbb{T} \rangle\!\rangle_{\mathrm{P}}$ is not weakly saturated. This means that Questions 1.4.3 and 1.4.4 cannot be solved in the same way as Theorem 1.2.10.

Lemma 1.4.5. *There exist* $M, N \in \Lambda$ *and* $\alpha, \beta, \gamma \in \mathbb{T}$ *such that*

(A1) $\mathrm{FV}(M) = \{x\}$ *and* $\mathrm{FV}(N) = \emptyset$,

(A2) $\vdash_{\lambda\to} M[x := N] : \alpha$,

(A3) $\{x : \gamma\} \vdash_{\lambda\to} M : \alpha$,

(A4) $\vdash_{\lambda\to} N : \beta$,

(A5) $(\lambda x.M)N$ *is not typable in* $\lambda\!\to$.

Proof. Let M and N be the following terms:

$$\begin{aligned} M &\equiv \mathbf{KI}(\lambda y.\mathbf{K}(xy)(\lambda z.xzy)), \\ N &\equiv \mathbf{I}, \end{aligned}$$

where $\mathbf{K} \equiv \lambda xy.x$ and $\mathbf{I} \equiv \lambda x.x$. In addition, let α, β, γ be the following types:

$$\begin{aligned} \alpha &\equiv p \to p, \\ \beta &\equiv q \to q, \\ \gamma &\equiv r \to r \to r. \end{aligned}$$

It is not difficult to check that these terms and types satisfy the claims (A1)–(A4) (see also Figures 1.2 and 1.3).

$$\dfrac{\dfrac{\dfrac{\mathbf{I} : r \to r \quad y : r}{\vdots}}{\mathbf{K}(\mathbf{I}y) : ((r \to r) \to r) \to r} \qquad \dfrac{\dfrac{\mathbf{I} : (r \to r) \to r \to r \quad z : r \to r \quad y : r}{\vdots}}{\lambda z.\mathbf{I}zy : (r \to r) \to r}}{\begin{array}{c}\vdots \\ \lambda y.\mathbf{K}(\mathbf{I}y)(\lambda z.\mathbf{I}zy) : r \to r \\ \vdots \\ \mathbf{KI}(\lambda y.\mathbf{K}(\mathbf{I}y)(\lambda z.\mathbf{I}zy)) : p \to p\end{array}}$$

Figure 1.2: Outline of $\vdash_{\lambda\to} M[x := N] : \alpha$

$$\dfrac{\dfrac{\dfrac{}{x : r \to r \to r} \quad \dfrac{}{y : r}}{\vdots}}{\dfrac{\mathbf{K}(xy) : (r \to r) \to r \to r}{\vdots}} \qquad \dfrac{\dfrac{\dfrac{}{x : r \to r \to r} \quad \dfrac{}{z : r} \quad \dfrac{}{y : r}}{\vdots}}{\lambda z.xzy : r \to r}$$

$$\vdots$$

$$\lambda y.\mathbf{K}(xy)(\lambda z.xzy) : r \to r \to r$$

$$\vdots$$

$$\mathbf{KI}(\lambda y.\mathbf{K}(xy)(\lambda z.xzy)) : p \to p$$

Figure 1.3: Outline of $\{x : \gamma\} \vdash_{\lambda\to} M : \alpha$

Below, we show that these satisfy (A5). Suppose $\vdash_{\lambda\to} (\lambda x.M)N : \alpha$. Then the derivation should be of the following form:

$$\dfrac{\dfrac{\dfrac{\vdots}{\{x : \beta\} \vdash M : \alpha}}{\vdash \lambda x.M : \beta \to \alpha}\ (\to \mathrm{I}) \qquad \dfrac{\vdots}{\vdash N : \beta}}{\vdash (\lambda x.M)N : \alpha}\ (\to \mathrm{E}).$$

Here, because $N \equiv \lambda x.x$,

$$\beta \equiv \beta_1 \to \beta_1 \tag{1.1}$$

for some β_1. On the other hand, because both xy and xzy occur in M, there exist types γ, β_2, β_3, and β_4 such that:

$$\beta \equiv \gamma \to \beta_2, \tag{1.2}$$

$$\beta \equiv \beta_3 \to \gamma \to \beta_4. \tag{1.3}$$

However, (1.1), (1.2), and (1.3) cannot hold simultaneously. Therefore, $(\lambda x.M)N$ is not typable. □

Theorem 1.4.6. *For each rich basis* P*, the term space* $\langle\langle \mathbb{T} \rangle\rangle_{\mathrm{P}}$ *is not weakly saturated.*

Proof. Let P be a rich basis. Consider the term $M, N \in \Lambda$ and the types $\alpha, \beta, \gamma \in \mathbb{T}$ given in Lemma 1.4.5. Because of the condition of rich basis,

we can take a variable $y \notin \mathrm{FV}(MN)$ such that $y : \gamma \in \mathrm{P}$. Here, because $\{x : \gamma\} \vdash_{\lambda\to} M : \alpha$ we obtain $\{y : \gamma\} \vdash_{\lambda\to} M[x := y] : \alpha$, and hence

$$M[x := y] \in \langle\!\langle \alpha \rangle\!\rangle_{\mathrm{P}}. \tag{1.4}$$

Furthermore, from $\vdash_{\lambda\to} M[x := N] : \alpha$, we obtain

$$(M[x := y])[y := N] \equiv M[x := N] \in \langle\!\langle \alpha \rangle\!\rangle_{\mathrm{P}}. \tag{1.5}$$

And from $\vdash_{\lambda\to} N : \beta$,

$$N \in \langle\!\langle \beta \rangle\!\rangle_{\mathrm{P}}. \tag{1.6}$$

On the other hand, because $(\lambda x.M)N$ is not typable in $\lambda\to$ and $\lambda y.M[x := y]$ is α-equivalent to $\lambda x.M$, we obtain

$$(\lambda y.M[x := y])N \notin \langle\!\langle \alpha \rangle\!\rangle_{\mathrm{P}}. \tag{1.7}$$

Equations (1.4)–(1.7) show that $\langle\!\langle \mathbb{T} \rangle\!\rangle_{\mathrm{P}}$ does not satisfy the condition $(\sharp 2)^{+}$. □

1.5 Conclusions and future work

In this chapter, we provide four kinds of semantics ($\Vdash$, $\Vdash^{\mathrm{P}}$, $\Vdash^{\mathrm{W}}$, and $\Vdash^{\mathrm{S}}$) for $\lambda\to$ by generalizing Barendregt's semantics ($\models$). The relation between those semantics is as follows (see also Figure 1.4).

Theorem 1.5.1. *(S_i) implies (S_{i+1}), for every pair (S_i) and (S_{i+1}) below:*

(S_1) $\Gamma \Vdash M : \alpha$,

(S_2) $\Gamma \Vdash^{\mathrm{P}} M : \alpha$,

(S_3) $\Gamma \Vdash^{\mathrm{W}} M : \alpha$,

(S_4) $\Gamma \Vdash^{\mathrm{S}} M : \alpha$,

(S_5) $\Gamma \models M : \alpha$.

Theorem 1.5.2. *$\lambda\to$ is unsound with respect to $\Vdash$, but sound with respect to all others ($\Vdash^{\mathrm{P}}$, $\Vdash^{\mathrm{W}}$, $\Vdash^{\mathrm{S}}$, and $\models$).*

Theorem 1.5.3. *$\lambda\to$ is complete with respect to both $\Vdash$ and $\Vdash^{\mathrm{P}}$, but incomplete with respect to $\models$.*

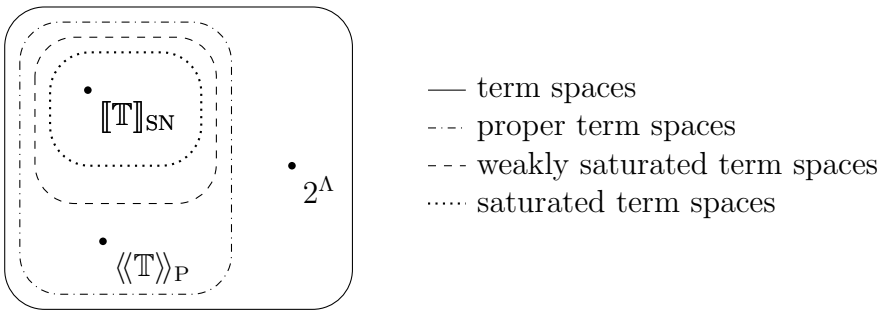

Figure 1.4: Relationship between term spaces

However, the following questions remain unsolved and are subject to further investigation.

Question 1.5.4. Is $\lambda\!\!\rightarrow$ complete with respect to $\Vdash^{\mathrm{W}}$?

Question 1.5.5. Is $\lambda\!\!\rightarrow$ complete with respect to $\Vdash^{\mathrm{S}}$?

Chapter 2

Hilbert's Tenth Problem over Generic Subrings of the Rational Numbers

2.1 Introduction

Hilbert's tenth problem is, originally, a decision problem as to whether a given polynomial equation $f = 0$ has a solution in the integers $\mathbb{Z}$, where f is a multivariate polynomial in $\mathbb{Z}[X_1, X_2, \dots]$. In 1970, Matiyasevich [Mat70] showed that Hilbert's tenth problem is undecidable, based on the work by Davis, Putnam and Robinson [DPR61]. This problem is naturally generalized to an arbitrary ring R: Hilbert's tenth problem for a ring R, denoted by $\mathrm{HTP}(R)$, is a decision problem as to whether a given polynomial equation $f = 0$ for a polynomial $f \in R[X_1, X_2, \dots]$ has a solution in R. With this terminology, what Matiyasevich established is that the halting problem $\emptyset'$ is 1-reducible to $\mathrm{HTP}(\mathbb{Z})$. For known results about these variants of the problem, the reader is referred to the conference proceedings [DLPVG00] or a survey by Poonen [Poo03b].

However, for the ring $\mathbb{Q}$ of rational numbers, undecidability of $\mathrm{HTP}(\mathbb{Q})$ is still an open problem. A naïve approach to prove undecidability of $\mathrm{HTP}(\mathbb{Q})$, and similarly for other rings, is to show that $\mathbb{Z}$ is Diophantine (i.e., existentially definable) in $\mathbb{Q}$. If this is true, then one can easily construct a 1-reduction $\mathrm{HTP}(\mathbb{Z}) \leq_1 \mathrm{HTP}(\mathbb{Q})$ and deduce that $\mathrm{HTP}(\mathbb{Q})$ is undecidable. However, it is known that $\mathbb{Z}$ cannot have even Diophantine model (i.e., a ring

isomorphic to $\mathbb{Z}$ whose underlying set and graphs of addition and multiplication are Diophantine) in $\mathbb{Q}$ under a plausible number-theoretic assumption, known as Mazur's conjecture (see [CZ00] for more details). It is, therefore, important to develop an entirely new method to approach undecidability of $\mathrm{HTP}(\mathbb{Q})$.

The main target of this chapter is $\mathrm{HTP}(R)$ for subrings R of $\mathbb{Q}$, including $R = \mathbb{Q}$ itself. Formally, for a subring $R \subseteq \mathbb{Q}$, Hilbert's tenth problem for R is defined as the set

$$\mathrm{HTP}(R) := \{\, f \in \mathbb{Z}[X_1, X_2, \dots] \mid \exists \bar{x} \in R^{<\omega}[f(\bar{x}) = 0] \,\},$$

where $R^{<\omega} := \bigcup_{n\in\omega} R^n$. Here we consider $\mathrm{HTP}(R)$ as a decision problem by identifying with its membership problem. In the rest of the chapter, in order to mention the Turing degree of $\mathrm{HTP}(R)$ consistently, we fix a computable enumeration $(f_i)_{i\in\omega}$ of the polynomials in $\mathbb{Z}[X_1, X_2, \dots]$. For every subring $R \subseteq \mathbb{Q}$, there exists a unique set W of prime numbers such that

$$R = \mathbb{Z}[W^{-1}] = \{\, n/d \in \mathbb{Q} \mid n, d \in \mathbb{Z}, \text{ every prime factor of } d \text{ is in } W \,\}.$$

We write R_W for the subring $\mathbb{Z}[W^{-1}]$. The mapping $W \mapsto R_W$ from the power set $2^{\mathbb{P}}$ of the set $\mathbb{P} := \{2, 3, 5, 7, 11, \dots\}$ of prime numbers to the set of subrings of $\mathbb{Q}$ is bijective. Thus each subring $R \subseteq \mathbb{Q}$ is naturally considered as a point of the Cantor space $2^{\mathbb{P}}$.

There are several previous studies about $\mathrm{HTP}(R_W)$ for $W \in 2^{\mathbb{P}}$, mainly by Russell G. Miller. Eisenträger, Miller, Park and Shlapentokh [EMPS17] showed, by a priority argument, that there exists a coinfinite c.e. set $W \in 2^{\mathbb{P}}$ such that $W \equiv_{\mathrm{T}} \mathrm{HTP}(R_W) \equiv_{\mathrm{T}} \mathrm{HTP}(\mathbb{Q})$. Poonen [Poo03a] constructed continuum many set $W \in 2^{\mathbb{P}}$ such that R_W admits a Diophantine model of $\mathbb{Z}$, i.e., $\emptyset' \leq_1 \mathrm{HTP}(R_W)$. However, Miller [Mil16] showed that there exist only meager many such sets in $2^{\mathbb{P}}$ unless $\mathbb{Q}$ admits a Diophantine model of $\mathbb{Z}$. Therefore Poonen's result cannot be extended to a non-meager subset of $2^{\mathbb{P}}$ unless Mazur's conjecture is false. In the same paper, Miller introduced the notion of *HTP-genericity* (Definition 2.2.4). An HTP-generic set is defined to be a set which avoids the boundary set of every polynomial. Miller showed that the Turing degree of $\mathrm{HTP}(R_W)$ for an HTP-generic set $W \in 2^{\mathbb{P}}$ is determined by that of $\mathrm{HTP}(\mathbb{Q})$, vis., the Turing equivalence $\mathrm{HTP}(R_W) \equiv_{\mathrm{T}} W \oplus \mathrm{HTP}(\mathbb{Q})$ holds for every HTP-generic set $W \in 2^{\mathbb{P}}$ (Lemma 2.2.6). Also they showed that for every set $C \subseteq \omega$, $\mathrm{HTP}(\mathbb{Q})$ computes C if and only if there are non-meager many set $W \in 2^{\mathbb{P}}$ such that $\mathrm{HTP}(R_W)$ computes C.

In [Mil18], they focused on the measure-theoretic structure of $2^{\mathbb{P}}$ and studied the noncomputability of the measure of the boundary set of a polynomial. However, the measure of the set of HTP-generic sets still remains unknown. In [KM19], Kramer and Miller viewed HTP as an operator on $2^{\mathbb{P}}$ and studied its properties. In particular, they showed that HTP does not preserve Turing equivalence, i.e., there exist $U, V \in 2^{\mathbb{P}}$ such that $U \equiv_{\mathrm{T}} V$ and $\mathrm{HTP}(R_U) \not\equiv_{\mathrm{T}} \mathrm{HTP}(R_V)$. For m-equivalence, Miller [Mil19] showed that if HTP preserves m-equivalences, then $\emptyset' \leq_1 \mathrm{HTP}(\mathbb{Q})$. In the same paper, they also showed that every Turing degree contains a set $W \in 2^{\mathbb{P}}$ such that $W' \leq_1 \mathrm{HTP}(R_W)$, while the set of such sets is meager of measure 0. On the other hand, they pointed out that it is possible for the set $\{ W \in 2^{\mathbb{P}} \mid W' \leq_{\mathrm{T}} \mathrm{HTP}(R_W) \}$ to be not small. (Beware the difference between $\leq_1$ and $\leq_{\mathrm{T}}$.) Our Theorem 2.1.1 below says that the size of this set depends on the Turing degree of $\mathrm{HTP}(\mathbb{Q})$. In [Mil20], Miller showed that $\mathrm{HTP}(\mathbb{Q})$ is low if and only if $\mathrm{HTP}(R_W)' \leq_{\mathrm{T}} W'$ for comeager many sets $W \in 2^{\mathbb{P}}$. This fact is also obtained as a consequence of Theorem 2.1.1 below.

In this chapter, we continue and enhance the program by Miller. In section 2.3, we prove that the Turing degree of $\mathrm{HTP}(R_W)$ for a generic set W "almost" determines that of $\mathrm{HTP}(\mathbb{Q})$:

Theorem 2.1.1 (part of Corollary 2.3.2)**.** *The following equivalences hold.*

(1) $\mathrm{HTP}(R_W) \equiv_{\mathrm{T}} W$ *for some or all generic set* W *if and only if* $\mathrm{HTP}(\mathbb{Q})$ *is decidable.*

(2) $\mathrm{HTP}(R_W) >_{\mathrm{T}} W$ *for some or all generic set* W *if and only if* $\mathrm{HTP}(\mathbb{Q})$ *is undecidable.*

(3) $\mathrm{HTP}(R_W)' \leq_{\mathrm{T}} W'$ *for some or all generic set* W *if and only if* $\mathrm{HTP}(\mathbb{Q})$ *is low.*

(4) $\mathrm{HTP}(R_W)' \geq_{\mathrm{T}} W''$ *for some or all generic set* W *if and only if* $\mathrm{HTP}(\mathbb{Q})$ *is high.*

(5) $\mathrm{HTP}(R_W) \equiv_{\mathrm{T}} W'$ *for some or all generic set* W *if and only if* $\mathrm{HTP}(\mathbb{Q}) \equiv_{\mathrm{T}} \emptyset'$.

Moreover, under an additional assumption, these statements remain true with "generic" being replaced by "arithmetically random".

Theorem 2.1.1 is a further generalization of Theorem 1 and Proposition 1 in [Mil20]. In particular, a consequence of the theorem is that Proposition 1 in [Mil20] holds without any assumption.

In section 2.4, with more detailed analysis of the proof of Theorem 2.1.1, we give a new characterization of undecidability of $\mathrm{HTP}(\mathbb{Q})$ in terms of Banach–Mazur game.

Theorem 2.1.2 (part of Theorem 2.4.6)**.** *Let* $\mathcal{N} := \{ W \in 2^{\mathbb{P}} \mid W <_{\mathrm{T}} \mathrm{HTP}(R_W) \}$*. The following conditions are equivalent.*

(1) $\mathrm{HTP}(\mathbb{Q})$ *is undecidable.*

(2) Player I *has a winning strategy for Banach–Mazur game for* $\mathcal{N}$*.*

(3) Player II *does not have a winning strategy for Banach–Mazur game for* $\mathcal{N}$*.*

Theorem 2.1.2 provides a new way to prove undecidability of $\mathrm{HTP}(\mathbb{Q})$: all one has to do is to develop a winning strategy for such a game. In addition, it is worth noting that Theorem 2.1.2 characterizes *absence* of deciding algorithm for $\mathrm{HTP}(\mathbb{Q})$ as *existence* of a winning strategy for a game.

To our knowledge, for every "natural" undecidable problem arising in mathematics, its undecidability is proved by reducing the halting problem $\emptyset'$ to it. If undecidability of $\mathrm{HTP}(\mathbb{Q})$ is proved by our approach using Theorem 2.1.2, then $\mathrm{HTP}(\mathbb{Q})$ will become the first natural decision problem whose undecidability is proved without reducing $\emptyset'$. Note that undecidability proof based on Theorem 2.1.2 works even if $\emptyset <_{\mathrm{T}} \mathrm{HTP}(\mathbb{Q}) <_{\mathrm{T}} \emptyset'$ (see also Question 2.3.6).

In Section 2.5, we show several interesting results deducible from the assumption that $\mathbb{Z}$ is Diophantine in $\mathbb{Q}$, contrary to Mazur's conjecture. In particular, under the Diophantineness assumption, we show that every coinfinite HTP-generic set is cohyperimmune in Theorem 2.5.6. Although this topic is slightly different from the subject of the chapter, we believe the results to be useful for this field of study, as well as for future development of our approach.

2.2 Preliminaries

We first review some of the basic properties of HTP.

Lemma 2.2.1. *The following properties hold.*

(1) $W \leq_1 \mathrm{HTP}(R_W) \leq_1 W'$ *for all* $W \in 2^{\mathbb{P}}$. *Moreover,* HTP *is an enumeration operator.*

(2) $\mathrm{HTP}(\mathbb{Q}) \leq_1 \mathrm{HTP}(R_W)$ *for all* $W \in 2^{\mathbb{P}}$.

(3) $\mathrm{HTP}(R_V) \leq_1 \mathrm{HTP}(\mathbb{Q})$ *for all cofinite set* $V \in 2^{\mathbb{P}}$.

Proof. We give only brief outlines of the proofs here.

(1) The former reduction is given by the map $p \mapsto pX - 1$. The latter reduction holds since $\mathrm{HTP}(R_W)$ is c.e. in W. For enumeration operators, see e.g. [Mil19, section 5].

(2) Convert each variable X_i occurring in a given polynomial into the fraction Y_i/Z_i of two new variables Y_i and Z_i. See [EMPS17, Corollary 5.2] or [Mil18, section 2.2] for details.

(3) For every $p \in \mathbb{P}$, it is known that the local ring $\mathbb{Z}_{(p)} = \{\, n/d \in \mathbb{Q} \mid n, d \in \mathbb{Z}, p \nmid d \,\}$ is Diophantine in $\mathbb{Q}$. See [EMPS17, Proposition 5.4] for more details. □

Both ends of the inequation in the first assertion of Lemma 2.2.1 are attained as follows.

Proposition 2.2.2. *The following properties hold.*

(1) There are continuum many set $W \in 2^{\mathbb{P}}$ *such that* $W \equiv \mathrm{HTP}(R_W)$.

(2) There are continuum many set $W \in 2^{\mathbb{P}}$ *such that* $\mathrm{HTP}(R_W) \equiv W'$.

Proof.

(1) Suppose $W = V'$ for some set $V \in 2^{\mathbb{P}}$. Then $\mathrm{HTP}(R_W) \leq_1 W$ since HTP is an enumeration operator and thus $\mathrm{HTP}(R_W)$ is c.e. in V. There are continuum many such W by Friedberg's jump inversion theorem.

(2) By the result due to Miller [Mil19, Theorem 4.1], every Turing degree contains a set $W \in 2^{\mathbb{P}}$ such that $W' \leq_1 \mathrm{HTP}(R_W)$. □

2.2.1 Topology and measure on the Cantor space $2^{\mathbb{P}}$

The Cantor space $2^{\mathbb{P}}$ is the topological space defined as the countably infinite product of the discrete space $2 = \{0, 1\}$. For each binary string $\sigma \in 2^{<\mathbb{P}}$ of finite length, a basic clopen set for σ is given by

$$[\![\sigma]\!] := \{\, W \in 2^{\mathbb{P}} \mid \sigma \subseteq W \,\}$$

where $\sigma \subseteq W$ denotes that σ is an initial segment of W, viewing W as a binary string of infinite length. The topology on $2^{\mathbb{P}}$ is generated by $\{\, [\![\sigma]\!] \mid \sigma \in 2^{<\mathbb{P}} \,\}$. Also, the Cantor space $2^{\mathbb{P}}$ is equipped with the probability measure μ satisfying that $\mu([\![\sigma]\!]) = 2^{-|\sigma|}$ for each $\sigma \in 2^{<\mathbb{P}}$, where $|\sigma|$ denotes the length of σ.

Definition 2.2.3. A subset of $2^{\mathbb{P}}$ is called *nowhere dense* if its topological closure has no interior points. The countable union of nowhere dense sets is said to be *meager*. (It is also known as a *set of first category*.) The complement of a meager set is called *comeager*.

Comeager sets and sets of measure 1 are considered as "large" subsets of $2^{\mathbb{P}}$.

2.2.2 Boundary sets, HTP-genericity and generalized HTP-lowness

Definition 2.2.4 (cf. [Mil16, section 2], [Mil18, section 3])**.** For a polynomial $f \in \mathbb{Z}[X_1, X_2, \dots]$, we write

- $\mathcal{A}(f) := \{\, W \in 2^{\mathbb{P}} \mid f \in \mathrm{HTP}(R_W) \,\}$, which is an open set in $2^{\mathbb{P}}$ since $f \in \mathrm{HTP}(R_W)$ is witnessed by some finite subset of W,
- $\mathcal{B}(f) := \{\, W \in 2^{\mathbb{P}} \mid f \notin \mathrm{HTP}(R_W) \wedge \forall \sigma \subseteq W \exists V \in [\![\sigma]\!]\, [f \in \mathrm{HTP}(R_V)] \,\}$, which is the topological boundary of $\mathcal{A}(f)$, and
- $\mathcal{C}(f) := \{\, W \in 2^{\mathbb{P}} \mid \exists \sigma \subseteq W\, \forall V \in [\![\sigma]\!]\, [f \notin \mathrm{HTP}(R_V)] \,\}$, which is the topological exterior of $\mathcal{A}(f)$.

A set $W \in 2^{\mathbb{P}}$ is called *HTP-generic* if $W \notin \mathcal{B} := \bigcup_{f \in \mathbb{Z}[X_1, X_2, \dots]} \mathcal{B}(f)$. Since each $\mathcal{A}(f)$ is open, $\mathcal{B}(f)$ is nowhere dense in $2^{\mathbb{P}}$. Thus the entire boundary set $\mathcal{B}$ is meager, and HTP-genericity is comeager.

Note that the measure $\mu(\mathcal{B})$ of the entire boundary set $\mathcal{B}$ is unknown.

For notational convenience, we introduce a new notion called generalized HTP-lowness.

Definition 2.2.5. A set $W \in 2^{\mathbb{P}}$ is called *generalized HTP-low* if $\mathrm{HTP}(R_W) \leq_{\mathrm{T}} W \oplus \mathrm{HTP}(\mathbb{Q})$. (Note that the opposite direction of the reduction always holds.) We write $\mathbf{GL}^{\mathrm{HTP}}$ for the set of generalized HTP-low sets, and define $\mathbf{GL}^{\mathrm{HTP}}_e := \{\, W \in 2^{\mathbb{P}} \mid \mathrm{HTP}(R_W) = \Phi_e^{W \oplus \mathrm{HTP}(\mathbb{Q})} \,\}$ for each index $e \in \omega$. Clearly, $\mathbf{GL}^{\mathrm{HTP}} = \bigcup_{e \in \omega} \mathbf{GL}^{\mathrm{HTP}}_e$.

HTP-generic sets and generalized HTP-low sets are analogues of 1-generic sets and generalized low_1 sets, respectively, which will be defined in section 2.2.3. The following lemma corresponds to the fact that every 1-generic set is also generalized low_1.

Lemma 2.2.6. *There exists $e \in \omega$ such that $\overline{\mathcal{B}} \subseteq \mathbf{GL}^{\mathrm{HTP}}_e$, where $\overline{\mathcal{B}}$ is the complement of $\mathcal{B}$.*

Proof. The lemma follows from the fact that, for an HTP-generic set $W \in 2^{\mathbb{P}}$, $f \notin \mathrm{HTP}(R_W)$ is a $\Sigma_1^{\mathrm{HTP}(\mathbb{Q})}$ condition by Lemma 2.2.1.(3). For details, see [Mil16, Proposition 2]. □

Remark 2.2.7. Note that if two sets $U, V \in 2^{\mathbb{P}}$ satisfy $U \equiv_{\mathrm{T}} V$ and $U, V \in \mathbf{GL}^{\mathrm{HTP}}$, then $\mathrm{HTP}(R_U) \equiv_{\mathrm{T}} \mathrm{HTP}(R_V)$. That is, HTP preserves Turing equivalence on the comeager set $\mathbf{GL}^{\mathrm{HTP}}$.

2.2.3 Genericity and randomness

In this subsection, we introduce two notions of typicality of a point of $2^{\mathbb{P}}$, called genericity and randomness. For more details, the reader may consult [DH10] for example.

Definition 2.2.8. Let $n \in \omega$. A subset $\mathcal{A} \subseteq 2^{\mathbb{P}}$ is a Σ^0_n set if there exists a computable relation R such that

$$\mathcal{A} = \{\, W \in 2^{\mathbb{P}} \mid \exists k_1 \forall k_2 \cdots Q k_n R(W\restriction k_1, \ldots, W\restriction k_n) \,\}$$

where $Q = \forall$ if n is even and $Q = \exists$ if n is odd. A subset of $2^{\mathbb{P}}$ is called *arithmetical* if it is Σ^0_n for some $n \in \omega$.

A set $W \in 2^{\mathbb{P}}$ is called *n-generic* if it is not contained in the topological boundary $\partial\mathcal{A}$ of any Σ^0_n open subset $\mathcal{A} \subseteq 2^{\mathbb{P}}$. A set $W \in 2^{\mathbb{P}}$ is called *(arithmetically) generic* if it is n-generic for every $n \in \omega$.

Since there exist only countably many Σ^0_n open subsets of $2^{\mathbb{P}}$, there exist comeager many generic set in $2^{\mathbb{P}}$. For every polynomial $f \in \mathbb{Z}[X_1, X_2, \dots]$, the set $\mathcal{A}(f)$ is Σ^0_1 open set. So every 1-generic set is also HTP-generic.

Lemma 2.2.9. *An arithmetical subset $\mathcal{A} \subseteq 2^{\mathbb{P}}$ is comeager if and only if it contains every generic set in $2^{\mathbb{P}}$.*

Proof. Suppose that $\mathcal{A}$ is a Σ^0_n set and $G \notin \mathcal{A}$ for some generic set $G \in 2^{\mathbb{P}}$. Let $\mathcal{A} = \{\, W \in 2^{\mathbb{P}} \mid \exists k_1 \forall k_2 \cdots Q k_n R(W\restriction k_1, \dots W\restriction k_n) \,\}$. Then the topological interior

$$
\begin{aligned}
&\operatorname{int}(\mathcal{A}) \\
&= \{\, W \in 2^{\mathbb{P}} \mid \exists \sigma \subseteq W \, \forall V \in [\![\sigma]\!] \, [V \in \mathcal{A}] \,\} \\
&= \left\{ W \in 2^{\mathbb{P}} \;\middle|\; \exists n \forall t \exists k_1 \cdots Q k_n \left[\begin{array}{c} (t \text{ is a code for a string } \tau \supseteq W\restriction n) \\ \wedge \max\{k_2, k_4, \dots\} \leq |\tau| \\ \rightarrow \max\{k_1, k_3, \dots\} \leq |\tau| \\ \wedge R(\tau\restriction k_1, \dots, \tau\restriction k_n) \end{array} \right] \right\}
\end{aligned}
$$

is a Σ^0_{n+2} open set $\subseteq \mathcal{A}$. Since G is $(n+2)$-generic, we have $G \notin \partial\mathcal{A}$. Thus G is in the topological exterior $\operatorname{int}(\overline{\mathcal{A}}) = 2^{\mathbb{P}} - (\operatorname{int}(\mathcal{A}) \cup \partial\mathcal{A})$. Then $\mathcal{A}$ is not comeager since the complement $\overline{\mathcal{A}}$ contains a nonempty open subset $\operatorname{int}(\overline{\mathcal{A}}) \ni G$. The converse is clear. □

Similarly, there is a measure-theoretic counterpart of generic sets.

Definition 2.2.10. Let $n \in \omega$. A Σ^0_n *Martin-Löf test* is a sequence $(\mathcal{U}_i)_{i\in\omega}$ of uniformly Σ^0_n subsets of $2^{\mathbb{P}}$ such that $\mu(\mathcal{U}_i) \leq 2^{-i}$ for all $i \in \omega$. A set $W \in 2^{\mathbb{P}}$ is called *n-random* if $W \notin \bigcap_{i\in\omega} \mathcal{U}_i$ for every Σ^0_n Martin-Löf test $(\mathcal{U}_i)_{i\in\omega}$. A set $W \in 2^{\mathbb{P}}$ is called *arithmetically random* if it is n-random for every $n \in \omega$.

Since there are only countably many Σ^0_n Martin-Löf test and the intersection $\bigcap_{i\in\omega} \mathcal{U}_i$ of each Σ^0_n Martin-Löf test $(\mathcal{U}_i)_{i\in\omega}$ is of measure 0, the set of arithmetically random sets has measure 1 in $2^{\mathbb{P}}$.

Lemma 2.2.11. *An arithmetical subset $\mathcal{A} \subseteq 2^{\mathbb{P}}$ is of measure 1 if and only if it contains every arithmetically random set in $2^{\mathbb{P}}$.*

Proof. Suppose that $\mu(\mathcal{A}) = 1$. Since $\mathcal{A}$ is arithmetical, the complement $\overline{\mathcal{A}}$ is Σ^0_n subset for some $n \in \omega$. Then the constant sequence $(\overline{\mathcal{A}})_{i\in\omega}$ is a Σ^0_n Martin-Löf test, so $\overline{\mathcal{A}}$ contains no arithmetically random set. The converse is clear. □

Definition 2.2.12. A set $W \in 2^{\mathbb{P}}$ is called *generalized low*$_1$ if $W' \leq_{\mathrm{T}} W \oplus \emptyset'$. (Note that the opposite direction of the reduction always holds.) We write $\mathbf{GL}_1$ for the set of generalized low$_1$ sets.

2.3 Turing degrees of $\mathrm{HTP}(R_W)$ for typical W

Theorem 2.3.1. *Let θ be one of the following statements:*

$$\begin{array}{rrl}
\mathrm{HTP}(\mathbb{Q}) \leq_{\mathrm{T}} \emptyset, & \mathrm{HTP}(\mathbb{Q}) >_{\mathrm{T}} \emptyset, & (\textit{decidable or not}) \\
\mathrm{HTP}(\mathbb{Q}) \geq_{\mathrm{T}} \emptyset', & \mathrm{HTP}(\mathbb{Q}) <_{\mathrm{T}} \emptyset', & (\mathrm{T}\textit{-complete or not}) \\
\mathrm{HTP}(\mathbb{Q})^{(n)} \leq_{\mathrm{T}} \emptyset^{(n)}, & \mathrm{HTP}(\mathbb{Q})^{(n)} >_{\mathrm{T}} \emptyset^{(n)}, & (\textit{low}_n \textit{ or not}) \\
\mathrm{HTP}(\mathbb{Q})^{(n)} \geq_{\mathrm{T}} \emptyset^{(n+1)}, & \mathrm{HTP}(\mathbb{Q})^{(n)} <_{\mathrm{T}} \emptyset^{(n+1)}, & (\textit{high}_n \textit{ or not})
\end{array}$$

where $n > 0$. Let θ^W be the corresponding statement obtained by replacing $\emptyset$, $\mathrm{HTP}(\mathbb{Q})$ in θ by W, $\mathrm{HTP}(R_W)$ respectively (for example, $(\mathrm{HTP}(\mathbb{Q}) \leq_{\mathrm{T}} \emptyset)^W = (\mathrm{HTP}(R_W) \leq_{\mathrm{T}} W)$). If θ holds, then the set $\mathcal{X}_\theta := \{\, W \in 2^{\mathbb{P}} \mid \theta^W \,\}$ is comeager. In addition, $\mu(\mathcal{X}_\theta) = 1$ if $\mu(\mathbf{GL}^{\mathrm{HTP}}) = 1$.

This immediately gives the following corollary, which is a sort of zero-one law, or an analogue of the Łoś's theorem.

Corollary 2.3.2. *Let θ and $\mathcal{X}_\theta$ be as in Theorem 2.3.1. Then the following conditions are equivalent.*

(1) θ holds.

(2) $\mathcal{X}_\theta$ is comeager.

(3) $\mathcal{X}_\theta$ contains every generic set.

(4) $\mathcal{X}_\theta$ is not meager.

(5) $\mathcal{X}_\theta$ contains some generic set.

Moreover, if $\mu(\mathbf{GL}^{\mathrm{HTP}}) = 1$, then the conditions above are also equivalent to the following ones.

(6) $\mu(\mathcal{X}_\theta) = 1$.

(7) $\mathcal{X}_\theta$ contains every arithmetically random set.

(8) $\mu(\mathcal{X}_\theta) > 0$.

(9) $\mathcal{X}_\theta$ *contains some arithmetically random set.*

Proof. The implication ((1) $\Longrightarrow$ (2) $\wedge$ (6)) holds by Theorem 2.3.1. The implications ((2) $\Longrightarrow$ (4)) and ((6) $\Longrightarrow$ (8)) are trivial. Since $\mathcal{X}_\theta$ is arithmetical, the equivalences ((2) $\Longleftrightarrow$ (3)) and ((4) $\Longleftrightarrow$ (5)) hold by Lemma 2.2.9. Similarly, the equivalences ((6) $\Longleftrightarrow$ (7)) and ((8) $\Longleftrightarrow$ (9)) hold by Lemma 2.2.11. Finally, the implication ((4) $\vee$ (8) $\Longrightarrow$ (1)) is obtained by Theorem 2.3.1 for the negation $\neg\theta$. □

To simplify the proof of Theorem 2.3.1, we introduce a notation for "almost all" reducibility.

Definition 2.3.3. Let $t_1(W)$ and $t_2(W)$ be terms representing a set in $2^{\mathbb{P}}$. Then we write $t_1(W) \leq^*_{\mathrm{T}} t_2(W)$ if the set $\{\, W \in 2^{\mathbb{P}} \mid t_1(W) \leq_{\mathrm{T}} t_2(W) \,\}$ is comeager of measure 1. Similarly, we write $t_1(W) <^*_{\mathrm{T}} t_2(W)$ if the set $\{\, W \in 2^{\mathbb{P}} \mid t_1(W) <_{\mathrm{T}} t_2(W) \,\}$ is comeager of measure 1.

Lemma 2.3.4. *The following relations hold.*

(1) *If* $\mu(\mathbf{GL}^{\mathrm{HTP}}) = 1$, *then* $\mathrm{HTP}(R_W) \leq^*_{\mathrm{T}} W \oplus \mathrm{HTP}(\mathbb{Q})$.

(2) $W' \leq^*_{\mathrm{T}} W \oplus \emptyset'$.

(3) $(W \oplus A)' \leq^*_{\mathrm{T}} W \oplus A'$ *for any set* $A \in 2^{\mathbb{P}}$. *Moreover,* $(W \oplus A)^{(n)} \leq^*_{\mathrm{T}} W \oplus A^{(n)}$.

(4) *If* $A <_{\mathrm{T}} B$, *then* $W \oplus A <^*_{\mathrm{T}} W \oplus B$.

Proof.

(1) By definition of $\mathbf{GL}^{\mathrm{HTP}}$.

(2) This reduction holds on the set $\mathbf{GL}_1$ of generalized low_1 sets. It is known that $\mathbf{GL}_1$ is comeager of measure 1 (see e.g. [Mil16, Lemma 1] and [Mil18, Lemma 2.1]).

(3) Relativize the proof for $\mathbf{GL}_1$ to A. The moreover part follows from induction on n.

(4) Suppose $A <_{\mathrm{T}} B$. Then, it is known that the set $\mathcal{C} := \{ W \in 2^{\mathbb{P}} \mid A \oplus W \geq_{\mathrm{T}} B \}$ is meager of measure 0 (see e.g. [Mil16, Lemma 2] and [Mil18, Lemma 2.3]). Thus the set $\{ W \in 2^{\mathbb{P}} \mid W \oplus A \geq_{\mathrm{T}} W \oplus B \} \subseteq \mathcal{C}$ is also meager of measure 0. □

Proof of Theorem 2.3.1. The proof proceeds with Lemma 2.3.4 as follows.

- If $\mathrm{HTP}(\mathbb{Q}) \leq_{\mathrm{T}} \emptyset$, then
$$\mathrm{HTP}(R_W) \leq^*_{\mathrm{T}} W \oplus \mathrm{HTP}(\mathbb{Q}) \leq_{\mathrm{T}} W.$$
- If $\emptyset <_{\mathrm{T}} \mathrm{HTP}(\mathbb{Q})$, then
$$W \leq_1 W \oplus \emptyset <^*_{\mathrm{T}} W \oplus \mathrm{HTP}(\mathbb{Q}) \leq_1 \mathrm{HTP}(R_W).$$
- If $\emptyset' \leq_{\mathrm{T}} \mathrm{HTP}(\mathbb{Q})$, then
$$W' \leq^*_{\mathrm{T}} W \oplus \emptyset' \leq_{\mathrm{T}} W \oplus \mathrm{HTP}(\mathbb{Q}) \leq_1 \mathrm{HTP}(R_W).$$
- If $\mathrm{HTP}(\mathbb{Q}) <_{\mathrm{T}} \emptyset'$, then
$$\mathrm{HTP}(R_W) \leq^*_{\mathrm{T}} W \oplus \mathrm{HTP}(\mathbb{Q}) <^*_{\mathrm{T}} W \oplus \emptyset' \leq_1 W'.$$
- If $\mathrm{HTP}(\mathbb{Q})^{(n)} \leq_{\mathrm{T}} \emptyset^{(n)}$, then
$$\begin{aligned}\mathrm{HTP}(R_W)^{(n)} &\leq^*_{\mathrm{T}} (W \oplus \mathrm{HTP}(\mathbb{Q}))^{(n)} \leq^*_{\mathrm{T}} W \oplus \mathrm{HTP}(\mathbb{Q})^{(n)} \\ &\leq_{\mathrm{T}} W \oplus \emptyset^{(n)} \leq_1 W^{(n)}.\end{aligned}$$
- If $\emptyset^{(n)} <_{\mathrm{T}} \mathrm{HTP}(\mathbb{Q})^{(n)}$, then
$$\begin{aligned}W^{(n)} &\leq^*_{\mathrm{T}} (W \oplus \emptyset')^{(n-1)} \leq^*_{\mathrm{T}} W \oplus \emptyset^{(n)} \\ &<^*_{\mathrm{T}} W \oplus \mathrm{HTP}(\mathbb{Q})^{(n)} \leq_1 \mathrm{HTP}(R_W)^{(n)}.\end{aligned}$$
- If $\emptyset^{(n+1)} \leq_{\mathrm{T}} \mathrm{HTP}(\mathbb{Q})^{(n)}$, then
$$\begin{aligned}W^{(n+1)} &\leq^*_{\mathrm{T}} (W \oplus \emptyset')^{(n)} \leq^*_{\mathrm{T}} W \oplus \emptyset^{(n+1)} \\ &\leq_{\mathrm{T}} W \oplus \mathrm{HTP}(\mathbb{Q})^{(n)} \leq_1 \mathrm{HTP}(R_W)^{(n)}.\end{aligned}$$

- If $\mathrm{HTP}(\mathbb{Q})^{(n)} <_{\mathrm{T}} \emptyset^{(n+1)}$, then

$$\begin{aligned}\mathrm{HTP}(R_W)^{(n)} &\leq^*_{\mathrm{T}} (W \oplus \mathrm{HTP}(\mathbb{Q}))^{(n)} \leq^*_{\mathrm{T}} W \oplus \mathrm{HTP}(\mathbb{Q})^{(n)} \\ &<^*_{\mathrm{T}} W \oplus \emptyset^{(n+1)} \leq_1 W^{(n+1)}.\end{aligned}$$

□

Theorem 2.3.1 generalizes Theorem 1 and Proposition 1 in [Mil20]. Moreover, it follows from Theorem 2.3.1 that HTP cannot be a positive instance for Question 1 in [Mil20]:

Corollary 2.3.5. *The operator* HTP *does not satisfy Question* 1 *in* [Mil20] *for Baire category (also for Lebesgue measure if* $\mu(\mathbf{GL}^{\mathrm{HTP}}) = 1$*).*

Proof. Suppose that HTP is non-coding for Baire category (see [Mil20, Definition 2] for the definition of non-coding operators). Then for every non-computable set C, the set $\{ W \in 2^{\mathbb{P}} \mid C \leq_{\mathrm{T}} \mathrm{HTP}(R_W) \}$ is meager. So it follows from [Mil16, Corollary 1] that $\mathrm{HTP}(\mathbb{Q}) \equiv_{\mathrm{T}} \emptyset$. Then Theorem 2.3.1 yields that the set $\{ W \in 2^{\mathbb{P}} \mid \mathrm{HTP}(R_W) \leq_{\mathrm{T}} W \}$ is comeager. The proof for Lebesgue measure is similar. □

Related to Theorem 2.3.1, we pose the following question:

Question 2.3.6. Is it possible that $\emptyset <_{\mathrm{T}} \mathrm{HTP}(\mathbb{Q}) <_{\mathrm{T}} \emptyset'$?

Suppose that the answer to Question 2.3.6 is positive. Then it follows from Theorem 2.3.1 that there exist comeager many sets $W \in 2^{\mathbb{P}}$ such that $W <_{\mathrm{T}} \mathrm{HTP}(R_W) <_{\mathrm{T}} W'$. By Remark 2.2.7, we conclude that HTP is a *degree invariant uniform solution to Post's problem* on a comeager subset of $2^{\mathbb{P}}$. On the other hand, Lachlan [Lac75] showed that there is no degree invariant uniform solution to Post's problem entirely defined on the Cantor space.

Remark 2.3.7. By Lemma 2.2.6, The assumption $\mu(\mathbf{GL}^{\mathrm{HTP}}) = 1$ in Theorem 2.3.1 is weaker than the condition $\mu(\overline{\mathcal{B}}) = 1$. Moreover, it is possible that $\mu(\mathbf{GL}^{\mathrm{HTP}} - \overline{\mathcal{B}}) = 1$. We will discuss this point in section 2.5.1.

2.4 Comeagerness and Banach–Mazur game

Banach–Mazur game is an infinite game played by two persons, Player I and Player II. For a subset $\mathcal{A}$ of $2^{\mathbb{P}}$, the *Banach–Mazur game* for $\mathcal{A}$, denoted by $\mathrm{BM}(\mathcal{A})$, is defined as follows. First, Player I chooses a binary string $\sigma_0 \in 2^{<\mathbb{P}}$.

Then Player II chooses $\sigma_1 \in 2^{<\mathbb{P}}$ such that $\sigma_0 \subsetneq \sigma_1$. For given $\sigma_{2i-1} \in 2^{<\mathbb{P}}$ ($i \geq 1$), Player I chooses $\sigma_{2i} \in 2^{<\mathbb{P}}$ such that $\sigma_{2i-1} \subsetneq \sigma_{2i}$ and then Player II chooses $\sigma_{2i+1} \in 2^{<\mathbb{P}}$ such that $\sigma_{2i} \subsetneq \sigma_{2i+1}$. Player I wins $\mathrm{BM}(\mathcal{A})$ if the resulting point $W = \bigcup_{n\in\omega} \sigma_n$ of $2^{\mathbb{P}}$ belongs to $\mathcal{A}$. Player II wins otherwise.

Definition 2.4.1. A *strategy* for Player I is a map $\alpha\colon \bigcup_{i\in\omega}(2^{<\mathbb{P}})^{2i} \to 2^{<\mathbb{P}}$ such that $\alpha(\sigma_0, \dots, \sigma_{2i-1}) \supseteq \sigma_{2i-1}$ for any finite sequence $(\sigma_0, \dots, \sigma_{2i-1})$ of even length, where $\sigma_{-1} := \emptyset$. Similarly, a strategy for Player II is also defined as a map $\beta\colon \bigcup_{i\in\omega}(2^{<\mathbb{P}})^{2i+1} \to 2^{<\mathbb{P}}$. A strategy $\alpha\colon \bigcup_{i\in\omega}(2^{<\mathbb{P}})^{2i} \to 2^{<\mathbb{P}}$ for Player I is a *Markov strategy* if there is a map $\tilde{\alpha}\colon 2^{<\mathbb{P}} \times \omega \to 2^{<\mathbb{P}}$ such that $\alpha = \tilde{\alpha} \circ ((\sigma_0, \dots, \sigma_{2i-1}) \mapsto (\sigma_{2i-1}, 2i \dot{-} 1))$. We also say that $\tilde{\alpha}$ is a Markov strategy. Markov strategies for Player II are defined in similar manner. The *play* $\alpha * \beta$ for strategies α and β is the resulting set $W = \bigcup_{n\in\omega} \sigma_n$ when Player I follows α and Player II follows β. A strategy α for Player I is called a *winning strategy* for $\mathrm{BM}(\mathcal{A})$ if $\alpha * \beta \in \mathcal{A}$ for any strategy β for Player II. Similarly, a strategy β for Player II is a winning strategy for $\mathrm{BM}(\mathcal{A})$ if $\alpha * \beta \notin \mathcal{A}$ for any strategy α for Player I.

Proposition 2.4.2. *For every set $\mathcal{A} \subseteq 2^{\mathbb{P}}$, the following properties hold.*

(1) If $\mathcal{A}$ is comeager, then Player I *has a Markov winning strategy for* $\mathrm{BM}(\mathcal{A})$.

(2) If $\mathcal{A}$ is meager, then Player II *has a Markov winning strategy for* $\mathrm{BM}(\mathcal{A})$.

Proof. Suppose that $\mathcal{A}$ is comeager. Then there exists a countable family $(\mathcal{U}_n)_{n\in\omega}$ of dense open sets in $2^{\mathbb{P}}$ such that $\bigcap_{n\in\omega} \mathcal{U}_n \subseteq \mathcal{A}$. Define a Markov strategy $\alpha\colon 2^{<\mathbb{P}} \times \omega \to 2^{<\mathbb{P}}$ as follows. For given $(\sigma, 2i \dot{-} 1) \in 2^{<\mathbb{P}} \times \omega$, the intersection $[\![\sigma]\!] \cap \mathcal{U}_i$ is a nonempty open set since $\mathcal{U}_i$ is dense. Thus there exists $\tau \supsetneq \sigma$ such that $[\![\tau]\!] \subseteq [\![\sigma]\!] \cap \mathcal{U}_i$. Define $\alpha(\sigma, 2i \dot{-} 1) := \tau$, and then clearly α is a winning strategy for $\mathrm{BM}(\mathcal{A})$. The proof for the latter case is similar. □

Corollary 2.4.3. *Let θ and $\mathcal{X}_\theta$ be as in Theorem 2.3.1. The game* $\mathrm{BM}(\mathcal{X}_\theta)$ *is determined, i.e., either Player* I *or Player* II *has a winning strategy for* $\mathrm{BM}(\mathcal{X}_\theta)$.

Note that this is also deducible from the fact that every Borel set has the Baire property.

2.4.1 Constructing HTP-generic sets via the Banach–Mazur game

The following proposition generalizes [EMPS17, Proposition 3.1] in terms of Banach–Mazur game.

Proposition 2.4.4. *For a string $\tau \in 2^{<\mathbb{P}}$ and a real number $r \in [0,1)$ which is computably approximable from above, there exists a set $W \in 2^{\mathbb{P}}$ such that*

(1) $\tau \subseteq W$.

(2) $W \leq_{\mathrm{T}} \mathrm{HTP}(\mathbb{Q})$.

(3) W *is HTP-generic.*

(4) $\mathrm{HTP}(R_W) \leq_{\mathrm{T}} \mathrm{HTP}(\mathbb{Q})$.

(5) The lower density of W *is* r*, i.e.,*

$$\liminf_{n\to\infty} \frac{|W \cap \{p_0, p_1, \dots, p_{n-1}\}|}{n} = r$$

where p_i denotes ith prime number.

In particular, W is a coinfinite set such that $\mathrm{HTP}(R_W) \equiv_{\mathrm{T}} \mathrm{HTP}(\mathbb{Q})$.

Proof. Recall that we have fixed a computable enumeration $(f_i)_{i\in\omega}$ of the polynomials in $\mathbb{Z}[X_1, X_2, \dots]$. Let $(q_i)_{i\in\omega}$ be a computable decreasing sequence of rational numbers such that $\lim_{i\to\infty} q_i = r$. Now each player follows the following Markov strategies.

(1) Define $\alpha(\sigma, 0) := \tau$. For given $(\sigma, 2i+1) \in 2^{<\mathbb{P}} \times \omega$, Player I checks whether $f_i \in \mathrm{HTP}(R_{\sigma^\frown 1^\infty})$. If so, take a solution $\bar{x} \in (R_{\sigma^\frown 1^\infty})^{<\omega}$ of $f_i = 0$. Let $m > 0$ be the minimum number such that $\bar{x} \in (R_{\sigma^\frown 1^m 0^\infty})^{<\omega}$. Then Player I chooses $\alpha(\sigma, 2i+1) := \sigma^\frown 1^m$ so that $[\![\alpha(\sigma, 2i+1)]\!] \cap \mathcal{B}(f_i) = \emptyset$. If $f_i \notin \mathrm{HTP}(R_{\sigma^\frown 1^\infty})$, define $\alpha(\sigma, 2i+1) := \sigma^\frown 1^{i+1}$.

(2) For given $(\sigma, 2i) \in 2^{<\mathbb{P}} \times \omega$, let $m > 0$ be the minimum number such that

$$\frac{|\sigma^\frown 0^m|_1}{|\sigma^\frown 0^m|} \leq q_i + 2^{-i}$$

where $|\sigma^\frown 0^m|_1$ denotes the number of 1's occurring in $\sigma^\frown 0^m$. Then Player II chooses $\beta(\sigma, 2i) := \sigma^\frown 0^m$.

The play $W := \alpha * \beta$ is computable in $\mathrm{HTP}(\mathbb{Q})$ since the both strategies are computable in $\mathrm{HTP}(\mathbb{Q})$ by Lemma 2.2.1.(3). The HTP-genericity of W follows from α. Then it follows from Lemma 2.2.6 that $\mathrm{HTP}(R_W) \leq_{\mathrm{T}} W \oplus \mathrm{HTP}(\mathbb{Q}) \leq_{\mathrm{T}} \mathrm{HTP}(\mathbb{Q})$. The lower density of W is r because of β. □

The following corollary follows immediately from the construction above.

Corollary 2.4.5. *Player* I *(resp. Player* II*) has an* $\mathrm{HTP}(\mathbb{Q})$*-computable Markov winning strategy for* $\mathrm{BM}(\overline{\mathcal{B}})$ *(resp.* $\mathrm{BM}(\mathcal{B})$*).*

2.4.2 Characterizing undecidability of $\mathrm{HTP}(\mathbb{Q})$ via the Banach–Mazur game

Theorem 2.4.6. *Let* $\mathcal{N} := \{ W \in 2^{\mathbb{P}} \mid \mathrm{HTP}(R_W) >_{\mathrm{T}} W \}$*. The following conditions are equivalent.*

(1) $\mathrm{HTP}(\mathbb{Q}) >_{\mathrm{T}} \emptyset$*, i.e.,* $\mathrm{HTP}(\mathbb{Q})$ *is undecidable.*

(2) $\mathcal{N}$ *contains every* 1*-generic set.*

(3) $\mathcal{N}$ *is comeager.*

(4) Player I *has a Markov winning strategy for* $\mathrm{BM}(\mathcal{N})$*.*

(5) Player II *does not have a winning strategy for* $\mathrm{BM}(\mathcal{N})$*.*

(6) For every index $e \in \omega$*, Player* II *does not have a computable Markov winning strategy for* $\mathrm{BM}(\{ W \in 2^{\mathbb{P}} \mid \mathrm{HTP}(R_W) \neq \Phi_e^W \})$*.*

(7) $\mathcal{N}$ *is not meager.*

(8) $\mathcal{N}$ *contains some* 1*-generic set.*

(9) $\overline{\mathcal{B}} \cap \mathcal{N} \neq \emptyset$*, i.e.,* $\mathcal{N}$ *contains some HTP-generic set.*

Proof. Although some of the conditions above have been already seen to be equivalent, we give full proof here.

((1) $\Longrightarrow$ (2)) Contrary, suppose that there exists a 1-generic set W such that $\mathrm{HTP}(R_W) \leq_{\mathrm{T}} W$. Then we have $\mathrm{HTP}(\mathbb{Q}) \leq_1 \mathrm{HTP}(R_W) \leq_{\mathrm{T}} W$. On the other hand, 1-generic set does not compute any noncomputable c.e. set (see e.g. [Soa16, Exercise 6.3.5 (iii)]), so $\mathrm{HTP}(\mathbb{Q})$ must be decidable.

((2) $\Longrightarrow$ (3)) By comeagerness of 1-generic sets.

((3) $\Longrightarrow$ (4)) By Proposition 2.4.2.(1).

((4) $\Longrightarrow$ (5) $\Longrightarrow$ (6)) By definition of winning strategies and $\mathcal{N}$.

((6) $\Longrightarrow$ (1)) Suppose that $\mathrm{HTP}(\mathbb{Q})$ is decidable. Then, by Lemma 2.2.6 there exists an index $e \in \omega$ such that $\mathrm{HTP}(R_W) = \Phi_e^W$ for all HTP-generic set W. By Corollary 2.4.5, there exists a $\mathrm{HTP}(\mathbb{Q})$-computable Markov winning strategy for Player II for $\mathrm{BM}(\mathcal{B})$. Thus it is a computable Markov winning strategy for Player II for $\mathrm{BM}(\{\, W \in 2^{\mathbb{P}} \mid \mathrm{HTP}(R_W) \neq \Phi_e^W \,\})$.

((5) $\Longrightarrow$ (7)) By Proposition 2.4.2.(2).

((7) $\Longrightarrow$ (8)) In general, the intersection of a comeager set and a non-meager set is not empty.

((8) $\Longrightarrow$ (9)) Since every 1-generic set is also HTP-generic.

((9) $\Longrightarrow$ (1)) Let $W \in \overline{\mathcal{B}} \cap \mathcal{N}$. Then we have $W <_{\mathrm{T}} \mathrm{HTP}(R_W) \leq_{\mathrm{T}} W \oplus \mathrm{HTP}(\mathbb{Q})$, so $\mathrm{HTP}(\mathbb{Q})$ must be undecidable. □

In particular, to prove undecidability of $\mathrm{HTP}(\mathbb{Q})$, it suffices to show that for every $e \in \omega$ and computable Markov strategy β, there exists a (possibly noncomputable) strategy α which forces $W := \alpha * \beta$ to satisfy $\mathrm{HTP}(R_W) \neq \Phi_e^W$.

2.5 Some consequences of Diophantineness of $\mathbb{Z}$ in $\mathbb{Q}$

In this section, we collect some interesting facts that can be deduced from Diophantineness of $\mathbb{Z}$ in $\mathbb{Q}$.

2.5.1 Difference between $\overline{\mathcal{B}}$ and $\mathbf{GL}^{\mathrm{HTP}}$

Here we see the difference between two conditions $\mu(\overline{\mathcal{B}}) = 1$ and $\mu(\mathbf{GL}^{\mathrm{HTP}}) = 1$, as we noted in Remark 2.3.7.

Lemma 2.5.1. *It holds that* $\emptyset' \leq_{\mathrm{T}} \mathrm{HTP}(\mathbb{Q})$ *if and only if* $\mathbf{GL}_1 \subseteq \mathbf{GL}^{\mathrm{HTP}}$. *In particular,* $\emptyset' \leq_{\mathrm{T}} \mathrm{HTP}(\mathbb{Q})$ *implies* $\mu(\mathbf{GL}^{\mathrm{HTP}}) = 1$.

Proof. Suppose $\emptyset' \leq_{\mathrm{T}} \mathrm{HTP}(\mathbb{Q})$ and let $W \in \mathbf{GL}_1$. Then we have $\mathrm{HTP}(R_W) \leq_1 W' \leq_{\mathrm{T}} W \oplus \emptyset' \leq_{\mathrm{T}} W \oplus \mathrm{HTP}(\mathbb{Q})$ and $W \in \mathbf{GL}^{\mathrm{HTP}}$. If $\mathrm{HTP}(\mathbb{Q}) <_{\mathrm{T}} \emptyset'$, then we have $\mathrm{HTP}(\mathbb{Z}) \not\leq_{\mathrm{T}} \emptyset \oplus \mathrm{HTP}(\mathbb{Q})$ and $\emptyset \in \mathbf{GL}_1 - \mathbf{GL}^{\mathrm{HTP}}$. The latter follows from the fact that $\mu(\mathbf{GL}_1) = 1$. □

Proposition 2.5.2. *If* $\mathbb{Z}$ *is Diophantine in* $\mathbb{Q}$, *then* $\mu(\mathbf{GL}^{\mathrm{HTP}} - \overline{\mathcal{B}}) = 1$.

Proof. Since the assumption implies $\emptyset' \leq_1 \mathrm{HTP}(\mathbb{Q})$, Lemma 2.5.1 yields $\mu(\mathbf{GL}^{\mathrm{HTP}}) = 1$. By [Mil19, Theorem 6.7], Diophantineness of $\mathbb{Z}$ in $\mathbb{Q}$ also implies $\mu(\overline{\mathcal{B}}) = 0$. □

2.5.2 HTP-genericity implies cohyperimmunity

Definition 2.5.3. For a subset $\mathcal{X} \subseteq 2^{\mathbb{P}}$, we say that $\mathcal{X}$ is *upward closed* if $\mathcal{X} \ni U \subseteq V$ implies $V \in \mathcal{X}$.

Lemma 2.5.4. *Suppose that* $\mathbb{Z}$ *is Diophantine in* $\mathbb{Q}$. *For every upward closed* Σ^0_1 *subset* $\mathcal{X} \subseteq 2^{\mathbb{P}}$, *there exists a polynomial* $f \in \mathbb{Z}[X_1, X_2, \dots]$ *such that* $\mathcal{A}(f) = \mathcal{X}$. *Moreover, such* f *is uniformly computable from the code for* $\mathcal{X}$.

Proof. Let $S \subseteq 2^{<\mathbb{P}}$ be a c.e. set of strings such that $\mathcal{X} = \bigcup_{\sigma \in S} [\![\sigma]\!]$. Put $C := \{ \prod_{p \in \sigma^{-1}(1)} p \mid \sigma \in S \}$. Since C is a c.e. subset of $\mathbb{Z}$, [Mil19, Lemma 6.1] yields a polynomial $g(X, \bar{Y})$ such that $C = \{ a \in R_W \mid \exists \bar{b} \in R_W^{<\omega} [g(a, \bar{b}) = 0] \}$ for every $W \in 2^{\mathbb{P}}$. Put $f(X, \bar{Y}, T) := g(X, \bar{Y})^2 + (XT - 1)^2$. Then we have

$$\begin{aligned} W \in \mathcal{A}(f) &\iff f \in \mathrm{HTP}(R_W) \\ &\iff \exists a \in C [1/a \in R_W] \\ &\iff \exists \sigma \in S [\sigma^{-1}(1) \subseteq W] \\ &\iff \exists \sigma \in S [\sigma \subseteq W] \qquad \text{(by upward closedness of } \mathcal{X}) \\ &\iff W \in \mathcal{X}. \end{aligned}$$

□

Definition 2.5.5. For $n \in \omega$, let D_n denotes the finite subset of $\mathbb{P}$ uniquely coded by n. (for example, one may use the code satisfying $n = \sum_{i \in D_n} 2^i$ for every n.) A sequence $(F_n)_{n \in \omega}$ of finite subsets of $\mathbb{P}$ is called *strong array* if there exists a computable function $h \colon \omega \to \omega$ such that $F_n = D_{h(n)}$. A strong array $(F_n)_{n \in \omega}$ is called *disjoint* if $F_m \cap F_n = \emptyset$ whenever $m \neq n$. A set

$W \in 2^{\mathbb{P}}$ is called *hyperimmune* if it is infinite and for every disjoint strong array $(F_n)_{n\in\omega}$, there exists some n such that $W \cap F_n = \emptyset$. A set $W \in 2^{\mathbb{P}}$ is called *cohyperimmune* if its complement $\overline{W}$ is hyperimmune. A set $W \in 2^{\mathbb{P}}$ is called *hypersimple* if it is c.e. and cohyperimmune.

Theorem 2.5.6. *Suppose that $\mathbb{Z}$ is Diophantine in $\mathbb{Q}$. Then every HTP-generic set $W \in \overline{\mathcal{B}}$ is either cofinite or cohyperimmune.*

Proof. Let W be a coinfinite set. Let $(F_n)_{n\in\omega}$ be a disjoint strong array such that $F_n = D_{h(n)}$ for some computable function $h\colon \omega \to \omega$. Put $\mathcal{X}_h := \{\, W \in 2^{\mathbb{P}} \mid \exists n \in \omega[W \supseteq F_n] \,\}$. Since $\mathcal{X}_h$ is an upward closed Σ^0_1 set, it follows from Lemma 2.5.4 that there exists a polynomial $f_h \in \mathbb{Z}[X_1, X_2, \dots]$ such that $\mathcal{A}(f_h) = \mathcal{X}_h$. Since $\mathcal{X}_h$ is dense in $2^{\mathbb{P}}$, we have $\mathcal{C}(f_h) = \emptyset$. Thus we have

$$\begin{aligned}
\overline{W} \text{ is hyperimmune} &\iff \forall (F_n)_n \exists n[F_n \cap \overline{W} = \emptyset] \\
&\iff \forall (F_n)_n \exists n[F_n \subseteq W] \\
&\iff \forall h[W \in \mathcal{X}_h] \\
&\iff W \in \bigcap_h \mathcal{A}(f_h)
\end{aligned}$$

and

$$W \notin \mathcal{B} \implies W \notin \bigcup_h \mathcal{B}(f_h) \iff W \in \bigcap_h \mathcal{A}(f_h) \iff \overline{W} \text{ is hyperimmune.}$$

□

Corollary 2.5.7 ([Mil19, Theorem 6.7])**.** *If $\mathbb{Z}$ is Diophantine in $\mathbb{Q}$, then $\mu(\mathcal{B}) = 1$.*

Proof. Since the set of hyperimmune sets is of measure 0 (see e.g. [DH10, Theorem 9.14.15]). □

Corollary 2.5.8. *If $\mathbb{Z}$ is Diophantine in $\mathbb{Q}$, then the following properties hold.*

(1) There is no coinfinite computable HTP-generic set.

(2) Every coinfinite c.e. HTP-generic set is hypersimple.

(3) Every coinfinite HTP-generic set has upper density 1*.*

In particular, the question in [EMPS17, Remark 3.20] *cannot be solved by constructing an HTP-generic set, and each c.e. set $\mathcal{S} \in 2^{\mathbb{P}}$ constructed in* [EMPS17, Theorem 3.18 and Theorem 4.1] *is hypersimple and has upper density* 1*.*

2.5.3 Size of $\mathbf{GL}_e^{\mathrm{HTP}}$

By Lemma 2.2.6, there exists some $i \in \omega$ such that $\mathbf{GL}_i^{\mathrm{HTP}}$ is comeager, while it follows from Proposition 2.5.2 that there exists $j \in \omega$ such that $\mu(\mathbf{GL}_j^{\mathrm{HTP}}) > 0$. However, these properties cannot hold simultaneously.

Proposition 2.5.9. *Suppose that $\mathbb{Z}$ is Diophantine in $\mathbb{Q}$. Let $e \in \omega$. If $\mathbf{GL}_e^{\mathrm{HTP}}$ is dense, then $\mu(\mathbf{GL}_e^{\mathrm{HTP}}) = 0$.*

In other words, if there exists $e \in \omega$ such that $\mathbf{GL}_e^{\mathrm{HTP}}$ is dense and $\mu(\mathbf{GL}_e^{\mathrm{HTP}}) > 0$, then $\mathbb{Z}$ is not Diophantine in $\mathbb{Q}$. Note that $\mathbf{GL}_e^{\mathrm{HTP}}$ is dense if and only if it is comeager since $\overline{\mathbf{GL}_e^{\mathrm{HTP}}}$ is Σ^0_2. It is known that Proposition 2.5.9 holds for $\mathbf{GL}_1$ without the Diophantineness assumption.

Proof. Suppose that $m := \mu(\mathbf{GL}_e^{\mathrm{HTP}}) > 0$. It follows from the proof of [Mil19, Theorem 6.7] that there exists a polynomial $f \in \mathbb{Z}[X_1, X_2, \dots]$ such that $1 - m < \mu(\mathcal{B}(f)) < 1$ and $\mathcal{A}(f)$ is dense. Hence there exists a set $W \in \mathcal{B}(f) \cap \mathbf{GL}_e^{\mathrm{HTP}}$. Then there exists some $n \in \omega$ such that $\mathrm{HTP}(R_W)(f) = \Phi_e^{W\upharpoonright n \oplus \mathrm{HTP}(\mathbb{Q})}(f)\downarrow = 0$. Since every $V \in [\![W\upharpoonright n]\!] \cap \mathcal{A}(f)$ satisfies $\Phi_e^{V \oplus \mathrm{HTP}(\mathbb{Q})}(f)\downarrow = 0$ and $\mathrm{HTP}(R_V)(f) = 1$, we have $[\![W\upharpoonright n]\!] \cap \mathcal{A}(f) \subseteq \overline{\mathbf{GL}_e^{\mathrm{HTP}}}$. Since $\mathcal{A}(f)$ is a dense open set, $[\![W\upharpoonright n]\!] \cap \mathcal{A}(f)$ is a nonempty open set. Thus $\mathbf{GL}_e^{\mathrm{HTP}}$ is not dense. □

Chapter 3

Groups whose Word Problem is Accepted by an Abelian G-automaton

3.1 Introduction

For a group G, a *G-automaton* is a finite automaton augmented with a register that stores an element of G. Such an automaton first initializes the register with the identity element 1_G of G and may update the register content by multiplying by an element of G during the computation. The automaton accepts an input word if the automaton can reach a terminal state and the register content is 1_G when the entire word is read. (For the precise definition, see Section 3.2.4.) For a positive integer n, $\mathbb{Z}^n$-automata are the same as *blind n-counter automata*, which were defined and studied by Greibach [Gre75, Gre78].

The notion of G-automata is discovered repeatedly by several different authors. The name "G-automaton" is due to Kambites [Kam06]. (In fact, they defined the notion of M-automata for any monoid M.) Dassow–Mitrana [DM00] and Mitrana–Stiebe [MS01] use *extended finite automata* (EFA) over G instead of G-automata.

For a finitely generated group G, the *word problem* of G, with respect to a fixed finite generating set of G, is the set of words over the generating set representing the identity element of G (see Section 3.2.2 for the precise definitions). For several language classes, the class of finitely generated groups

whose word problem is in the class is determined [Anī72, MS83, BH74, Hig61, EKO08, HOT08, NT15], and many attempts are made for other language classes [Bro14, CSCF+15, HRRT05, GMS22, KS12, HR06, KS19, GKS18]. One of the most remarkable theorems about word problems is the well-known result due to Muller and Schupp [MS83], which states that, with the theorem by Dunwoody [Dun85], a group has a context-free word problem if and only if it is virtually free. These theorems suggest deep connections between group theory and formal language theory.

Involving both G-automata and word problems, the following broad question was posed implicitly by Elston and Ostheimer [EO04] and explicitly by Kambites [Kam06].

Question 3.1.1. For a given group G, is there any connection between the structural property of G and of the collection of groups whose word problems are accepted by *non-deterministic* G-automata?

Note that by G-automata, we always mean non-deterministic G-automata. As for *deterministic* G-automata, the following theorem is known.

Theorem 3.1.2 (Kambites [Kam06, Theorem 1], 2006)**.** *Let G and H be groups with H finitely generated. Then the word problem of H is accepted by a* deterministic *G-automaton if and only if H has a finite index subgroup which embeds in G.*

For non-deterministic G-automata, several results are known for specific types of groups. For a free group F of rank ≥ 2, it is known that a language is accepted by an F-automaton if and only if it is context-free [CS63, Proposition 2; Cor05, Corollary 4.5; Kam09, Theorem 7]. Combining with the Muller–Schupp theorem, the class of groups whose word problems are accepted by F-automata is the class of virtually free groups. The class of groups whose word problems are accepted by $(F \times F)$-automata is exactly the class of recursively presentable groups [Cor05, Corollary 3.5; Kam09, Theorem 8; MS01, Theorem 10]. For the case where G is (virtually) abelian, the following result was shown by Elder, Kambites, and Ostheimer.

Theorem 3.1.3 (Elder, Kambites, and Ostheimer [EKO08], 2008)**.**

(1) Let H be a finitely generated group and n be a positive integer. Then the word problem of H is accepted by a $\mathbb{Z}^n$-automaton if and only if H is virtually free abelian of rank at most n [EKO08, Theorem 1].

(2) *Let G be a virtually abelian group and H be a finitely generated group. Then the word problem of H is accepted by a G-automaton if and only if H has a finite index subgroup which embeds in G* [EKO08, Theorem 4].

However, their proof is somewhat indirect in the sense that it depends on a deep theorem by Gromov [Gro81], which states that every finitely generated group with polynomial growth function is virtually nilpotent. In fact, their proof proceeds as follows. Let H be a group whose word problem is accepted by a $\mathbb{Z}^n$-automaton. They first develop some techniques to compute several bounds for linear maps and semilinear sets. Then a map from H to $\mathbb{Z}^n$ with certain geometric conditions is constructed to prove that H has polynomial growth function. By Gromov's theorem, H is virtually nilpotent. Finally, they conclude that H is virtually abelian, using some theorems about nilpotent groups and semilinear sets. Because of the indirectness of their proof, the embedding in Theorem 3.1.3 (2) is obtained only *a posteriori* and hence has no relation with the combinatorial structure of the G-automaton.

To our knowledge, there are almost no attempts so far to obtain explicit algebraic connections between G and H, where H is a group that has a word problem accepted by a G-automaton. The only exception is the result due to Holt, Owens, and Thomas [HOT08, Theorem 4.2], where they gave a combinatorial proof to a special case of Theorem 3.1.3 (1), for the case where $n = 1$. (In fact, their theorem is slightly stronger than Theorem 3.1.3 (1) for $n = 1$ because it is for *non-blind* one-counter automata. See also [EKO08, Section 7].)

In this paper, we give a new, elementary, and purely combinatorial proof to Theorem 3.1.3. Our proof in Section 3.3 proceeds as follows. Suppose that the word problem of a finitely generated group H is accepted by an abelian G-automaton A. We first prove that there exist only finitely many *minimal accepting paths* in A. For each vertex p of A and each minimal accepting path μ in A, we then define a set $M(\mu, p)$ of closed paths that is *pumpable* in μ and starts from p, and we then prove that each $M(\mu, p)$ forms a monoid. With this terminology, our main result is:

Theorem 3.1.4. *Let G be an abelian group and H be a finitely generated group. Suppose that the word problem of H is accepted by a G-automaton A. The finite collection of monoids $(M(\mu, p))_{\mu,p}$ defined in* Definition 3.3.6 *satisfies that*

(1) each $M(\mu, p)$ induces a group homomorphism $\tilde{f}_{\mu,p}$ from a subgroup $G(\mu, p)$ of G onto a subgroup $H(\mu, p)$ of H, and

(2) at least one of $H(\mu, p)$'s is a finite index subgroup of H.

For the implication from Theorem 3.1.4 to Theorem 3.1.3, see Section 3.2.4.

Note that the direction of the group homomorphisms $\tilde{f}_{\mu,p}$ in Theorem 3.1.4 is opposite to the embeddings in Theorem 3.1.2 and Theorem 3.1.3 (2). This direction seems more natural for the non-deterministic case; this observation suggests the following question.

Question 3.1.5. Let G and H be groups with H finitely generated. Suppose that the word problem of H is accepted by a G-automaton. Does there exist a group homomorphism from a subgroup of G onto a finite index subgroup of H? If so, is it obtained combinatorially?

Our Theorem 3.1.4 is the very first step for approaching Question 3.1.5. Note that an affirmative answer to Question 3.1.5 would generalize Theorem 3.1.2.

3.2 Preliminaries

3.2.1 Words, subwords, and scattered subwords

For a set Σ, we write Σ^* for the free monoid generated by Σ, i.e., the set of *words* over Σ. For a word $u = a_1 a_2 \cdots a_n \in \Sigma^*$ $(n \geq 0, a_i \in \Sigma)$, the number n is called the *length* of u, which is denoted by $|u|$. For two words $u, v \in \Sigma^*$, the *concatenation* of u and v are denoted by $u \cdot v$, or simply uv. The identity element of Σ^* is the *empty word*, denoted by ε, which is the unique word of length zero. For an integer $n \geq 0$, the n-fold concatenation of a word $u \in \Sigma^*$ is denoted by u^n. For an integer $n > 0$, we write $\Sigma^{<n}$ for the set of words of length less than n.

A word $u \in \Sigma^*$ is a *subword* of a word $v \in \Sigma^*$, denoted by $u \sqsubseteq v$, if there exist two words $u_1, u_2 \in \Sigma^*$ such that $u_1 u u_2 = v$. A word $u \in \Sigma^*$ is a *scattered subword* of a word $v \in \Sigma^*$, denoted by $u \sqsubseteq_{\mathrm{sc}} v$, if there exist two finite sequences of words $u_1, u_2, \ldots, u_n \in \Sigma^*$ $(n \geq 0)$ and $v_0, v_1, \ldots, v_n \in \Sigma^*$ such that $u = u_1 u_2 \cdots u_n$ and $v = v_0 u_1 v_1 u_2 v_2 \cdots u_n v_n$. That is, v is obtained from u by inserting some words. Note that the two binary relations $\sqsubseteq$ and $\sqsubseteq_{\mathrm{sc}}$ are both partial orders on Σ^*.

3.2.2 Word problem for groups

Let H be a finitely generated group. A *choice of generators* for H is a surjective monoid homomorphism ρ from the free monoid Σ^* on a finite alphabet Σ onto H. The *word problem* of H with respect to ρ, denoted by $\mathrm{WP}_\rho(H)$, is the set of words in Σ^* mapped to the identity element 1_H of H via ρ, i.e., $\mathrm{WP}_\rho(H) = \rho^{-1}(1_H)$.

Although the word problem $\mathrm{WP}_\rho(H)$ depends on the choice of generators ρ, this does not cause problems:

Lemma 3.2.1 (e.g., [HRRT05, Lemma 1])**.** *Let $\mathcal{C}$ be a class of languages closed under inverse homomorphisms and let H be a finitely generated group. Then* $\mathrm{WP}_\rho(H) \in \mathcal{C}$ *for* some *choice of generators ρ if and only if* $\mathrm{WP}_\rho(H) \in \mathcal{C}$ *for* any *choice of generators ρ.*

Proof. Suppose $\mathrm{WP}_\rho(H) \in \mathcal{C}$, and let $\hat{\rho}\colon \hat{\Sigma}^* \to H$ be another choice of generators for H. Since $\hat{\Sigma}^*$ is free and ρ is surjective, there exists a monoid homomorphism $\varphi\colon \hat{\Sigma}^* \to \Sigma^*$ such that $\rho \circ \varphi = \hat{\rho}$. Then we have $\mathrm{WP}_{\hat{\rho}}(H) = \hat{\rho}^{-1}(1_H) = \varphi^{-1}(\rho^{-1}(1_H)) = \varphi^{-1}(\mathrm{WP}_\rho(H)) \in \mathcal{C}$. □

This is the reason why we use "*the* word problem of H" rather than "*a* word problem of H."

3.2.3 Graphs and paths

A *graph* is a 4-tuple $(V, E, \mathsf{s}, \mathsf{t})$, where V is the set of vertices, E is the set of (directed) edges, $\mathsf{s}\colon E \to V$ and $\mathsf{t}\colon E \to V$ are functions assigning to every edge $e \in E$ the *source* $\mathsf{s}(e) \in V$ and the *target* $\mathsf{t}(e) \in V$, respectively. A graph is *finite* if it has only finitely many vertices and edges.

A *path* (of *length* n) in a graph $\Gamma = (V, E, \mathsf{s}, \mathsf{t})$ is a word $e_1 e_2 \cdots e_n \in E^*$ ($n \geq 0$) of edges $e_i \in E$ such that $\mathsf{t}(e_i) = \mathsf{s}(e_{i+1})$ for $i = 1, 2, \ldots, n-1$. We usually use Greek letters to denote paths in a graph. For a non-empty path $\omega = e_1 e_2 \cdots e_n \in E^*$, the source and the target of ω are defined as $\mathsf{s}(\omega) = \mathsf{s}(e_1)$ and $\mathsf{t}(\omega) = \mathsf{t}(e_n)$, respectively. If $\omega = e_1 e_2 \cdots e_n$ and $\omega' = e'_1 e'_2 \cdots e'_k$ are non-empty paths such that $\mathsf{t}(\omega) = \mathsf{s}(\omega')$, or at least one of ω and ω' is empty, then the concatenation of ω and ω', denoted by $\omega \cdot \omega'$ or $\omega\omega'$, is the path $e_1 e_2 \cdots e_n e'_1 e'_2 \cdots e'_k$ of length $n + k$, i.e., the concatenation as words. A path ω in Γ is *closed* if $\mathsf{s}(\omega) = \mathsf{t}(\omega)$, or $\omega = \varepsilon$. For a closed path σ and an integer $n \geq 0$, we write σ^n for the n-fold concatenation of σ.

For a graph $\Gamma = (V, E, \mathsf{s}, \mathsf{t})$, an *edge-labeling function* is a function ℓ from E to a set M. If M is a monoid and $\omega = e_1 e_2 \cdots e_n$ is a path in Γ, then the label of ω is defined as $\ell(\omega) = \ell(e_1)\ell(e_2)\cdots\ell(e_n)$ via the multiplication of M.

3.2.4 G-automata

For a group G, a (non-deterministic) *G-automaton* over a finite alphabet Σ is defined as a 5-tuple $(\Gamma, \ell_G, \ell_\Sigma, p_{\mathrm{init}}, p_{\mathrm{ter}})$, where $\Gamma = (V, E, \mathsf{s}, \mathsf{t})$ is a finite graph, $\ell_G \colon E \to G$ and $\ell_\Sigma \colon E \to \Sigma^*$ are edge-labeling functions, $p_{\mathrm{init}} \in V$ is the *initial vertex*, and $p_{\mathrm{ter}} \in V$ is the *terminal vertex*. For simplicity, we assume that $\ell_\Sigma(e) \in \Sigma \cup \{\varepsilon\}$ for each $e \in E$. (Note that this assumption does not decrease the accepting power of G-automata. Indeed, if necessary, one can subdivide an edge e with labels $\ell_\Sigma(e) = uv, \ell_G(e) = g$ into two new edges e_1, e_2 with labels $\ell_\Sigma(e_1) = u, \ell_G(e_1) = g$ and $\ell_\Sigma(e_2) = v, \ell_G(e_2) = 1_G$.) An *accepting path* in a G-automaton $A = (\Gamma, \ell_G, \ell_\Sigma, p_{\mathrm{init}}, p_{\mathrm{ter}})$ is a path α in Γ such that $\mathsf{s}(\alpha) = p_{\mathrm{init}}$, $\mathsf{t}(\alpha) = p_{\mathrm{ter}}$, and $\ell_G(\alpha) = 1_G$ (we consider that the empty path $\varepsilon \in E^*$ is accepting if and only if $p_{\mathrm{init}} = p_{\mathrm{ter}}$). We say that a path ω in Γ is *promising* if ω is a subword of some accepting path in A, i.e., there exist two paths $\omega_1, \omega_2 \in E^*$ such that the concatenation $\omega_1\omega\omega_2 \in E^*$ is an accepting path in A. The *language accepted* by a G-automaton A, denoted by $L(A)$, is the set of all words $u \in \Sigma^*$ such that u is the label of some accepting path in A, i.e., $L(A) = \{\, \ell_\Sigma(\alpha) \in \Sigma^* \mid \alpha \text{ is an accepting path in } A \,\}$. We say that a G-automaton A is *abelian* if the register group G is abelian.

Proposition 3.2.2 (e.g., [Kam09, Proposition 2])**.** *For a group G, the class of languages accepted by G-automata are closed under inverse homomorphisms.*

Proof. Let $A = (\Gamma = (V, E, \mathsf{s}, \mathsf{t}), \ell_G, \ell_\Sigma, p_{\mathrm{init}}, p_{\mathrm{ter}})$ be a G-automaton over Σ and $\varphi \colon \hat{\Sigma}^* \to \Sigma^*$ be a monoid homormophism. Let $m = 1 + \max_{\hat{a}\in\Sigma} |\varphi(\hat{a})|$. Define a G-automaton $\hat{A} = (\hat{\Gamma} = (\hat{V}, \hat{E}, \hat{\mathsf{s}}, \hat{\mathsf{t}}), \hat{\ell}_G, \ell_{\hat{\Sigma}}, p_{\mathrm{init}}, p_{\mathrm{ter}})$, where

$$\begin{aligned}
\hat{V} &= V \cup (V \times \Sigma^{<m}),\\
\hat{E} &= \{\, \mathsf{Read}(p, \hat{a}) \mid p \in V, \hat{a} \in \hat{\Sigma} \cup \{\varepsilon\} \,\} \cup \{\, \mathsf{Escape}(p) \mid p \in V \,\}\\
&\qquad \cup \{\, \mathsf{Consume}(e, w) \mid e \in E, \ell_\Sigma(e)w \in \Sigma^{<m} \,\},
\end{aligned}$$

$$
\begin{aligned}
\hat{\mathsf{s}}(\mathsf{Read}(p,\hat{a})) &= p, & \hat{\mathsf{s}}(\mathsf{Escape}(p)) &= (p,\varepsilon),\\
\hat{\mathsf{t}}(\mathsf{Read}(p,\hat{a})) &= (p,\varphi(\hat{a})), & \hat{\mathsf{t}}(\mathsf{Escape}(p)) &= p,\\
\hat{\ell}_G(\mathsf{Read}(p,\hat{a})) &= 1_G, & \hat{\ell}_G(\mathsf{Escape}(p)) &= 1_G,\\
\ell_{\hat{\Sigma}}(\mathsf{Read}(p,\hat{a})) &= \hat{a}, & \ell_{\hat{\Sigma}}(\mathsf{Escape}(p)) &= \varepsilon,\\
\hat{\mathsf{s}}(\mathsf{Consume}(e,w)) &= (\mathsf{s}(e),\ell_\Sigma(e)w),\\
\hat{\mathsf{t}}(\mathsf{Consume}(e,w)) &= (\mathsf{t}(e),w),\\
\hat{\ell}_G(\mathsf{Consume}(e,w)) &= \ell_G(e),\\
\ell_{\hat{\Sigma}}(\mathsf{Consume}(e,w)) &= \varepsilon.
\end{aligned}
$$

Then we have $\varphi^{-1}(L(A)) = L(\hat{A})$. □

Replacing the register group G by its finite index subgroup or finite index overgroup does not change the class of languages accepted by G-automata:

Proposition 3.2.3 (e.g., [EKO08, Proposition 8])**.** *Let G be a group and H be a subgroup of G. Then every language accepted by a H-automaton is accepted by a G-automaton. If H has finite index in G, then the converse holds.*

Proof. The first half is obvious. Let $A = (\Gamma = (V, E, \mathsf{s}, \mathsf{t}), \ell_G, \ell_\Sigma, p_{\mathrm{init}}, p_{\mathrm{ter}})$ be a G-automaton. Suppose that H has finite index in G. Let $R \subseteq G$ be a complete system of representatives of $H\backslash G$ such that $R \ni 1_G$. Then R is finite since H has finite index in G. For each element $g \in G$, we write $(h[g], r[g])$ for the unique pair in $H \times R$ such that $g = h[g] \cdot r[g]$. Define an H-automaton $B = (\Gamma' = (V', E', \mathsf{s}', \mathsf{t}'), \ell_H, \ell_\Sigma, p'_{\mathrm{init}}, p'_{\mathrm{ter}})$, where

$$
\begin{aligned}
&V' = V \times R, \quad E' = R \times E,\\
&\mathsf{s}'(r,e) = (\mathsf{s}(e), r), \quad \mathsf{t}'(r,e) = (\mathsf{t}(e), r[r \cdot \ell_G(e)]), \quad \ell_H(r,e) = h[r \cdot \ell_G(e)],\\
&p'_{\mathrm{init}} = (p_{\mathrm{init}}, 1_G), \quad p'_{\mathrm{ter}} = (p_{\mathrm{ter}}, 1_G).
\end{aligned}
$$

Then we have $L(B) = L(A)$. □

Since the word problem of H is trivially accepted by an H-automaton for every finitely generated group H, we obtain the following corollary.

Corollary 3.2.4. *Theorem 3.1.4 implies Theorem 3.1.3.* □

3.3 Proof of the main theorem

Throughout this section, we fix an abelian group G, a finitely generated group H, a choice of generators $\rho\colon \Sigma^* \to H$, and an abelian G-automaton $A = (\Gamma = (V, E, \mathsf{s}, \mathsf{t}), \ell_G, \ell_\Sigma, p_{\mathrm{init}}, p_{\mathrm{ter}})$ such that $\mathrm{WP}_\rho(H) = L(A)$. We write the group operation of G additively and 0_G for the identity element of G.

The following lemma is a starting point of our proof.

Lemma 3.3.1. *Let ω and ω' be paths in Γ such that $\mathsf{s}(\omega) = \mathsf{s}(\omega')$ and $\mathsf{t}(\omega) = \mathsf{t}(\omega')$, and suppose that ω is promising. Then $\ell_G(\omega) = \ell_G(\omega')$ implies $\rho(\ell_\Sigma(\omega)) = \rho(\ell_\Sigma(\omega'))$.*

Proof. Since ω is promising, there exist two paths ω_1, ω_2 in Γ such that $\omega_1\omega\omega_2$ is an accepting path in A. It follows from the assumption that $\ell_G(\omega_1\omega'\omega_2) = \ell_G(\omega_1) + \ell_G(\omega') + \ell_G(\omega_2) = \ell_G(\omega_1) + \ell_G(\omega) + \ell_G(\omega_2) = \ell_G(\omega_1\omega\omega_2) = 0_G$, and $\omega_1\omega'\omega_2$ is also an accepting path in A. That is, $\ell_\Sigma(\omega_1\omega\omega_2), \ell_\Sigma(\omega_1\omega'\omega_2) \in \mathrm{WP}_\rho(H)$, and $\rho(\ell_\Sigma(\omega_1))\rho(\ell_\Sigma(\omega))\rho(\ell_\Sigma(\omega_2)) = 1_H = \rho(\ell_\Sigma(\omega_1))\rho(\ell_\Sigma(\omega'))\rho(\ell_\Sigma(\omega_2))$ in H. Thus we have $\rho(\ell_\Sigma(\omega)) = \rho(\ell_\Sigma(\omega'))$. □

Definition 3.3.2. An accepting path α in A is *minimal* if it is minimal with respect to the scattered subword relation $\sqsubseteq_{\mathrm{sc}}$ on E^*. An accepting path α in A *dominates* a minimal accepting path μ in A if $\mu \sqsubseteq_{\mathrm{sc}} \alpha$.

A similar notion of minimal accepting paths can be found in [CEO06, Section 4].

Remark 3.3.3. Note that, by Higman's lemma [Hig52, Theorem 4.4], the scattered subword relation $\sqsubseteq_{\mathrm{sc}}$ on Σ^* is a *well-quasi-order*. In particular, there are only finitely many minimal accepting paths in A, and every accepting path on A dominates some minimal accepting path in A.

Definition 3.3.4. Let $\mu = e_1e_2\cdots e_n \in E^*$ ($e_i \in E$) be a minimal accepting path in A. A closed path $\sigma \in E^*$ in Γ is *pumpable in μ* if there exists an accepting path α in A dominating μ such that $\alpha = \alpha_0e_1\alpha_1e_2\alpha_2\cdots e_n\alpha_n$ for some paths $\alpha_0, \alpha_1, \ldots, \alpha_n \in E^*$ in Γ and $\sigma \sqsubseteq \alpha_j$ for some $j \in \{0, 1, \ldots, n\}$.

Remarks 3.3.5.

(1) In Definition 3.3.4, each α_i is a closed path in Γ and satisfies $\ell_G(\alpha_0) + \ell_G(\alpha_1) + \cdots + \ell_G(\alpha_n) = \ell_G(\alpha) = 0_G$ since $\ell_G(\mu) = 0_G$ and G is abelian.

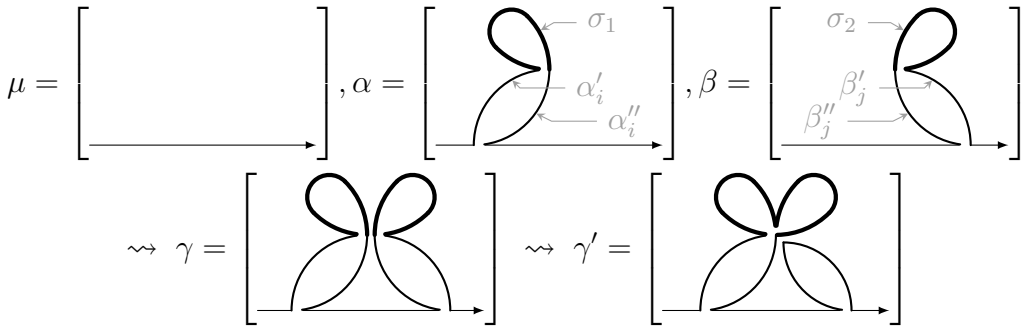

Figure 3.1: Construction of the accepting path γ' in (3.1)

(2) Every closed path pumpable in a minimal accepting path μ is promising.

Definition 3.3.6. For a minimal accepting path μ in A and a vertex $p \in V$, define

$$M(\mu, p) = \left\{ \sigma \in E^* \;\middle|\; \begin{array}{c} \sigma \text{ is a closed path in } \Gamma \text{ pumpable in } \mu \\ \text{such that } \mathsf{s}(\sigma) = p, \text{ or } \sigma = \varepsilon \end{array} \right\}.$$

Lemma 3.3.7. *Each $M(\mu, p)$ is a monoid with respect to the concatenation operation, i.e., $\sigma_1, \sigma_2 \in M(\mu, p)$ implies $\sigma_1\sigma_2 \in M(\mu, p)$.*

Proof. Since both σ_1 and σ_2 are pumpable in $\mu = e_1e_2\cdots e_n \in E^*$ ($e_i \in E$), there exist two accepting paths $\alpha = \alpha_0e_1\alpha_1e_2\alpha_2\cdots e_n\alpha_n$ ($\alpha_i \in E^*$) and $\beta = \beta_0e_1\beta_1e_2\beta_2\cdots e_n\beta_n$ ($\beta_i \in E^*$) such that $\sigma_1 \sqsubseteq \alpha_i$ and $\sigma_2 \sqsubseteq \beta_j$ for some $i, j \in \{0, 1, \ldots, n\}$. Then we have $\alpha_i = \alpha'_i\sigma_1\alpha''_i$ for some $\alpha'_i, \alpha''_i \in E^*$ and $\beta_j = \beta'_j\sigma_2\beta''_j$ for some $\beta'_j, \beta''_j \in E^*$. We may assume that $i \leq j$. Since G is abelian, the merged path $\gamma = (\alpha_0\beta_0)e_1(\alpha_1\beta_1)e_2(\alpha_2\beta_2)\cdots e_n(\alpha_n\beta_n)$ and its permutation

$$\gamma' = (\alpha_0\beta_0)e_1(\alpha_1\beta_1)e_2(\alpha_2\beta_2)\cdots e_i(\alpha'_i\sigma_1\sigma_2\alpha''_i)e_{i+1}\cdots e_j(\beta'_j\beta''_j)e_{j+1}\cdots e_n(\alpha_n\beta_n) \tag{3.1}$$

are accepting paths in A (Figure 3.1). □

For each $M(\mu, p)$, Lemma 3.3.7 allows us to define a surjective monoid homomorphism $f_{\mu,p}\colon M(\mu, p) \to \rho(\ell_\Sigma(M(\mu, p)))$ as the composition function

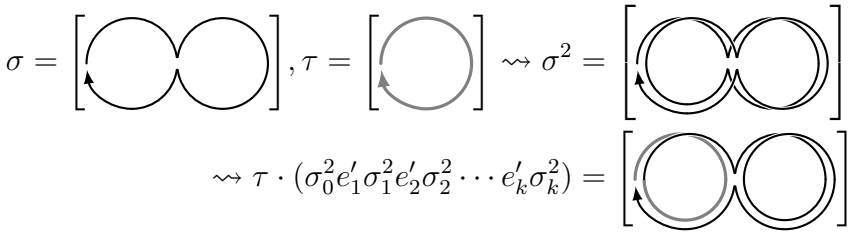

Figure 3.2: Construction of the path $\tau \cdot (\sigma_0^2 e_1' \sigma_1^2 e_2' \sigma_2^2 \cdots e_k' \sigma_k^2)$ in (3.2)

$\rho \circ \ell_\Sigma$. By Lemma 3.3.1, $f_{\mu,p}$ induces a well-defined surjective monoid homomorphism $\bar{f}_{\mu,p} \colon \ell_G(M(\mu,p)) \to \rho(\ell_\Sigma(M(\mu,p)))$. Let $G(\mu,p)$ (resp. $H(\mu,p)$) denotes the subgroup of G generated by $\ell_G(M(\mu,p))$ (resp. the subgroup of H generated by $\rho(\ell_\Sigma(M(\mu,p)))$). One can easily extend $\bar{f}_{\mu,p}$ to a unique surjective group homomorphism $\tilde{f}_{\mu,p} \colon G(\mu,p) \to H(\mu,p)$. The remaining task is to prove that at least one of the $H(\mu,p)$'s is a finite index subgroup of H.

Lemma 3.3.8. *Each $M(\mu,p)$ is downward closed with respect to $\sqsubseteq_{\mathrm{sc}}$, i.e., if σ is an element of $M(\mu,p)$ and τ is a closed path in Γ with $\mathsf{s}(\tau) = p$ such that $\tau \sqsubseteq_{\mathrm{sc}} \sigma$, then $\tau \in M(\mu,p)$.*

Proof. Suppose that $\tau = e_1' e_2' \cdots e_k'$ $(k \geq 0, e_i' \in E)$ and $\sigma = \sigma_0 e_1' \sigma_1 e_2' \cdots e_k' \sigma_k$ $(\sigma_i \in E^*)$. Each σ_i is a closed path in Γ. Since, by Lemma 3.3.7, σ^2 is pumpable in $\mu = e_1 e_2 \cdots e_n$ $(n \geq 0, e_i \in E)$, there exists an accepting path $\alpha = \alpha_0 e_1 \alpha_1 e_2 \alpha_2 \cdots e_n \alpha_n$ dominating μ such that $\sigma^2 \sqsubseteq_{\mathrm{sc}} \alpha_i$ for some $i \in \{0, 1, \ldots, n\}$. If $\alpha_i = \alpha_i' \sigma^2 \alpha_i''$, then the path

$$\gamma = \alpha_0 e_1 \alpha_1 e_2 \alpha_2 \cdots e_i (\alpha_i' \cdot \tau \cdot (\sigma_0^2 e_1' \sigma_1^2 e_2' \sigma_2^2 \cdots e_k' \sigma_k^2) \cdot \alpha_i'') e_{i+1} \cdots e_n \alpha_n \quad (3.2)$$

is an accepting path in A (Figure 3.2). □

Lemma 3.3.9. *Let $\sigma \in M(\mu,p)$ and $\omega \sqsubseteq \sigma$ be a path. Then there exist two paths $\omega_1, \omega_2 \in E^{<|V|}$ such that $\omega_1 \omega \omega_2 \in M(\mu,p)$.*

Proof. Let $(\omega_1, \omega_2) \in E^* \times E^*$ be a pair of two paths such that $\omega_1 \omega \omega_2 \in M(\mu,p)$ and $\max\{|\omega_1|, |\omega_2|\}$ is minimum. Such a pair exists since $\omega \sqsubseteq \sigma \in M(\mu,p)$. Suppose the contrary that $\max\{|\omega_1|, |\omega_2|\} \geq |V|$, say $|\omega_1| \geq |V|$. By the pigeonhole principle, ω_1 must visit some vertex $p \in V$ at least twice. That is, there exist three paths α, β, γ such that $\omega_1 = \alpha\beta\gamma$ and β is a non-empty closed path. Now we have $\alpha\gamma\omega\omega_2 \sqsubseteq_{\mathrm{sc}} \omega_1\omega\omega_2 \in M(\mu,p)$, and Lemma 3.3.8 implies $\alpha\gamma\omega\omega_2 \in M(\mu,p)$, which contradicts the minimality of (ω_1, ω_2). □

Proof of Theorem 3.1.4. Let $h \in H$ and fix a word $v \in \Sigma^*$ such that $\rho(v) = h$. There exists a word $\bar{v} \in \Sigma^*$ such that $v\bar{v} \in \mathrm{WP}_\rho(H)$. Define

$$N = 1 + \max\{\, |\mu| \mid \mu \in E^* \text{ is a minimal accepting path in } A \,\},$$

and then $N < \infty$ by Remark 3.3.3. Since $(v\bar{v})^N \in \mathrm{WP}_\rho(H)$, there exists an accepting path

$$\alpha = \omega_1\bar{\omega}_1\omega_2\bar{\omega}_2\cdots\omega_N\bar{\omega}_N \tag{3.3}$$

in A such that $\ell_\Sigma(\omega_i) = v$ and $\ell_\Sigma(\bar{\omega}_i) = \bar{v}$ for $i = 1, 2, \ldots, N$. Let $\mu = e_1e_2\cdots e_n$ $(e_i \in E)$ be a minimal accepting path such that α dominates μ. Then we have another decomposition

$$\alpha = \alpha_0e_1\alpha_1e_2\alpha_2\cdots e_n\alpha_n \tag{3.4}$$

for some closed paths $\alpha_0, \alpha_1, \ldots, \alpha_n \in E^*$. Since $N > n$ and each e_i in the decomposition (3.4) is contained in at most one ω_i in the decomposition (3.3), at least one of the ω_i's is disjoint from all e_i's, i.e., there exist $i \in \{1, 2, \ldots, N\}$ and $j \in \{0, 1, \ldots, n\}$ such that $\omega_i \sqsubseteq \alpha_j$. Since α_j is a pumpable closed path in μ, α_j is an element of $M(\mu, \mathsf{s}(\alpha_j))$. By Lemma 3.3.9, there exist $\alpha'_j, \alpha''_j \in E^{<|V|}$ such that $\alpha'_j\omega_i\alpha''_j \in M(\mu, \mathsf{s}(\alpha_j))$. Then we have $\left|\ell_\Sigma(\alpha'_j)\right|, \left|\ell_\Sigma(\alpha''_j)\right| < |V|$ and $\rho(\ell_\Sigma(\alpha'_j))\rho(\ell_\Sigma(\omega_i))\rho(\ell_\Sigma(\alpha''_j)) \in H(\mu, \mathsf{s}(\alpha))$, hence

$$h = \rho(v) = \rho(\ell_\Sigma(\omega_i)) \in \rho(\ell_\Sigma(\alpha'_j))^{-1}H(\mu, \mathsf{s}(\alpha))\rho(\ell_\Sigma(\alpha''_j))^{-1}.$$

From the above argument, we obtain

$$H = \bigcup \left\{ h_1^{-1}H(\mu, p)h_2^{-1} \;\middle|\; \begin{array}{c} \mu \text{ is a minimal accepting path in } A, \\ p \in V, \text{ and } h_1, h_2 \in \rho(\Sigma^{<|V|}) \end{array} \right\},$$

where the right-hand side is a finite union of cosets of H by Remark 3.3.3. Thus, by B. H. Neumann's lemma [Neu54, (4.1) Lemma and (4.2)], at least one of $H(\mu, p)$'s has finite index in H. □

Bibliography

[Anī72] A. V. Anīsīmov, *Certain algorithmic questions for groups and context-free languages*, Kibernetika (Kiev) **2** (1972), 4–11. MR312774 ↑39

[Bar92] H. P. Barendregt, *Lambda calculi with types*, Handbook of logic in computer science, Vol. 2, 1992, pp. 117–309. MR1381697 ↑6, 7, 8, 9, 11, 13

[BCDC83] Henk Barendregt, Mario Coppo, and Mariangiola Dezani-Ciancaglini, *A filter lambda model and the completeness of type assignment*, J. Symbolic Logic **48** (1983), no. 4, 931–940 (1984). MR727784 ↑7

[BH74] William W. Boone and Graham Higman, *An algebraic characterization of groups with soluble word problem*, J. Austral. Math. Soc. **18** (1974), 41–53. Collection of articles dedicated to the memory of Hanna Neumann, IX. MR0357625 ↑39

[Bro14] Tara Brough, *Groups with poly-context-free word problem*, Groups Complex. Cryptol. **6** (2014), no. 1, 9–29. MR3200359 ↑39

[CEO06] Sean Cleary, Murray Elder, and Gretchen Ostheimer, *The word problem distinguishes counter languages*, arXiv, 2006. arXiv:math.GR/0606415. ↑45

[CF58] Haskell B. Curry and Robert Feys, *Combinatory logic. Vol. I*, Studies in Logic and the Foundations of Mathematics, North-Holland Publishing Co., Amsterdam, 1958. MR0094298 ↑6

[Cor05] Jon M. Corson, *Extended finite automata and word problems*, Internat. J. Algebra Comput. **15** (2005), no. 3, 455–466. MR2151422 ↑39

[CS63] N. Chomsky and M. P. Schützenberger, *The algebraic theory of context-free languages*, Computer programming and formal systems, 1963, pp. 118–161. MR0152391 ↑39

[CSCF+15] Tullio Ceccherini-Silberstein, Michel Coornaert, Francesca Fiorenzi, Paul E. Schupp, and Nicholas W. M. Touikan, *Multi-pass automata and group word problems*, Theoret. Comput. Sci. **600** (2015), 19–33. MR3394671 ↑39

[CZ00] Gunther Cornelissen and Karim Zahidi, *Topology of Diophantine sets: remarks on Mazur's conjectures*, Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), 2000, pp. 253–260. MR1802017 ↑20

[DH10] Rodney G. Downey and Denis R. Hirschfeldt, *Algorithmic randomness and complexity*, Theory and Applications of Computability, Springer, New York, 2010. MR2732288 ↑25, 36

[DLPVG00] Jan Denef, Leonard Lipshitz, Thanases Pheidas, and Jan Van Geel (eds.), *Hilbert's tenth problem: relations with arithmetic and algebraic geometry*, Contemporary Mathematics, vol. 270, American Mathematical Society, Providence, RI, 2000. Papers from the workshop held at Ghent University, Ghent, November 2–5, 1999. MR1802007 ↑19

[DM00] Jürgen Dassow and Victor Mitrana, *Finite automata over free groups*, Internat. J. Algebra Comput. **10** (2000), no. 6, 725–737. MR1809380 ↑38

[DPR61] Martin Davis, Hilary Putnam, and Julia Robinson, *The decision problem for exponential diophantine equations*, Ann. of Math. (2) **74** (1961), 425–436. MR133227 ↑19

[Dun85] M. J. Dunwoody, *The accessibility of finitely presented groups*, Invent. Math. **81** (1985), no. 3, 449–457. MR807066 ↑39

[EKO08] Murray Elder, Mark Kambites, and Gretchen Ostheimer, *On groups and counter automata*, Internat. J. Algebra Comput. **18** (2008), no. 8, 1345–1364. MR2483126 ↑39, 40, 44

[EMPS17] Kirsten Eisenträger, Russell Miller, Jennifer Park, and Alexandra Shlapentokh, *As easy as $\mathbb{Q}$: Hilbert's tenth problem for subrings of the rationals and number fields*, Trans. Amer. Math. Soc. **369** (2017), no. 11, 8291–8315. MR3695862 ↑20, 23, 32, 36

[EO04] Gillian Z. Elston and Gretchen Ostheimer, *On groups whose word problem is solved by a counter automaton*, Theoret. Comput. Sci. **320** (2004), no. 2-3, 175–185. MR2064297 ↑39

[Ghi96] Silvia Ghilezan, *Strong normalization and typability with intersection types*, Notre Dame J. Formal Logic **37** (1996), no. 1, 44–52. MR1379548 ↑7

[GKS18] Robert H. Gilman, Robert P. Kropholler, and Saul Schleimer, *Groups whose word problems are not semilinear*, Groups Complex. Cryptol. **10** (2018), no. 2, 53–62. MR3871464 ↑39

[GMS22] Kilian Gebhardt, Frédéric Meunier, and Sylvain Salvati, *O_n is an n-MCFL*, J. Comput. System Sci. **127** (2022), 41–52. MR4388995 ↑39

[Gre75] S. A. Greibach, *Remarks on the complexity of nondeterministic counter languages*, Theoret. Comput. Sci. **1** (1975/76), no. 4, 269–288. MR411257 ↑38

[Gre78] S. A. Greibach, *Remarks on blind and partially blind one-way multicounter machines*, Theoret. Comput. Sci. **7** (1978), no. 3, 311–324. MR513714 ↑38

[Gro81] Mikhael Gromov, *Groups of polynomial growth and expanding maps*, Inst. Hautes Études Sci. Publ. Math. **53** (1981), 53–73. MR623534 ↑40

[Hig52] Graham Higman, *Ordering by divisibility in abstract algebras*, Proc. London Math. Soc. (3) **2** (1952), 326–336. MR49867 ↑45

[Hig61] G. Higman, *Subgroups of finitely presented groups*, Proc. Roy. Soc. London Ser. A **262** (1961), 455–475. MR130286 ↑39

[Hin83] Roger Hindley, *The completeness theorem for typing λ-terms*, Theoret. Comput. Sci. **22** (1983), no. 1-2, 1–17. MR693047 ↑6, 7

[Hin97] J. Roger Hindley, *Basic simple type theory*, Cambridge Tracts in Theoretical Computer Science, vol. 42, Cambridge University Press, Cambridge, 1997. MR1466699 ↑6

[HOT08] Derek F. Holt, Matthew D. Owens, and Richard M. Thomas, *Groups and semigroups with a one-counter word problem*, J. Aust. Math. Soc. **85** (2008), no. 2, 197–209. MR2470538 ↑39, 40

[HR06] Derek F. Holt and Claas E. Röver, *Groups with indexed co-word problem*, Internat. J. Algebra Comput. **16** (2006), no. 5, 985–1014. MR2274726 ↑39

[HRRT05] Derek F. Holt, Sarah Rees, Claas E. Röver, and Richard M. Thomas, *Groups with context-free co-word problem*, J. London Math. Soc. (2) **71** (2005), no. 3, 643–657. MR2132375 ↑39, 42

[Kam06] Mark Kambites, *Word problems recognisable by deterministic blind monoid automata*, Theoret. Comput. Sci. **362** (2006), no. 1-3, 232–237. MR2259632 ↑38, 39

[Kam09] Mark Kambites, *Formal languages and groups as memory*, Comm. Algebra **37** (2009), no. 1, 193–208. MR2482816 ↑39, 43

[KM19] Kenneth Kramer and Russell Miller, *The Hilbert's-Tenth-Problem operator*, Israel J. Math. **230** (2019), no. 2, 693–713. MR3940432 ↑21

[KMY20] Ryo Kashima, Naosuke Matsuda, and Takao Yuyama, *Term-space semantics of typed lambda calculus*, Notre Dame J. Form. Log. **61** (2020), no. 4, 591–600. MR4200352 ↑6

[KS12] Makoto Kanazawa and Sylvain Salvati, *MIX is not a tree-adjoining language*, Proceedings of the 50th annual meeting of the association for computational linguistics (volume 1: Long papers), July 2012, pp. 666–674. ↑39

[KS19] Robert P. Kropholler and Davide Spriano, *Closure properties in the class of multiple context-free groups*, Groups Complex. Cryptol. **11** (2019), no. 1, 1–15. MR4000593 ↑39

[Lac75] A. H. Lachlan, *Uniform enumeration operations*, J. Symbolic Logic **40** (1975), no. 3, 401–409. MR379156 ↑30

[Mat70] Ju. V. Matijasevič, *The Diophantineness of enumerable sets*, Dokl. Akad. Nauk SSSR **191** (1970), 279–282. MR0258744 ↑19

[Mil16] Russell Miller, *Baire category theory and Hilbert's tenth problem inside* $\mathbb{Q}$, Pursuit of the universal, 2016, pp. 343–352. MR3535176 ↑20, 24, 25, 28, 29, 30

[Mil18] Russell Miller, *Measure theory and Hilbert's tenth problem inside* $\mathbb{Q}$, Sets and computations, 2018, pp. 253–269. MR3700865 ↑21, 23, 24, 28, 29

[Mil19] Russell Miller, *HTP-complete rings of rational numbers*, arXiv Preprint (2019), available at `http://arxiv.org/abs/1907.03147v1`. ↑21, 23, 35, 36, 37

[Mil20] Russell Miller, *Non-coding enumeration operators*, Beyond the horizon of computability, 2020, pp. 112–123. ↑21, 22, 30

[MS01] Victor Mitrana and Ralf Stiebe, *Extended finite automata over groups*, Discrete Appl. Math. **108** (2001), no. 3, 287–300. MR1807922 ↑38, 39

[MS83] David E. Muller and Paul E. Schupp, *Groups, the theory of ends, and context-free languages*, J. Comput. System Sci. **26** (1983), no. 3, 295–310. MR710250 ↑39

[Neu54] B. H. Neumann, *Groups covered by permutable subsets*, J. London Math. Soc. **29** (1954), 236–248. MR62122 ↑48

[NT15] Gabriela Aslı Rino Nesin and Richard M. Thomas, *Groups whose word problem is a Petri net language*, Descriptional complexity of formal systems, 2015, pp. 243–255. MR3375036 ↑39

[Plo94] Gordon Plotkin, *A semantics for static type inference*, 1994, pp. 256–299. International Conference on Theoretical Aspects of Computer Software (TACS '91) (Sendai, 1991). MR1269377 ↑7

[Poo03a] Bjorn Poonen, *Hilbert's tenth problem and Mazur's conjecture for large subrings of* $\mathbb{Q}$, J. Amer. Math. Soc. **16** (2003), no. 4, 981–990. MR1992832 ↑20

[Poo03b] Bjorn Poonen, *Hilbert's tenth problem over rings of number-theoretic interest* (2003), available at http://www-math.mit.edu/~poonen/papers/aws2003.pdf. ↑19

[Soa16] Robert I. Soare, *Turing computability*, Theory and Applications of Computability, Springer-Verlag, Berlin, 2016. Theory and applications. MR3496974 ↑33

[Tai67] W. W. Tait, *Intensional interpretations of functionals of finite type. I*, J. Symbolic Logic **32** (1967), 198–212. MR219400 ↑7, 9