國立臺灣大學電機資訊學院資訊工程學系
碩士論文
Department of Computer Science and Information Engineering
College of Electrical Engineering and Computer Science
National Taiwan University
Master Thesis

# 回顧雙變量邏輯之可滿足性
# Revisiting the Satisfiability of Two Variable Logic

丁恩琳
En-Lin Ting

指導教授：陳偉松博士
Advisor: Tony Tan, Ph.D.

中華民國 107 年 7 月
July, 2018

doi:10.6342/NTU201802560

doi:10.6342/NTU201802560

# 國立臺灣大學碩士學位論文
# 口試委員會審定書

## 回顧雙變量邏輯之可滿足性

## Revisiting the Satisfiability of Two Variable Logic

本論文係丁恩琳君（學號 R04922047）在國立臺灣大學資訊工程學系完成之碩士學位論文，於民國 107 年 7 月 10 日承下列考試委員審查通過及口試及格，特此證明

口試委員：

（指導教授）

廖純中　　蔡益坤

系 主 任　莊永裕



doi:10.6342/NTU201802560

doi:10.6342/NTU201802560

# 誌謝

這篇論文的成文，除了要感謝過去在此領域做出貢獻的研究者，更要感謝許多我身邊的人。

首先，一定要感謝我的指導教授陳偉松老師。謝謝老師在我換指導教授時的接納，謝謝他對學生的關心與幫助，更要謝謝他的悉心教導，無論是在知識上、研究方法上或是待人處世上，我皆獲益良多。這篇論文能完成，都要感謝陳偉松老師。

另外，也要感謝我之前的指導教授呂學一老師。雖然沒有能夠跟著老師完成碩士論文，但他的指點與包容，令我由衷感謝，亦是難以報答。

我要感謝碩士學位考試的口試委員蔡益坤老師及廖純中老師，感謝他們花時間與心力針對我的論文提問討論，並且給予寶貴的意見。

還要謝謝在我攻讀碩士期間實驗室的同學學長學弟，以及修課時的老師以及一起討論的同學們，在溝通交流中擴展了我的想法、啟發我的思維並激發我的靈感。

最後要感謝我的家人，他們的關懷與鼓勵往往給予我動力，更是在我遭遇挫折時成為我的支持與幫助。

謝謝你們。



doi:10.6342/NTU201802560

doi:10.6342/NTU201802560

# Acknowledgements

This thesis would not have been possible if it had not been for the researchers who have devoted themselves to this area before us, and it would not have been possible without the help from many people around me.

First of all, I would like express my profuse gratitude towards my advisor Tony Tan, who accepted me as his student during my change of advisor. I am very thankful for his teachings, whether it be the specialized knowledge in the area, the methods of researching, or the mindset in general, for all of them help me greatly. The completion of this paper is all thanks to him.

Next, my sincere thanks goes to my previous advisor Hsueh-I Lu. Although I did not manage to finish my master thesis with him, I am truly grateful for his advising and understanding, and I am deeply indebted.

I would like to thank the committee members of my oral defense - Yih-Kuen Tsai and Churn-Jung Liau. I am very grateful for their time and effort to inquire and discuss about my thesis, and I value their helpful advices greatly.

I would also like to thank my fellow labmates, the teachers of the classes I have taken, and classmates who had discussion with me. The exchange of ideas with them broadened my horizons, improved my way of thinking, and provided me with inspirations.

Last but not least, I give my deep thanks to my family, whose loving care and encouragement often boost my motivation. They are always willing to lend me support and help whenever I am feeling frustrated.

Thank you all.



doi:10.6342/NTU201802560

doi:10.6342/NTU201802560

# 摘要

含計數量詞的二階邏輯 ($C^2$) 有著許多應用，特別像是本體知識語言的應用，例如用於語意網的 OWL。一個著名的結果是：$C^2$ 的可滿足性問題可以在非確定性指數時間 (NEXPTIME) 內決定，而且這樣的複雜度是最佳的。然而，目前已知的解決技巧較為複雜，通常必須去猜測一個滿足目標式子結構或表示方法，而導致難以實作。

在這篇論文中，我們關注於具有反向關係封閉性並且是 Scott's 正規型態的 $C^2$ 句子 ($\mathcal{RCS}$)。直觀上，如果一個句子 $\varphi$ 是 Scott's 正規型態而且其使用的二元關係具有反向封閉性，$\varphi$ 就屬於 $\mathcal{RCS}$。我們基於 Kopczyński 和 Tan 的技巧 [9]，針對 $\mathcal{RCS}$ 的可滿足性問題及有限可滿足性問題提出一個新的決策程序，利用將 $\mathcal{RCS}$ 的式子轉換成 Presburger 的存在量化式來解決問題。雖然此方法的時間複雜度比最佳時間高：2-NEXPTIME，但其有幾個優勢：

1. 刻劃出 $\mathcal{RCS}$ 式子模型的特性，亦即任一 $\mathcal{RCS}$ 式子的模型皆是由正則圖及二分正則圖組成。
2. 顯示出一 $\mathcal{RCS}$ 式子的頻譜是否為有限是可決定的。
3. 此方法為解決可滿足性問題及有限可滿足性問題的簡單決策程序。

當原式為 Scott's 正規型態並且詞彙表固定時，我們演算法的時間複雜度為 NEXPTIME。我們期待我們的結果能提供討論 $C^2$ 式子的另類技巧，並擴展至其他諸多的本體知識語言。

關鍵字： 含計數量詞的二階邏輯；可滿足性；Presburger 算數；整數規劃；正則圖



doi:10.6342/NTU201802560

doi:10.6342/NTU201802560

# Abstract

Two variable logic with counting quantifiers ($C^2$) has found many applications, especially in ontology language such as OWL used in semantic web. It is well known that the satisfiability problem for $C^2$ is decidable in nondeterministic exponential time ($\mathrm{NEXPTIME}$), and the complexity is optimal. However, the known techniques are quite complicated and they typically involve guessing a structure or a representation that satisfies the input formula, which can be hard to implement.

In this thesis, we consider a subclass of $C^2$ formulas, which we call *Reversal closed* $C^2$ *formulas in Scott's normal form* ($\mathcal{RCS}$). Intuitively, a $C^2$ formula $\varphi$ is in $\mathcal{RCS}$, if it is in Scott's normal form and the binary relations used in $\varphi$ are closed under reversal. We present a decision procedure for the satisfiability and finite satisfiability problems for $\mathcal{RCS}$ formulas, which is based on the technique by Kopczyński and Tan [9]. Our approach is by converting an $\mathcal{RCS}$ formula into an existential Presburger formula. Though the complexity is higher: $2\text{-}\mathrm{NEXPTIME}$ (double exponential time), it has a few advantages:

1. It provides a characterization of models of $\mathcal{RCS}$ formulas, i.e., every model of an $\mathcal{RCS}$ formula is a collection of regular digraphs and biregular graphs.
2. It implies the decidability of checking whether the spectrum of an $\mathcal{RCS}$ formula is infinite.
3. It gives simple decision procedures for satisfiability and finite satisfia-



doi:10.6342/NTU201802560

bility problems.

When the input is in Scott's normal form and the vocabulary is fixed, our algorithm yields time complexity $\mathrm{NEXPTIME}$. We hope that our result can be used to provide an alternative technique to reason about $\mathrm{C}^2$ formula, thus many other ontology languages.

**Keywords:** two variable logic with counting quantifiers; satisfiability; Presburger arithmetics; integer programming; regular graphs



doi:10.6342/NTU201802560

# Contents





doi:10.6342/NTU201802560

doi:10.6342/NTU201802560

# Chapter 1

# Introduction

Many areas in computer science and information technology utilize first-order logic (FO) and its variances. For example, the currently booming artificial intelligence research uses FO as the basis of knowledge and data representation. Typically, FO sentences are used to describe the knowledge, so it is important to check the consistency of a sentence. By Gödel's completeness theorem, consistency and satisfiability are equivalent [4].

Formally, the *satisfiability problem* (SAT) for a class $C \subseteq \mathrm{FO}$ is defined as follows. Given an input formula $\varphi \in C$, decide whether there is a model that satisfies $\varphi$. The *finite satisfiability problem* (FIN-SAT) for $C$ is to decide whether there is a *finite* model that satisfies $\varphi$.

However, the general FO is known to be undecidable [2, 1, 20, 18]. Hence, researchers are looking for restricted but decidable classes of FO. In this paper, we discuss one such class: the $\mathrm{C}^2$ logic, i.e., the FO formulas using only two variables but allowing counting quantifiers.

## 1.1 Related works

From the classical work of Church [2, 1], Turing [20] and later, Trakhtenbrot [18], the satisfiability problem of FO is known to be undecidable, and it is necessary to find compromises in order to achieve more practical results. Some FO classes of interest are derived by restricting the number of variables. It was shown that the satisfiability problem



doi:10.6342/NTU201802560

of $\mathrm{FO}$ with only two variables ($\mathrm{FO}^2$) is decidable [11], whereas the three variable class is undecidable [8].

Another widely discussed class is $\mathrm{C}^2$, which is a more generalized class of $\mathrm{FO}^2$ by allowing counting quantifiers. The decidability of $\mathrm{C}^2$ was first proved by Grädel, Otto and Rosen [7]. However, the proof is done by showing both the satisfiability problem and its complement are recursively enumerable. Thus, its complexity cannot be deduced. The time complexity for both $\mathrm{SAT}$ and $\mathrm{FIN\text{-}SAT}$ problem is proved to be double exponential time by Pacholski, Szwast and Tendera [13], and later to be $\mathrm{NEXPTIME}$ by Pratt-Hartmann [15]. An immediate implication from this is that $\mathrm{C}^2$ is $\mathrm{NEXPTIME}$-complete, since $\mathrm{FO}^2$ is already known to be $\mathrm{NEXPTIME}$-hard [10, 3]. As a side note, the algorithms proposed in both [13, 15] involve many non-trivial guessing that would be difficult to implement.

It is worth to note that $\mathrm{FO}^2$ has finite model property. More precisely, if an $\mathrm{FO}^2$ formula $\varphi$ is satisfiable, then it is satisfied by a model with cardinality $O(2^{|\varphi|})$ [5]. On the other hand, $\mathrm{C}^2$ lacks such property. There are some $\mathrm{C}^2$ sentences that are only satisfiable by infinite structures. This is one such example:

$$\psi \quad := \quad \forall x \exists^{\geq 2} y E(x,y) \wedge \forall x \neg \exists^{\geq 2} y E(y,x)$$

Intuitively, $\psi$ states that each vertex in the model has at least two out-going edges but has only one or none in-coming edge. Therefore, the satisfiability problem and finite satisfiability problem for $\mathrm{C}^2$ are not equivalent, unlike for $\mathrm{FO}^2$.

## 1.2 Summary of contributions

In this paper, we take another approach to the satisfiability and finite satisfiability problem for $\mathrm{C}^2$.

It has been proved that for a sentence $\phi$ of $\mathrm{C}^2$, there is a corresponding Presburger formula $\mathrm{PREB}_\phi$ such that there exists a complete structure $\mathfrak{A}$ with $\mathfrak{A} \models \phi$ if and only if $\mathrm{PREB}_\phi(|\mathfrak{A}|)$ holds as long as $|\mathfrak{A}|$ is finite [9]. However, the conversion to Presburger



doi:10.6342/NTU201802560

formula make use of the conversion to QMLC and yields a sextuple exponential time complexity.

Here, we will utilize the Scott's normal form to simplify the conversion from a $\mathrm{C}^2$ sentence to an existential Presburger formula to achieve a less complicated algorithm in terms of both the procedure and the time complexity *under the assumption that the binary relations used in Scott's normal form are closed under reversal*. Moreover, we prove such conversion retains its properties even when we allow the structure to be infinite by allowing the Presburger formula to admit infinity $\infty$ in the solution.

On input $\mathcal{RCS}$ formula $\phi$, our algorithm does the following.

1. Convert it into an instance of Linear Integer Programming (LIP).

2. Solve the LIP problem.

Step 1 is of non-deterministic double exponential time, while step 2 is of non-deterministic polynomial time (in the size of the input). So, overall, our algorithm for both SAT and FIN-SAT runs in 2-NEXPTIME.

## 1.3 Outline

We will go through some definitions related to $\mathrm{C}^2$ and $\mathcal{RCS}$ in chapter 2, and the definitions and theorems regarding Presburger arithmetics and its extension to infinity are discussed in chapter 3. In chapter 4, we introduce some important tools for the conversion between $\mathcal{RCS}$ formulas and Presburger formulas. These tools primarily consist of regular and biregular graphs and their corresponding Presburger formula expressions. Our main result is derived in chapter 5, where we utilize the tools in chapter 4 to convert an $\mathcal{RCS}$ formula to a corresponding existential Presburger formula that preserves its satisfiability, and then solve the satisfiability problem for the Presburger formula with theorems derived from LIP in chapter 3. We conclude chapter 5 by analyzing the complexity for the algorithm. In chapter 6, we show some other results that can be inferred from our algorithm.



doi:10.6342/NTU201802560

doi:10.6342/NTU201802560

# Chapter 2

# Two variable logic with counting

In this chapter, we introduce the formal definition of two-variable logic with counting, which we denote by $\mathrm{C}^2$. We start by reviewing the syntax and semantics of first order logic in section 2.1. Then, in section 2.2 we formally define the class $\mathrm{C}^2$.

## 2.1 First order logic ($\mathrm{FO}$)

We fix a set $\mathcal{R}$ of relation symbols. Each $R \in \mathcal{R}$ is associated with a positive integer, which is called its *arity* and denoted by $\mathrm{ar}(R)$. We also fix a set $\mathrm{VAR}$ of first order variables. For simplicity, let $\mathcal{R} = \{R_1, \ldots, R_k\}$. [1]

**The syntax of first order logic** The syntax of first order logic sentence is defined inductively as follows:

- For any $x, y \in \mathrm{VAR}$, $x = y$ is an FO formula.
- If $R \in \mathcal{R}$ is of arity $n$ and $x_1, \ldots, x_n \in \mathrm{VAR}$, then $R(x_1, \ldots, x_n)$ is an FO formula.
- If $\alpha$ and $\beta$ are FO formulas, then so are $\neg\alpha$, $\alpha \wedge \beta$ and $\alpha \vee \beta$.
- If $\alpha$ is an FO formula and $x \in \mathrm{VAR}$, then $\exists x\alpha$ and $\forall x\alpha$ are FO formulas as well.

A formula is *existential* if it is of the form $\exists x_1 \ldots \exists x_m \psi(x_1, \ldots, x_m)$ where $\psi(x_1, \ldots, x_m)$ is quantifier-free, and a formula is *universal* if it is of the form $\forall x_1 \ldots \forall x_m \psi(x_1, \ldots, x_m)$.

[1] For the sake of simplicity, we do not consider function and constant symbols for the vocabulary.



doi:10.6342/NTU201802560

A variable $x$ is *quantified* if $\forall$ or $\exists$ preceded $x$ in the formula. *Free variables* are the variables that are *not* quantified. For instance, in the formula $\exists x \forall y R(x, y, z)$, $x, y$ are quantified and $z$ is a free variable. Formulas without free variables are called *sentences*.

**The semantics of first order logic** A *structure* is $\mathfrak{A} = (A, R_1^{\mathfrak{A}}, \ldots, R_k^{\mathfrak{A}})$, where

- $A$ is a set of elements, called the *domain* , or the *universe* of $\mathfrak{A}$.
- each $R_i^{\mathfrak{A}}$ is a relation over $A$ of arity $\mathrm{ar}(R_i)$, i.e., $R_i^{\mathfrak{A}} \subseteq A^{\mathrm{ar}(R_i)}$.

Let $\mathfrak{A} = (A, R_1^{\mathfrak{A}}, \ldots, R_k^{\mathfrak{A}})$ be a structure. A *valuation* in $A$ is a mapping from $\mathrm{VAR}$ to $A$. An *model* is a pair $(\mathfrak{A}, val)$ where $\mathfrak{A}$ is a structure and $val$ is a valuation.

Given an FO formula $\varphi$, and a model $(\mathfrak{A}, val)$, we define $(\mathfrak{A}, val)$ to be *a model of* $\varphi$, denoted by $(\mathfrak{A}, val) \models \varphi$, inductively as follows.

- $(\mathfrak{A}, val) \models x = y$, if and only if $val(x) = val(y)$.
- $(\mathfrak{A}, val) \models R(x_1, \ldots, x_n)$, if and only if $(val(x_1), \ldots, val(x_n)) \in R^{\mathfrak{A}}$.
- $(\mathfrak{A}, val) \models \neg\alpha$, if and only if it is *not true* that $(\mathfrak{A}, val) \models \alpha$.
- $(\mathfrak{A}, val) \models \alpha \wedge \beta$, if and only if $(\mathfrak{A}, val) \models \alpha$ and $(\mathfrak{A}, val) \models \beta$.
- $(\mathfrak{A}, val) \models \alpha \vee \beta$, if and only if $(\mathfrak{A}, val) \models \alpha$ or $(\mathfrak{A}, val) \models \beta$.
- $(\mathfrak{A}, val) \models \exists x\ \alpha$, if and only if *there is* some $a \in A$ such that $(\mathfrak{A}, val') \models \alpha$ where $val'$ is the valuation defined as follows:

$$val'(z) \quad = \quad \begin{cases} val(z), & \text{if } z \neq x \\ a, & \text{if } z = x \end{cases}$$

- $(\mathfrak{A}, val) \models \forall x\ \alpha$, if and only if *for every* $a \in A$, $(\mathfrak{A}, val') \models \alpha$ where $val'$ is the valuation defined as follows:

$$val'(z) \quad = \quad \begin{cases} val(z), & \text{if } z \neq x \\ a, & \text{if } z = x \end{cases}$$



doi:10.6342/NTU201802560

When $\varphi$ is a sentence, i.e., there is no free variable in $\varphi$, we can omit the valuation and write $\mathfrak{A} \models \varphi$.

An FO formula $\varphi$ is said to be *satisfiable* if $\varphi$ has a model, and $\varphi$ is *finitely satisfiable* if $\varphi$ has a finite model. We define the following two problems.

| SAT(FO) | |
|---|---|
| **Input:** | An FO formula $\varphi$ |
| **Task:** | Output TRUE, if $\varphi$ is satisfiable. Otherwise, output FALSE. |

| FIN-SAT(FO) | |
|---|---|
| **Input:** | An FO formula $\varphi$ |
| **Task:** | Output TRUE, if $\varphi$ is finitely satisfiable. Otherwise, output FALSE. |

It is well known that in general satisfiability problem of FO is undecidable.

**Theorem 2.1.1 [2, 1, 20, 18]** $\mathrm{SAT}(\mathrm{FO})$ *is undecidable.*

**Theorem 2.1.2 [18]** $\text{FIN-SAT}(\mathrm{FO})$ *is undecidable.*

Therefore, we are not considering the general FO in this thesis.

## 2.2 Two variable logic with counting quantifiers ($\mathrm{C}^2$)

The syntax of $\mathrm{C}^2$ is defined inductively as follows:

$$\phi \ ::= \ z = z \ \mid \ R(z,z) \ \mid \ \neg\phi \ \mid \ \phi \wedge \phi \ \mid \ \exists^{\geq k} z\, \phi$$

where $z$ ranges over $x, y$, $R \in \mathcal{R}$, and $k$ is a nonnegative integer. Here, $\exists^{\geq k} z\phi(z)$ semantically means there exists at least $k$ instances of $z$'s such that $\phi(z)$ holds. Observe that $\forall$ is well-defined, since $\forall x\varphi$ is equivalent to $\neg\exists x\neg\varphi$ for any formula $\varphi$. We note that $x$ and $y$ can be reused, for example, $\forall x(\exists y(\exists x\phi_1(x,y))) \wedge \forall y(\forall x\phi_2(x,y))$ where $\phi_1(x,y)$ and $\phi_2(x,y)$ are quantifier-free formulas is an instance of $\mathrm{C}^2$ formula.

Similar to FO we define $\mathrm{SAT}(\mathrm{C}^2)$ and $\text{FIN-SAT}(\mathrm{C}^2)$ below.



doi:10.6342/NTU201802560

| $\mathrm{SAT}(\mathrm{C}^2)$ | |
|---|---|
| **Input:** | A $\mathrm{C}^2$ formula $\varphi$ |
| **Task:** | Output TRUE, if $\varphi$ is satisfiable. Otherwise, output FALSE. |

| $\mathrm{FIN\text{-}SAT}(\mathrm{C}^2)$ | |
|---|---|
| **Input:** | A $\mathrm{C}^2$ formula $\varphi$ |
| **Task:** | Output TRUE, if $\varphi$ is finitely satisfiable. Otherwise, output FALSE. |

**Theorem 2.2.1 [7, 13, 15, 3, 10]** $\mathrm{SAT}(\mathrm{C}^2)$ *is* NEXPTIME-*complete.*

**Theorem 2.2.2 [7, 15]** $\mathrm{FIN\text{-}SAT}(\mathrm{C}^2)$ *is* NEXPTIME-*complete.*

### 2.2.1 The class $\mathcal{RCS}$

The following is a standard normalization lemma, which is often used in the decision procedures for $\mathrm{FO}^2$ and $\mathrm{C}^2$ formulas [17, 6, 15].

**Lemma 2.2.3 (Scott's normal form)** *For every* $\mathrm{C}^2$ *sentence* $\phi$*, there is a formula*

$$\phi^* \quad := \quad \big(\forall x\ \alpha\big) \wedge \big(\forall x \forall y\ (\beta \vee x = y)\big) \wedge \bigwedge_{1 \le h \le p} \forall x \exists^{=C_h} y\ (f_h(x,y) \wedge x \neq y) \tag{2.1}$$

*that can be constructed in polynomial time in the length of* $\phi$*, and satisfies the following conditions:*

*(C1)* $\alpha$ *is quantifier-free and equality-free.*

*(C2)* $\beta$ *is quantifier-free and equality-free.*

*(C3)* $p$ *is a positive integer.*

*(C4) For any* $h \in \{1, \ldots, p\}$*,* $f_h$ *is a binary predicate and* $C_h$ *is a positive integer.*

*(C5) For any positive integer* $\mu \geq K := \max_{1 \le h \le p} C_h$*,*

$\phi$ *has a model of size* $\mu$ *if and only if* $\phi^*$ *has a model of size* $\mu$*.*

A $\mathrm{C}^2$ sentence of the form 2.1 is called *Scott's normal form*. In this thesis, we assume the set of binary relations used is closed under reversal. Formally, it is stated as follows.



doi:10.6342/NTU201802560

**Definition 2.2.4** A $\mathrm{C}^2$ formula $\varphi$ is an $\mathcal{RCS}$ formula, if it is in Scott's normal form as in (2.1) and for every binary relation $f_h$ appearing in $\bigwedge_{1\leq h\leq p} \forall x \exists^{=C_h} y(f_h(x,y) \wedge x \neq y)$, there is some $h'$ such that $f_h$ is the reversal of $f_{h'}$.

As mentioned before, the proofs in [7, 13, 15] are rather complicated and involve a lot of guessing. In this thesis, we will present decision procedures for $\mathrm{SAT}(\mathrm{C}^2)$ and $\mathrm{FIN}$-$\mathrm{SAT}(\mathrm{C}^2)$ problems, when the input formulas are restricted to $\mathcal{RCS}$ formulas with an entirely different technique. As mentioned earlier, our approach yields a few advantages:

1. It provides a characterization of models of $\mathcal{RCS}$ formulas, i.e., every model of an $\mathcal{RCS}$ formula is a collection of regular digraphs and biregular graphs.
2. It implies the decidability of checking whether the spectrum of an $\mathcal{RCS}$ formula is infinite.
3. It yields a simple decision procedures for satisfiability and finite satisfiability problems.

**Remark 2.2.5** It is worth stating that the satisfiability and finite satisfiability problems for three-variable logic are already undecidable. [8]



doi:10.6342/NTU201802560

doi:10.6342/NTU201802560

# Chapter 3

# Presburger arithmetics

In this chapter, we introduce the formal definition of Presburger arithmetic and its extension with infinity. We will also discuss the satisfiability problem in both cases.

## 3.1 Standard Presburger arithmetic

We define the following structure $\mathcal{N} := \langle \mathbb{N}, +, \leq, 0 \rangle$, where $+, \leq, 0$ are interpreted in the standard way. A formula on Presburger arithmetic is an FO formula over the vocabulary $\{+, \leq, 0\}$.

The satisfiability problem for Presburger arithmetic is defined as follows.

| $\mathrm{SAT}$(Presburger) | |
|---|---|
| **Input:** | A Presburger formula $\varphi$ |
| **Task:** | Output TRUE, if $\mathcal{N} \models \varphi$. Otherwise, output FALSE. |

It is known that $\mathrm{SAT}$(Presburger) is decidable[16, 12], and the algorithm given by Presburger has nonelementary time complexity. The following theorem states that, in fact, the problem $\mathrm{SAT}(Presburger)$ is elementary.

**Theorem 3.1.1** **[12]** $\mathrm{SAT}(Presburger)$ *with input length* $n$ *can be decided in* $O(2^{2^{2^{cn}}})$ *for some constant* $c > 1$.

However, the result above is not efficient enough for our need. So, we turn into a subclass of Presburger formulas.



doi:10.6342/NTU201802560

**Theorem 3.1.2** *When the input Presburger formula $\varphi$ is restricted to existential formula, then* $\mathrm{SAT}(Presburger)$ *is in* $\mathrm{NP}$.

Theorem 3.1.2 follows from Papadimitriou's result for LIP [14], and the detailed discussion can be found in section 3.3.

## 3.2 Presburger arithmetic with infinity

Presburger arithmetic can in fact be further extended to include infinity in its domain. Let $\mathbb{N}_\infty := \mathbb{N} \cup \{\infty\}$. We denote the following structure $\mathcal{N}_\infty := \langle \mathbb{N}_\infty, +, \leq, 0 \rangle$.

- The constant $0$ is interpreted as the standard zero.
- The operator $+$ on $\mathbb{N}$ is interpreted in the standard way, and when $\infty$ is involved, it is defined as follows.

$$\text{For every } a \in \mathbb{N}, \quad a + \infty = \infty + a = \infty + \infty = \infty$$

- The relation $\leq$ on $\mathbb{N}$ is interpreted in the standard way, and when $\infty$ is involved, it is defined as follows.

$$\text{For every } a \in \mathbb{N}, \quad a \leq \infty \text{ and } \infty \leq \infty$$

Notice that the definition above is consistent with our intuition on infinity. We now define the following problem.

| $\mathrm{SAT}$(Presburger-inf) | |
|---|---|
| **Input:** | A Presburger formula $\varphi$ |
| **Task:** | Output TRUE, if $\mathcal{N}_\infty \models \varphi$. Otherwise, output FALSE. |



doi:10.6342/NTU201802560

## 3.3 The satisfiability of Presburger formula

In this section, we will only consider the existential Presburger sentences, i.e., the Presburger sentences of the form:

$$\phi \;=\; \exists X_1 \exists X_2 \ldots \exists X_n \, \varphi(X_1, X_2, \ldots, X_n)$$

where $\varphi$ is quantifier-free. We will show that deciding whether $\mathcal{N} \models \phi$ or $\mathcal{N}_\infty \models \phi$ can be solved using the technique of linear integer programming (LIP).

We first recall the following theorem proved by Christos H. Papadimitriou [14].

**Theorem 3.3.1 [14]** *Let $A$ be an $m \times n$ matrix and $b$ an $m$-vector such that the absolute value of every entry of $A$ or $b$ is no larger than $a$. Then if there exists a solution $x \in \mathbb{N}^n$ for $Ax = b$, there is some $y \in \{0, 1, \ldots n(ma)^{2m+1}\}^n$ such that $Ay = b$.*

From theorem 3.3.1, we can obtain the following corollary.

**Corollary 3.3.2** *Let $A$ be an $m \times n$ matrix and $b$ an $m$-vector such that the absolute value of any entry of $A$ or $b$ is no larger than $a$. Then if there exists a solution $x \in \mathbb{N}^n$ for $Ax \leq b$, there is some $y \in \{0, 1, \ldots (n+m)(ma)^{2m+1}\}^n$ such that $Ay \leq b$.*

**Proof.** Let $I_m$ denoted the $m \times m$ identity matrix, in other words,

$$I_m \;:=\; \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix}$$

It follows immediately by letting

$$A' \;:=\; \left( A \,\middle|\, I_m \right)$$

and noting that $A'x' = b$ has a solution if and only if $Ax \leq b$ has the solution $x$ where $x$ consists of the first $n$ entries of $x'$. By theorem 3.3.1, $x'$ exists if and only if there is



doi:10.6342/NTU201802560

$y' \in \{0, 1, \ldots (n+m)(ma)^{2m+1}\}^{n+m}$ such that $A'y' = b$. Finally, we can conclude that if $Ax \leq b$ has a solution, there exists $y \in \{0, 1, \ldots (n+m)(ma)^{2m+1}\}^n$ where $y$ consists of the first $n$ entries of $y'$ and $Ay \leq b$. ■

Now we can prove the following theorem.

**Theorem 3.3.3** *Both* $\mathrm{SAT}$(Presburger) *and* $\mathrm{SAT}$(Presburger-inf) *are in* $\mathrm{NP}$ *when the input formula* $\varphi$ *is restricted to existential formulas.*

**Proof.** We will describe the polynomial time nondeterministic algorithm here.

Via nondeterminism, for each disjunction $A \vee B$ in $\varphi(X_1, \ldots, X_n)$, we can eliminate either $A$ or $B$ by guessing correctly, since $\varphi(X_1, \ldots, X_n)$ is of quantifier free. Therefore, we can assume $\varphi(X_1, \ldots, X_n)$ is of the form $\phi_1(X_1, \ldots, X_n) \wedge \ldots \wedge \phi_k(X_1, \ldots, X_n)$ where each $\phi_\ell(X_1, \ldots, X_n)$ is a linear inequality, which can be converted into an LIP instance $Ax \leq b$.

For $\mathrm{SAT}$(Presburger), by corollary 3.3.2 and nondeterminism, we can guess the value of each $X_i$ for $i \in \{1, \ldots, n\}$ from $\{0, 1, \ldots (n+k)(na)^{2n+1}\}$ where $a$ is the largest absolute values of the coefficients in all linear equations $\phi_1(X_1, \ldots, X_n), \ldots, \phi_k(X_1, \ldots, X_n)$. Then we check whether the guessed values satisfy all $\phi_1(X_1, \ldots, X_n), \ldots, \phi_k(X_1, \ldots, X_n)$, and conclude the Presburger formula is satisfiable if so, not satisfiable otherwise.

For $\mathrm{SAT}$(Presburger-inf), it works similarly. ■



doi:10.6342/NTU201802560

# Chapter 4

# Regular graphs

In this chapter, we will introduce some tools that we are going to use later on. In particular, we introduce two classes of regular graphs: bipartite regular graphs (biregular graphs) and regular directed graphs (regular digraphs). Intuitively, biregular graphs are bipartite graphs where the degree of each vertex is already fixed, and regular digraphs are directed graphs where the in-degree and out-degree of each vertex are already fixed.

We will show how to construct the existential Presburger formulas that characterize the existence of biregular graphs and regular digraphs. We present the formal definitions in section 4.1. The construction of the Presburger formulas for biregular graphs can be found in section 4.2. A similar construction for regular digraphs can be found in section 4.3.

## 4.1 Definitions

Section 4.1.1 contains the definition of biregular graphs and section 4.1.2 contains the definition of regular digraphs.

### 4.1.1 Biregular graphs

A undirected graph $G$ is an *$\ell$-type bipartite graph* if $G = (U, V, E_1, E_2, \ldots, E_\ell)$ is a bipartite graph where $U$ and $V$ are the partitions of the vertices and $E_1, E_2, \ldots, E_\ell$ are the pairwise disjoint subset of $U \times V$.



doi:10.6342/NTU201802560

For any vertex $u$, the *degree* of $u$, denoted by deg$(u)$, is the number of edges adjacent to $u$ in $G$. The degree of $u$ in the edge set $E_i$ is denoted by $\deg_{E_i}(u)$ for any $i \in \{1, \dots, \ell\}$. Observe that for vertex $u$ in $G$, $\deg(u) = \sum_{i=1,\dots,\ell} \deg_{E_i}(u)$.

In the following, for any set $S$ and $d, e \in \mathbb{N}$, $S^{d \times e}$ is defined to be the set of all $d \times e$ matrices whose entries are in $S$. For $C \in \mathbb{N}^{\ell \times m}$ and $D \in \mathbb{N}^{\ell \times n}$, an $\ell$-type bipartite graph $G = (U, V, E_1, E_2, \dots, E_\ell)$ is $(C, D)$-biregular if there exists some partitions $U_1 \cup \dots \cup U_m$ of $U$ and $V_1 \cup \dots \cup V_n$ of $V$ such that:

- For every $i = 1, \dots \ell$ and $j = 1, \dots, m$, and for any vertex $u \in U_j$, $\deg_{E_i}(u) = C_{i,j}$.
- For every $i = 1, \dots, \ell$ and $j = 1, \dots, n$, and for any vertex $v \in V_j$, $\deg_{E_i}(v) = D_{i,j}$.

We say a $(C, D)$-biregular graph $G$ is of size $(\bar{M}, \bar{N})$ if $\bar{M} = (|U_1|, \dots, |U_m|)$ and $\bar{N} = (|V_1|, \dots, |V_n|)$, and we call $U_1 \cup \dots \cup U_m$ and $V_1 \cup \dots \cup V_n$ a *witness* of $G$.

Note that we do not restrict the graph to be finite. In which case, some entry in $\bar{M}$ or $\bar{N}$ is infinite.

### 4.1.2 Regular digraphs

An $\ell$-type directed graph (digraph) $G = (V, E_1, E_2, \dots, E_\ell)$ is defined similarly, where $E_1, E_2, \dots, E_\ell$ are pairwise disjoint directed edges. For convenience, we always assume that the set $E_1 \cup E_2 \cup \dots \cup E_\ell$ is asymmetric, i.e., if $(u, v) \in E_1 \cup E_2 \cup \dots \cup E_\ell$, then $(v, u) \notin E_1 \cup E_2 \cup \dots \cup E_\ell$.

Similar to how we define the degree of a vertex in an undirected graph, we define the out-going degree and incoming degree of a vertex in a directed graph. The formal definition is as follows: For any vertex $u$, the *out-going degree* of $u$, denoted by out-deg$(u)$, is the number of out-going edges from $u$, and the *incoming degree* of $u$, denoted by in-deg$(u)$, is the number of incoming edges to $u$. The out-going degree of $u$ in the edge set $E_i$ is denoted by out-deg$_{E_i}(u)$, and the incoming degree of $u$ in the edge set $E_i$ is denoted by in-deg$_{E_i}(u)$ for any $i \in \{1, \dots, \ell\}$. Observe that for any vertex $u$ in $G$, out-deg$(u) = \sum_{i=1,\dots,\ell}$ out-deg$_{E_i}(u)$ and in-deg$(u) = \sum_{i=1,\dots,\ell}$ in-deg$_{E_i}(u)$.



doi:10.6342/NTU201802560

For $C, D \in \mathbb{N}^{\ell \times n}$, an $\ell$-type digraph $G = (V, E_1, E_2, \ldots, E_\ell)$ is a $(C, D)$-regular-digraph if there exists a partition of $V = V_1 \cup \ldots \cup V_n$, such that for every $i = 1, \ldots, \ell$ and $j = 1, \ldots, n$, and for any vertex $v \in V_j$, in-deg$_{E_i}(v) = C_{i,j}$ and out-deg$_{E_i}(v) = D_{i,j}$.

We say a $(C, D)$-regular digraph $G$ is of size $\bar{N}$ if $\bar{N} = (|V_1|, \ldots, |V_n|)$, and we call $V_1 \cup \ldots \cup V_n$ a *witness* of $G$.

Observe that $\bar{N}$ has infinite entry if and only if the number of vertices in $G$ is infinite.

## 4.2 Presburger characterization of the existence of biregular graph

In this section, we will prove the following theorem.

**Theorem 4.2.1** *For every two matrices $C \in \mathbb{N}^{\ell \times m}$ and $D \in \mathbb{N}^{\ell \times n}$, there is a (quantifier-free) Presburger formula $\mathrm{BiREG}_{C,D}(\bar{X}, \bar{Y})$, where $\bar{X} = (X_1, \ldots, X_m)$ and $\bar{Y} = (Y_1, \ldots, Y_n)$, such that the followings hold: For any $\bar{M} \in \mathbb{N}_\infty^m$ and $\bar{N} \in \mathbb{N}_\infty^n$, there is an $\ell$-type $(C, D)$-biregular graph of size $(\bar{M}, \bar{N})$ if and only if $\mathrm{BiREG}_{C,D}(\bar{M}, \bar{N})$ holds.*

As a matter of fact, in the finite case, i.e., when $\bar{M}$ and $\bar{N}$ are over $\mathbb{N}$ instead of $\mathbb{N}_\infty$, theorem 4.2.1 has already been proven by Kopczyński and Tan [9]. Our goal is to extend it to infinite case. The proof is divided into parts. We discuss the case of one dimensional matrices in subsection 4.2.1 and extend it to all matrices in 4.2.2.

From now on, for any matrix or vector $M$, we denote the sum of all entries of $M$ by $\sum M$, and we denote the maximum among the sums of the columns of $M$ by $\mathrm{MC}(M)$, i.e., $\mathrm{MC}(M) := \max_j\{\sum_i M_{i,j}\}$.

### 4.2.1 $1$-type biregular graphs

We will first prove the simpler case of theorem 4.2.1 where $C$ and $D$ both only have one row. We will make use of the following notation: For any $m, n, \ell \in \mathbb{N}$ and any two



doi:10.6342/NTU201802560

matrices $C \in \mathbb{N}^{m\times \ell}$ and $D \in \mathbb{N}^{n\times \ell}$,

$$H_{C,D} := \left\{ (\bar{M},\bar{N}) \;\middle|\; \begin{array}{l} \sum \bar{M} + \sum \bar{N} < 2\ell \cdot \mathrm{MC}(C) \cdot \mathrm{MC}(D) + 3\ell \text{ and} \\ \text{there exists a } (C,D)\text{-biregular graph of size } (\bar{M},\bar{N}) \end{array} \right\} \tag{4.1}$$

Below is the special case of theorem 4.2.1, where the matrices consist of a single row.

**Lemma 4.2.2** *For every two vectors $\bar{c} \in \mathbb{N}^{1\times m}$ and $\bar{d} \in \mathbb{N}^{1\times n}$, there is a (quantifier-free) Presburger formula $\mathrm{BiREG}_{\bar{c},\bar{d}}(\bar{X},\bar{Y})$, where $\bar{X} = (X_1,\ldots,X_m)$ and $\bar{Y} = (Y_1,\ldots,Y_n)$, such that the followings hold: For any $\bar{M} \in \mathbb{N}_\infty^m$ and $\bar{N} \in \mathbb{N}_\infty^n$, there exists a $(\bar{c},\bar{d})$-biregular graph of size $(\bar{M},\bar{N})$ if and only if $\mathrm{BiREG}_{\bar{c},\bar{d}}(\bar{M},\bar{N})$ holds.*

**Proof.** Let $\bar{c} = (c_1,\ldots,c_m)$, and $\bar{d} = (d_1,\ldots,d_n)$. Let $I := \{i \mid c_i = 0\}$ and $J := \{j \mid d_j = 0\}$, i.e., the zero entries in $\bar{c}$ and $\bar{d}$. Let $\bar{c}'$ and $\bar{X}'$ be $\bar{c}$ and $\bar{X}$ without entries in $I$, and $\bar{d}'$ and $\bar{Y}'$ be $\bar{d}$ and $\bar{Y}$ without entries in $J$. Observe that both $\bar{c}'$ and $\bar{d}'$ do not have zero entry.

Now define $\mathrm{BiREG}_{\bar{c},\bar{d}}(\bar{X},\bar{Y})$ as follows.

$$\begin{aligned} \mathrm{BiREG}_{\bar{c},\bar{d}}(\bar{X},\bar{Y}) \;:=\; & \Big( \sum \bar{X}' + \sum \bar{Y}' \geq 2 \cdot \mathrm{MC}(\bar{c}') \cdot \mathrm{MC}(\bar{d}') + 3 \;\wedge\; (\bar{X}' \cdot \bar{c}' = \bar{Y}' \cdot \bar{d}') \Big) \\ & \vee \;\Big( \bigvee_{(\bar{M},\bar{N}) \in H_{\bar{c}',\bar{d}'}} \bar{X} = \bar{M} \quad \wedge \quad \bar{Y} = \bar{N} \Big) \end{aligned} \tag{4.2}$$

where

$$H_{\bar{c}',\bar{d}'} = \left\{ (\bar{M},\bar{N}) \;\middle|\; \begin{array}{l} \sum \bar{M} + \sum \bar{N} < 2 \cdot \mathrm{MC}(\bar{c}') \cdot \mathrm{MC}(\bar{d}') + 3 \text{ and} \\ \text{there exists a } (\bar{c}',\bar{d}')\text{-biregular graph of size } (\bar{M},\bar{N}) \end{array} \right\}$$

by definition in 4.1.

The set $H_{\bar{c}',\bar{d}'}$ can be obtained by checking whether there exists a $(\bar{c}',\bar{d}')$-biregular graph of size $(\bar{M},\bar{N})$ for every $(\bar{M},\bar{N})$ such that $\sum \bar{M} + \sum \bar{N} < 2 \cdot \mathrm{MC}(\bar{c}') \cdot \mathrm{MC}(\bar{d}') + 3$.

Note that $\mathrm{BiREG}_{\bar{c},\bar{d}}(\bar{X},\bar{Y})$ holds means the vertices corresponding to $\bar{X}'$ and $\bar{Y}'$ form a $(\bar{c}',\bar{d}')$ -biregular graph while the rest of the vertices can be arbitrary, since they do not have adjacent edges.



doi:10.6342/NTU201802560

**Claim 1** *For any two vectors $\bar{M} \in \mathbb{N}_\infty^m$ and $\bar{N} \in \mathbb{N}_\infty^n$, there exists a $(\bar{c}, \bar{d})$-biregular graph of size $(\bar{M}, \bar{N})$ if and only if $\mathrm{BiREG}_{\bar{c},\bar{d}}(\bar{M}, \bar{N})$ holds.*

**Proof of claim.** By theorem 7.3 of Kopczyński and Tan [9], we know the claim is true when $\bar{M} \in \mathbb{N}^m$ and $\bar{N} \in \mathbb{N}^n$. Let $\bar{M}'$ denote $\bar{M}$ without entries in $I$ and $\bar{N}'$ denote $\bar{N}$ without entries in $J$. We can observe that if both $\bar{M}'$ and $\bar{N}'$ only have finite entries, the claim holds, since $X_i$ for $i \in I$ and $Y_j$ for $j \in J$ can be arbitrary. So,without loss of generality, we can consider the case where there is some infinite entry in $\bar{M}'$.

To prove the "only if" direction, we assume there exists a $(\bar{c}, \bar{d})$-biregular graph of size $(\bar{M}, \bar{N})$. Observe that it is trivial that $\sum \bar{M}' + \sum \bar{N}' \geq 2 \cdot \mathrm{MC}(\bar{c}') \cdot \mathrm{MC}(\bar{d}') + 3$ holds. Finally, both $\bar{M}' \cdot \bar{c}'$ and $\bar{N}' \cdot \bar{d}'$ are the number of edges in the biregular graph, implying $\bar{M}' \cdot \bar{c}' = \bar{N}' \cdot \bar{d}' = \infty$. Hence, $\mathrm{BiREG}_{\bar{c},\bar{d}}(\bar{M}, \bar{N})$ holds.

For the "if" direction, we first observe that $(\bar{M}', \bar{N}') \notin H_{\bar{c}',\bar{d}'}$ since $\bar{M}'$ has infinite entry. Therefore, in order for $\mathrm{BiREG}_{\bar{c},\bar{d}}(\bar{M}, \bar{N})$ to hold, $\bar{M}' \cdot \bar{c}' = \bar{N}' \cdot \bar{d}' = \infty$ must hold, and we can conclude there is some infinite entry in $\bar{N}'$ as well. Let $U = U_1 \cup \ldots \cup U_m$ be a partition where $|U_i| = M_i$ and let $V = V_1 \cup \ldots \cup V_n$ be a partition where $|V_j| = N_j$. Now we can construct a $(\bar{c}, \bar{d})$ biregular graph recursively by repeating the steps below.

- Assume the vertices in each $U_i$ and $V_j$ are ordered, and we iterate through the sets $U_1, \ldots, U_m, V_1, \ldots, V_n$.
- Suppose the set we are currently at is $U_i$. We find the first vertex $u$ such that its current degree is less than $c_i$. Since $\bar{N}'$ has at least one infinite entry, say $N_j = \infty$, we can always find a vertex $v$ in $V_j$ with its number of edges less than $d_j$ during the construction, and we connect $u$ and $v$ with an edge.
- Similarly, suppose the set we are currently at is $V_j$. We find the first vertex $v$ such that its current degree is less than $d_j$. Since $\bar{M}'$ has at least one infinite entry, say $M_i = \infty$, we can always find a vertex $u$ in $U_i$ with its number of edges less than $c_i$ during the construction, and we connect $u$ and $v$ with an edge.

With such construction, we will achieve a $(\bar{c}, \bar{d})$-biregular graph in infinite steps.



doi:10.6342/NTU201802560

By symmetry, the claim also holds for the case where there is some infinite entry in $\bar{N}'$. Thus the claim holds. $\square$

The claim concludes the proof for lemma 4.2.2. $\blacksquare$

### 4.2.2 Proof of theorem 4.2.1

By deleting any zero column $\bar{c}_i$ (or $\bar{d}_i$) of $C$ (or $D$, respectively) and adding the constraint $X_i \geq 0$ (or $Y_i \geq 0$) to the resulting Presburger formula, we can assume both $C, D$ do not contain any zero-column.

The formal construction of $\mathrm{BiREG}_{C,D}(\bar{X}, \bar{Y})$ is as follows. First, we define the characteristic function $\chi : \mathbb{N}^* \to \{0,1\}^*$ where $\mathbb{N}^* := \bigcup_{k\geq 1} \mathbb{N}^k$ and $\{0,1\}^* := \bigcup_{k\geq 1}\{0,1\}^k$.

$\chi(a_1, \ldots, a_k) := (b_1, \ldots, b_k)$, where $b_i = 0$ if $a_i = 0$ and $b_i = 1$ otherwise.

Also, let $\bar{c}_1, \bar{c}_2, \ldots, \bar{c}_\ell$ be the row vectors of $C$, and $\bar{d}_1, \bar{d}_2, \ldots, \bar{d}_\ell$ be the row vectors of $D$. That is,

$$C = \begin{pmatrix} \bar{c}_1 \\ \bar{c}_2 \\ \vdots \\ \bar{c}_\ell \end{pmatrix} \quad \text{and} \quad D = \begin{pmatrix} \bar{d}_1 \\ \bar{d}_2 \\ \vdots \\ \bar{d}_\ell \end{pmatrix}.$$

Now we can construct $\mathrm{BiREG}_{C,D}(\bar{X}, \bar{Y})$ inductively:

- When $\ell = 1$,

$$\mathrm{BiREG}_{C,D}(\bar{X}, \bar{Y}) \quad := \quad \mathrm{BiREG}_{\bar{c}_1, \bar{d}_1}(\bar{X}, \bar{Y}).$$



doi:10.6342/NTU201802560

- When $\ell \geq 2$,

$$\begin{aligned}\mathrm{BiREG}_{C,D}(\bar{X},\bar{Y}) := & \bigvee_{(\bar{M},\bar{N})\in H_{C,D}} \bar{X}=\bar{M} \quad \wedge \quad \bar{Y}=\bar{N} \\ & \vee \bigvee_{i=1,\ldots,\ell} \Big( \bar{X}\cdot\chi(\bar{c}_i)+\bar{Y}\cdot\chi(\bar{d}_i) \geq 2\cdot \mathrm{MC}(C)\cdot \mathrm{MC}(D)+3 \\ & \qquad \wedge \ \mathrm{BiREG}_{C\setminus\bar{c}_i,D\setminus\bar{d}_i}(\bar{X},\bar{Y}) \\ & \qquad \wedge \ \mathrm{BiREG}_{\bar{c}_i,\bar{d}_i}(\bar{X},\bar{Y}) \Big)\end{aligned} \tag{4.3}$$

where $C \setminus \bar{c}_i$ denotes the matrix $C$ without $\bar{c}_i$, and $D \setminus \bar{d}_i$ denotes the matrix $D$ without $\bar{d}_i$. Observe that $H_{C,D}$ is defined with equation 4.1 and can be greedily computed with the same method as before.

Then we shall prove that there exists an $\ell$-type $(C, D)$-biregular graph of size $(\bar{M}, \bar{N})$ if and only if $\mathrm{BiREG}_{C,D}(\bar{M}, \bar{N})$ holds by induction. First, the case for $\ell = 1$ is equivalent to the statement in lemma 4.2.2. Now suppose the induction hypothesis holds when $C$ and $D$ have no more than $\ell - 1$ rows. We will prove for the case $\ell$.

- For the "if" direction, we assume $\mathrm{BiREG}_{C,D}(\bar{M}, \bar{N})$ holds. If the first part of formula 4.3 holds, that is $\bigvee_{(\bar{M},\bar{N})\in H_{C,D}} \bar{X} = \bar{M} \wedge \bar{Y} = \bar{N}$ holds, the biregular graph exists trivially. Therefore, we only have to consider the case where

  $$\bar{M}\cdot\chi(\bar{c}_i)+\bar{N}\cdot\chi(\bar{d}_i) \geq 2\cdot \mathrm{MC}(C)\cdot \mathrm{MC}(D)+3$$
  $$\wedge$$
  $$\mathrm{BiREG}_{C\setminus\bar{c}_i,D\setminus\bar{d}_i}(\bar{M},\bar{N}) \ \wedge \ \mathrm{BiREG}_{\bar{c}_i,\bar{d}_i}(\bar{M},\bar{N})$$

  holds for some $i \in \{1, \ldots, \ell\}$.

  We first consider the case where $|E_i| \neq \infty$. By induction hypothesis, there exist a $(C\setminus\bar{c}_i, D\setminus\bar{d}_i)$-biregular graph with edge partition $E_1\cup\ldots\cup E_{i-1}\cup E_{i+1}\cup\ldots\cup E_\ell$ and a $(\bar{c}_i, \bar{d}_i)$-biregular graph with edge partition $E_i$ both of size $(\bar{M}, \bar{N})$. The vertices of the two graphs can be merged one-to-one since they have the same size. However, the edge set $\{E_1, \ldots, E_\ell\}$ may not be pairwise disjoint, as there may be some some edge in $E_i \cap (E_1 \cup \ldots \cup E_{i-1} \cup E_{i+1} \cup \ldots \cup E_\ell)$, and suppose $(u, v)$ is such an edge.



doi:10.6342/NTU201802560

Observe that there are at most $2 \cdot \mathrm{MC}(C) \cdot \mathrm{MC}(D) + 2$ vertices that can be reached within 2 edges in $E_1 \cup \ldots \cup E_\ell$ from either $u$ or $v$, including $u$ and $v$ themselves. Since $\bar{M} \cdot \chi(\bar{c}_i) + \bar{N} \cdot \chi(\bar{d}_i) \geq 2 \cdot \mathrm{MC}(C) \cdot \mathrm{MC}(D) + 3$, there exists some edge $(u', v') \in E_i$ such that $(u, v'), (u', v) \notin E_1 \cup \ldots \cup E_{i-1} \cup E_{i+1} \cup \ldots \cup E_\ell$. By removing $(u, v), (u', v')$ from $E_i$ and adding $(u, v'), (u', v)$ to $E_i$, the resulting edge set $E_i'$ will still be an edge partition for a $(\bar{c}_i, \bar{d}_i)$-biregular graph. Moreover,

$$|E_i \cap (E_1 \cup \ldots \cup E_{i-1} \cup E_{i+1} \cup \ldots \cup E_\ell)| > |E_i' \cap (E_1 \cup \ldots \cup E_{i-1} \cup E_{i+1} \cup \ldots \cup E_\ell)|$$

holds. Hence, by repeating the step of replacing the edges in $E_i$, we will eventually get a set $E_i''$ such that $|E_i'' \cap (E_1 \cup \ldots \cup E_{i-1} \cup E_{i+1} \cup \ldots \cup E_\ell)| = 0$ when $|E_i| \neq \infty$. This completes the construction of $(C, D)$-biregular graph for finite $E_i$.

Now, we assume $|E_i| = \infty$. Observe that in this case, $\bar{M} \cdot \chi(\bar{c}_i) + \bar{N} \cdot \chi(\bar{d}_i) = \infty$, and hence $\bar{M} \cdot \chi(\bar{c}_i) = \bar{N} \cdot \chi(\bar{d}_i) = \infty$.

By induction hypothesis, we can let $G = (U, V, E_1, \ldots, E_{i-1}, E_{i+1}, \ldots, E_\ell)$ be a $(C \setminus \bar{c}_i, D \setminus \bar{d}_i)$-biregular graph, and let $U = U_1 \cup \ldots \cup U_m$ and $V = V_1 \cup \ldots \cup V_n$ be a witness of $G$. We will construct the $(C, D)$-biregular graph recursively by repeating the steps below.

- Assume the vertices in each $U_{i'}$ and $V_{j'}$ are ordered, and then we can iterate through the sets $U_1, \ldots, U_m, V_1, \ldots, V_n$.
- Suppose the set we are currently at is $U_{i'}$. We find the first vertex $u$ such that its current degree in $E_i$ is less than $C_{i,i'}$. Since $\bar{N} \cdot \chi(\bar{d}_i) = \infty$, $\bar{N}$ has at least one infinite entry, say $N_{j'} = \infty$, such that $D_{i,j'} > 0$, so we can always find a vertex $v$ in $V_{j'}$ with its number of edges less than $D_{i,j'}$ during the construction, and we add $(u, v)$ into $E_i$.
- Similarly, suppose the set we are currently at is $V_{j'}$. We find the first vertex $v$ such that its current degree in $E_i$ is less than $D_{i,j'}$. Since $\bar{M} \cdot \chi(\bar{c}_i) = \infty$, $\bar{M}$ has at least one infinite entry, say $M_{i'} = \infty$, such that $C_{i,i'} > 0$, so we can always find a vertex $u$ in $U_{i'}$ with its number of edges less than $C_{i,i'}$ during the



doi:10.6342/NTU201802560

construction, and we add $(u, v)$ into $E_i$.

By repeating the steps above, we will obtain a $(C, D)$-biregular graph over infinite steps.

- Finally, we prove the " only if " direction. Suppose there is a $(C, D)$-biregular graph $G = (U, V, E_1, \ldots, E_\ell)$ of size $(\bar{M}, \bar{N})$. If $\sum \bar{M} + \sum \bar{N} < 2\ell \cdot \mathrm{MC}(C) \cdot \mathrm{MC}(D) + 3\ell$, then $(\bar{M}, \bar{N}) \in H_{C,D}$ and $\mathrm{BiREG}_{C,D}(\bar{M}, \bar{N})$ holds trivially.

  Consider the case where $\sum \bar{M} + \sum \bar{N} \geq 2\ell \cdot \mathrm{MC}(C) \cdot \mathrm{MC}(D) + 3\ell$. Since $C$ and $D$ both do not have zero-column, we can find some $i \in \{1, \ldots, \ell\}$ such that $\bar{M} \cdot \chi(\bar{c}_i) + \bar{N} \cdot \chi(\bar{d}_i) \geq 2 \cdot \mathrm{MC}(C) \cdot \mathrm{MC}(D) + 3$. Also, we notice that $G_1 := (U, V, E_1, \ldots, E_{i-1}, E_{i+1}, \ldots, E_\ell)$ is a $(C \setminus \bar{c}_i, D \setminus \bar{d}_i)$-biregular graph and $G_2 := (U, V, E_i)$ is a $(\bar{c}_i, \bar{d}_i)$-biregular graph. Therefore, by induction hypothesis, $\mathrm{BiREG}_{C \setminus \bar{c}_i, D \setminus \bar{d}_i}(\bar{M}, \bar{N})$ and $\mathrm{BiREG}_{\bar{c}_i, \bar{d}_i}(\bar{M}, \bar{N})$ both hold.

This completes our proof.

## 4.3 Presburger characterization of the existence of regular digraph

Using similar technique, regular digraphs can be characterized by Presburger formulas as well as stated in the following theorem.

**Theorem 4.3.1** *For every two matrices $C, D \in \mathbb{N}^{\ell \times m}$, there is a (quantifier-free) Presburger formula $\mathrm{REG}_{C,D}(\bar{X})$, where $\bar{X} = (X_1, \ldots, X_m)$, such that the following holds: For any $\bar{M} \in \mathbb{N}^m$, there exists a $(C, D)$-regular-digraph of size $\bar{M}$ if and only if $\mathrm{REG}_{C,D}(\bar{M})$ holds.*

Before proving theorem 4.3.1, we first prove some auxiliary lemmas.

**Lemma 4.3.2** *Let $\bar{c}, \bar{d} \in \mathbb{N}^{1 \times m}$ be one-row vectors. For every $\bar{M} \in \mathbb{N}^m$ that satisfies the inequality $2 \cdot \sum \bar{M} \geq 2 \cdot \mathrm{MC}(\bar{c}) \cdot \mathrm{MC}(\bar{d}) + 3$, the following holds.*



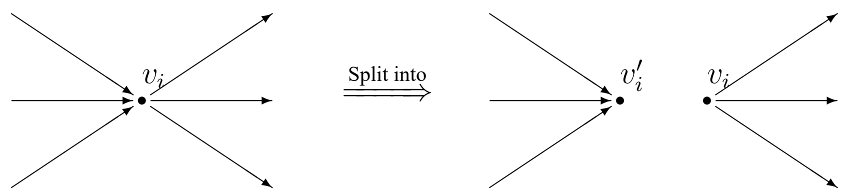
doi:10.6342/NTU201802560

*There is a $(\bar{c}, \bar{d})$-regular-digraph of size $\bar{M}$ if and only of there exists a $(\bar{c}, \bar{d})$-biregular graph of size $(\bar{M}, \bar{M})$.*

**Proof.** For the "only if" direction, we assume there exists a $(\bar{c}, \bar{d})$-regular-digraph $G = (V, E)$ of size $\bar{M}$. Then we "split" each vertex in $V$ as follows.

- Let $V = \{v_1, v_2, \ldots, v_n\}$ (or $V = \{v_1, v_2, \ldots\}$ when $V$ has infinite vertices).
- Let $V' := \{v'_1, v'_2, \ldots, v'_n\}$ (or $V' := \{v'_1, v'_2, \ldots\}$ when $V$ has infinite vertices) be a set where there is an one-to-one correspondence between the elements in $V'$ and $V$.
- $E' := \{(v_j, v'_k) \mid (v_j, v_k) \in E\}$.

The following figure describe the intuitive meaning. Each vertex $v_i$ is split into two: one has all the out-going edges and the other has all the incoming edges.



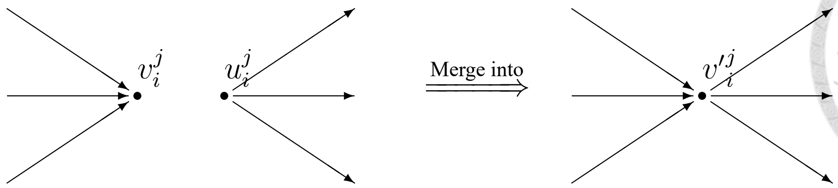

The resulting graph is a biregular graph of size $(\bar{M}, \bar{M})$.

For the "if" direction, we assume there exists a $(\bar{c}, \bar{d})$-biregular graph $G = (U, V, E)$ of size $(\bar{M}, \bar{M})$ with witness $U = U_1 \cup \ldots \cup U_m$ and $V = V_1 \cup \ldots \cup V_m$. Note that $|U_i| = |V_i|$ for all $i$. Suppose $U_i = \{u_i^j \mid 0 \leq i < |U_i|\}$ and $V_i = \{v_i^j \mid 0 \leq i < |V_i|\}$. To construct a regular digraph, we first *merge* the vertex set $U_i$ and $V_i$ for all $i = 1, \ldots, m$ into a new set $V' = \{{v'}_i^j \mid 0 \leq i < |V_i|\}$ by considering $u_i^j$ and $v_i^j$ as the same vertex ${v'}_i^j$ for all $0 \leq j < |U_i|$. Then we construct the directed edge set $E'$ in the new directed graph by defining

$$E' := \{({v'}_i^j, {v'}_{i'}^{j'}) \mid 1 \leq i \leq m, 1 \leq i' \leq m, 0 \leq j < |U_i|, 0 \leq j' < |U_i| \text{ and } (u_i^j, v_{i'}^{j'}) \in E\}.$$



doi:10.6342/NTU201802560




We note here the new graph $G' := (V', E')$ might not be a regular digraph since there could be self-loop or inverse edges in $G'$. However, since $2 \cdot \sum \bar{M} \geq 2 \cdot \mathrm{MC}(\bar{c}) \cdot \mathrm{MC}(\bar{d}) + 3$ holds, we can eliminate them with the technique as in lemma 4.2.2. Specifically, for any self-loop $(v, v) \in E$, there exists an edge $(u, u') \in E$ that is not adjacent to $v$, and we can replace the edges $(v, v), (u, u')$ with $(u, v), (v, u')$. Likewise, for any two inverse edges $(v, v'), (v', v) \in E$, there is an edge $(u, u')$ that is not adjacent to both $v$ and $v'$, and we can replace $(v, v')$ and $(u, u')$ with $(v, u')$ and $(u, v')$ to eliminate the inverse edges. Therefore, we conclude that there is a $(\bar{c}, \bar{d})$-biregular graph of size $(\bar{M}, \bar{M})$. ■

We require another lemma as stated below.

**Lemma 4.3.3** *Let $C, D \in \mathbb{N}^{\ell \times m}$ be matrices of same size. When $\bar{M} \in \mathbb{N}^m$ satisfies the inequality $\bar{M} \cdot \chi(\bar{c}_i) + \bar{M} \cdot \chi(\bar{d}_i) \geq 2 \cdot \mathrm{MC}(C) \cdot \mathrm{MC}(D) + 3$ for some $i \in \{1, \ldots, \ell\}$, the following two statements are equivalent.*

*(1) There is a $(C, D)$-regular-digraph of size $\bar{M}$.*

*(2) There exist a $(\bar{c}_i, \bar{d}_i)$-regular digraph and a $(C \setminus \bar{c}_i, D \setminus \bar{d}_i)$-regular digraph both of size $\bar{M}$.*

**Proof.** The direction from the first to second follows immediately from the structure of regular digraph.

To prove the direction from the second to first, we first construct a directed graph $G = (V, E_1, \ldots, E_\ell)$ such that

- $G = (V, E_i)$ is a $(\bar{c}_i, \bar{d}_i)$-regular digraph of size $\bar{M}$, and



doi:10.6342/NTU201802560

- $G = (V, E_1, \ldots, E_{i-1}, E_{i+1}, \ldots E_\ell)$ is a $(C \setminus \bar{c}_i, D \setminus \bar{d}_i)$-regular digraph of size $\bar{M}$.

Although there might be parallel edges with this construction, they can be eliminated with the same technique in theorem 4.2.1 since $\bar{M} \cdot \chi(\bar{c}_i) + \bar{M} \cdot \chi(\bar{d}_i) \geq 2 \cdot \mathrm{MC}(C) \cdot \mathrm{MC}(D) + 3$. This completes our proof. ■

Before proving theorem 4.3.1, we define the following set

$$H'_{C,D} \quad := \quad \left\{ (\bar{M}, \bar{M}) \;\middle|\; \begin{array}{l} 2 \cdot \sum \bar{M} < 2\ell \cdot \mathrm{MC}(C) \cdot \mathrm{MC}(D) + 3\ell \text{ and there} \\ \text{exists a } (C, D)\text{-regular digraph of size } (\bar{M}, \bar{M}) \end{array} \right\} \tag{4.4}$$

for any $m, n, \ell \in \mathbb{N}$ and any two matrices $C \in \mathbb{N}^{m \times \ell}$ and $D \in \mathbb{N}^{n \times \ell}$. Notice the difference between $H'_{C,D}$ and $H_{C,D}$ in equation 4.1 is that $H'_{C,D}$ is defined with respect to biregular graphs whereas $H'_{C,D}$ is defined with respect to regular digraphs. The proof of theorem 4.3.1 follows.

**Proof of theorem 4.3.1** The formula $\mathrm{REG}_{C,D}(\bar{X})$ can be similarly defined as in equations 4.2 and 4.3, by replacing any $H_{C',D'}$ with $H'_{C',D'}$ for any matrices $C', D'$ such that $H_{C',D'}$ is in the $\mathrm{BiREG}_{C,D}(\bar{X}, \bar{X})$ formula. The correctness of the base case where $C, D$ are single-row matrices is ensured by lemma 4.3.2. The correctness of the induction step is ensured by lemma 4.3.3. This completes our proof. ■



doi:10.6342/NTU201802560

# Chapter 5

# Satisfiability of $\mathcal{RCS}$ formulas via Presburger arithmetics

For this chapter we will show that every $\mathcal{RCS}$ sentence can be converted effectively to a Presburger formula that preserve satisfiability. The construction of such Presburger formula can be found in section 5.1. The proof of correctness is in section 5.2, and the complexity analysis is in section 5.3.

## 5.1 Constructing Presburger formula from an $\mathcal{RCS}$ sentence

In this section and the next, we will prove the following theorem.

**Theorem 5.1.1** *For every $\mathcal{RCS}$ sentence $\phi$, there is a Presburger formula $\mathrm{PREB}_\phi$ such that*

- *$\phi$ has a finite model if and only if $\mathrm{PREB}_\phi$ is satisfiable in $\mathcal{N}$*
- *$\phi$ has a model if and only if $\mathrm{PREB}_\phi$ is satisfiable in $\mathcal{N}_\infty$.*

Recall from Definition 2.2.4 that a formula $\varphi$ is an $\mathcal{RCS}$ formula, if it is in Scott's



doi:10.6342/NTU201802560

normal form:

$$\phi \ := \ \big(\forall x\ \alpha\big) \wedge \big(\forall x \forall y\ (\beta \vee x = y)\big) \wedge \bigwedge_{1 \le h \le p} \forall x \exists^{=C_h} y\ (f_h(x,y) \wedge x \neq y),$$

where $\alpha$ and $\beta$ are quantifier-free and equality-free, and for every binary relation $f_h$, there is some $h'$ such that $f_h$ is the reversal of $f_{h'}$.

**The algorithm for** $\mathrm{SAT}$ **and** $\mathrm{FIN\text{-}SAT}$**.** Overall our algorithm for checking the satisfiability and finite-satisfiability works as follows.

---

**Algorithm 1** Algorithm for $\mathrm{SAT}$ and $\mathrm{FIN\text{-}SAT}$

**Input:** An $\mathcal{RCS}$ sentence $\phi$

1: Convert $\phi$ into Presburger formula $\mathrm{PREB}_\phi$ according to theorem 5.1.1.

2: If $\mathrm{PREB}_\phi$ holds, then output TRUE. Otherwise, output FALSE.

---

We will show that Step 2 is in $2\text{-NEXPTIME}$ and yields an instance of LIP of double exponential size. Since the satisfiability of LIP is in $\mathrm{NP}$, overall, our algorithm runs in $2\text{-NEXPTIME}$. The crucial part is of course the construction of the Presburger formula. We will explain it in the following.

**The construction of** $\mathrm{PREB}_\phi$**.** Now given an $\mathcal{RCS}$ sentence $\phi$ as in 2.1 we will describe the construction of the desired Presburger formula $\mathrm{PREB}_\phi$ below.

We define a one-type to be a maximal consistent set of unary predicates in $\phi$ and their negations, and a two-type to include $(x \neq y)$ and a maximal consistent set of binary predicates in $\phi$ and their negations.

Let $\mathcal{T} = \{T_1, T_2, \ldots, T_n\}$ be the set of all one-types and $\mathcal{E} = \{E_1, \ldots, E_\ell, \overleftarrow{E}_1, \ldots, \overleftarrow{E}_\ell\}$, where $\overleftarrow{E}_i(x,y) = E_i(y,x)$ for all $i = 1, \ldots, \ell$, be the set of the two-types of $\phi$ such that for every $E \in \mathcal{E}$, $E \models (f_h \wedge (x \neq y))$ for some $h \in \{1, \ldots, p\}$. Notice $\mathcal{E}$ is well-defined since the set of binary predicates is closed under reversal. Observe that for an arbitrary structure $\mathfrak{A}$, the sets $A_1, \ldots, A_n$ where $A_i := \{a \in \mathfrak{A} \text{ s.t. } \mathfrak{A}, a \models T_i\}$ form a pairwise-disjoint partition of $A$. For convenience, we sometimes refer to $A_i$ as $T_i$ when it won't cause confusion. (eg. writing an element of $A_i$ as an element of $T_i$). Also for simplicity, we sometimes use $S$ to represent $\bigwedge_{s \in S} s$ for some $S \in \mathcal{T} \cup \mathcal{E}$.



doi:10.6342/NTU201802560

Observe that for any quantifier-free and equality-free subformula $f$ of $\phi$, $f \wedge (x \neq y)$ can be rewritten as $\bigvee_{E \in \hat{\mathcal{E}}} E$ where $\hat{\mathcal{E}} \subsetneq \mathcal{E}$. Also observe that $\mathcal{E}$ is a pairwise disjoint partition of a subset of $\{(x, y) \in A \times A \mid x \neq y\}$.

A function $g : \mathcal{T} \times \mathcal{E} \times \mathcal{T} \to \{0, 1, \ldots, C\}$ is said to be *consistent* if

- for any fixed $T \in \mathcal{T}$ and $h \in \{1, \ldots, p\}$,

$$\sum_{E \in \mathcal{E} \text{ s.t. } E \models (f_h \wedge (x \neq y))} \quad \sum_{T' \in \mathcal{T}} g(T, E, T') \quad = \quad C_h.$$

Let $\mathcal{G} = \{g_1, g_2, \ldots, g_m\}$ be the set enumerating all consistent functions.

Given a structure $\mathfrak{A}$, an element $a \in A$ is called a $(T, g)$-element if it is of type $T$ and the number of its out-going $E$-edges towards the elements of any type $T'$ is exactly $g(T, E, T')$.

Our desired formula $\mathrm{PREB}_\phi$ will be defined as follows:

$$\mathrm{PREB}_\phi := \exists X_{(T_1, g_1)} \ldots \exists X_{(T_n, g_m)} \, \mathrm{FORALL}_1(\bar{X}) \wedge \mathrm{FORALL}_2(\bar{X}) \wedge \mathrm{CON}(\bar{X}) \quad (5.1)$$

where $\bar{X} := (X_{(T_1,g_1)}, X_{(T_1,g_2)}, \ldots, X_{(T_n,g_m)})$. Intuitively, $X_{(T_i,g_j)}$ represent the number of $(T_i, g_j)$-elements.

Now, we define $\mathrm{FORALL}_1$, $\mathrm{FORALL}_2$ and CON below:

- The formula $\mathrm{CON}(\bar{X})$: We first define matrices $D_{S \to T}, \overleftarrow{D}_{S \to T} \in \mathbb{N}^{\ell \times m}$ as follows for any $S$ and $T \in \mathcal{T}$.

$$D_{S \to T} \quad := \quad \begin{pmatrix} g_1(S, E_1, T) & g_2(S, E_1, T) & \cdots & g_m(S, E_1, T) \\ g_1(S, E_2, T) & g_2(S, E_2, T) & \cdots & g_m(S, E_2, T) \\ \vdots & \vdots & \ddots & \vdots \\ g_1(S, E_\ell, T) & g_2(S, E_\ell, T) & \cdots & g_m(S, E_\ell, T) \\ g_1(S, \overleftarrow{E}_1, T) & g_2(S, \overleftarrow{E}_1, T) & \cdots & g_m(S, \overleftarrow{E}_1, T) \\ g_1(S, \overleftarrow{E}_2, T) & g_2(S, \overleftarrow{E}_2, T) & \cdots & g_m(S, \overleftarrow{E}_2, T) \\ \vdots & \vdots & \ddots & \vdots \\ g_1(S, \overleftarrow{E}_\ell, T) & g_2(S, \overleftarrow{E}_\ell, T) & \cdots & g_m(S, \overleftarrow{E}_\ell, T) \end{pmatrix}$$



doi:10.6342/NTU201802560

and

$$\overleftarrow{D}_{S\to T} := \begin{pmatrix} g_1(T,\overleftarrow{E}_1,S) & g_2(T,\overleftarrow{E}_1,S) & \cdots & g_m(T,\overleftarrow{E}_1,S) \\ g_1(T,\overleftarrow{E}_2,S) & g_2(T,\overleftarrow{E}_2,S) & \cdots & g_m(T,\overleftarrow{E}_2,S) \\ \vdots & \vdots & \ddots & \vdots \\ g_1(T,\overleftarrow{E}_\ell,S) & g_2(T,\overleftarrow{E}_\ell,S) & \cdots & g_m(T,\overleftarrow{E}_\ell,S) \\ g_1(T,E_1,S) & g_2(T,E_1,S) & \cdots & g_m(T,E_1,S) \\ g_1(T,E_2,S) & g_2(T,E_2,S) & \cdots & g_m(T,E_2,S) \\ \vdots & \vdots & \ddots & \vdots \\ g_1(T,E_\ell,S) & g_2(T,E_\ell,S) & \cdots & g_m(T,E_\ell,S) \end{pmatrix}$$

Then for any $T \in \mathcal{T}$, $D_T, \overleftarrow{D}_T \in \mathbb{N}^{\ell\times m}$ is defined as follows:

$$D_T := \begin{pmatrix} g_1(T,E_1,T) & g_2(T,E_1,T) & \cdots & g_m(T,E_1,T) \\ g_1(T,E_2,T) & g_2(T,E_2,T) & \cdots & g_m(T,E_2,T) \\ \vdots & \vdots & \ddots & \vdots \\ g_1(T,E_\ell,T) & g_2(T,E_\ell,T) & \cdots & g_m(T,E_\ell,T) \end{pmatrix}$$

and

$$\overleftarrow{D}_T := \begin{pmatrix} g_1(T,\overleftarrow{E}_1,T) & g_2(T,\overleftarrow{E}_1,T) & \cdots & g_m(T,\overleftarrow{E}_1,T) \\ g_1(T,\overleftarrow{E}_2,T) & g_2(T,\overleftarrow{E}_2,T) & \cdots & g_m(T,\overleftarrow{E}_2,T) \\ \vdots & \vdots & \ddots & \vdots \\ g_1(T,\overleftarrow{E}_\ell,T) & g_2(T,\overleftarrow{E}_\ell,T) & \cdots & g_m(T,\overleftarrow{E}_\ell,T) \end{pmatrix}$$

Let $\bar{X}_{T_i}$ denotes $(X_{(T_i,g_1)},\ldots,X_{(T_i,g_m)})$. Define CON as follows.

$$\begin{aligned} \mathrm{CON}(\bar{X}) &:= \bigwedge_{1\le i\le n} \mathrm{REG}_{D_{T_i},\overleftarrow{D}_{T_i}}(\bar{X}_{T_i}) && (5.2) \\ &\quad \wedge \bigwedge_{1\le i<j\le n} \mathrm{BiREG}_{D_{T_i\to T_j},\overleftarrow{D}_{T_i\to T_j}}(\bar{X}_{T_i},\bar{X}_{T_j}) && (5.3) \end{aligned}$$

For the part $\bigwedge_{1\le h\le p} \forall x \exists^{=C_h} y\, (f_h(x,y) \wedge x \neq y)$ in $\phi$, CON ensures that the formula



doi:10.6342/NTU201802560

is satisfiable if and only if there exists a structure such that each of its subgraph formed by any two distinct one-types is a biregular graph, each of its subgraph of a one-type is a regular digraph, and the biregular graphs and regular digraphs are all consistent with the formula.

- The formula $\mathrm{FORALL}_1(\bar{X})$ is to capture the part $\forall x\alpha$ in $\phi$. Note that $\forall x\alpha$ is equivalent to $\neg\exists x\neg\alpha$. Thus, we can define $\mathrm{FORALL}_1(\bar{X})$ as follows:

$$\mathrm{FORALL}_1(\bar{X}) \quad := \quad \bigwedge_{T\in\mathcal{T} \text{ s.t. } T\models\neg\alpha} \quad \bigwedge_{1\le j\le m} X_{(T,g_j)} = 0$$

- Similarly, the formula $\mathrm{FORALL}_2(\bar{X})$ is to capture $\forall x\forall y(\beta\vee x=y)$ in $\phi$, which is equivalent to $\neg\exists x\exists y(\neg\beta\wedge x\ne y)$. We first define the following set:

$$H \quad := \quad \left\{ (T,g)\in\mathcal{T}\times\mathcal{G} \;\middle|\; \begin{array}{l} \text{For some } S\in\mathcal{T} \text{ and some } E\in\mathcal{E} \text{ s.t.} \\ E\models(\neg\beta\wedge(x\ne y)), g(T,E,S)>0. \end{array} \right\} \tag{5.4}$$

And $\mathrm{FORALL}_2$ will be as follows:

$$\mathrm{FORALL}_2(\bar{X}) \quad := \quad \bigwedge_{(T,g)\in H} X_{(T,g)} = 0$$

This completes our construction of formula 5.1. The correctness of construction can be found in section 5.2 and the complexity analysis can be found in section 5.3.

## 5.2 The preservation of satisfiability

Now that $\mathrm{PREB}_\phi$ is defined, we will prove the satisfiability of $\mathrm{PREB}_\phi$ is preserved in both finite and infinite cases in this section.

**Lemma 5.2.1** *For any $\mathcal{RCS}$ sentence $\phi$, the following holds.*

- *$\phi$ has a model if and only if $\mathcal{N}_\infty \models \mathrm{PREB}_\phi$.*
- *$\phi$ has a finite model if and only if $\mathcal{N} \models \mathrm{PREB}_\phi$.*



doi:10.6342/NTU201802560

**Proof.** We will divide our proof into the "if" direction and the "only of" direction. For the if direction:

**Claim 2** *For any $\mathcal{RCS}$ sentence $\phi$, the following holds.*

- *$\phi$ has a model if $\mathcal{N}_\infty \models \mathrm{PREB}_\phi$.*
- *$\phi$ has a finite model if $\mathcal{N} \models \mathrm{PREB}_\phi$.*

**Proof of claim.** Let $\bar{M} := (M_{T_1,g_1}, M_{T_1,g_2}, \ldots, M_{T_n,g_m})$ be a vector such that $\mathrm{FORALL}_1(\bar{M})$, $\mathrm{FORALL}_2(\bar{M})$ and $\mathrm{CON}(\bar{M})$ all holds. Our goal is to prove there exists a structure $\mathfrak{A}$ that satisfies $\forall x\, \alpha$, $\forall x \forall y\, (\beta \vee x = y)$ and $\bigwedge_{1\le h\le p} \forall x \exists^{=C_h} y\, (f_h(x,y) \wedge x \neq y)$.

First, we will construct $\mathfrak{A}$. Let $A_{T_1,g_1} \cup A_{T_1,g_2} \ldots \cup A_{T_n,g_m}$ be a pair-wise disjoint division of $A$, where $|A_{T_i,g_j}| = M_{T_i,g_j}$ for any $1 \le i \le n$ and $1 \le j \le m$. The set of elements $A_{T_i,g_1} \cup A_{T_i,g_2} \ldots \cup A_{T_i,g_m}$ is denoted by $A_{T_i}$, and $(M_{T_i,g_1}, M_{T_i,g_2}, \ldots, M_{T_i,g_m})$ by $\bar{M}_{T_i}$.

Since $\mathrm{CON}(\bar{M})$ holds, we can apply theorem 4.3.1 to construct a $(D_T, \overleftarrow{D}_T)$ regular digraph $G^T = (A_T, E_1^T, E_2^T, ..., E_\ell^T)$ for any $T \in \mathcal{T}$, where $A_{T,g_1} \cup A_{T,g_2} \ldots \cup A_{T,g_m}$ is a witness of $G^T$. Let $G_T = (A_T, E_1^T, E_2^T, ..., E_\ell^T, \overleftarrow{E}_1^T, \overleftarrow{E}_2^T, ..., \overleftarrow{E}_\ell^T)$ with $\overleftarrow{E}_i$ defined to be the inverse of $E_i$ for all $i = 1, \ldots, \ell$. Observe that in $G_T$ for any $a \in A_{T,g_j}$ and any $i \in \{1, \ldots, \ell\}$,

- in-$\mathrm{deg}_{E_i}(a) = g_j(T, \overleftarrow{E}_i, T)$ by definition of regularity, which is consistent with out-$\mathrm{deg}_{\overleftarrow{E}_i}(a)$, and
- out-$\mathrm{deg}_{E_i}(a) = g_j(T, E_i, T)$ by definition of regularity, which is consistent with in-$\mathrm{deg}_{\overleftarrow{E}_i}(a)$.

Similarly, we can apply theorem 4.2.1 to construct a $(D_{S\to T}, \overleftarrow{D}_{S\to T})$ biregular graph $G^{S,T} = (A_S, A_T, E_1^{S\to T}, E_2^{S\to T}, ..., E_\ell^{S\to T}, \overleftarrow{E}_1^{S\to T}, \overleftarrow{E}_2^{S\to T}, ..., \overleftarrow{E}_\ell^{S\to T})$ for any $S = T_{k_1}$ and $T = T_{k_2} \in \mathcal{T}$ where $k_1 < k_2$ and $A_{S,g_1} \cup A_{S,g_2} \ldots \cup A_{S,g_m}$ and $A_{T,g_1} \cup A_{T,g_2} \ldots \cup A_{T,g_m}$ are witness of $G^T$. Now define

- $E_i^{S,T}$ to be the set that consists of the edges of $E_i^{S\to T}$ and the inverse of $\overleftarrow{E}_i^{S\to T}$, and



doi:10.6342/NTU201802560

- $\overleftarrow{E}_i^{S,T}$ to be the set that consists of the edges of $\overleftarrow{E}_i^{S\to T}$ and the inverse of $E_i^{S\to T}$.

Let $G_{S,T} := (A_S, A_T, E_1^{S,T}, E_2^{S,T}, ..., E_\ell^{S,T}, \overleftarrow{E}_1^{S,T}, \overleftarrow{E}_2^{S,T}, ..., \overleftarrow{E}_\ell^{S,T})$. Hence, in $G_{S,T}$ for any $a \in A_{S,g_j}$ and any $i \in \{1, \ldots, \ell\}$,

- in-deg$_{E_i}(a) = g_j(S, \overleftarrow{E_i}, T)$ by definition of biregularity, which is consistent with out-deg$_{\overleftarrow{E_i}}(a)$, and
- out-deg$_{E_i}(a) = g_j(S, E_i, T)$ by definition of regularity, which is consistent with in-deg$_{\overleftarrow{E_i}}(a)$,

and vertices of $A_T$ has consistent in-deg and out-deg by symmetry.

Finally, we can construct the graph $G$ for $\mathfrak{A}$ by combining all $G_T$ and $G_{S,T}$, i.e., let

$$E_k \;:=\; \bigcup_{T\in\mathcal{T}} E_k^T \cup \bigcup_{i<j} E_k^{T_i,T_j}$$

and

$$\overleftarrow{E}_k \;:=\; \bigcup_{T\in\mathcal{T}} \overleftarrow{E}_k^T \cup \bigcup_{i<j} \overleftarrow{E}_k^{T_i,T_j}$$

for all $k = 1, \ldots, \ell$.

Now we will prove $\mathfrak{A} \models \phi$:

- Proof of $\mathfrak{A} \models \bigwedge_{1\le h\le p} \forall x \exists^{=C_h} y\, (f_h(x,y) \wedge x \neq y)$:

  Let $a \in A$ be an arbitrary vertex. Since $A = A_{T_1,g_1} \cup A_{T_1,g_2} \ldots \cup A_{T_n,g_m}$, there is some $(T, g) \in \mathcal{T} \times \mathcal{G}$ such that $a \in A_{T,g}$.

  For every $h \in \{1, \ldots, p\}$, we have

$$\text{out-deg}_{f_h}(a) \;=\; \sum_{E\in\mathcal{E} \text{ s.t. } E\models(f_h\wedge(x\neq y))} \text{out-deg}_E(a)$$

  and

$$\text{out-deg}_E(a) \;=\; \sum_{T'\in\mathcal{T}} g(T, E, T')$$



doi:10.6342/NTU201802560

Hence,

$$\text{out-deg}_{f_h}(a) \;=\; \sum_{E\in\mathcal{E}\text{ s.t. } E\models(f_h\wedge(x\neq y))} \;\sum_{T'\in\mathcal{T}} g(T,E,T') \;=\; C_h$$

by the definition of $\mathcal{G}$.

We conclude that $\mathfrak{A}$ is a model of $\bigwedge_{1\leq h\leq p} \forall x\exists^{=C_h} y\ (f_h(x,y)\wedge x\neq y)$.

- Proof of $\mathfrak{A}\models\forall x\alpha$:

  Since $\text{FORALL}_1(\bar{M})$ holds, we have $|A_{T,g}| = M_{T,g} = 0$ for any $g\in\mathcal{G}$ and $T\in\mathcal{T}$ such that $T\models\neg\alpha$. It implies $|A_T| = 0$ for all $T\in\mathcal{T}$ such that $T\models\neg\alpha$. Therefore, there does not exist any element $a\in A$ such that $\alpha(a)$ holds; in other words, $\forall x\alpha$ holds in $\mathfrak{A}$.

- Proof of $\mathfrak{A}\models\forall x\forall y\ (\beta\vee x=y)$:

  Recall that for any $T\in\mathcal{T}$, $g\in\mathcal{G}$, $E\in\mathcal{E}$ and $a\in A_{T,g}$,

  $$\text{out-deg}_E(a) = \sum_{S\in\mathcal{T}} g(T,E,S).$$

  Since $\text{FORALL}_2(\bar{M})$ holds, $|A_{T,g}| = M_{T,g} = 0$ for any $(T,g)\in\mathcal{T}\times\mathcal{G}$ such that $g(T,E,S) > 0$ for some $E\models(\neg\beta\wedge(x\neq y))$. Therefore, for any $a\in A$ and $E\models(\neg\beta\wedge(x\neq y))$, $\text{out-deg}_E(a) = 0$, so there does not exist any $\neg\beta$-edge in $\mathfrak{A}$.

  We arrive at the conclusion that $\mathfrak{A}$ is a model of $\neg\exists x\exists y\ (\neg\beta\wedge(x\neq y))$, which is equivalent to $\forall x\forall y\ (\beta\vee(x=y))$.

Thus, $\mathfrak{A}\models\phi$. Notice that if the entries in $\bar{M}$ are all finite, then $|A|$ is finite by construction.

□

Now for the "only if" direction, we have the following claim:

**Claim 3** *For any $\mathcal{RCS}$ sentence $\phi$,* $\text{PREB}_\phi$ *holds in $\mathcal{N}$ if $\phi$ has a finite model, and* $\text{PREB}_\phi$ *holds in $\mathcal{N}_\infty$ if $\phi$ has a model.*



doi:10.6342/NTU201802560

**Proof of claim.** Let $\mathfrak{A}$ be a structure that $\mathfrak{A} \models \phi$. We can divide $A$ into a pairwise disjoint partition $A_{T_1,g_1} \cup \ldots \cup A_{T_n,g_m}$ by letting $A_{T_i,g_j}$ consist of all the $(T_i, g_j)$-elements. Let $M_{T_i,g_j} := |A_{T_i,g_j}|$ for all $i = 1, \ldots, n$ and all $j = 1, \ldots, m$. Let $\bar{M} := (M_{T_1,g_1}, \ldots, M_{T_n,g_m})$ and $\bar{M}_{T_i} := (M_{T_i,g_1}, \ldots, M_{T_i,g_m})$. We claim that $\mathrm{FORALL}_1(\bar{M})$, $\mathrm{FORALL}_2(\bar{M})$ and $\mathrm{CON}(\bar{M})$ all holds.

- $\mathrm{FORALL}_1(\bar{M})$ holds: Since $\forall x\ \alpha$ holds in $\mathfrak{A}$, i.e., $\neg\exists x\ \neg\alpha$ holds, there does not exist any element in any $T \in \mathcal{T}$ such that $T \models \neg\alpha$. We have $\sum_{j=1,\ldots,m} M_{T,g_j} = 0$ for any $T \models \neg\alpha$.

  Since all $M_{T,g}$ are nonnegative, $\bigwedge_{T\in\mathcal{T} \text{ s.t. } T\models\neg\alpha} \bigwedge_{1\leq j\leq m} M_{(T,g_j)} = 0$ holds.

- $\mathrm{FORALL}_2(\bar{M})$ holds: We have $\forall x \forall y\ \beta \vee (x = y)$ holds in $\mathfrak{A}$, which is equivalent to $\neg\exists x\exists y\ (\neg\beta \wedge (x \neq y))$ holds in $\mathfrak{A}$. Therefore, there does not exist any $E$-edge for $E \in \mathcal{E}$ such that $E \models \neg(\neg\beta \wedge (x \neq y))$.

  Recall

  $$H = \left\{ (T,g) \in \mathcal{T} \times \mathcal{G} \;\middle|\; \begin{array}{l} g(T,E,S) > 0 \text{ for some } S \in \mathcal{T} \\ \text{ and some } E \in \mathcal{E} \text{ s.t. } E \models (\neg\beta \wedge (x \neq y)). \end{array} \right\}$$

  Suppose, to the contrary, there exists some non-empty $A_{T,g}$ with $(T,g) \in H$. Let $a$ be a vertex in $A_{T,g}$. Then by the definition of $H$, there is some $S \in \mathcal{T}$ and some $E \models (\neg\beta \wedge (x \neq y))$ such that $g(T,E,S) > 0$, and for such $a$, the number of outgoing $E$-edges towards the elements of $S$ is $g(T,E,S)$. Hence, there exist some $b$ of $S$ such that $(a,b)$ is an $E$-edge, and we get $\mathfrak{A}, a, b \models (\neg\beta \wedge (x \neq y))$, which contradicts to $\mathfrak{A} \models \phi$.

- $\mathrm{CON}(\bar{M})$ holds: We will divide this part into two, and prove that $\mathrm{BiREG}_{D_{T_i\to T_j}, \overleftarrow{D}_{T_i\to T_j}}(\bar{M}_{T_i}, \bar{M}_{T_j})$ holds for any $i < j$ and $\mathrm{REG}_{D_{T_i}, \overleftarrow{D}_{T_i}}(\bar{M}_{T_i})$ holds for any $i$.

  - For any $i$ and $j \in \{1, \ldots, n\}$ such that $i < j$, we can partition $A_{T_i}$ with $A_{T_i,g_1} \cup \ldots \cup A_{T_i,g_m}$, and $A_{T_j}$ with $A_{T_j,g_1} \cup \ldots \cup A_{T_j,g_m}$. Let $G_{T_i,T_j}$ denote the subgraph of $\mathfrak{A}$ consisting of the vertices of $A_{T_i} \cup A_{T_j}$ and the edges between $A_{T_i}$



doi:10.6342/NTU201802560

and $A_{T_j}$. For any $E \in \mathcal{E}$, $g \in \mathcal{G}$ and $a \in A_{T_i,g}$, $\deg_E(a) = g(T_i, E, T_j)$, and for any $E' \in \mathcal{E}$, $g' \in \mathcal{G}$ and $a' \in A_{T_j,g'}$, $\deg_{E'}(a') = g'(T_j, E', T_i)$ in $G_{T_i,T_j}$. Thus, $G_{T_i,T_j}$ is a $(D_{T_i \to T_j}, \overleftarrow{D}_{T_i \to T_j})$-biregular graph with witness $A_{T_i,g_1} \cup \ldots \cup A_{T_i,g_m}$ and $A_{T_j,g_1} \cup \ldots \cup A_{T_j,g_m}$, and $\mathrm{BiREG}_{D_{T_i \to T_j}, \overleftarrow{D}_{T_i \to T_j}}(\bar{M}_{T_i}, \bar{M}_{T_j})$ holds.

– For any $i \in \{1, \ldots, n\}$, $A_{T_i,g_1} \cup \ldots \cup A_{T_i,g_m}$ forms a partition of $A_{T_i}$. Let $G_{T_i}$ denote the subgraph of $\mathfrak{A}$ consisting of the vertices of $A_{T_i}$ and the directed edges between any two vertices in $A_{T_i}$. Note that in $G_{T_i}$, for any $a \in A_{T_i}$, $j \in \{1, \ldots, \ell\}$ and $g \in \mathcal{G}$, we have out-$\deg_{E_j}(a) = g(T_i, E_j, T_i)$ and in-$\deg_{E_j}(a) =$ out-$\deg_{\overleftarrow{E_j}}(a) = g(T_i, \overleftarrow{E_j}, T_i)$. Hence, $G_{T_i}$ is a $(D_{T_i}, \overleftarrow{D}_{T_i})$-regular digraph with witness $A_{T_i,g_1} \cup \ldots \cup A_{T_i,g_m}$, and thus $\mathrm{REG}_{D_{T_i}, \overleftarrow{D}_{T_i}}(\bar{M}_{T_i})$ holds.

Therefore, $\mathrm{PREB}_\phi$ holds in $\mathcal{N}$ if $|A|$ is finite, and $\mathrm{PREB}_\phi$ holds in $\mathcal{N}_\infty$ in either case. □

By the above two claims, corollary 5.2.1 follows. ■

From corollary 5.2.1, we conclude the satisfiability is preserved in the conversion from $\phi$ to $\mathrm{PREB}_\phi$, and thus theorem 5.1.1 is proved.

## 5.3 Complexity analysis

We are going to analyze the time complexity of obtaining $\mathrm{PREB}_\phi$ from a $\mathcal{RCS}$ sentence $\phi$. Let $r$ be the number of distinct predicates and $k$ be the largest quantifier in $\phi$. We denote the length of a formula $\psi$ by $|\psi|$. Define the length of a formula to be the summation of the length of all the symbols in it with repeats, and the length of a formula $\psi$ is defined inductively as follows:

- $|z = z| = O(1)$ where $z$ ranges over $\{x, y\}$.
- $|R(z, z)| = O(\log r)$ where $z$ ranges over $\{x, y\}$ and $R$ is an arbitrary binary predicate.



doi:10.6342/NTU201802560

- $|P(z,z)| = O(\log r)$ where $z$ ranges over $\{x,y\}$ and $P$ is an arbitrary unary predicate.

- $|\neg\psi| = |\psi| + O(1)$ for any formula $\psi$.

- $\psi_1 \wedge \psi_2 = |\psi_1| + |\psi_2| + O(1)$ for any formula $\psi_1, \psi_2$.

- $\exists^{\geq c} z\psi = |\psi| + O(\log k)$ for any formula $\psi$.

We can easily see $|\mathcal{T}| = 2^{O(r)}$ and $|\mathcal{E}| = 2^{O(r)}$. Also, $|\mathcal{G}| = O(k^{|\mathcal{T}|\times|\mathcal{E}|\times|\mathcal{T}|})$, and we get $|\mathcal{G}| = 2^{2^{O(r\log\log k)}}$. Since

$$\phi \;=\; \exists X_{(T_1,g_1)} \ldots \exists X_{(T_n,g_m)}\ \mathrm{FORALL}_1(\bar{X}) \wedge \mathrm{FORALL}_2(\bar{X}) \wedge \mathrm{CON}(\bar{X}),$$

there are $|\mathcal{T}| \times |\mathcal{G}| = 2^{2^{O(r\log\log k)}}$ variables in $\phi$. For the subformula $\mathrm{FORALL}_2(\bar{X})$, it takes $2^{O(r)}$ time to find the maximal subset $\mathcal{S}$ of $\mathcal{E}$ such that $\mathcal{S} \models (\neg\beta \wedge x \neq y)$, and the set $H$ defined as in formula 5.4 can be obtained by going through the set $\mathcal{G}\times\mathcal{T}\times\mathcal{S}\times\mathcal{T}$ greedily in $2^{2^{O(r\log\log k)}}$ time, and thus $\mathrm{FORALL}_2(\bar{X})$ is found. Similarly, $\mathrm{FORALL}_1(\bar{X})$ can be constructed in $2^{2^{O(r\log\log k)}}$ time by computing greedily.

To analyze the part $\mathrm{CON}(\bar{X})$, we start with analyzing its subformulas. In particular, we analyze $\mathrm{BiREG}$, and $\mathrm{REG}$ has the same complexity by symmetry. Observe that equation 5.2, for each $\mathrm{BiREG}_{D_{T_i\to T_j},\overleftarrow{D}_{T_i\to T_j}}(\bar{X}_{T_i}, \bar{X}_{T_j})$, the subscripted matrices are of size $2|\mathcal{E}| \times |\mathcal{G}|$, and each entry is an integer between $1$ to $k$. First, for the base case defined as in equation 4.2 where the subscripted matrices of $\mathrm{BiREG}$ are of size $1 \times |\mathcal{G}|$, we can easily see the length of first two lines is $O(|\mathcal{G}|\times\log(|\mathcal{T}||\mathcal{G}|)) = 2^{2^{O(r\log\log k)}}$, and the largest constant in them is no greater than $2k^2|\mathcal{G}|^2+3 = 2^{2^{O(r\log\log k)}}$. Now, for the third line, since the length of $\bar{X}_{T_i}, \bar{X}_{T_j}$ are $|\mathcal{G}| = 2^{2^{O(r\log\log k)}}$, and each element of any $(\bar{M},\bar{N}) \in H_{\bar{c},\bar{d}}$ has value between $0$ and $2\cdot\mathrm{MC}(\bar{c})\cdot\mathrm{MC}(\bar{d})+3$, which is no greater than $2k^2+3$, the length of the $H_{\bar{c},\bar{d}}$ as defined in equation 4.1 is $(2k^2+3)^{2^{2^{O(r\log\log k)}}} = 2^{2^{2^{O(r\log\log k)}}}$. Therefore, for the base case, the length of the formula is bounded by $2^{2^{2^{O(r\log\log k)}}}$. Now we consider the inductive construction of $\mathrm{BiREG}$ for matrices with $2|\mathcal{E}|$ rows. Observe that, by equation 4.3, in each induction step, the total length is the summation of $H_{(C,D)}$ and the multiplication of $|\mathcal{E}|$ and the length of the previous step. Like the base case, we can conclude the largest



doi:10.6342/NTU201802560

constant is also no greater than $2 \times 2|\mathcal{E}| \times k^2(|\mathcal{G}| \times 2|\mathcal{E}|)^2 + 3 \times 2|\mathcal{E}| = 2^{2^{O(r \log\log k)}}$, the length of $H_{C,D}$ is also $2^{2^{2^{O(r \log\log k)}}}$, and thence the total length of $\mathrm{BiREG}_{D_{T_i \to T_j}, \overleftarrow{D}_{T_i \to T_j}}(\bar{X}_{T_i}, \bar{X}_{T_j})$ is bounded by $2^{2^{O(r \log\log k)}} \times 2^{2^{2^{O(r \log\log k)}}} = 2^{2^{2^{O(r \log\log k)}}}$.

Therefore, the length of $\mathrm{PREB}_\phi$ is bounded by $2^{O(r)} \times (2^{O(r)})^2 \times 2^{2^{2^{O(r \log\log k)}}} = 2^{2^{2^{O(r \log\log k)}}}$, and thus bounded by $2^{2^{2^{O(|\phi|)}}}$. Moreover, the largest constant in $\mathrm{PREB}_\phi$ is bounded by $2^{2^{O(|\phi|)}}$. With nondeterminism, however, for each $H_{C,D}$, we can simply guess the correct $(\bar{M}, \bar{N}) \in H_{C,D}$ and guess the order of rows in the induction step of equation 4.3, and therefore the length of $\mathrm{PREB}_\phi$ should be bounded by $2^{2^{O(|\phi|)}}$.

Observe that $\mathrm{FORALL}_1(\bar{X}) \wedge \mathrm{FORALL}_2(\bar{X}) \wedge \mathrm{CON}(\bar{X})$ is quantifier free and has length less than $|\mathrm{PREB}_\phi|$. Therefore, by applying theorem 3.3.3. our algorithm runs in nondeterministic double exponential time, which is stated formally in the following theorem.

**Theorem 5.3.1** *There is a constant $c$ and a nondeterministic algorithm $\mathcal{A}$ such that on input $\mathcal{RCS}$ sentence $\phi$, $\mathcal{A}$ decide whether $\phi$ is (finitely) satisfiable in time $O(2^{2^{c|\phi|}})$.*



doi:10.6342/NTU201802560

# Chapter 6

# Concluding remarks

In this thesis, we present new decision procedures for the satisfiability and finite satisfiability problems for $\mathcal{RCS}$ formulas. The decision procedures, which are based on the technique by Kopczyński and Tan [9], are simple compared to existing procedures. It is by converting an $\mathcal{RCS}$ formula into an existential Presburger formula. Furthermore, some interesting remarks can be derived from our approach.

First, note that in $\mathrm{PREB}_{\phi}$ we can assume the part $\mathrm{FORALL}_1(\bar{X}) \wedge \mathrm{FORALL}_2(\bar{X}) \wedge \mathrm{CON}(\bar{X})$ does not contain any disjunction by guessing via nondeterminism as in theorem 3.3.3. Thus, the length of the resulting formula is still $2^{2^{O(|\phi|)}}$, and the largest constant $a$ is no greater than $2^{2^{O(|\phi|)}}$ by the analysis in section 5.3.

Let us denote by $\varphi(\bar{X})$ the part $\mathrm{FORALL}_1(\bar{X}) \wedge \mathrm{FORALL}_2(\bar{X}) \wedge \mathrm{CON}(\bar{X})$ (which is without any disjunction). By corollary 3.3.2, if there exists a solution $\bar{X} \in \mathbb{N}^{|\mathcal{T}||\mathcal{G}|}$ for $\varphi(\bar{X})$, there is also some solution $\bar{Y}$ in $\{0, 1, \ldots, (|\mathcal{T}||\mathcal{G}| + |\varphi|)(|\varphi| \cdot a)^{(2|\varphi|+1)}\}^{|\mathcal{T}||\mathcal{G}|}$ such that $\varphi(\bar{Y})$ holds. Notice that $(|\mathcal{T}||\mathcal{G}| + |\varphi|)(|\varphi| \cdot a)^{(2|\varphi|+1)} = (2^{2^{O(|\phi|)}})^{2^{2^{O(|\phi|)}}} = 2^{2^{2^{O(|\phi|)}}}$ and $|\mathcal{T}||\mathcal{G}| = 2^{2^{O(|\phi|)}}$. Therefore, if $\phi$ has a finite model, i.e., there is a solution for $\mathrm{FORALL}_1(\bar{X}) \wedge \mathrm{FORALL}_2(\bar{X}) \wedge \mathrm{CON}(\bar{X})$ in $\mathbb{N}^{|\mathcal{T}||\mathcal{G}|}$, then there is also a solution $\bar{Y}$ such that $\sum Y = 2^{2^{2^{O(|\phi|)}}} \times 2^{2^{O(|\phi|)}} = 2^{2^{2^{O(|\phi|)}}}$, which implies there is a model of size $2^{2^{2^{O(|\phi|)}}}$ for $\phi$. This observation is stated formally as the following corollary.

**Corollary 6.0.1** *There is a constant $c$ such that for every $\mathcal{RCS}$ sentence $\phi$, $\phi$ has a finite model if and only if $\phi$ has a model of size $O(2^{2^{2^{c|\phi|}}})$.*



doi:10.6342/NTU201802560

Second, note that we can also derive the decidability of checking whether the spectrum of an $\mathcal{RCS}$ formula is infinite via the following formula:

$$\varphi \;:=\; \forall y \exists \bar{X} \left(\mathrm{FORALL}_1(\bar{X}) \wedge \mathrm{FORALL}_2(\bar{X}) \wedge \mathrm{CON}(\bar{X}) \wedge \sum \bar{X} \geq y\right),$$

Since satisfiability of Presburger formula is decidable [12, 16], we obtain the following corollary.

**Corollary 6.0.2** *Checking whether an $\mathcal{RCS}$ sentence has a infinite spectrum is decidable.*

For future work, we plan to extend our result to the whole $\mathrm{C}^2$ class and provide an alternative technique to reason about $\mathrm{C}^2$ formula, thus many other ontology languages.



doi:10.6342/NTU201802560

# Bibliography


[1] A. Church. A note on the entscheidungsproblem. *J. Symb. Log.*, 1(1):40–41, 1936.

[2] A. Church. An unsolvable problem of elementary number theory. *American Journal of Mathematics*, 58(2):pp. 345–363, 1936.

[3] M. Fürer. The computational complexity of the unconstrained limited domino problem (with implications for logical decision problems). In *Logic and Machines: Decision Problems and Complexity, Proceedings of the Symposium "Rekursive Kombinatorik" held from May 23-28, 1983 at the Institut für Mathematische Logik und Grundlagenforschung der Universität Münster/Westfalen*, pages 312–319, 1983.

[4] K. Gödel. Über die vollständigkeit der axiome des logischen funktionenkalküls. *Monatshefte für Mathematik und Physik*, 36:349–360, 1930.

[5] E. Grädel, P. G. Kolaitis, and M. Y. Vardi. On the decision problem for two-variable first-order logic. *Bulletin of Symbolic Logic*, 3(1):53–69, 1997.

[6] E. Grädel and M. Otto. On logics with two variables. *Theor. Comput. Sci.*, 224(1-2):73–113, 1999.

[7] E. Grädel, M. Otto, and E. Rosen. Two-variable logic with counting is decidable. In *Proceedings, 12th Annual IEEE Symposium on Logic in Computer Science, Warsaw, Poland, June 29 - July 2, 1997*, pages 306–317, 1997.

[8] A. Kahr, E. Moore, and H. Wang. Entscheidungsproblem reduced to the $\forall\exists\forall$ case. *Proc. Nat. Acad. Sci. U.S.A.*, 48:365–377, 1962.




doi:10.6342/NTU201802560

[9] E. Kopczyński and T. Tan. Regular graphs and the spectra of two-variable logic with counting. *SIAM J. Comput.*, 44(3):786–818, 2015.

[10] H. R. Lewis. Complexity results for classes of quantificational formulas. *J. Comput. Syst. Sci.*, 21(3):317–353, 1980.

[11] M. Mortimer. On languages with two variables. *Math. Log. Q.*, 21(1):135–140, 1975.

[12] D. C. Oppen. A $2^{2^{2^{p(n)}}}$ upper bound on the complexity of presburger arithmetic. *Journal of Computer and System Sciences*, 16(3):323–332, 1978.

[13] L. Pacholski, W. Szwast, and L. Tendera. Complexity results for first-order two-variable logic with counting. *SIAM J. Comput.*, 29(4):1083–1117, 2000.

[14] C. H. Papadimitriou. On the complexity of integer programming. *J. ACM*, 28(4):765–768, 1981.

[15] I. Pratt-Hartmann. Complexity of the two-variable fragment with counting quantifiers. *Journal of Logic, Language and Information*, 14(3):369–395, 2005.

[16] M. Presburger. Über de vollständigkeit eines gewissen systems der arithmetik ganzer zahlen, in welchen, die addition als einzige operation hervortritt. In *Comptes Rendus du Premier Congrès des Mathématicienes des Pays Slaves*, pages 92–101. Warsaw, 1927.

[17] D. Scott. A decision method for validity of sentences in two variables. *Journal of Symbolic Logic*, 27:377, 1962.

[18] B. A. Trakhtenbrot. Impossibility of an algorithm for the decision problem in finite classes. *Doklady Akademii Nauk SSSR*, 70:569–572, 1950. English translation in [19].

[19] B. A. Trakhtenbrot. Impossibility of an algorithm for the decision problem in finite classes. *American Mathematical Society Translations*, 23:1–6, 1950.



doi:10.6342/NTU201802560

[20] A. M. Turing. On computable numbers, with an application to the entscheidungsproblem. *Proceedings of the London Mathematical Society*, 42:230–265, 1936.



doi:10.6342/NTU201802560