Universita Karlova

Fakulta filosofická

Bakalářská práce

Monadic NP Sets

Martin Putzer

Kathedra logiky

Vedoucí práce: prof. RNDr. Jan Krajíček, DrSc.

Studijní program: Logika

Studijní obor: Logika - Sinologie

Praha, 2023

I hereby declare this bachelor thesis to be a product of my own work solely. While writing it, I used only the materials cited and it has not been used to obtain another or the same degree.

I understand that my work relates to the rights and obligations regulated by the Act No. 121/2000 Sb. (the copyright act of Czech Republic), as amended, whereby is Charles University free to conclude a license agreement on the use of this work as a school work pursuant to section 60, subsection 1 of said copyright act.

In Praha Date: 7.5.2023 PuSzer

Author's signature

Poděkování

Děkuji v prvé řadě svému vedoucímu, prof. Janu Krajíčkovi, za uvedení do úchvatného thematu, za projevenou trpělivost a za užitečné připomínky k této práci. Dále děkuji svým rodičům za podporu při studiu, zvláště pak své matce, která mi vždy byla citovou oporou v těžkých chvílích.

Název: Monadické **NP** množiny

Autor: Martin Putzer

Kathedra: Kathedra logiky, Filosofická fakulta

Školitel: prof. RNDr. Jan Krajíček, DrSc.

Pracoviště školitele: Kathedra algebry, Mathematicko-fysikální fakulta

Abstrakt: Jako zobecněná spektra se označují třídy konečně axiomatisovatelné v existenční druhořádové logice s relací platnosti omezenou na konečné struktury. Jest známým faktem, že korrespondují dle Faginovy věty s prvky složitostní třídy **NP**. Problém uzavřenosti **NP** na komplementaci se tedy redukuje na problém uzavřenosti zobecněných spekter na komplementaci. Důkaz $\mathbf{P} \neq \mathbf{NP}$, za předpokladu, že ono tvrzení skutečně platí, by tak mohl spočívat v nalezení konkretního zobecněného spektra (a tedy třídy v **NP**), jehož doplněk, jsa arci v co**NP**, by nebyl prvkem **NP**. Hledání takového důkazu ovšem též nepřineslo úspěch. Částečné rozřešení tohoto problému (an sám je toliko speciálním příkladem obecnějšího tak zvaného problému Asserova) přinesla Fagin-Hájkova věta, tvrdící, že jistá podtřída **NP**, třída tak zvaných `monadických` **NP** `množin` vskutku netvoří třídu uzavřenou na komplementaci. Reprodukce Faginova původního důkazu této věty, spolu s uvedením veškerého potřebného apparátu, je cílem této práce.

Klíčová slova: spektrum zobecněné spektrum Asserův problém existenční druhořádová logika Ehrenfeucht-Fraïssého hry monadické **NP** Fagin-Hájkova věta

Sázeno systémem LaTeX v písmech Antykwa Toruńska (text) a Adobe Utopia (mathematika). Kompilace enginem pdfLaTeX.

Title: Monadic **NP** Sets

Author: Martin Putzer

Department: Department of Logic, Faculty of Arts

Supervisor: prof. RNDr. Jan Krajíček, DrSc.

Supervisor's department: Department of Algebra, Faculty of Mathematics and Physics

Abstract: Generalised spectra, *id est* classes finitely axiomatisable in existential second-order logic restricted to finite structures, are known by Fagin's theorem to coincide with members of the complexity class **NP**. Thereby, the problem of **NP** being closed under complementation reduces to the problem whether every class of finite structures complementary to a generalised spectrum is, too, a generalised spectrum. Provided $\mathbf{P} \neq \mathbf{NP}$, a proof thereof could then possibly be based on finding a particular generalised spectrum (thereby an **NP** class) whose complement, while in co**NP** would not be in **NP**. Pursuits of such a proof, too, however, have been to no avail. A partial resolution of this problem (itself a special case to so called Asser's problem) is Fagin-Hájek theorem, claiming that a subclass of **NP**, the class of so called `monadic` **NP** `sets` is not closed under complementation. Reproducing Fagin's original proof of the theorem is the aim of this thesis, along with introducing the reader to all preliminary apparatus needed for the proof.

Keywords: spectrum generalised spectrum Asser's problem existential second-order logic Ehrenfeucht-Fraïssé games monadic **NP** Fagin-Hájek theorem

Typeset using LaTeX in Antikwa Toruńska (text) and Adobe Utopia (mathematics). Compiled by pdfLaTeX engine.

Contents

Introduction 2

List of notation 5

1 Spectra and generalised spectra 6
- 1.1 Spectra and their basic properties 6
- 1.2 Second-order logic and the theorem of Fagin 16
- 1.3 Applications and open problems 23

2 The Fagin-Hájek theorem 26
- 2.1 The games of Ehrenfeucht and Fraïssé 26
- 2.2 Fagin's original proof 31

Résumé 38

References 40

Introduction

This thesis is concerned with certain classes of integers and structures, known as *spectra* and *generalised spectra*, respectively. The problem whether every class complementary to a member of those also is a spectrum or a generalised spectrum, respectively, is among the oldest unsolved problems in mathematical logic. It is of interest that both the class of all spectra and the class of all generalised spectra may be very easily characterised in terms of computational complexity, thereby reducing the problem in logic to an other problem in computational complexity theory. This deep connection has given rise to at least two branches of research bordering both mathematical logic and theoretical computer science: finite model theory and descriptive complexity theory. For a detailed overview of this topic and it's history, see [MM09]).

Although the most prominent problem of computational complexity, the **P** vs. **NP** problem and the most related problems remain as of now still unresolved, even in the light of this profound connection, the said connection allows for a more detailed classification of **NP** problems. In particular, **NP** sets are thereby divided into a hierarchy of **NP** sets which are *nulladic*, *monadic*, *dyadic*, *triadic* and so on for other $n \in \mathbb{N}$. For every $n \in \mathbb{N}$, $(n+1)$-adic **NP** sets form a superset to n-adic **NP** sets and we may for example ask whether the inclusion of the class of all n-adic sets in the class of all $(n+1)$-adic sets is strict or not. In general, not much is known even of basic properties of this hierarchy, but it is known that nulladic **NP** sets are closed under complementation, whereas monadic **NP** sets are not. Even so, it is unknown whether there exists any monadic **NP** set, which would not be an **NP** set in general, as that would answer not only the complementation problem for generalised spectra, but would even yield positive answer to the renowned $\mathbf{P} \neq \mathbf{NP}$ problem.

Monadic **NP** sets nevertheless form an interesting subclass of **NP** in this regard. The main goal of this thesis is to prove the aforesaid property of the hierarchy described above, that it does not collapse at $n = 1$; that is, that monadic **NP** sets do not form a class closed under complementation. For the sake of self-containedness, all the needed mathematical apparatus is introduced, with the only prerequisites being basic knowledge of mathematical logic and a limited exposure to notions of complexity theory, along with some general fragmentary knowledge of certain mathematical notions (for which references will be given at respective places).

For mathematical logic, the standard references are [Soc01; Šve02] in Czech and [Sho67; Kle67; Cur77] in English. As for computational complexity, probably the most accessible standard reference is [Sip06]. For concepts which presumably should be known to the reader, but whose notation might not be standardised enough, a list of notation was compiled, so as to avoid both confusion and introducing much too elementary concepts in the thesis.

The first chapter introduces background for the problem, first overviewing properties of spectra, and then the aforesaid connection of spectra and generalised spectra with computational complexity. The second chapter is then to prove the non-complementarity of monadic **NP** sets, after having introduced apparatus of the

so called Ehrenfeucht-Fraïssé games which is specifically needed for the proof. The proof will be a reproduction of the one to be found in [Fag75].

We conclude this introduction by specifying some conventions regarding the stated prerequisites and recalling some of their key notions.

First-order logic will be considered with equality; that is, a formula whose every atomic subformula is of the form $a = b$ for some terms a and b, is considered a formula over an empty language. So as to emphasise the difference between $=$ to be found in formulae and the equality of two formulae, we denote the latter by $\doteq$ (as it is done, too, in [Mlč22]). The notation φ^P for the relativisation of φ to set P is utilised in order to make this operation easily denotable. The same goes for other, mostly non-standard, notations.

For a certain connection between logic and complexity theory will be explored, we recall here some of the basic complexity classes which will be referred to, and some basic information about them. For more detailed information, [Sip06] may be consulted.

Definition: Let L_M be a decidable language accepted by a Turing machine M in time equal to or lesser than $f(n)$, for each n the length of the input word. Then we denote:

1. $L_M \in \mathbf{E}$ if and only if M is deterministic and f has an upper bound which is a function exponential in some polynomial of n.
2. $L_M \in \mathbf{NE}$ if and only if M is non-deterministic and f has an upper bound which is a function exponential in some polynomial of n.
3. $L_M \in \mathbf{P}$ if and only if M is deterministic and f has an upper bound which is a function polynomial in n.
4. $L_M \in \mathbf{NP}$ if and only if M is non-deterministic and f has an upper bound which is a function polynomial in n.
5. $L_M \in \mathrm{co}\mathbf{C}$ for class $\mathbf{C}$ if and only if L_M's complement is in $\mathbf{C}$.

A set $A \in \mathbf{NP}$ (or the query regarding membership within the set or the property thereof) is **NP**-*complete* if and only if there is for every $B \in \mathbf{NP}$ a function $g(n)$ computable in time polynomial with respect to n such that for all $b \in B$ holds $g(b) \in A \Leftrightarrow b \in B$. ◀

It is known that classes defined in this manner for deterministic machines are actually closed under complementation, so $\mathbf{E} = \mathrm{co}\mathbf{E}$ and $\mathbf{P} = \mathrm{co}\mathbf{P}$. Whether the analogue holds for **NP** and **NE** is as of yet unknown, as well as whether **E** equals **NE** or **P** equals **NP**. That is the famous **P** vs. **NP** problem.

The last compact prerequisite is formed of some rudimentary knowledge regarding non-directed graphs. For directed graphs will not be considered, let us conclude to understand the term "graph" to be synonymous with "non-directed graph".

Definition: Let R be a binary predicate symbol. A structure of signature $\{R\}$ is a *(non-directed) graph* if and only if realisation of R within the structure be antireflexive and symmetric. R is then called the *reachability relation*, members of graph's universe are called *vertices*, pairs of vertices a and b such that R relate

a and *b* are called *edges*. A graph is said to be *tricolourable* if there may be found three disjoint subsets of it's universe, called *colours*, such that every vertex be in one of the three colours and every edge be between two elements of different colour. A graph is said to be connected if there be for every two vertices *a* and *b* a sequence *s* such that *a* be it's first member, *b* it's final member and the graph contain edge between every member of *s* and it's successor within *s*. We say a graph is a *cycle*, or that it is *cyclic*, if it be connected, it's universe be finite and every two vertices be contained in precisely two edges. ◀

Tricolourability is well-known to be an **NP**-complete property (it also may be seen named as such in [Sip06]).

List of notation

$\mathbb{N}^+$	the set of all positive natural numbers
$\mathrm{Mod}(\varphi, L)$	the class of all structures of signature L, satisfying the theory $\{\varphi\}$
$\|\mathbb{A}\|$	the cardinality of structure $\mathbb{A}$'s universe
$\mathbb{A} \upharpoonright \mathbb{B}$	$\mathbb{A}$ is expansion of $\mathbb{B}$ in some language
ϵ_n	the formula "there are precisely n different elements" (as in [Mlč22])
$\epsilon_{\geq n}$	the formula "there are at least n different elements" (as in [Mlč22])
$\epsilon_{\leq n}$	the formula "there are at most n different elements" (as in [Mlč22])
$\mathrel{\mathring{=}}$	the equality of words over a same alphabet, like $A \mathrel{\mathring{=}} A$, but not $\neg\neg A \mathrel{\mathring{=}} A$
$\bar{x}$	a finite sequence (or ordered tuple) of members denoted x_0, x_1 and so on
$(\exists \bar{x})\varphi$	consecutive quantification over all members of $\bar{x}$
$L(\varphi)$	the set of symbols occuring within φ
φ^S	formula φ modified so that all it's quantifiers be relativised to S
$L(\mathbb{A})$	the signature of structure $\mathbb{A}$
$\lceil \mathtt{l}(n) \rceil$	ceiled binary logarithm of n (length of n's binary expansion)
$l(\bar{x})$	the length of tuple (or finite sequence) $\bar{x}$
$\|\mathbb{A}\|$	the universe of structure $\mathbb{A}$
$\varphi(x/e)$	the formula φ with all free occurences of x replaced by e
$\mathbb{A} \restriction S$	substructure of $\mathbb{A}$, such that $\|\mathbb{A} \restriction S\| = S$
$\mathrm{dom}(f)$	the domain of function f
$\mathrm{rng}(f)$	the range of function f
$f \circ g$	composition of functions: $f \circ g(x) = f(g(x))$
$[a, b]$	an ordered double with a the first element and b the second one
$\mathbb{A} \cong \mathbb{B}$	structures $\mathbb{A}$ and $\mathbb{B}$ are isomorphic
a_b	the concatenation of sequences a and b

1. Spectra and generalised spectra

In this chapter, we shall discuss two fundamental notions: that of a spectrum and that of a generalised spectrum, along with presenting some of the basic theorems thereof. Only basic knowledge of first-order logic and a limited number of elementary notions of complexity theory will be assumed throughout.

1.1 Spectra and their basic properties

Definition 1. The *spectrum* of a given first-order sentence, let us say φ, is the set of all finite cardinalities pertaining to some model of $\{\varphi\}$. More formally:

$$\mathrm{Spec}(\varphi) = \{n \in \mathbb{N}^+ ; \text{there is } \mathbb{M} \in \mathrm{Mod}(\varphi, L) \text{ such that } \|\mathbb{M}\| = n\}.$$

The class

$$\mathrm{GenSpec}(\varphi, L) = \{\mathbb{A} \in \mathrm{Mod}(\top, L); \text{there is finite } \mathfrak{A} \in \mathrm{Mod}(\varphi, L \cup L(\varphi)) \text{ such that } \mathfrak{A} \restriction \mathbb{A}\}$$

is called the *generalised spectrum* of φ in language L. ◀

The notion of spectrum was first addressed by Scholz in [Sch52] and a spectrum-like notion was also considered and investigated by Asser in [Ass55]. Generalised spectra indeed may be thought of as a generalisation of ordinary spectra, as their members - positive natural numbers - are in this context effectively rendered as structures over the empty signature. The notion of generalised spectrum was first introduced by Tarski in [Tar56].

Spectra are known to have many notable properties. For example, that they are closed under certain arithmetical operations, as we shall see. [MM09] gives an overview of many of spectra's known properties and we ourselves shall now name some examples of spectra.

Example 1. The trivial subsets of $\mathbb{N}^+$ (*id est* $\emptyset$ and $\mathbb{N}^+$) are spectra. The former is the spectrum of an arbitrary contradiction (or of a formula with non-finite models only), the latter is the spectrum of an arbitrary logically valid formula, for instance a tautology. ⊠

Example 2. All singletons in $\mathscr{P}(\mathbb{N}^+)$ are spectra. Particularly:

$$\{n\} = \mathrm{Spec}(\epsilon_n) = \mathrm{Spec}\left((\exists \bar{x})(\forall y)\Big(\bigwedge_{\substack{a,b \in \bar{x} \\ a \mathring{\neq} b}} a \neq b \;\; \& \bigvee_{x \in \bar{x}} y = x\Big)\right)$$

where n is the length of $\bar{x}$. ⊠

Example 3. Initial segments of $\mathbb{N}^+$ are spectra:

$$\langle 1; n\rangle \cap \mathbb{N}^+ = \mathrm{Spec}(\epsilon_{\leq n}) = \mathrm{Spec}(\epsilon_{<n+1}) = \mathrm{Spec}\left((\exists \bar{x})(\forall y)\Big(\bigvee_{x \in \bar{x}} y = x\Big)\right)$$

where n is the length of $\bar{x}$ again. ⊠

Example 4. Unbounded intervals of positive natural numbers are spectra:

$$\langle n;\infty) \cap \mathbb{N}^+ = \mathrm{Spec}(\epsilon_{\geq n}) = \mathrm{Spec}(\epsilon_{>n-1}) = \mathrm{Spec}\left((\exists \bar{x}) \bigwedge_{\substack{a,b\in\bar{x}\\ a\overset{\circ}{\neq}b}} a \neq b\right)$$

where n is, again, the length of $\bar{x}$. ⊠

Example 5. Finite unions and intersections of spectra are spectra. We clearly have $\mathrm{Spec}(\varphi) \cup \mathrm{Spec}(\psi) = \mathrm{Spec}(\varphi \vee \psi) = \mathrm{Spec}(\neg\varphi \to \psi)$.

Yet it is not true that $\mathrm{Spec}(\varphi) \cap \mathrm{Spec}(\psi) = \mathrm{Spec}(\varphi \,\&\, \psi)$: see for instance the case $\varphi \overset{\circ}{=} \neg\psi$; it does indeed hold, however, when $L(\varphi) \cap L(\psi) = \emptyset$. Let thus ψ' be a formula created from ψ by replacing all signature symbols (outside of equality sign) by some other ones not present within φ, of the same respective arities. Then we have $\mathrm{Spec}(\varphi) \cap \mathrm{Spec}(\psi) = \mathrm{Spec}(\varphi \,\&\, \psi')$. General finite unions and intersections follow trivially by induction.

Also, it is not true that $\mathrm{Spec}(\neg\varphi) = \mathbb{N}^+ \setminus \mathrm{Spec}(\varphi)$. The case with complements turns out to be much more complicated, as we shall see. ⊠

Example 6. Finite and cofinite subsets of $\mathbb{N}^+$ are spectra. Let $A \subset \mathbb{N}^+$ be finite. Then $\{\epsilon_a\}$ is a spectrum for each $a \in A$, $\bigvee_{a\in A} \epsilon_a$ is first-order, and, by previous example, $\mathrm{Spec}(\bigvee_{a\in A} \epsilon_a) = A$.

Let A now be cofinite in $\mathbb{N}^+$. $\mathbb{N}^+ \setminus A$ is then finite, thus rendering A the spectrum of the then first-order formula $\bigwedge_{a\in\mathbb{N}\setminus A} \neg\epsilon_a$. Follows trivially that all intervals of positive natural numbers are spectra. ⊠

Example 7. The set difference of two spectra, $A \setminus B$ is a spectrum whenever the complement of B in $\mathbb{N}^+$ be a spectrum, as $A \setminus B = (\mathbb{N} \setminus B) \cap A$ becomes then an intersection of two spectra; a spectrum by previous example. ⊠

Example 8. Natural powers of 2 form a spectrum. The theory of boolean algebrae $\mathtt{BA}$ in the language $\{\wedge, \vee, \bar{}, 0, 1\}$ is axiomatised by all the formulae

$$(\forall a)(\forall b)(\forall c)((a \diamond (b \diamond c) = (a \diamond b) \diamond c) \,\&\, (a \diamond b = b \diamond a) \,\&\, (a \vee \bar{a} = 1) \,\&\, (a \wedge \bar{a} = 0)),$$

$$(\forall x)(\forall y)(\forall z)((x \diamond (x \diamond' y) = x) \,\&\, (x \diamond (y \diamond' z) = (x \diamond' y) \diamond (x \diamond' z))),$$

where $\diamond \in \{\wedge, \vee\}$ and $\diamond'$ is then the second one of the two binary operations. This finitely axiomatised theory can be proven (see [Hon16] or [Ně90]) only to have such finite models whose cardinalities are precisely powers of two with natural exponents and thus indeed holds that $\{n \in \mathbb{N}; (\exists k \in \mathbb{N})(2^k = n)\} = \mathrm{Spec}(\bigwedge \mathtt{BA})$. ⊠

Example 9. The set of all powers of all prime numbers is a spectrum. The theory of fields $\mathtt{F}$ in the language $\{+, \cdot, 0, 1, -, ^{-1}\}$ is axiomatised precisely by all formulae of the form:

$$(\forall a)(\forall b)(\forall c)((a \diamond (b \diamond c) = (a \diamond b) \diamond c) \,\&\, (a \cdot (b + c) = (a \cdot b) + (a \cdot c))),$$

$$(\forall x)((x + (-x) = 0)) \,\&\, (x + 0 = x) \,\&\, (x \cdot 1 = x) \,\&\, (x \cdot x^{-1} = 1),$$

where $\diamond \in \{+, \cdot\}$. It could be proved (for this, you may see [Ně90] or [BML41]) that finite models of $\mathtt{F}$ have precisely those cardinalities which are natural powers of

primes, that is: $\{n; (\exists p \in \mathbb{P})(\exists k \in \mathbb{N})(p^k = n)\} = \mathrm{Spec}(\bigwedge \mathtt{F})$, whereby we may derive as well that the set of all natural powers of some particular prime p is a spectrum; in fact, it is the spectrum of the formula $\sum_{k=1}^{p} 1 = 0 \,\&\, \bigwedge \mathtt{F}$ (that is, it pertains to the theory of fields of characteristic p); see again [Ně90] or [BML41] for proof. ⊠

Example 10. The set $\mathbb{P}$ of all prime numbers is a spectrum. Consider the theory F_{Ordered} obtained by endowing $\mathtt{F}$ (from the previous example) with the axioms of partial ordering for the symbol $\leq$ and further with the axioms:

$$(\forall x)(0 \leq x) \,\&\, (\forall x)(x + 1 = 0 \to (\forall y)(x \leq y \to y = x))$$

$$(\forall x)(x + 1 \neq 0 \to (\forall y)((x \leq y \,\&\, x \neq y) \to x + 1 \leq y))$$

which ensure that 0 be the least element, all x such that $x + 1 = 0$ be maximal elements and that $x + 1 \leq y$ for all $x < y$ for all x such that $x + 1 \neq 0$ (in particular, $x + 1$ is for such x it's successor). Thereby the set comprised of elements *ab* 0 *ad* $p - 1$ form a linearly ordered set with respect to $\leq$. Thus, in finite fields whose universe has a non-prime size, as we may note, are besides 1 other elements which are successors to 0: 0 is the least element, 1 it's successor, and so on up to respective $p - 1$ such that the respective field's order is p^k for some $k \in \mathbb{N}^+$; this $p - 1$ is a maximal element and if $0 \neq k \neq 1$, there must be at least one other successor of zero. Let therefore $\gamma \doteq (\exists! x \neq 0)(\forall y)((x \leq y \,\&\, x \neq y) \to x + 1 \leq y)$ (informally, γ says that there be one and only one element a successor to 0, *id est* $1 \neq 0$). Then, $\mathrm{Spec}(\gamma \,\&\, \bigwedge F_{\mathrm{Ordered}}) = \mathbb{P}$.

Moreover, note that if we denote δ the formula

$$(\exists x_1)(\exists x_2 \neq x_1)\Big(x_1 \neq 0 \neq x_2 \,\&\, (\forall y) \bigwedge_{i \in \{1,2\}} \big(x_i \leq y \,\&\, x_i \neq y \to x_i + 1 \leq y\big)\Big),$$

we have it that the set of all non-trivial powers of prime numbers forms a spectrum as well (δ says that there are at least two members which are successors of 0, as opposed to γ claiming there be solely and only one such element). Symbolically written: $\{n; (\exists p \in \mathbb{P})(\exists k \in \mathbb{N} \setminus \{0, 1\})(p^k = n)\} = \mathrm{Spec}(\delta \,\&\, \bigwedge F_{\mathrm{Ordered}})$. ⊠

Example 11. The sets of all odd numbers and all even numbers are both spectra. Let P and Q be unary predicates and F a unary function. We axiomatise the theory T of two disjoint sets and a function mapping them one to another:

$$(\forall x)(P(x) \veebar Q(x)), (\forall x)(P(x) \to Q(F(x))), (\forall x)(Q(x) \to P(F(x)))$$

$$(\forall x)(\forall y \neq x)(P(x) \,\&\, P(y) \to F(x) \neq F(y)) \qquad \text{(F is an injection from P to Q)}$$

We define now these two axioms:

$$(\forall x)(\forall y \neq x)(Q(x) \,\&\, Q(y) \to F(x) \neq F(y)) \qquad \text{(E)}$$

$$(\exists! x)(Q(x) \,\&\, (\forall y)(F(y) \neq x)) \qquad \text{(O)}$$

(E) forces that F also behave injectively in the direction from Q to P (note it is only a slight modification of the axiom above), whereas (O) provides existence of an odd element causing Q not to be injectible to P when the model considered be finite. Clearly, the set of all even numbers is the spectrum of (E) $\,\&\, \bigwedge T$, whereas the set of all odd numbers turns out to be the spectrum of (O) $\,\&\, \bigwedge T$. ⊠

Example 12. The set of all positive natural numbers divisible by n is a spectrum for every $n \in \mathbb{N}^+$. To prove this, we generalise the theory from the previous example. The language will consist of one unary function symbol F and n unary predicate symbols denumerated P_0, P_1 *et cetera* up to P_{n-1}. Heuristics will again be that the theory T_n being now constructed describe n disjoint sets (in this case, of the same cardinality, as was also the case with the set of all even numbers). We denote now I the index set $\langle 0; n-1\rangle \cap \mathbb{N}$, $s(x) = (x+1) \bmod n$ and add as axioms to T_n:

$$(\forall x) \bigvee_{a\in I} \Big(P_a(x) \,\&\, \bigwedge_{\substack{b\in I \\ a\neq b}} \neg P_b(x) \Big), \qquad \text{(all sets realised by } P_a \text{ are mutually disjoint)}$$

$$(\forall x) \bigwedge_{a\in I} \Big(P_a(x) \to P_{s(a)}(F(x)) \Big), \qquad (F \text{ maps the sets one to another cyclically})$$

$$(\forall x)(\forall y \neq x)(F(x) \neq F(y)). \qquad (F \text{ is an injection})$$

Again, it is not hard to see that all finite models of T_n as constructed above are precisely $n-$folds of positive natural numbers. More formally, we write that $\mathrm{Spec}(\bigwedge T_n) = \{a; (\exists k \in \mathbb{N})(a = kn)\}$. ⊠

Example 13. Modulo congruence classes are spectra. Again, we get this by generalising the previous example. We create a modification $T_{n,k}$ of T_n such that it's finite models have cardinality congruent to k modulo n. $L(T_{n,k})$ shall consist of all the symbols already present within $L(T_n)$ and further there will be a new unary predicate symbol S. There will be two new axioms in $T_{n,k}$:

$$(\forall x) \Big(S(x) \veebar \bigvee_{a\in I} P_a(x) \Big), \qquad (S \text{ is disjoint with } P_a \text{ for all choices of } a \in I)$$

$$(\exists x) P_0(x) \,\&\, \epsilon^S_k. \qquad (\text{set } P_0 \text{ is non-empty, } S \text{ has } k \text{ elements})$$

and further we add to $T_{n,k}$ the afore seen axioms $(\forall x)(\forall y \neq x)(F(x) \neq F(y))$ and $(\forall x) \bigwedge_{a\in I}(P_a(x) \to P_{s(a)}(F(x)))$ (making non-emptiness of P_n cause non-emptiness of $P_{s(n)}$ for all $n \in I$) and the axiom forcing sets realised by P_a to be disjoint:

$$(\forall x) \bigwedge_{i\in I} \Big(P_i(x) \to \bigwedge_{\substack{j\in I \\ i\neq j}} \neg P_j(x) \Big)$$

Informally, models of $T_{n,k}$ are created by expanding models of T_n by a set (represented by the unary symbol S) of size k. Thus, finite models of $T_{n,k}$ truly have sizes congruent with k modulo n and modulo congruence classes are spectra as was claimed by us. ⊠

Example 14. We may define sum and product of two integer sets as follows: let A and B be sets of integers; then denote $A + B = \{n; (\exists a \in A)(\exists b \in B)(a + b = n)\}$ and $A \cdot B = \{n; (\exists a \in A)(\exists b \in B)(a \cdot b = n)\}$. Let $A = \mathrm{Spec}(\varphi)$ and $B = \mathrm{Spec}(\psi)$. Then $A + B$ and $A \cdot B$ are spectra.

First we prove that $A + B = \mathrm{Spec}(\zeta)$ for some formula ζ. We shall use the language $L(\varphi) \cup L(\psi) \cup \{P_A, P_B\}$, where P_A and P_B are unary predicate symbols not in $L(\varphi) \cup \cup L(\psi)$. Let $\zeta \doteq (\exists x) P_A(x) \,\&\, (\exists x) P_B(x) \,\&\, (\forall x)(P_A(x) \veebar P_B(x)) \,\&\, \varphi^{P_A} \,\&\, \psi^{P_B}$, which is,

let ζ say it's models consist of two non-empty mutually disjoint substructures which be in turn models of φ and ψ, respectively. Clearly, $\mathrm{Spec}(\zeta) = \mathrm{Spec}(\varphi) + \mathrm{Spec}(\psi)$.

Now let us search for formula ζ such that $A \cdot B = \mathrm{Spec}(\zeta)$. $L(\zeta)$, we put down as $L(\varphi) \cup L(\psi) \cup \{P_A, P_B, C\}$, where P_A and P_B be unary predicate symbols as before (now, we shall call them *the coordinate sets*) and C be a ternary predicate symbol, which we shall call *the coordinate relation*. These will be taken by us as axioms of the theory T:

$$(\exists x)(\exists y)(P_A(x) \,\&\, P_B(y)) \,\&\, (\forall x)(P_A(x) \to \neg P_B(x)) \,\&\, \varphi^{P_A} \,\&\, \psi^{P_B},$$

$$(\forall z)(\exists! x)(\exists! y) C(x, y, z),$$

$$(\forall x)(\forall y)(\forall z)(C(x, y, z) \to P_A(x) \,\&\, P_B(y)),$$

$$(\forall x)(\forall y)(P_A(x) \,\&\, P_B(y) \to (\exists! z) C(x, y, z)).$$

Those might be translated as: the coordinate sets are non-empty, they are mutually disjoint and they are models of φ and ψ, respectively; every element z has it's coordinates x and y, which are unique; if x and y are coordinates of some point, they must be members of their corresponding coordinate sets; and if x and y indeed are members of the coordinate sets, they are coordinates of a uniquely determined point z. That is, if the coordinate substructures (which are models of φ and ψ) have sizes a and b, respectively, there are $a \cdot b$ many distinct coordinates which do have exactly one associated element, wherefore we indeed have $\mathrm{Spec}(\bigwedge T) = A \cdot B$. ⊠

Example 15. The set of all composite numbers forms a spectrum as it is equal to $(\mathbb{N}^+ \setminus \{1\})^2$ - a spectrum by examples 6 and 14. ⊠

Example 16. If $A = \mathrm{Spec}(\delta)$ be a spectrum, the set A' of all n-th powers of members of A is a spectrum as well. We will slightly modify the construction used for proving that product of two spectra is a spectrum: we will consider the coordinate relation $C_n \notin L(\delta)$ to be $(n+1)$-ary, but we will only have one coordinate set (unary predicate) $P \notin L(\delta)$. A' then equals $\mathrm{Spec}(\bigwedge T_n)$ for T_n made of these axioms:

$$(\exists x) P(x) \,\&\, \delta^P \,\&\, (\forall z)(\exists! \bar{x}) C_n(\bar{x}, z),$$

$$(\forall \bar{x})(\forall z)\Big(C_n(\bar{x}, z) \to \bigwedge_{x \in \bar{x}} P(x)\Big),$$

$$(\forall \bar{x})\Big(\bigwedge_{x \in \bar{x}} P(x) \to (\exists! z) C_n(\bar{x}, z)\Big),$$

again forcing that the coordinate set be non-empty, that it form a model of δ, that every element have it's unique coordinates and that every n-tuple of elements in the coordinate set be a coordinate for some distinct element. In contrast to the case of product of two spectra, we utilise now merely one coordinate set both for abscissae and ordinates, thus forcing the resulting model to necessarily have cardinality which then be a power of the size of the coordinate set. Which particular power, depends then on the arity (dimension) of the axiomatised coordinate relation.

There, from this construction, we may derive a more general result, that spectra are closed under well-behaved polynomial mappings - *videlicet*, that images of

spectra under polynomial functions of positive natural coefficients again form spectra. Let $f(x) = \sum_{k=0}^{d} a_k x^k$ be a non-trivial polynomial of degree d with all the coefficients $a_k \in \mathbb{N}$. The language L of the formula υ such that $f[\mathrm{Spec}(\delta)] = \mathrm{Spec}(\upsilon)$ will use, outside of symbols from $L(\delta)$, the unary predicates F, P (the coordinate set as before) and additional $\sum_{k=1}^{d} a_k$ many unary predicates denoted $Q_{k,l}$ (we shall call those *the substructure relations*) where $l \in \mathbb{N}^+$ is lesser than or equal to a_k and further we will have a $(k+1)$-ary coordinate relation C_k for each $k \in \mathbb{N}^+$ lesser than $d+1$. Then we write

$$\upsilon \doteq \epsilon_{a_0}^F \,\&\, \bigwedge_{i=1}^{d} \bigwedge_{k=1}^{a_i} \Big((\exists x) Q_{k,i}(x) \,\&\, \Big(\bigwedge T_i \Big)^{Q_{k,i}} \Big) \,\&\, (\forall x) \bigvee_{\substack{P \neq U \in L \\ U \text{ is unary}}} \Big(U(x) \,\&\, \bigwedge_{\substack{V \in L \setminus \{P,U\} \\ V \text{ is unary}}} \neg V(x) \Big).$$

It is the third conjunct in υ which guarantees disjointness (and non-emptiness) of all unary predicates and the first two conjuncts are what guarantees the size. Heuristically, for better understanding, we could perhaps write:

$$\text{Model of } \upsilon = (\text{Structure of size } a_0) + \sum_{i=1}^{d} a_i \cdot (\text{Structure of size } x^i)$$

where $x \in \mathrm{Spec}(\delta)$. υ's models are therefore cardinal sums of an a_0-sized structure and all the cardinal sums of a_i many models of T_i for each i such that $0 < i < d+1$. Models of T_i are in turn of size of the i-th power of the cardinality pertaining to some fixed model of δ. Thus we have it that $f[\mathrm{Spec}(\delta)] = \mathrm{Spec}(\upsilon)$. ⊠

Example 17. As our final non-trivial example, we will show that spectra are as well closed under exponentiation, namely that the set operation $A^B = \{x; (\exists n \in \in A)(\exists k \in B)(n^k = x)\}$ yields a spectrum when A and B are both spectra. As is well known, n^k is the number of mappings of domain sized k to a set sized n. Let $A = \mathrm{Spec}(\varphi)$, $B = \mathrm{Spec}(\psi)$, $\mathrm{Spec}(\gamma) = A^B$ will be proved for some sentence γ. We axiomatise a base set, represented by the unary predicate symbol E, and an exponent set, represented by the unary predicate X. Finally we shall have a ternary predicate F, such that meaning of the atomic formula $F(a,b,c)$ correspond to the sentence "a is a function whose value at b is c"; the members of γ's universes are therefore to be isomorphically equivalent to mappings from respective B's model's universe to A's respective model's universe. Of course assume without loss of generality that $E, X, F \notin L(\varphi) \cup L(\psi)$. We put $\gamma = \bigwedge Z$ where Z is the theory of the following axioms:

$$\varphi^E \,\&\, \psi^X \qquad (E \text{ forms a model of } \varphi,\ X \text{ a model of } \psi)$$

$$(\forall a)(\forall x)(\forall y)(F(a,x,y) \to X(x) \,\&\, E(y)) \qquad (a \text{ may only map members of } X \text{ to } E)$$

$$(\forall a)(\forall x)(X(x) \to (\exists! y) F(a,x,y)) \qquad (a \text{ are functions of domain a superset of } X)$$

$$(\forall a)(\forall b)(a = b \equiv (\forall x)(\forall y)(F(a,x,y) \equiv F(b,x,y)))$$

$$(\forall a)(\forall x)(\forall y)(\exists! b)(F(b,x,y) \,\&\, (\forall x' \neq x)(\forall y')(F(a,x',y') \equiv F(b,x',y'))$$

The fourth axiom defines that two elements-functions are equal precisely when they coincide on all possible function values and the fifth axiom tells us that from every function a we may construct function b such that it differ from a at most at one point, denoted x, so that $b(x) = y$. The second and third axiom combined give

us that all members of γ's model indeed correspond to functions of a common domain, which in turn happens to be the set realised by X. The fifth axiom then ensures that every possible function from X to E be included in γ's finite models, for if we assume a function b not included, we may construct from an arbitrary function a (by the said axiom) a sequence of functions replacing a's function values at respective points one by one, until we get b. That is, every thinkable function b is included in finite models of γ. As the fourth axiom sets all functions to be equal precisely when their function values in every point equal, we have it that indeed, if and only if there be $n \in A$ and $k \in B$, is there then a model of γ of size n^k, specifically, every one whose base set's size was set to n and the exponent set's size to k. ⊠

Note. By a modification of the above example, we could obtain the result that the set of all factorials of Spec(φ)'s elements forms a spectrum for every φ. We only would have to put $\varphi \doteq \psi$ and axiomatise that all members be bijections (permutations of n elements) and the fifth axiom were then to ensure instead the possibility of exchange of two different function values at two different points (in other words, ensure the possibility of applying cycles of length 2 on the elements-permutations). Another possible modification, involving a unary function symbol, axiomatised to be a bijection between the base and exponent set, would then yield that the range of the function n^n on $\mathbb{N}^+$ be a spectrum.

Example 18. Example 17 trivially implies that the set of all powers of an arbitrary (even composite, as opposed to example 10) $a \in \mathbb{N}^+$ is a spectrum. Furthermore, the set of all non-trivial powers of all composite numbers is a spectrum as well.⊠

As evidenced by these examples, spectra constitute rather an extensive family of sets. Moreover, instead of simply being an extensive list of particular instances of the notion, numerous or not, some of the examples cannot but be considered investigations *par excellence* of spectra's general properties: namely that they are closed under finite unions and intersections (example 5) and under certain arithmetical set operations (examples 14, 16, 17). Specific examples of generalised spectra, however, do not turn out to be of any interest for now: the question of a class of structures being a general spectrum comes down to seeing whether it is an intersection of the class of all finite structures and some finitely axiomatisable elementary class of structures, *id est*, it is reduced to an unrelated, albeit non-trivial problem.

We conclude this section by showing the following theorem (a slightly generalised version of what is to be found at the beginning of [Fag74]). For simplicity, understand (only for this theorem's statement) under the term "set" a subset of $\mathbb{N}^+$.

Theorem 1. *All spectra are recursively enumerable and primitive recursive. Complements of spectra are primitive recursive. There is a recursive set which is not a spectrum. There is a primitive recursive set which is not a spectrum.*

Before proving this, we define encoding of finite structures so as to "computationalise" them, having them become a subject possible to be worked with in classical computational models. To do this, we assume all first-order formulae to be finite

words over natural numbers, where each symbol (be it a paren, a quantifier, a variable) have a unique natural number assigned to them - in the very same manner do modern-day computers encode text. This way, we may only have countably many variables, countably many k-ary predicate symbols for each k, which we assume monotonely enumerated by (primitive) recursive functions ν and p_k, respectively. We assume also a less traditional category of symbols: the category of substituted structure elements monotonely enumerated by some fixed recursive (or primitive recursive, we may again assume) function e (that is, all structures of size n have precisely elements $ab\ e(0)\ ad\ e(n-1)$).

Definition 2. Let $\mathbb{A}$ be a finite relational structure such that $\|\mathbb{A}\| = n$. Without loss of generality, assume $L(\mathbb{A})$ to be relational, each function symbol (constant symbols included) may be simulated by a predicate symbol and one additional axiom. Let s be the greatest arity pertaining to some symbol of $L(\mathbb{A})$ and let m be the size of $L(\mathbb{A})$. We define *encoding of* $\mathbb{A}$ in $\mathbb{N}$ to be the number $c(\mathbb{A}) \in \mathbb{N}$ such that for it's shortest binary expansion represented by the finite sequence a hold:

1. $a_k = 1$ for all $k \in \mathbb{N}$ such that $0 \leq k < \lceil \mathtt{l}(n) \rceil$ (that is, $c(\mathbb{A})$ begins with unary expansion of $\lceil \mathtt{l}(n) \rceil$).
2. $a_{\lceil \mathtt{l}(n) \rceil} = 0$ (demarcates the end of the aforesaid unary expansion of $\lceil \mathtt{l}(n) \rceil$).
3. a_k is equal to the k-th member of n's shortest binary expansion when $\lceil \mathtt{l}(n) \rceil < k \leq 2 \cdot \lceil \mathtt{l}(n) \rceil$ (that is, a continues with n's binary expansion).
4. $a_k = 1$ for all $k \in \mathbb{N}$ such that $2 \cdot \lceil \mathtt{l}(n) \rceil < k \leq 2 \cdot \lceil \mathtt{l}(n) \rceil + s$ (this is unary expansion of s).
5. $a_{2 \cdot \lceil \mathtt{l}(n) \rceil + s + 1} = 0$, again to demarcate the end of said unary expansion.
6. a continues on with a sequence of length $|L(\mathbb{A})| \cdot n^s$, comprised of $|L(\mathbb{A})|$ consecutive *encodings of* all *relations* from $L(\mathbb{A})$, as defined in the following.

Assume $|\mathbb{A}|$ linearly ordered by $\leq$. Denote by $\leq_s$ the lexicographical ordering of ordered s-tuples of $|\mathbb{A}|$'s elements induced by $\leq$. The *encoding of an s-ary relation* R is a binary sequence of length n^s such that it's m-th member equal 1 if and only if for the ordered s-tuple $\bar{e}$ which be m-th least element with respect to $\leq_s$ hold $\mathbb{A} \models R(\bar{e})$. When in need of *encoding relation S of lesser arity*, let us say d, we choose it to be the encoding of the s-ary relation R_S uniquely determined by the definitional axiom $(\forall \bar{x})(\forall \bar{y})(R_S(\bar{x}, \bar{y}) \equiv S(\bar{x}))$, where $l(\bar{x}) = d$, $l(\bar{y}) = s - d$. Finally, we conclude the license that all numbers which are not encodings as defined above be considered encodings of a formal `null` structure of empty signature wherein hold whatsoever no formulae (thus entirely contradicting Tarski's truth definition). ◄

For this encoding, though it is not the most effective one possible (we could allow relations of different arities in encoding of one structure, for example), if we keep the definition's notation, we have it that the length of $c(\mathbb{A})$'s binary expansion is *ex definitionem* $(\lceil \mathtt{l}(n) \rceil + 1) + \lceil \mathtt{l}(n) \rceil + (s+1) + |L(\mathbb{A})| \cdot n^s$, that is: it is polynomial in n and $|L(\mathbb{A})|$ and exponential in s whereby $c(\mathbb{A})$ itself is exponential in n and $|L(\mathbb{A})|$ and superexponential in s. Clearly, the set of encodings of all finite structures

gives us a primitive recursive set and we may primitively recursively compute size of the encoded structure's universe.

Proof (of Theorem 1). We know that encoding and decoding of finite sequences as well as manipulating binary expansion of given numbers are primitive recursive operations. Now we construct a recursive function c_{gs}, getting a first-order sentence φ and a finite structure $\mathbb{A}$ (or, to be precise, it's encoding $c(\mathbb{A})$) as input and returning whether $\mathbb{A}$ is a model of φ or not (represented by output values 1 and 0, respectively). Fixing φ then yields recursivity of GenSpec(φ). c_{gs} is derived by a variant of primitive recursion on φ as follows:

1. if $\varphi \doteq (\forall x)\psi$ for some word ψ and some variable x, we put $c_{\mathrm{gs}}\big(\varphi, c(\mathbb{A})\big) = \\ = c_{\mathrm{gs}}\big(\bigwedge_{k=0}^{|\mathbb{A}|-1} \psi(x/e(k)), c(\mathbb{A})\big)$.
2. analogically, if $\varphi \doteq (\exists x)\psi$, we put $c_{\mathrm{gs}}\big(\varphi, c(\mathbb{A})\big) = c_{\mathrm{gs}}\big(\bigvee_{k=0}^{|\mathbb{A}|-1} \psi(x/e(k)), c(\mathbb{A})\big)$.
3. if $\varphi \doteq (\psi \,\&\, \chi)$, we put $c_{\mathrm{gs}}\big(\varphi, c(\mathbb{A})\big) = c_{\mathrm{gs}}\big(\psi, c(\mathbb{A})\big) \cdot c_{\mathrm{gs}}\big(\chi, c(\mathbb{A})\big)$.
4. if $\varphi \doteq (\psi \vee \chi)$, we put $c_{\mathrm{gs}}\big(\varphi, c(\mathbb{A})\big) = c_{\mathrm{gs}}\big(\psi, c(\mathbb{A})\big) + c_{\mathrm{gs}}\big(\chi, c(\mathbb{A})\big) - c_{\mathrm{gs}}\big((\psi \,\&\, \chi), c(\mathbb{A})\big)$.
5. if $\varphi \doteq \neg\chi$, we put $c_{\mathrm{gs}}\big(\varphi, c(\mathbb{A})\big) = 1 - c_{\mathrm{gs}}\big(\chi, c(\mathbb{A})\big)$.

and accordingly for all other logical operations if established.

6. if $\varphi \doteq a = b$ for some a and b, then return
   (a) $c_{gs}\big(\varphi, c(\mathbb{A})\big) = 0$ if a and b are two different structure elements (that is, $a = e(j)$ and $b = e(k)$ for some natural indices j and k and $j \neq k$) or either a or b is a variable.
   (b) $c_{gs}\big(\varphi, c(\mathbb{A})\big) = 1$ if a and b are both the same structure element (that is, $a = b = e(j)$ for some $j \in \mathbb{N}$).
7. if $\varphi \doteq R(\bar{\mathrm{x}})$ for some k-ary predicate symbol R and ordered k-tuple $\bar{\mathrm{x}}$, then if the arity of predicates encoded to $c(\mathbb{A})$ (clearly a recursively computable number) is s:
   (a) if $k < s$ and $R = p_k(a)$, put $c_{\mathrm{gs}}\big(\varphi, c(\mathbb{A})\big) = c_{\mathrm{gs}}\big(p_s(a)(\bar{\mathrm{x}}, \bar{y}), c(\mathbb{A})\big)$ where $\bar{y}$ is ordered $(s-k)$-tuple of structure elements $e(0)$.
   (b) if $k > s$, put $c_{\mathrm{gs}}\big(\varphi, c(\mathbb{A})\big) = 0$.
   (c) if $k = s$, and $\bar{\mathrm{x}}$ contains some variables, put $c_{\mathrm{gs}}\big(\varphi, c(\mathbb{A})\big) = 0$ instantly.
   (d) if $k = s$, and $\bar{\mathrm{x}}$ is a tuple of structure elements (that is, of numbers within range of the function e), put $c_{gs}\big(\varphi, c(\mathbb{A})\big) = e_v\big(\varphi, c(\mathbb{A})\big)$, where e_v is a recursive function defined so that
      i. if $R = p_s(n)$ and $\mathbb{A}$ has signature of size lesser than n, return the value $e_v\big(\varphi, c(\mathbb{A})\big) = 0$.
      ii. else if $R = p_s(n)$, search for the n-th relation encoded in $c(\mathbb{A})$ and find out whether $\bar{\mathrm{x}}$ has assigned 0 or 1 within R's encoding. $e_v\big(\varphi, d(\mathbb{A})\big)$ then equals this respective value.
8. or else, return $c_{\mathrm{gs}}\big(\varphi, c(\mathbb{A})\big) = 0$.

Note that if φ has some free variable, c_{gs} returns 0. We have established that every generalised spectrum is recursive (and primitive recursive, too, as we did not use minimisation and derived c_{gs} from primitive recursive functions only) and thus recursively enumerable as well.

Assume now a function $c_{\mathrm{Spec}}(\varphi, n)$ which is derived by bounded quantification from c_{gs} as follows: $(\exists x \leq m(n,\varphi))(c_{\mathrm{gs}}(\varphi, x)\ \&\ |x| = n)$, where $m(n,\varphi)$ is defined to be the greatest possible encoding pertaining to some structure $\mathbb{B}$ of n elements, whose signature's size is equal to the greatest number b such that $p_k(b) \in L(\varphi)$ for some k and whose signature's elements are all s-ary, where s is the greatest arity pertaining to some predicate symbol from φ. $m(\varphi, n)$ defined like this then has binary expansion consisting of $\lceil \mathtt{l}(n) \rceil$ consecutive 1s, followed by a 0 and n's binary expansion, then s many 1s again followed by a 0 and $b \cdot n^s$ many 1s (that is, this structure satisfies every evaluated atomic formula, except equalities and inequalities).

As $m(\varphi, n)$ is primitive recursive, and both $c_{\mathrm{gs}}(\varphi, x)$ and $|x| = n$ are primitive recursive, we obtain that c_{Spec} is also a primitive recursive function. Rephrasing the formal definition, c_{Spec} is constructed so as to return 1 if and only if there be a model of φ of size n, search for which is bounded by having established the greatest feasible solution $m(\varphi, n)$ - models with a bigger integer assigned as their code would either have more than n elements, or would have unnecessarily vast signature. Thus $c_{\mathrm{Spec}}(\varphi, n)$ with fixed φ indeed is the characteristic function of $\mathrm{Spec}(\varphi)$. All spectra are thus primitive recursive and as a consequence are also recursively enumerable and the same goes for their complements, because $1 - c_{\mathrm{Spec}}\big(\varphi, c(\mathbb{A})\big)$ is also a primitive recursive function. If we wanted to talk of complements in $\mathbb{N}^+$ instead of $\mathbb{N}$, the same goes with the primitive recursive function $\Big(1 - c_{\mathrm{Spec}}\big(\varphi, c(\mathbb{A})\big)\Big) \cdot \mathrm{sgn}(n)$.

Because we know that not every recursive subset of $\mathbb{N}^+$ is primitive recursive, we may conclude instantly that not every recursive subset of $\mathbb{N}^+$ is a spectrum. To be more explicit, however, we will use the diagonal argument to construct a recursive set demonstrating this. What's more, we will even construct it primitive recursive. Let $f(n)$ be a primitive recursive function enumerating all formulae of language $\bigcup_{n=0}^{\infty}\{p_k(n); k \in \mathbb{N}\}$ (possibly not monotonely) and let $t(n)$ be function defined as $\big(1 - c_{\mathrm{Spec}}\big(f(n), n\big)\big) \cdot \mathrm{sgn}(n)$; this is the characteristic function of set $T \subset \mathbb{N}^+$ which differs from $\mathrm{Spec}(f(n))$ for all $n \in \mathbb{N}^+$ so that if $n \in \mathrm{Spec}(f(n))$, then $n \notin T$ and vice-versa: if $n \notin \mathrm{Spec}(f(n))$, then $n \in T$. Thus, we have T a primitive recursive subset of $\mathbb{N}^+$ which is not a spectrum. ***Quod Erat Demonstrandum***

This theorem gives us certain information about ease of spectra's recognition. Although too broad a property to be considered characterising spectra complexity-wise, primitive recursivity guarantees, that spectra, are, in a sense, feasibly computable. In the next section, spectra will be uniquely characterised in terms of complexity theory.

1.2 Second-order logic and the theorem of Fagin

We will now introduce the system of second-order logic. You may notice most of the introduced terms defined as analogues to those already seen when dealing with first-order logic.

Definition 3. Let L (whose members shall we call *second-order variables*) and L_c be two disjoint signatures. Conclude that all second-order variables are capital latin letters or variants thereof, in a similar manner are all first-order variables denoted by some latin minuscule form. *A second-order constructing sequence in L with built-in signature L_c* is finite sequence of words such that for it's every member φ holds at least one of the following:

1. φ is a first-order formula in language $L \cup L_c$.
2. $\varphi \stackrel{\circ}{=} \square\psi$, where ψ precedes φ in the same sequence and $\square$ is either $\neg$ or is of the form $(\int \mathtt{A})$ where $\int \in \{\exists, \forall\}$ and $\mathtt{A}$ is either a variable (which yields well-known first-order quantification), or a symbol from L, in which case shall we speak of *second-order quantification* or more specifically, of quantification over relations or predicates, constants and functions.
3. $\varphi \stackrel{\circ}{=} \psi \diamond \chi$, where ψ and χ precede φ in the same sequence and $\diamond$ is some first-order binary connective.

Word φ is a *second-order formula in language L with built-in signature L_c* (if L and L_c be clear from the context, we shall omit them) if and only if there is a second-order constructing sequence in L with built-in signature L_c such that φ be it's last member. Clearly, every first-order formula in language $L \cup L_c$ is a second-order formula. A second-order formula is said to be *second-order subformula* of another second-order formula when former is a subword to the latter. We further define that:

1. every occurrence of every symbol from L in a first-order formula is *free*, or that in first-order formulae all symbols from L *occur freely*.
2. if a second-order formula φ is of the form $\psi \diamond \chi$, where $\diamond$ is a first-order binary connective and either ψ or χ have free or bound occurrences, respectively, of a symbol from L (or that the symbol occurs freely), so is the case with φ,
3. if a second-order formula φ is of the form $\square\psi$, where $\square$ is either $\neg$ or of the form $(\int x)$ for some $\int \in \{\exists, \forall\}$ and some variable x, and in ψ a symbol from L occurs freely or bound, respectively, so it does in φ,
4. in every second-order formula of the form $(\int X)\psi$, where $X \in L$ and $\int \in \in \{\exists, \forall\}$ have only bound occurrences of X (or that the symbol only occurs bound).

Second-order formula is said to be a *sentence* if every occurrence of every symbol from L it contains is bound. Second-order formula φ is said to be in *prenex normal form*, if it has constructing sequence a of length n such that:

1. a_0 is first-order, $a_n = \varphi$.

2. for every non-zero k in domain of a holds that $a_k \stackrel{\circ}{=} (\int \mathtt{X}) a_{k-1}$ for some $\int \in \{\forall, \exists\}$ and $\mathtt{X}$ a symbol from L or a variable.

and it is said to be in *strong prenex normal form* if a further satisfies:

3. there exists k in domain of a such that all formulae from a_0 to a_k be first-order and no formula upwards from a_k be first-order.

For formulae in prenex normal form we may consider their *matrices* - the therein longest contained quantifier-free subformulae - and *prefixes qua* complements thereof in the original formula, in the manner we know it from first-order logic. For formulae in strong prenex normal form we may further consider *first-order matrices*: the therein longest contained quantifier-free **first-order** subformulae. L is said to be *n-adic* if it is relational and all it's elements are n-ary. Second-order formula in L with built-in $L_{\mathfrak{c}}$ is *n-adic* if L is n-adic. Let $\mathbb{A}$ be a structure in $L_{\mathfrak{c}}$. A *second-order evaluation over* $\mathbb{A}$ is a function assigning $\mathbb{A}$ an expansion $\mathbb{A}'$ in $L \cup L_{\mathfrak{c}}$. Let e_{II} be a second-order evaluation over $\mathbb{A}$ and let e_{I} be a first-order variable evaluation. First six parts of this inductive definition are found already as parts of Tarski's truth definition, only second-order quantification's validity is novel there. We define *second-order satisfaction of φ through e_{II} and e_I in* $\mathbb{A}$ (symbolically: $\mathbb{A}\left|\frac{\mathrm{II}}{=\!=}_{L}\varphi[e_{\mathrm{II}}, e_{\mathrm{I}}]\right.$) as follows:

1. for $\varphi \stackrel{\circ}{=} \psi \vee \chi$, define: $\mathbb{A}\left|\frac{\mathrm{II}}{=\!=}_{L}\varphi[e_{\mathrm{II}}, e_{\mathrm{I}}] \Leftrightarrow \left(\mathbb{A}\left|\frac{\mathrm{II}}{=\!=}_{L}\psi[e_{\mathrm{II}}, e_{\mathrm{I}}] \text{ vel } \mathbb{A}\right|\frac{\mathrm{II}}{=\!=}_{L}\chi[e_{\mathrm{II}}, e_{\mathrm{I}}]\right)\right.$.
2. for $\varphi \stackrel{\circ}{=} \psi \,\&\, \chi$, define: $\mathbb{A}\left|\frac{\mathrm{II}}{=\!=}_{L}\varphi[e_{\mathrm{II}}, e_{\mathrm{I}}] \Leftrightarrow \left(\mathbb{A}\left|\frac{\mathrm{II}}{=\!=}_{L}\psi[e_{\mathrm{II}}, e_{\mathrm{I}}] \text{ et } \mathbb{A}\right|\frac{\mathrm{II}}{=\!=}_{L}\chi[e_{\mathrm{II}}, e_{\mathrm{I}}]\right)\right.$.
3. for $\varphi \stackrel{\circ}{=} \neg\psi$, define: $\mathbb{A}\left|\frac{\mathrm{II}}{=\!=}_{L}\varphi[e_{\mathrm{II}}, e_{\mathrm{I}}] \Leftrightarrow \text{ not } \mathbb{A}\right|\frac{\mathrm{II}}{=\!=}_{L}\psi[e_{\mathrm{II}}, e_{\mathrm{I}}]$.
4. accordingly for other first-order connectives.
5. if $\varphi \stackrel{\circ}{=} (\exists x)\psi$, have: $\mathbb{A}\left|\frac{\mathrm{II}}{=\!=}_{L}\varphi[e_{\mathrm{II}}, e_{\mathrm{I}}] \Leftrightarrow \left(\text{exists } s \in |\mathbb{A}| \text{ so that } \mathbb{A}\right|\frac{\mathrm{II}}{=\!=}_{L}\varphi(x/s)[e_{\mathrm{II}}, e_{\mathrm{I}}]\right)\right.$.
6. if $\varphi \stackrel{\circ}{=} (\forall x)\psi$, have: $\mathbb{A}\left|\frac{\mathrm{II}}{=\!=}_{L}\varphi[e_{\mathrm{II}}, e_{\mathrm{I}}] \Leftrightarrow \left(\text{for all } s \in |\mathbb{A}| \text{ holds } \mathbb{A}\right|\frac{\mathrm{II}}{=\!=}_{L}\varphi(x/s)[e_{\mathrm{II}}, e_{\mathrm{I}}]\right)\right.$.
7. if $\varphi \stackrel{\circ}{=} (\exists X)\psi$, define that $\mathbb{A}\left|\frac{\mathrm{II}}{=\!=}_{L}\varphi[e_{\mathrm{II}}, e_{\mathrm{I}}]\right.$ if and only if there is an expansion $\mathfrak{A} \restriction \mathbb{A}$ in $L(\psi) \cup \{X\}$ such that $\mathfrak{A}\left|\frac{\mathrm{II}}{=\!=}_{L}\psi[e_{\mathrm{II}}, e_{\mathrm{I}}]\right.$.
8. if $\varphi \stackrel{\circ}{=} (\forall X)\psi$, define that $\mathbb{A}\left|\frac{\mathrm{II}}{=\!=}_{L}\varphi[e_{\mathrm{II}}, e_{\mathrm{I}}]\right.$ if and only if for all expansions $\mathfrak{A} \restriction \mathbb{A}$ in $L(\psi) \cup \{X\}$ hold $\mathfrak{A}\left|\frac{\mathrm{II}}{=\!=}_{L}\psi[e_{\mathrm{II}}, e_{\mathrm{I}}]\right.$.

If the satisfaction of φ is in particular independent of chosen evaluations (which clearly happens precisely when φ be a second-order sentence with no first-order variables occurring freely) , we may as well reduce the full notation to $\mathbb{A}\left|\frac{\mathrm{II}}{=\!=}_{L}\varphi\right.$ and when φ's validity be even independent of $\mathbb{A}$, we shall only write $\left|\frac{\mathrm{II}}{=\!=}_{L}\varphi\right.$. We call such formula *second-order logically valid.*

Second-order formulae φ and ψ are *equivalent* if and only if φ is satisfied if and only if ψ be satisfied (either in general, or in some structure under some evaluation). Second-order formula is said to be *existential*, or *universal*, respectively, when it is equivalent to a formula which contains no subword of the respective

form $(\forall X)$ or $(\exists X)$, with $X \in L$ and none occurrence of $\neg$ precede any occurrence of quantifier. In the following, we no longer need consider L in general, so conclude that $L = \bigcup_{n=0}^{\infty}\{p_k(n); k \in \mathbb{N}\}$ in the same manner we have seen it in the previous section. For L is now chosen fixed, we write only $\models^{\text{II}}$ in place of $\models^{\text{II}}_{L}$. ◀

Second-order logic is almost never introduced in logic textbooks: all of the standard references [Soc01; Šve02; Kle67; Sho67; Cur77] merely mention it, not even introducing it formally. Yet it is to be found discussed in some sources, you may see for example [Mlč22] where many of the results listed in this section are to be found as well. Second-order logic arguably is quite a natural and simple extension of first-order logic, yet it's expressive power is much broader:

Theorem 2. *There is second-order formula ϵ_{Fin} satisfied precisely by finite structures, and formula ϵ_∞ satisfied precisely by infinite structures, we may even express countable and uncountable infiniteness by respective formulae $\epsilon_{\aleph_0}$ and $\epsilon_\infty \,\&\, \neg\epsilon_{\aleph_0}$. There is formula* CH *whose satisfaction in every structure is equivalent to validity of continuum hypothesis. There are* **NP***-complete properties expressible in* ***existential*** *second-order logic.*

Proof. Let F be a unary function symbol and put

$$\epsilon_{\text{Fin}} \stackrel{\circ}{=} (\forall F)((\forall x)(\forall y)(\forall z)((F(x) = z \,\&\, F(y) = z \to x = y) \to (\forall y)(\exists x)(F(x) = y)),$$

informally: "every injection is a surjection", which is one of the possible definitions of finiteness[1]. Then we may put, for example, $\epsilon_\infty \stackrel{\circ}{=} \neg\epsilon_{\text{Fin}}$.

As for CH, we have to first find said $\epsilon_{\aleph_0}$ and $\epsilon_{2^{\aleph_0}}$, satisfied precisely in structures of countably infinite universe and of universe of continuum's size, respectively. Let X be a unary predicate and set $\epsilon_{\aleph_0}$ to be

$$\epsilon_\infty \,\&\, (\forall X)(\epsilon_\infty^X \to (\exists F)\phi_F)$$

where by notation ρ^X we mean, similarly as in first-order logic, formula ρ with all first-order quantifier's relativised to X and where ϕ_F is a shorthand notation for the first-order formula $(\forall y)(\exists x)(P(x) \,\&\, F(x) = y)$ ("F restricted to domain P is onto the whole universe"). Validity of $\epsilon_{\aleph_0}$ in $\mathbb{A}$ then translates to "$|\mathbb{A}|$ is infinite and it's every infinite subset is bijective with it", so $\epsilon_{\aleph_0}$ truly lives up to it's expectation.

To construct $\epsilon_{2^{\aleph_0}}$ of desired properties, it is needed to employ a little more sophisticated trick: satisfying of $\epsilon_{2^{\aleph_0}}$ will be equivalent to the possibility of endowing the particular model with field structure isomorphic to $\mathbb{R}$. Thereby we designate:

$$\epsilon_{2^{\aleph_0}} \stackrel{\circ}{=} (\exists +)(\exists \cdot)(\exists^{-1})(\exists -)(\exists 0)(\exists 1)(\exists <)(\textstyle\bigwedge \mathrm{F} \,\&\, \Omega \,\&\, \alpha),$$

where $\Omega \stackrel{\circ}{=} \bigwedge \mathrm{LO} \,\&\, (\forall a)(\forall b)(\forall c)(\forall d)((a < b \;\&\, c < d \to a + c < b + d \,\&\, (0 < a \;\&\, 0 < c \to a \cdot c < b \cdot d))$ (linear ordering - LO is the theory of strict linear ordering for $<$ - and compatibility of $<$ with endowed ring structure), F is the theory of fields (already seen in example 9) and α represents the property of every non-empty set

[1] Note that some definitions of finiteness are non-equivalent over ZF; this one in particular requires the axiom of choice in order to be equivalent with Tarski's the definition of finiteness (see [BŠ86])

having a supremum. As is well known, real numbers form the only ordered field of such a property (see [BŠ86]), wherefore the only detail remaining to complete construction of $\epsilon_{2^{\aleph_0}}$ of desired property is to explicitly write down α in second order logic:

$$(\forall X)(((\exists x)X(x)\,\&\,(\exists y)(\forall x)(X(x)\to x<y))\to(\exists y)((\forall x)(X(x)\to x<y\ \vee\ x=y)\,\&\\ \&\,(\forall z)(z<y\to(\exists x)(z<x\,\&\,X(x))))).$$

Now, using another unary predicate Y it is finally possible for us to formulate CH naturally as "All subsets of every set of continuum's size either satisfy $\epsilon_{\aleph_0}$ or $\epsilon_{2^{\aleph_0}}$":

$$\mathtt{CH}\stackrel{\circ}{=}(\forall X)(\epsilon^X_{2^{\aleph_0}}\to(\forall Y\subseteq X)(\epsilon^Y_\infty\to\epsilon^Y_{\aleph_0}\vee\epsilon^Y_{2^{\aleph_0}})).$$

Perhaps, for utter precision, it only remains to note that $(\forall Y\subseteq X)(...)$ is actually a shorthand for $(\forall Y)\big((\forall y)(Y(y)\to X(y))\to...\big)$.

Before moving on to the part about **NP**-completeness, recall from introduction that a graph is a structure in the language $\{R\}$, where R is axiomatised as an antireflexive symmetric binary predicate. We call a graph tricolourable if it is separable into three disjoint substructures such that two of the graphs's vertices being reachable by R imply pertinence to two different of the three substructures.

As for the **NP**-complete properties, we shall name the following two:

1. Let U be unary predicate and consider a binary predicate R built-in. Then satisfaction of the formula

   $$(\exists U)(\forall x)(\exists!y)(R(x,y)\,\&\,U(y))$$

   in given structure is an **NP**-complete query. This formula is brought up in [Fag75] and the corresponding query was proven to be **NP**-complete in [Fag73] and [Fag74]. We shall not prove it here.

2. Tricolourability is well-known to be an **NP**-complete property (this, too, may be seen named in [Sip06]). We will show that the question of a graph being tricolourable may be formulated by an existential second order sentence which we shall prove now. Note that this example is classical and may be found in almost every reference, see for example [SV95] and [Imm99].

Assume the binary relation R built-in, as the input structure is supposed to be a (non-directed) graph. Then it is enough to consider three unary predicates (colours) C_1, C_2 and C_3 within $\bar{C}$ and designate

$$\mathtt{3COL}\stackrel{\circ}{=}(\exists\bar{C})\Big((\forall x)\bigvee_{i=1}^{3}\Big(C_i(x)\,\&\bigwedge_{\substack{j\in\{1,2,3\}\\ j\neq i}}\neg C_j(x)\Big)\,\&\,(\forall x)(\forall y)\big(\bigwedge_{i=1}^{3}(C_i(x)\,\&\,C_i(y)\to\neg R(x,y))\big)\Big).$$

Now, the formula 3COL, translating as "there are three colours such that every vertex has precisely one of these colours and every two vertices of the same colour go mutually unconnected", indeed is a paraphrasing of tricolourability. ***Q.E.D.***

However, this expressive power is turning out to have it's drawbacks, as second-order logic lacks many of first-order logic's important properties.

Theorem 3. *Compactness theorem and Löwenheim-Skolem theorem fail to hold for second-order logic. Second-order logic is essentially incomplete and essentially undecidable.*

Proof. Let $\mathscr{E} = \{\epsilon_{\geq n}; n \in \{\mathrm{Fin}\} \cup \mathbb{N}\}$. For every finite subset of $\mathscr{E}$ does exist a structure satisfying all it's members, yet every infinite subset of $\mathscr{E}$ containing ϵ_{Fin} is unsatisfiable as it would have to be infinite, in order to have more than n members for every index n of some of the infinitely many contained formulae of the form $\epsilon_{\geq x}$. Yet it is not possible then for said structure to satisfy ϵ_{Fin}. So compactness theorem indeed fails here.

Every structure satisfying $\epsilon_{2^{\aleph_0}}$ has cardinality of continuum, although the single formula of course contains merely finitely many signature symbols. Thus fails both downward and upward Löwenheim-Skolem theorem.

CH witnesses incompleteness of second-order logic as continuum hypothesis is known to be undecidable (see [BŠ86]). What is more, this can not be consistently dealt with by simply claiming recursively many additional formulae to be true, as then would it be possible to decide formula of the form $(\forall \in)(\bigwedge \mathtt{NBG} \rightarrow \varphi)$ for arbitrary φ, which is known to be impossible by first Gödel's theorem. By the same theorem and same example, the same goes for undecidability. ***Q.E.D.***

Following theorem is not necessary, but it strengthens insignificantly the eponymous theorem which is about to follow.

Theorem 4 (second-order prenex normal form theorem). *Every formula of second-order logic is equivalent to some formula in prenex normal form. Every formula of second-order logic is equivalent to some formula in* ***strong*** *prenex normal form.*

Proof. The proof goes the same way as for first-order version. We first notice it true for atomic formulae and then prove it inductively for $\neg$, $\&$ and $\vee$. Not even quantifications over second-order variables pose any difficulty undealt with in first-order version hereof.

- $\neg$: For $X \in L$ clearly $\neg(\forall X)\varphi \equiv (\exists X)\neg\varphi$ and $\neg(\exists X)\varphi \equiv (\forall X)\neg\varphi$ as well as already is the case with first-order quantification.
- $\&$: Without loss of generality, we may assume the considered formula to be of the form

$$\left(\int \mathrm{x}\right)\psi \,\&\, \left(\not\int \mathrm{y}\right)\chi \text{ clearly equivalent to } \left(\int \mathrm{x}'\right)\left(\not\int \mathrm{y}\right)(\psi' \,\&\, \chi),$$

  where ψ and χ are quantifier-free formulae, x and y are tuples of variables (first- or second-order) being quantified over, $(\int \mathrm{x})$ and $(\not\int \mathrm{y})$ are prefixes to ψ and χ (in the usual sense), ψ' is created of ψ by replacing every symbol from $L(\psi)$ and every bound variable in ψ with one of the same kind so that $L(\psi') \cap L(\chi) = \emptyset$ and no bound variables in ψ are present within χ, and finally, $(\int \mathrm{x}')$ is created of $(\int \mathrm{x})$ by replacing all members of x by respectively assigned members of $L(\psi')$.

3. precisely the same way for disjunction and accordingly for other first-order binary connectives.

4. The induction step goes *ex definitionem* for all types of quantification.

It remains to prove that every formula in prenex normal form has an equivalent formula in strong prenex normal form. That goes simply by showing that every "subprefix" of the form $(\int x)(\oint X)$ where $\int, \oint \in \{\forall, \exists\}$, where $P \in L$ (let us say it be a predicate symbol, without loss of generality) and x is a first-order variable, can be rewritten so that second-order quantifications precede the first-order one therein, along perhaps with some modification of the matrix of considered formula. This leaves us four cases to be considered.

1. $(\exists x)(\exists P)$ may clearly be rewritten as $(\exists P)(\exists x)$.

2. The same: $(\forall x)(\forall P)$, we rewrite as $(\forall P)(\forall x)$.

3. This case will require some modification of the formula as a whole as opposed to simply permuting parts of the prefix. Every formula of the form $(\forall x)(\exists P)\varphi$ may equivalently be written $(\exists P^+)(\forall x)\varphi'$, where P^+ is of arity by one bigger than arity of P and φ' is obtained from φ by replacing every subformula of the form $P(\bar{y})$ by $P^+(x, \bar{y})$. In other words, we reformulate the fact of there being a relation P of certain property for each x as a requirement of there being a broader relation P^+ wherefrom we may determine the respective P for given x by fixing x as the first variable: atomic subformulae of φ' are then of the form $P^+(x, \bar{y})$.

4. The last case, $(\exists x)(\forall P)$, goes by reducing to the previous case. For every formula ϕ we have $(\exists x)(\forall P)\phi \Leftrightarrow \neg(\forall x)(\exists P)\neg\phi$ which, by the previous case, may be written $\neg(\exists P^+)(\forall x)\neg\phi' \Leftrightarrow (\forall P^+)(\exists x)\phi'$.

Thus, every second-order formula truly may be equivalently expressed by a formula in strong prenex normal form. What's more, both universal and existential second-order formulae in strong prenex normal form are closed under all first-order quantifications and under respective second-order quantification. ***Q.E.D.***

The following theorem is the oldest result of descriptive complexity theory, a branch concerned, put simply, by characterising complexity classes based on logics they are describable by. Before moving on to the theorem, note that structure $\mathbb{A}$ satisfying an existential second-order formula φ is equivalent to $\mathbb{A}$ being a member of the generalised spectrum of φ's first order matrix in language $L(\mathbb{A})$.

Theorem 5 (Fagin's theorem). *Every isomorphism-closed class of finite first-order structures over a non-empty finite signature, which is a generalised spectrum, `id est` is definable by an existential second-order formula, is in complexity class* **NP**. *Every isomorphism-closed class of finite first-order structures over a non-empty finite signature, which is in complexity class* **NP**, *definable by an existential second-order formula, `ergo` a generalised spectrum.*

Proof (sketch). We only describe the overall principle behind the proof, omitting some necessary technicalities. The second direction, that is, that validity of a fixed existential second-order formula (in strong prenex normal form, without loss of

generality, as we know from the previous theorem) can be recognised by a non-deterministic Turing machine in polynomial time, is the easier one and may be derived by letting the machine non-deterministically expand the input structure (or, more precisely, the encoding thereof) by realisations of second-order variables quantified over and then subjecting this expansion to model checking algorithm described already in terms of recursive functions in theorem 1. By analysis of the algorithm, we could find it running in time proportionate to $|\varphi| + \mathrm{qr}(\varphi) \cdot 1\|K\|$, where K is the expanded structure, $\mathrm{qr}(\varphi)$ is the quantification rank of φ and $|\varphi|$ is the length of φ. Therefore the algorithm is polynomial in input.

The second direction is more technical: we have granted the existence of a non-deterministic Turing machine (assume over binary input alphabet) accepting in polynomial time the language consisting precisely of the encodings of members of said class of structures; now we are to finitely axiomatise it's behaviour in existential second-order logic. We may assume, without loss of generality, the machine to accept it's language in time under $n^k - 1$, where n is the length of the word on input and $k \in \mathbb{N}^+$. The formula will have built-in linear ordering on input structure's elements and thereby induced lexicographical ordering of k-tuples, thus allowing us to have the k-tuples of structure's elements denote positions on tape and in the input word, as well as time within the computation. Finally, we assume built-in the k-ary relation β_0, meaning that the member of the input binary word, on position represented by the k-tuple argument to β_0, is 0. $\neg\beta_0(\bar{s})$ for some k-tuple $\bar{s}$ will then mean that on the position $\bar{s}$ within the input word is instead 1.

The formula axiomatising the machine will begin by consecutive existential quantifications over the following relations:

1. The k-ary relation X_q for each state the machine can reach. These relations are supposed to model the property of the machine being in state q at time t represented by a k-tuple of input structure's elements.
2. The $(2k)$-ary relation Y_σ for every σ in machine's alphabet. Formula $Y_\sigma(\bar{t}, \bar{b})$ is then to mean that at time $\bar{t}$ (a k-tuple of given structure's elements again), the symbol σ is on the position $\bar{b}$ (again, a k-tuple).
3. The $(2k)$-ary relation Z, to model by formula $Z(\bar{t}, \bar{a})$ the statement: "at time $\bar{t}$, the machine's head is on the cell $\bar{a}$, in the same manner as we have seen it with the relations Y_σ.

Then, the following statements can be rewritten in now specified language:

1. "Let 0 be the least element with respect to $<$. Then, at the time 0^k (0^k is a k-tuple of zeroes, of course), is the machine in the initial state q_0, the head is on position 0^k, and if 0 or 1 are on a position $\bar{x}$ in the input word, it is the case at time 0^k as well."
2. "In the preceding configuration, the machine was in state q, the head was on cel $\bar{x}$ and the time was predecessor of current time."
3. "In the following configuration, the machine will be in state q, the symbol σ will be on current cell and the head will move left or right."
4. "Content of the cell, over which the head is at given time not situated, is not

changed during the transition to the next configuration."

5. "Every configuration transcedes to another, if there is time left." (recall the machine running in $n^k - 1$ steps, we have to use up n^k many time positions)
6. "The machine does not halt in any of rejecting states."

These are then enough for construction of said formula which fully axiomatises the machine. Thus, every isomorphism-closed class of finite structures over non-empty signature present within **NP** truly is definable by an existential second-order formula and therefore a generalised spectrum. ***Quod Erat Demonstrandum***

Fagin's theorem provides a very strong bond between logic and complexity theory, as it lets us identify certain classes of structures as equivalent to members of an important complexity class. It was first proved by Fagin in his dissertation [Fag73] and then it was published in [Fag74]. Probably the most detailed proof is to be found in [Imm99]. The manner of proof sketch above is in accordance with the proof as it is found in [Grä07].

1.3 Applications and open problems

Fagin's theorem allows us to reformulate the question of a class of structures of certain kind being in **NP** to the question of it being finitely axiomatisable in existential second-order logic. As it may easily be seen, negations of existential second-order formulae are equivalent to universal second-order fomulae. Thus, if we assume that a class of structures $K \in \mathbf{NP}$ be defined by an existential second-order formula φ, we may conclude immediately that K's complement $\bar{K}$ in class of all finite structures over the same signature, defined by $\neg\varphi$, belongs to the class co**NP**. Thus, Fagin's theorem as well might be equivalently stated relating universal second-order logic, complements of generalised spectra (with respect to the same class as before, of course) and the complexity class co**NP**. This brings us to notice an interesting reduction of the famous **NP** vs. co**NP** problem to the two following problems in logic:

1. Do complements of generalised spectra (classes of finite structures in co**NP**) happen to be generalised spectra (classes of finite structures in **NP**) as well?
2. Are existential second-order formulae (defining **NP** classes of structures - generalised spectra) equivalently expressible by universal second-order formulae (defining co**NP** classes of structures - complements of generalised spectra)? In other words, does existential second-order logic have the same expressive power as universal second-order logic?

Fagin's theorem also (though more indirectly) relates to the following, even simplierly stated problem, which, too, remains unresolved:

Asser's problem: Is complement of every spectrum (in $\mathbb{N}^+$) a spectrum as well?

This was originally asked by Asser in [Ass55], although he considered spectra only of sentences over the empty signature. As was the case with the problem of generalised spectra's complements, Asser's problem relates to another open problem in complexity theory:

Theorem 6 (Jones-Selman theorem). *Spectra are precisely those subsets of* $\mathbb{N}^+$ *which are in the complexity class* **NE**. *Thus, complements of spectra (within* $\mathbb{N}^+$*) are precisely those subsets of* $\mathbb{N}^+$ *present within the complexity class co***NE**. *Asser's problem thus reduces to the* **NE** *vs. co***NE** *problem.*

Proof. If we already have constructed proof of Fagin's theorem, we may therefrom easily deduce a proof to this theorem. Fagin's theorem speaks merely of finite structures over **non-empty** signatures. Right from our definition of structure's encoding follows that encoding of a structure of size n over the empty signature yields a number whose binary expansion consists of $\lceil \mathtt{l}(n) \rceil$ many 1s followed by a 0, n's binary expansion (of length $\lceil \mathtt{l}(n) \rceil$) and another 0, which altogether makes a binary string of length logarithmically proportional to n, as opposed to merely polynomial bound yielded by using non-empty signatures. We may repeat the proof of Fagin's theorem for both directions of the equivalence with the empty signature as well, with the difference of **only** discussing structures over the empty signature instead:

1. To verify satisfaction of an existential second-order formula (say ψ, assume in strong prenex normal form), we again let the non-deterministic Turing machine expand the encoded structure of size n and then verify (in polynomial time) satisfaction of ψ's first-order matrix in structure as expanded, being thus no longer over the empty signature. As the length of the word on input now was not polynomial but logarithmic in n, the initial non-deterministic expansion (polynomial in n, not in input) takes instead time exponential in terms of input's length (that is, in terms of $\lceil \mathtt{l}(n) \rceil$). This in particular thus gives recognition of n's membership in the spectrum of ψ's first-order matrix in non-deterministically exponential time.

2. The construction of the formula axiomatising the respective non-deterministic Turing machine can be, too, left unchanged as it is constructed so as to run in $n^k - 1$ steps for some k, whereby is the construction dependent on n, not on the input word whose length only is now not polynomial but logarithmic in n. As the machine considered in this case works in time polynomial with respect to n, the input encoded structure being of length $2\lceil \mathtt{l}(n) \rceil + 2$ causes it to run in time exponentially, not polynomially proportional to input's length. ***Quod Erat Demonstrandum***

This proof, too, is due to Fagin, again to be seen in [Fag73] and [Fag74]. It was, however, proved independently by Jones and Selman in [JS74], whence the name.

Because of above outlined connections to the most infamous problems of complexity theory, Asser's problem does not give much hope for itself to be resolved easily. If indeed every spectrum's complement formed a spectrum, then **NE** = co**NE**. If the same went for generalised spectra, we would have **NP** = co**NP**. If the opposite answer were to hold for any of these, it would impose even stronger consequences: as is well-known, **NE** ≠ co**NE** and **NP** ≠ co**NP** imply **E** ≠ **NE** and **P** ≠ **NP**, respectively; further, if spectra are not closed under complementation, *id est* **NE** ≠ co**NE** and so as well **E** ≠ **NE** by said consequence, we further have **P** ≠ **NP** in one shot, as **E** ≠ **NE** is, too, known to imply **P** ≠ **NP**.

There at least used to be (see introduction in [SV95]) hopes to prove $\mathbf{P} \neq \mathbf{NP}$ using this precise argumentation chain, that is, by showing non-closedness of spectra or generalised spectra under their respective complementations. Although this has not hitherto yielded fruits exactly as desired, there is an interesting result obtained this way. In general case, the problem of closedness of generalised spectra (**NP** sets) under complementation may be reformulated as the problem of existential second-order formulae (assume, without loss of generality, in strong prenex normal form) having their negations (universal second-order formulae) expressible equivalently using existential second-order quantification only; in other words the problem of second-order existential formulae being closed under negation. Assume now a restriction imposed on said existential second-order formula: that it only be nulladic, monadic, dyadic or n-adic for some other $n \in \mathbb{N}$. We may then ask a question perhaps simplier to resolve: do thereby restricted formulae form a fragment of second-order logic closed under negation?

For simplicity of statements, assume from now on the term n-adicity applied only to those formulae in strong prenex normal form and n-adic second-order logics to include precisely formulae n-adic in this sense.

Theorem 7 (Fagin-Hájek theorem, [Fag75; Háj75]). *The property of a graph being non-connected is expressible in monadic second-order logic, even with only the binary reachability relation built-in, whereas it's negation, although expressible in existential second-order logic in general, is **not** expressible in **monadic** existential second-order logic over the same built-in language. Thus, monadic existential second-order logic is not closed under negation and monadic existential second-order definable sets (or, as they are for now obvious reasons called for short, monadic generalised spectra, or **monadic** **NP** **sets**) are not closed under complementation.*

This theorem (or proof thereof), being the noteworthiest result on the eponymous `monadic` **NP** `sets`, is main focus of this work and will be proved in the next chapter. Note that nulladic **NP** sets, on the other hand, are easily proved to be closed under complementation.

2. The Fagin-Hájek theorem

As we wrote by the end of the previous chapter, the goal pursued in this thesis is to prove Fagin-Hájek theorem. The first section is still going to be more general in nature, introducing the Ehrenfeucht-Fraïssé games, which form the apparatus needed for the proof. Second section shall pursue the original proof as found in [Fag75], heavily relying on the first.

2.1 The games of Ehrenfeucht and Fraïssé

The games of Ehrenfeucht and Fraïssé (with origin in [Fra53; Fra54; Ehr61] and intermediary development in some other papers) should perhaps first be introduced informally, so as to elude the threat of obscurantism. Two given first-order relational structures $\mathfrak{A}$ and $\mathfrak{B}$ of a same signature may be thought of as game's setting and we assume two players to play (referred to differently at different places, among the most used are labels `player I` and `player II`, or *Spoiler* and *Duplicator*) and they play r rounds.

A round beginsby Spoiler choosing an element either in $|\mathfrak{A}|$ or in $|\mathfrak{B}|$ (this chosen structure may differ in each round) and Duplicator responds by choosing an element in the other structure, assigning the two elements to each other, creating in k rounds a function f_k of cardinality k. Duplicator wins in r rounds if f_r is an isomorphism between $\mathfrak{A} \restriction \mathrm{dom}(f_r)$ and $\mathfrak{B} \restriction \mathrm{rng}(f_r)$ (that is, he *duplicates* the pattern induced by Spoiler's choices of elements). Spoiler then, living up to his name, tries to spoil this for the Duplicator, winning in r-th round when there is no way to extend f_{r-1} to some f_r such that it have the aforesaid property. This will be formalised in following definition; the treatment is a slightly modified version of the formalisation found in [Mlč22].

Definition 4. Let $\mathfrak{A}$ and $\mathfrak{B}$ be structures over a same relational signature. Assume $r \in \mathbb{N}^+$ and let $\mathscr{H}$ be a sequence of sets of finite injective mappings with domains subsets of $|\mathfrak{A}|$ and ranges subsets of $|\mathfrak{B}|$. We say that $\mathscr{H}$ is an *r-round ZZ system* (ZZ is shorthand for "zig, zag") *over* $\mathfrak{A}$ *and* $\mathfrak{B}$, if the following criteria are met:

1. if $f \in \mathscr{H}_n$ for some $n \in \mathbb{N}$, f is an isomorphism between structures $\mathfrak{A} \restriction \mathrm{dom}(f)$ and $\mathfrak{B} \restriction \mathrm{rng}(f)$.
2. for every $n \in \mathbb{N}^+$ and $a \in |\mathfrak{A}|$ outside of $\mathrm{dom}(f)$, if $f \in \mathscr{H}_n$, there is $g \in \mathscr{H}_{n-1}$ such that $f \subset g$ and $\mathrm{dom}(g) = \mathrm{dom}(f) \cup \{a\}$ (so called property of *zig*).
3. for every $n \in \mathbb{N}^+$ and $b \in |\mathfrak{B}|$ outside of $\mathrm{rng}(f)$, if $f \in \mathscr{H}_n$, there is $g \in \mathscr{H}_{n-1}$ such that $f \subset g$ and $\mathrm{rng}(g) = \mathrm{rng}(f) \cup \{b\}$ (so called property of *zag*).
4. if $f \in \mathscr{H}_n$ for some $n \in \mathbb{N}^+$, then $f \in \mathscr{H}_{n-1}$. That is, $\mathscr{H}_n \subseteq \mathscr{H}_{n-1}$.
5. $\emptyset \in \mathscr{H}_n$ for each $n \leq r$.

We write $\mathfrak{A} \leftrightharpoons_r \mathfrak{B}$ if there exists a ZZ system over $\mathfrak{A}$ and $\mathfrak{B}$ with r rounds. If $\mathscr{H}_n$ is non-empty for every $n \in \mathbb{N}$, we write $\mathfrak{A} \leftrightharpoons_\omega \mathfrak{B}$. If for all $n, k \in \mathbb{N}$ holds the

implication $\mathscr{H}_n \neq \emptyset \neq \mathscr{H}_k \Rightarrow \mathscr{H}_n = \mathscr{H}_k$, we call $\mathscr{H}$ a *simple ZZ system* and we denote it's existence by $\mathfrak{A} \leftrightharpoons_s \mathfrak{B}$. ◂

The symbol $\leftrightharpoons_r$ is therefore to formalise the case when the game in r rounds over given structures may always be won by Duplicator. Being an element to some ZZ system's member $\mathscr{H}_k$ means that the existing partial isomorphism may be extended k-times by k more elements which is due to properties of zig and zag; zig property is there to formalise the case when Spoiler chooses an element in $\mathfrak{A}$ so as to be answered by respective element in $\mathfrak{B}$, chosen by Duplicator; analogically zag property formalises Spoiler choosing an element in $\mathfrak{B}$ and being responded to by Duplicator chosen element in $\mathfrak{A}$. Note that $\leftrightharpoons_s$ and $\leftrightharpoons_r$ for each $r \in \mathbb{N}^+ \cup \{\omega\}$ are equivalences. It may also be noted that $\mathfrak{A} \leftrightharpoons_r \mathfrak{B}$ implies that for every substructure $\mathbb{A}_r$ of $\mathbb{A}$ such that $\|\mathbb{A}_r\| \leq r$ exists an isomorphic substructure $\mathbb{B}_r$ of $\mathbb{B}$ (but not *vice-versa*, as one may easily verify). The existence of a ZZ system over two structures, although much weaker than, say, existence of an isomorphism, allows us to prove strong facts about the two structure's relationships. Before naming them, we formulate and prove a simple lemma:

Theorem 8. *For every s and n in $\mathbb{N}$ and an evaluation e of n variables within $\bar{v}$ in a structure $\mathbb{M}$ of finite signature, there is a (non-unique) set $\Phi^{n:s}$ of formulae in $L(\mathbb{M})$ such that every formula of free variables within $\bar{v}$ and quantification rank s is equivalent under the evaluation e to some formula within $\Phi^{n:s}$.*

Proof. This is proven by induction on s. For $L(\mathbb{M})$ is finite, we only have finitely many atomic formulae using at most n different variables within $\bar{v}$. Of these atomic formulae, we may form only finitely many non-equivalent primitive conjunctions, wherefrom are constructible only finitely many formulae in conjunctive normal form non-equivalent under e; denote the set thereof as $\mathfrak{F}_0$. Every quantifier-free formula (that is, formula of quantification rank 0) of variables $\bar{v}$ is equivalent under e to some conjunctive normal formula in variables $\bar{v}$. That is, we may put $\Phi^{n:0} = \mathfrak{F}_0$. Every formula of quantification rank s is a boolean combination of formulae created from formulae of lesser quantification rank by quantification over a fixed variable within $\bar{v}$. As there are only finitely many formulae of lesser quantification rank non-equivalent under e, the formulae created therefrom by quantifying over a variable are as well at most finitely many non-equivalent under e. Every boolean combination of these may equivalently under e be rewritten as a conjunctive normal combination, of which, too, may be found at most finitely many non-equivalent under e; choose some such finite set as $\Phi^{n:s}$. The lemma is thereby proven.

Theorem 9. *Let $\mathbb{A} \leftrightharpoons_r \mathbb{B}$. Then, if φ is a first-order sentence of quantification rank r, then $\mathbb{A} \models \varphi \Leftrightarrow \mathbb{B} \models \varphi$; if furthermore $L(\mathbb{A}) = L(\mathbb{B})$ be finite, the converse statement does hold: if $\mathbb{A}$ and $\mathbb{B}$ satisfy the same sentences of quantification rank r, there is an r-round ZZ system over $\mathbb{A}$ and $\mathbb{B}$; in particular, $\mathbb{A} \leftrightharpoons_\omega \mathbb{B}$ is equivalent to $\mathbb{A}$ and $\mathbb{B}$ being elementarily equivalent. If $\mathbb{A}$ and $\mathbb{B}$ are countably infinite, $\mathbb{A} \leftrightharpoons_s \mathbb{B}$ is equivalent to $\mathbb{A}$ and $\mathbb{B}$ being isomorphic.*

Proof. We shall prove this somewhat more generally. Assume $\mathbb{A} \leftrightharpoons_r \mathbb{B}$ *via* $\mathscr{H}$ and assume φ a formula of n free variables and quantification rank below $r+1$, with

all bound variables only once quantified over (without loss of generality), assume e an evaluation of all variables within φ and $\mathbb{A}\models\varphi[e]$; we are to prove that for some evaluation e_1 of variables in φ that $\mathbb{B}\models\varphi[e_1]$. This goes by (finite) induction on φ's complexity; all formulae of quantification rank r are created by quantification over a formula of lesser quantification rank, or is a boolean combination of formulae of the same or lesser quantification rank:

1. Let φ be atomic. For $\mathbb{A}\leftrightharpoons_r\mathbb{B}$, $\mathrm{rng}(e)$ is domain to some $f\in\mathscr{H}_k$ for respective $k\leq r$, which is an isomorphism between $\mathbb{A}\restriction\mathrm{rng}(e)$ and $\mathbb{B}\restriction\mathrm{rng}(f\circ e)$ (in other words, there is a substructure of $\mathbb{B}$ isomorphic to $\mathbb{A}\restriction\mathrm{rng}(e)$, as consequence of $\mathbb{A}\leftrightharpoons_r\mathbb{B}$). We may therefore put $e_1=f\circ e$; if $\mathbb{B}$ instead satisfied $\neg\varphi$ *via* e_1, f would defy properties of isomorphisms.
2. Let $\varphi\triangleq\neg\psi$. Then again exists f such that $\mathbb{A}\restriction\mathrm{rng}(e)\cong\mathbb{B}\restriction\mathrm{rng}(f\circ e)$ *via* f. Thus $\mathbb{B}\models\neg\varphi[e_1]$ for $e_1=f\circ e$ as expected from f being an isomorphism.
3. Let $\varphi\triangleq\psi\vee\chi$. Without loss of generality, assume $\mathbb{A}\models\psi[e]$. Then, for some evaluation e_2, $\mathbb{B}\models\psi[e_2]$ by induction assumption and we may choose e_1 to be any extension of e_2 evaluating all variables within φ.
4. Let $\varphi\triangleq\psi\,\&\,\chi$. If we again choose f in $\mathscr{H}$'s respective member so that it be isomorphism between $\mathbb{A}\restriction\mathrm{rng}(e)$ and $\mathbb{B}\restriction\mathrm{rng}(f\circ e)$, $\mathbb{B}\models\varphi[f\circ e_1]$ follows by basic properties of isomorphisms as well and we again put $e_1=f\circ e$.
5. Accordingly for other binary connectives.
6. Let $\varphi\triangleq(\exists x)\psi$ for some variable x. Then there exists an evaluation $e_2\supseteq e$ such that $\mathbb{A}\models\psi[e_2]$. By induction assumption exists e_3 such that $\mathbb{B}\models\psi[e_3]$ and thus $\mathbb{B}\models(\exists x)\psi[e_3\setminus\{[x,e_3(x)]\}]\Leftrightarrow\mathbb{B}\models\varphi[e_3\setminus\{[x,e_3(x)]\}]$ and so we may choose e_1 equal to $e_3\setminus\{[x,e_3(x)]\}$.
7. Let $\varphi\triangleq(\forall x)\psi$ for some variable x. Then every evaluation e_2 such that $\mathrm{dom}(e_2)=\mathrm{dom}(e)\cup\{x\}$ satisfies ψ in $\mathbb{A}$. If there now were an evaluation e_3 of domain $\mathrm{dom}(e)\cup\{x\}$ such that $\mathbb{B}\models\neg\psi[e_3]$, $\mathbb{B}$ would also satisfy $(\exists x)\psi$ under $e_3\setminus\{[x,e(x)]\}$. By previous case, there is e_4 such that $\mathbb{A}\models(\exists x)\neg\psi[e_4]$, thus contradicting the assumption $\mathbb{A}\models(\forall x)\psi[e]$.

If φ is a sentence, it's satisfaction is independent of evaluation, so we proved that existence of an r-round ZZ system indeed implies satisfaction of the same sentences of quantification rank up to r. If there is an r-round ZZ system for every r, we obtain satisfaction of all sentences of every quantification rank, *id est* we obtain elementary equivalence of the two structures.

Now we prove the converse by constructing an r-round ZZ system $\mathscr{H}$ over $\mathbb{A}$ and $\mathbb{B}$, assuming them to be of finite signature and to satisfy the same sentences of quantification rank r. Put $\emptyset\in\mathscr{H}_k$ for $k\leq r$ and $\mathscr{H}_n=\emptyset$ for $n>r$ (if $r\neq\omega$). We are to ensure satisfaction of properties of zig and zag and the inclusion of $\mathscr{H}_n$ in $\mathscr{H}_{n-1}$ for all $n\in\mathbb{N}^+$.

Now we may choose for every evaluation e of variables $\bar{v}$ in structure $\mathbb{M}\in\{\mathbb{A},\mathbb{B}\}$ unique $\Theta^{n:s}_e\subset\bigcup_{s=0}^r\Phi^{n:s}$ (where $\Phi^{n:s}$ is as in the previous theorem) such that $\mathbb{M}\models$

$\models \theta[e]$ for every formula $\theta \in \Theta_e^{n:s}$ and $\mathbb{M} \models \neg\upsilon[e]$ for every $\upsilon \in \Phi^{n:s} \setminus \Theta_e^{n:s}$. Now we will recursively add to $\mathscr{H}$'s members elements so as to uphold property of zig: $\emptyset \in \mathscr{H}_n$ for all $n \leq r$, and $\emptyset$ satisfies all formulae within $\Theta_e^{0:r}$ for they are sentences. Assume now $f \in \mathscr{H}_n$ for some $n \in \mathbb{N}^+$ and $a \in |\mathbb{A}|$. For every evaluation e_0 with range equal to $\mathrm{dom}(f)$ *ex definitionem* holds $\mathbb{A} \models \theta[e_0 \cup \{\langle v_{n+1}, a\rangle\}]$ for every $\theta \in \Theta^{n+1:s-1}_{e_0 \cup \{\langle v_{n+1}, a\rangle\}}$ and $\mathbb{A} \models \neg\upsilon[e_0 \cup \{\langle v_{n+1}, a\rangle\}]$ for every $\upsilon \in \Phi^{n+1:s-1} \setminus \Theta^{n+1:s-1}_{e_0 \cup \{\langle v_{n+1}, a\rangle\}}$. We may therefore write that

$$\mathbb{A} \models (\exists v_{n+1}) \bigwedge_{\theta \in \Theta^{n+1:s-1}_{e_0 \cup \{\langle v_{n+1}, a\rangle\}}} \theta \;\&\; (\forall v_{n+1}) \bigwedge_{\substack{\upsilon \in \Phi^{n+1:s-1} \\ \upsilon \notin \Theta^{n+1:s-1}_{e_0 \cup \{\langle v_{n+1}, a\rangle\}}}} \neg\upsilon\left[e_0\right]$$

for $\Phi^{n:s}$ is finite. As f is an isomorphism between $\mathbb{A} \restriction \mathrm{rng}(e_0)$ and $\mathbb{B} \restriction \mathrm{rng}(f \circ e_0)$, we have as well

$$\mathbb{B} \models (\exists v_{n+1}) \bigwedge_{\theta \in \Theta^{n+1:s-1}_{e_0 \cup \{\langle v_{n+1}, a\rangle\}}} \theta \;\&\; (\forall v_{n+1}) \bigwedge_{\substack{\upsilon \in \Phi^{n+1:s-1} \\ \upsilon \notin \Theta^{n+1:s-1}_{e_0 \cup \{\langle v_{n+1}, a\rangle\}}}} \neg\upsilon\left[f \circ e_0\right].$$

We may therefore choose some $b \in |\mathbb{B}|$ such that

$$\mathbb{B} \models \bigwedge_{\theta \in \Theta^{n+1:s-1}_{e_0 \cup \{\langle v_{n+1}, a\rangle\}}} \theta\ \left[f \circ e_0 \cup \{\langle v_n, b\rangle\}\right].$$

Now we put $f \cup \{\langle a, b\rangle\}$, having upheld property of zig. The very same method goes for upholding property of zag. So for two structures of finite signatures satisfying the same sentences of quantification rank r indeed exists an r-round ZZ system. In particular, if $\mathbb{A}$ and $\mathbb{B}$ satisfy the same sentences of an arbitrary quantification rank (that is, are elementarily equivalent), we obtain the existence of an arbitrarily long ZZ system.

It remains to prove that, for countably infinite $\mathbb{A}$ and $\mathbb{B}$, existence of a simple $\|\mathbb{A}\|$-round ZZ system is equivalent to their isomorphness. First assume the structures $\mathbb{A}$ and $\mathbb{B}$ countably infinite with a ZZ system $\mathscr{H}$ over them. By definition, $\emptyset \in \mathscr{H}_0$. For generic ZZ systems, $\mathscr{H}_n \subseteq \mathscr{H}_{n-1}$, being a simple ZZ system means also to satisfy $\mathscr{H}_n = \mathscr{H}_{n-1}$, and thus even $\mathscr{H}_n = \mathscr{H}_{n-1}$ as a consequence, if $\mathscr{H}_n \neq \emptyset$. Let a and b be sequences enumerating $|\mathbb{A}|$ and $|\mathbb{B}|$, respectively. We now construct the isomorphism f recursively: let $f = \bigcup_{n \in \mathbb{N}} f_n$, where $f_0 = \emptyset$ and construct for natural $n < r - 1$ the function f_{n+1} as follows: f_n is contained in $\mathscr{H}_0$. As $\mathbb{A}$ and $\mathbb{B}$ are not of an empty universe, $f_n \in \mathscr{H}_1$ and by property of zig, there is $g \in \mathscr{H}_0$ extending (possibly trivially) f_n so that $\mathrm{dom}(g) = \mathrm{dom}(f_n) \cup \{a_n\}$. By simplicity of $\mathscr{H}$, $g \in \mathscr{H}_1$. By property of zag, there is $h \in \mathscr{H}_0$ extending (again, it is possible that the inclusion be not strict) g so that $\mathrm{rng}(h) = \mathrm{rng}(g) \cup \{b\}$; put now $f_{n+1} = h$.

Now assume existence of an isomorphism f between at most countably infinite structures $\mathbb{A}$ and $\mathbb{B}$. Then $\mathscr{H}$ with

$$\mathscr{H}_n = \{f_0 \subset f; f_0 \text{ is finite}\}$$

for each $n \in \mathbb{N}$ truly is a simple ZZ system over $\mathbb{A}$ and $\mathbb{B}$. ***Q.E.D.***

Theorem 10. *There is a simple ZZ system over every two countable models of the theory* DNO *of dense linear ordering without endpoints. The same goes for the theory* RG *of random graphs.* DNO *and* RG *are therefore countably categorical.*

Proof. This is a simple corollary of the previous theorem. For a more detailed discussion of these specific cases, one may consult [BŠ86] and [Mar06]. ***Q.E.D.***

The proof of Fagin-Hájek theorem relies upon a certain kind of generalised Ehrefeucht-Fraïssé game. Let us again describe it informally. There are two structures $\mathbb{A}$ and $\mathbb{B}$ as a setting, the same way it is with normal Ehrenfeucht-Fraïssé game, and furthermore a finite set D of predicate symbols outside of $L(\mathbb{A}) = L(\mathbb{B})$. The first player (again labelable as *Spoiler*) chooses a structure $\mathfrak{A} \upharpoonright \mathbb{A}$ in $L(\mathbb{A}) \cup D$. The second player (*Duplicator*), chooses then a structure $\mathfrak{B} \upharpoonright \mathbb{B}$ in $L(\mathbb{A}) \cup D$. The two players now play the original Ehrenfeucht-Fraïssé game over $\mathfrak{A}$ and $\mathfrak{B}$, whose winner is as well declared the winner of the now described generalised game. Formally:

Definition 5. Let $\mathbb{A}$ and $\mathbb{B}$ of the same signature. We say that $\mathbb{B}$ *wins against* $\mathbb{A}$ *over* D *in* r *rounds* (symbolically, $\mathbb{A} \Rightarrow_r^D \mathbb{B}$)if and solely if for every expansion $\mathfrak{A} \upharpoonright \mathbb{A}$ in $L(\mathbb{A}) \cup D$ exists expansion $\mathfrak{B} \upharpoonright \mathbb{B}$ in $L(\mathbb{A}) \cup D$ such that $\mathfrak{A} \leftrightharpoons_r \mathfrak{B}$. ◂

The following theorem will be used in the following section as the main instrument in proving Fagin-Hájek theorem, albeit only in the specific case when D be monadic; in this case, the first step in the generalised game (expanding structures) is sometimes referred to as *colouring of the structures* (for example, in [SV95]).

Theorem 11 (Theorem 1 from [Fag75]). *Let $\mathscr{A}$ be a class of finite relational structures of finite signatures. Then, $\mathscr{A}$ is an n-adic generalised spectrum if and solely if for some $r \in \mathbb{N}^+$, some n-adic language S and for all finite structures $\mathbb{A}$ and $\mathbb{B}$ of the same finite signature holds: $\left(\mathbb{A} \in \mathscr{A} \text{ et } \mathbb{A} \Rightarrow_r^S \mathbb{B}\right) \Rightarrow \mathbb{B} \in \mathscr{A}$. In particular, if it be possible to find for every n-adic language S and every $r \in \mathbb{N}^+$ some $\mathbb{A} \in \mathscr{A}$ and some $\mathbb{B}$ such that $\mathbb{A} \in \mathscr{A}$, $\mathbb{A} \Rightarrow_r^S \mathbb{B}$ and $\mathbb{B} \notin \mathscr{A}$, then $\mathscr{A}$ is not an n-adic generalised spectrum.*

Proof. First assume $\mathscr{A}$ to be an n-adic generalised spectrum and thus to be defined by an n-adic existential second-order sentence φ in strong prenex normal form. Then for every $\mathbb{A} \in \mathscr{A}$ holds $\mathbb{A} \models^{\text{II}} \varphi$. Let r be the quantification rank of φ's first-order matrix. Further assume random $\mathbb{B}$ a finite structure of finite signature winning against $\mathbb{A}$ over the set of φ's second-order variables in r rounds; that is, such $\mathbb{B}$ that for every $\mathfrak{A} \upharpoonright \mathbb{A}$ there is a $\mathfrak{B} \upharpoonright \mathbb{B}$ such that $\mathfrak{A} \leftrightharpoons_r \mathfrak{B}$. By theorem 9 and our choice of r, $\mathfrak{B}$ satisfies φ's first-order matrix. That is, $\mathbb{B} \models^{\text{II}} \varphi$ and thus $\mathbb{B} \in \mathscr{A}$.

Now we are to prove the converse. Fix some n-adic language S and $r \in \mathbb{N}^+$ so that $\left(\mathbb{A} \in \mathscr{A} \text{ et } \mathbb{A} \Rightarrow_r^S \mathbb{B}\right) \Rightarrow \mathbb{B} \in \mathscr{A}$ hold for every $\mathbb{A}$ and $\mathbb{B}$; from this we want to prove that $\mathscr{A}$ is an n-adic generalised spectrum. Instead, we show the contraposition, that if $\mathscr{A}$ is not a generalised spectrum, then $\left(\mathbb{A} \in \mathscr{A} \text{ et } \mathbb{A} \Rightarrow_r^S \mathbb{B}\right)$ et $\mathbb{B} \notin \mathscr{A}$ for some $\mathbb{A}$ and $\mathbb{B}$. Indeed, as $\mathscr{A}$ is non-empty ($\varnothing$ would be a generalised spectrum), $\mathbb{A} \Rightarrow_r^S \mathbb{B}$ forces, by theorem 10, $\mathbb{B}$ to satisfy n-adic existential second-order sentences with second-order variables within S and first-order matrices of quantification rank up to r which $\mathbb{A}$ itself satisfies. For there are only finitely many such existential second-order sentences mutually non-equivalent (this may be easily derived from theorem 9), we may take their conjunction, which is itself equivalent to an n-adic existential second-order sentence ψ (albeit with more second-order variables). If $\mathbb{B}$ then were in $\mathscr{A}$, ψ would define $\mathscr{A}$, rendering it a generalised spectrum, which we assumed untrue. ***Quod Erat Demonstrandum***

2.2 Fagin's original proof

All preliminary notions are as of now introduced and we are ready to prove Fagin-Hájek theorem. That is, we prove that encodings of finite connected graphs do not form a monadic **NP** set, although encodings of non-connected finite graphs are easily verified to form a monadic **NP** set. To do this, we will utilise theorem 11: for every monadic second-order existential sentence φ in strong prenex normal form with second-order variables within D and for every $r \in \mathbb{N}^+$, we are to find a connected graph $\mathbb{A} \models^{\text{II}} \varphi$ and non-connected graph $\mathbb{B}$ such that $\mathbb{A} \rightrightarrows_r \mathbb{B}$. If $\mathbb{A} \rightrightarrows_r^D \mathbb{B}$, then $\mathbb{B} \models^{\text{II}} \varphi$ as well and thus φ does not define connectedness of graphs, for $\mathbb{B}$ was assumed non-connected. If such $\mathbb{A}$ and $\mathbb{B}$ be found for every said φ and r, then the class of connected graphs indeed is not defined by any monadic existential second-order formula, *id est*, it is not a **monadic** generalised spectrum.

A natural choice for $\mathbb{A}$ is a cycle and for $\mathbb{B}$ a cardinal sum of two cycles (that is, a graph consisting of two disjoint mutually non-connected subgraphs which are both cycles). Clearly, $\mathbb{A}$ is then connected and $\mathbb{B}$ non-connected. As it turns out, such considerations are sufficient.

Definition 6. Let $\mathfrak{A}$ expand a graph $\mathbb{A}$ to $L(\mathbb{A}) \cup D$ where D be a finite monadic language. The *weak marking* of a point $a \in |\mathfrak{A}|$ is the set denoted $\mathfrak{M}(a)$ of all members P of D such that $\mathfrak{A} \models P(x)[\{[x, a]\}]$.

Let $\bar{a}$ denote a finite sequence of elements from $|\mathfrak{A}|$ such that for natural n satisfying $0 \leq n < l(\bar{a})$ holds $R(a_n, a_{n+1})$ (that is, they form a path in $\mathbb{A}$, we shall call it a *connected sequence*). We define *weak marking* of *a connected sequence* $\bar{a}$ to be the sequence denoted $\mathfrak{M}(\bar{a})$ of length $l(\bar{a})$ such that for every member n satisfying $0 \leq n < l(\bar{a})$ hold $\mathfrak{M}(\bar{a})_n = \mathfrak{M}(a_n)$. We say that weak marking $\mathfrak{M}(\bar{a})$ of a connected sequence $\bar{a}$ *occurs n times in* $\mathfrak{A}$, if there are n different connected sequences $\bar{b}$ of elements within $|\mathbb{A}|$ such that $\mathfrak{M}(\bar{b}) = \mathfrak{M}(\bar{a})$. In particular $\mathfrak{M}(\bar{a})$ occurs once in $\mathfrak{A}$ if and only if the only sequence of the same weak marking as that of $\bar{a}$ is $\bar{a}$.

Let there be ZZ system $\mathscr{H}$ between $\mathfrak{A}$ and a structure $\mathfrak{B}$. Let f be a finite sequence of $\mathscr{H}$'s members' elements such that for all natural k such that $0 \leq k < l(f)$ hold $f_k \subset f_{k+1}$, $f_k \in \mathscr{H}_{l(f)-1-k}$ and $|f_k \setminus f_{k-1}| = 1$ if $k \neq 0$. f may be thought to formalise a particular instance of Ehrenfeucht-Fraïssé game of $l(f)$ rounds, as an element of f extends it's predecessor by one ordered double. The *strong marking* of an element $a \in |\mathfrak{A}| \cup |\mathfrak{B}|$ with respect to f is the set $\mathfrak{S}_f(a) = \mathfrak{M}(a) \cup \{i\}$ where i is the least integer such that $\mathrm{dom}(f_{i-1})$ or $\mathrm{rng}(f_{i-1})$ contain a. In case such i does not exist, define $\mathfrak{S}_f(a) = \mathfrak{M}(a)$. $\mathfrak{S}_f(a)$ is therefore to formalise the notion of a being chosen within either $\mathfrak{A}$ or $\mathfrak{B}$ in the course of Ehrenfeucht-Fraïssé game formalised by f.

Analogically to the notion of weak markings of connected sequences, define the *strong marking* $\mathfrak{S}_f(\bar{a})$ *of a connected sequence* $\bar{a}$ *with respect to* f by $\mathfrak{S}_f(\bar{a})_k = \mathfrak{S}_f(a_k)$ for all natural k such that $0 \leq k < l(\bar{a})$. We call strong marking of a connected sequence with respect to f *clean* if it be equal to the same sequence's weak marking, thereby formalising the notion of none element of a being chosen by either player in the particular instance of Ehrenfeucht-Fraïssé game being for-

malised by f. Finally, define the *neighbourhood of a point* $a \in |\mathfrak{A}|$ *with radius* r, symbolically written $\mathfrak{O}_r(a)$, to be the universe of the substructure of $\mathfrak{A}$ containing every point which is a member of some connected sequence of length at most $r+1$ and whose first member is a. If there be a connected sequence (then of length $2r+1$) enumerating all the members of $\mathfrak{O}_r(a)$, injectively, we shall also refer to it as to the neighbourhood of a with radius r and denote it $\mathfrak{O}_r(a)$, too.◀

Note: the said connected sequence denoted $\mathfrak{O}_r(a)$ is not unique for most graphs. Even so, for the sake of simplicity, we shall use the symbol to denote the one of such sequences to best satisfy our purpose. In particular, the notation $A \subset \subset \mathfrak{O}_r(a)$ is to be understood as: "A is a subsequence to some sequence injectively denumerating the neighbourhood of a with radius r".

Theorem 12 (Lemma 2 from [Fag75]). *Let D be a finite monadic language, let $\mathbb{A}$ and $\mathscr{C}$ be cycles and let $\mathbb{B}$ be the cardinal sum of cycles $\mathbb{A}$ and $\mathscr{C}$. Let $\mathfrak{A} \restriction \mathbb{A}$, $\mathfrak{C} \restriction \mathscr{C}$ and $\mathfrak{B} \restriction \mathbb{B}$ so that $L(\mathfrak{A}) = L(\mathfrak{B}) = L(\mathfrak{C}) = D \cup \{R\}$, $\mathfrak{B} \upharpoonright |\mathfrak{A}| = \mathfrak{A}$ and $\mathfrak{B} \upharpoonright |\mathfrak{C}| = \mathfrak{C}$. If $\|\mathbb{A}\| \geq 2^{r+2} - 1 \leq \|\mathfrak{C}\|$ and if weak marking of every connected sequence of length at most $2^{r+1} - 1$ within $\mathfrak{C}$ occurs at least $r \cdot (2^{r+1} - 1)$ many times in $\mathfrak{A}$, then $\mathfrak{A} \leftrightharpoons_r \mathfrak{B}$.*

Proof. Let F be a monomorphism of domain $|\mathfrak{A}|$ and range subset of $|\mathfrak{B}|$. As $\mathfrak{A}$ is a cycle, it's image $F(\mathfrak{A})$ under F is a cycle isomorphic to it. For $\mathbb{B}$ is created from $\mathbb{A}$ by a cardinal sum, such F always does exist. In order to prove the theorem, we are to construct under stated assumptions a ZZ system $\mathscr{H}$ between $\mathfrak{A}$ and $\mathfrak{B}$ of length r. Set $\mathscr{H}_r = \{\emptyset\}$, put $\emptyset$ in every $\mathscr{H}$'s member as well. We are to recursively extend for each s satisfying $0 < s \leq r$ the element $f \in \mathscr{H}_s$ to $g \in \mathscr{H}_{s-1}$ so that it satisfy the property of zig and the property of zag.

First we uphold the property of zig. Assume for all natural $p \geq s$:

1. $\mathfrak{A} \upharpoonright \mathrm{dom}(f) \cong \mathfrak{B} \upharpoonright \mathrm{rng}(f)$ *via* f .
2. $\mathfrak{S}_f \circ \mathfrak{O}_{2^{p+1}-1}(x) = \mathfrak{S}_f \circ \mathfrak{O}_{2^{p+1}-1} \circ f(x)$ for each $x \in \mathrm{dom}(f)$. Informally, short enough neighborhoods of $x \in \mathrm{dom}(f)$ (that is, of length $2^{p+2} - 1$; in other words, of radius $2^{p+1} - 1$) are isomorphic *via* f.
3. $\mathfrak{M} \circ \mathfrak{O}_{2^{p+1}-1} \circ f(x)$ occurs at least $r \cdot (2^{r+1} - 1)$ times for every $x \in \mathrm{dom}(f)$ such that $f(x) \neq F(x)$. If $f(x) \in |\mathfrak{B}| \setminus |F(\mathfrak{A})|$, this is already guaranteed by theorem's assumptions.

Let $a \in |\mathfrak{A}| \setminus \mathrm{dom}(f)$. All of the stated conditions are trivially satisfied for $f = \emptyset$ and $p = r$. We want to construct injective g to be put in $\mathscr{H}_{s-1}$, such that $\mathrm{dom}(g) = \mathrm{dom}(f) \cup \{a\}$, $f \subset g$ and the three conditions above hold for g in place of f for $p = s - 1$. When extending f to g, we have the following three cases of a to consider:

1. Assume a be chosen such that $\mathfrak{S}_f \circ \mathfrak{O}_{2^s-1}(a)$ is not clean. Informally, there is at least one point in the neighbourhood already chosen in some of the preceding $r - s$ rounds. Then there is a connected sequence $c \subset \mathfrak{O}_{2^s-1}(a)$ whose first member is a and whose final member is some $a_x \in \mathrm{dom}(f)$. In either case, there is a connected sequence $d \subset \mathfrak{O}_{2^s-1} \circ f(a_x)$ such that it's final member is $f(a_x)$ and, by the third condition, $\mathfrak{A} \upharpoonright \mathrm{rng}(c) \cong \mathfrak{B} \upharpoonright \mathrm{rng}(d)$.

Extend then f to g so that $g(a) = d_0$. The four conditions may be then easily verified to hold for g in place of f and $p = s-1$.

2. Assume $\mathfrak{S}_f \circ \mathfrak{O}_{2^s-1}(a) = \mathfrak{S}_f \circ \mathfrak{O}_{2^s-1} \circ F(a)$ to be clean. Informally, there is no point in $\mathfrak{O}_{2^s-1}(a)$ chosen in previous rounds. We may extend f to g so that $g(a) = F(a)$. All of the above stated conditions hold for $f = g$ and $p = s-1$, as may again be routinely verified.

3. Assume $\mathfrak{S}_f \circ \mathfrak{O}_{2^s-1}(a)$ clean and $\mathfrak{S}_f \circ \mathfrak{O}_{2^s-1} \circ F(a)$ not clean; informally said, Duplicator cannot choose $g(a)$ equal to $F(a)$ for some point in $F(a)$'s surroundings was already chosen in some of the preceding rounds. Formally, there is a connected sequence $c \subset \mathfrak{O}_{2^s-1} \circ F(a)$ whose first member is $F(a)$ and whose final member is some $b_x \in \mathrm{rng}(f)$. As $\mathfrak{S}_f \circ \mathfrak{O}_{2^s-1}(a)$ is clean, $f^{-1}(b_x) \neq F^{-1}(b_x)$ and thus by condition 3, $\mathfrak{M} \circ \mathfrak{O}_{2^{s+1}-1}(b_x)$, equal to $\mathfrak{M} \circ \mathfrak{O}_{2^{s+1}-1} \circ f^{-1}(b_x)$ by condition 2, occurs at least $r \cdot (2^{r+1}-1)$ times in $\mathfrak{A}$ and $F(\mathfrak{A})$.

   Now define

$$M = \bigcup_{x \in \mathrm{dom}(f)} \mathfrak{O}_{2^s-1} \circ f(x)$$

   which is, as $|f| \leq r-s$, of cardinality at most m for

$$\begin{aligned} m = (r-s) \cdot (2^{s+1}-1) = r \cdot (2^{s+1}-1) - s \cdot (2^{s+1}-1) \leq \\ \leq r \cdot (2^{s+1}-1) - (2^{s+1}-1) = (r-1)(2^{s+1}-1) \leq (r-1)(2^{r+1}-1) < \\ < r \cdot (2^{r+1}-1). \end{aligned}$$

   For short, $m < r \cdot (2^{r+1}-1)$; that is, less than $2^{r+1}-1$ sequences of weak marking equal to $\mathfrak{M} \circ \mathfrak{O}_{2^s-1}(a)$ have been used up. We may therefore find $d \in \in |\mathfrak{A}|$ outside of $\mathrm{rng}(f)$ such that $\mathfrak{M} \circ \mathfrak{O}_{2^s-1}(d) = \mathfrak{M} \circ \mathfrak{O}_{2^s-1}(a) = \mathfrak{S}_f \circ \mathfrak{O}_{2^s-1}(a)$ and the choice such that $g(a) = d$ again satisfies all four of the stated conditions for $p = s-1$.

Now we again assume the same three conditions as above to holds for all natural $p \geq s$, in order to uphold the property of zag. Let $b \in |\mathfrak{B} \setminus \mathrm{rng}(f)|$. We already know the three conditions to trivially hold for $\emptyset$ and $p = r$. We again construct extension g of f to be put in $\mathscr{H}_{s-1}$ so as to satisfy conditions 1 to 3. There are now even more cases to be considered, first for $b \in |F(\mathfrak{A})|$:

1. $\mathfrak{S}_f \circ \mathfrak{O}_{2^s-1}(b)$ is not clean. This case is analogical to case 1 dealt with when having upheld the property of zig. There is a connected sequence $c \subset \mathfrak{O}_{2^s-1}(b)$ whose first member is b and whose final member is some $b_x \in \mathrm{dom}(f)$. In either case, there is a connected sequence $d \subset \mathfrak{O}_{2^s-1} \circ$ $\circ f^{-1}(b_x)$ such that it's final member is $f^{-1}(b_x)$ and, by the third condition, $\mathfrak{A} \restriction \mathrm{rng}(c) \cong \mathfrak{B} \restriction \mathrm{rng}(d)$. Extend then f to g so that $b = g(d_0)$.

2. $\mathfrak{S}_f \circ \mathfrak{O}_{2^s-1} \circ F^{-1}(b) = \mathfrak{S}_f \circ \mathfrak{O}_{2^s-1}(b)$ is clean. This is analogical to case 2 of upholding the property of zig. Set $b = g \circ F^{-1}(b)$.

3. Analogically now to case 3 of upholding the property of zig, $\mathfrak{S}_f \circ \mathfrak{O}_{2^s-1}(b)$ is clean and $\mathfrak{S}_f \circ \mathfrak{O}_{2^s-1} \circ F^{-1}(b)$ is not, so there is a connected sequence $c \subset$ $\subset \mathfrak{O}_{2^s-1} \circ F^{-1}(b)$ whose first member is $F^{-1}(b)$ and whose final member is some $a_x \in \mathrm{dom}(f)$. As $\mathfrak{S}_f \circ \mathfrak{O}_{2^s-1}(b)$ is clean, $f(a_x) \neq F(a_x)$ and thus

by condition 3, $\mathfrak{M}\circ\mathfrak{O}_{2^{s+1}-1}(a_x)$, equal to $\mathfrak{M}\circ\mathfrak{O}_{2^{s+1}-1}\circ f(a_x)$ by condition 2, occurs at least $r\cdot(2^{r+1}-1)$ times in $F(\mathfrak{A})$ and $\mathfrak{A}$.

If we define, in manner already seen

$$M=\bigcup_{x\in\mathrm{rng}(f)\cap|F(\mathfrak{A})|}\mathfrak{O}_{2^s-1}\circ f^{-1}(x),$$

then for $m=|M|$ again holds $m<r\cdot(2^{r+1}-1)$; less than $2^{r+1}-1$ sequences of weak marking equal to $\mathfrak{M}\circ\mathfrak{O}_{2^s-1}\circ F^{-1}(b)$ have been used up. We may therefore find $d\in|\mathfrak{A}|$ outside of $\mathrm{dom}(f)$ such that $\mathfrak{M}\circ\mathfrak{O}_{2^s-1}(d)=\mathfrak{M}\circ\mathfrak{O}_{2^s-1}(b)=$ $=\mathfrak{S}_f\circ\mathfrak{O}_{2^s-1}(b)$ and we may choose g so that $b=g(d)$.

Now for $b\notin F(\mathfrak{A})$ (that is, b is in the subgraph of $\mathfrak{B}$ isomorphic to $\mathfrak{C}$):

1. $\mathfrak{S}_f\circ\mathfrak{O}_{2^s-1}(b)$ is not clean. This case is analogical to both of the previous cases labeled as 1. Choose a connected sequence $c\subset\mathfrak{O}_{2^s-1}(b)$ whose first member is b and whose final member is some $b_x\in\mathrm{dom}(f)$. Choose then a connected sequence $d\subset\mathfrak{O}_{2^s-1}\circ f^{-1}(b_x)$ such that it's final member be $f^{-1}(b_x)$ and, by the third condition, $\mathfrak{A}\restriction\mathrm{rng}(c)\cong\mathfrak{B}\restriction\mathrm{rng}(d)$. Put then $b=g(d_0)$.

2. $\mathfrak{S}_f\circ\mathfrak{O}_{2^s-1}(b)$ is clean. By theorem's assumption, $\mathfrak{M}\circ\mathfrak{S}_f\circ\mathfrak{O}_{2^s-1}(b)$ occurs in $\mathfrak{A}$ and $F(\mathfrak{A})$ at least $r\cdot(2^{r+1}-1)$ many times, but analogically to the afore investigated cases labeled as 3, only m many such sequences have been used up if $m=|M|$ where
$$M=\bigcup_{x\in\mathrm{rng}(f)\setminus|F(\mathfrak{A})|}\mathfrak{O}_{2^s-1}\circ f^{-1}(x).$$
M's cardinality is lesser than $r\cdot(2^{r+1}-1)$ and we may therefore choose $d\in|\mathfrak{A}|$, outside of $\mathrm{dom}(f)$ so that $\mathfrak{M}\circ\mathfrak{O}_{2^s-1}(d)=\mathfrak{M}\circ\mathfrak{O}_{2^s-1}(b)=\mathfrak{S}_f\circ\mathfrak{O}_{2^s-1}(b)$ and put $b=g(d)$.

Starting at $p=r$ and continuing recursively with one by one lesser p down to $p=0$, we have now endowed $\mathscr{H}$'s member with such elements that it truly is a ZZ system and the proof is now complete. ***Quod Erat Demonstrandum***

Theorem 13. *Let D be a finite monadic language and $\mathbb{A}$ a cycle of length at least*

$$w=r\cdot(2^{r+1}-1)\cdot 2^{|D|\cdot(2^{|D|\cdot(2^{r+1}-1)}+2^{r+1}-1)}.$$

Then, there is for every $\mathfrak{A}$ expanding $\mathbb{A}$ to signature $D\cup\{R\}$ a connected sequence $s(\mathfrak{A})$ of $\mathfrak{A}$'s elements such that it is of length at least $2^{r+1}-1$ and if s of length at most $2^{r+1}-1$ is a connected subsequence of the concatenation $s(\mathfrak{A})\_s(\mathfrak{A})$, then $\mathfrak{M}(s(\mathfrak{A}))$ occurs at least $r\cdot(2^{r+1}-1)$ many times in $\mathfrak{A}$.

Proof. By elementary combinatorics, there are at most $2^{|D|}$ different subsets of $S\subseteq D$ such that S be the weak marking to some element in the given graph. For each $d\in\mathbb{N}$, there are $(2^{|D|})^d=2^{|D|\cdot d}$ many different sequences of length d of members $S\subseteq D$, therefore there may for given graph be at most $2^{|D|\cdot d}$ many such sequences which are at the same time weak markings to some connected sequences of the given graph's elements.

In the particular case of the given graph being $\mathfrak{A}$, which is of length w, and d set as $2^{r+1}-1$, we then get that there must be a connected sequence t within $\mathfrak{A}$

of length $2^{r+1}-1$, whose weak marking occurs in $\mathfrak{A}$ at least

$$v = w \div 2^{|D|\cdot(2^{r+1}-1)} = r\cdot(2^{r+1}-1)\cdot 2^{|D|\cdot(2^{|D|\cdot(2^{r+1}-1)})}$$

many times (the divisor is obtained from $2^{|D|\cdot d}$ by substituting $2^{r+1}-1$ for d). We will now construct a sequence u of length $(2^{r+1}-1)+(2^{|D|\cdot(2^{r+1}-1)}) \geq 2^{r+1}-1$. Let $u_n = t_n$ for $n \in \mathbb{N}$ such that $0 \leq n < 2^{r+1}-1 = l(t)-1$. Define then inductively the sequences $q(k)$ and $q'(k)$ for k such that $l(u) > k > 2^{r+1}-2$:

1. $q(2^{r+1}-2) = t$, whose weak marking we know to occur at least v many times. v is equal to $r\cdot(2^{r+1}-1)\cdot 2^{|D|\cdot(2^{|D|\cdot(2^{r+1}-1)})-k}$ for $k=0$ and is clearly greater than $r\cdot(2^{r+1}-1)$.

2. $q'(k)$ is created from $q(k)$ by deleting the first element. For example, if $q_n(k)$ were equal to n for all $n \in \mathbb{N}$, $q'_n(k)$ would equal $n+1$ for all $n \in \mathbb{N}$. Weak marking of $q'(k)$ then occurs at least $r\cdot(2^{r+1}-1)$ many times as so does $q(k)$. More specifically, it occurs at least $r\cdot(2^{r+1}-1)\cdot 2^{|D|\cdot(2^{|D|\cdot(2^{r+1}-1)})-k}$ many times as does weak marking of $q(k)$.

3. $q(k+1) = q'(k)\_\{[2^{r+1}-2, e]\}$, where e is chosen so that $\mathfrak{M}(q(k+1))$ occur at least $r\cdot(2^{r+1}-1)$ many times in $\mathfrak{A}$. Such e can be found because weak marking of $q'(k)$ occurs at least $r\cdot(2^{r+1}-1)\cdot 2^{|D|\cdot(2^{|D|\cdot(2^{r+1}-1)})-k}$ many times in $\mathfrak{A}$ and there are only $2^{|D|}$ many potential weak markings of e occurrable; e can thus be chosen even so that $\mathfrak{M}(q(k+1))$ occur

   $$r\cdot(2^{r+1}-1)\cdot 2^{|D|\cdot(2^{|D|\cdot(2^{r+1}-1)})-k} \div 2^{|D|} = r\cdot(2^{r+1}-1)\cdot 2^{|D|\cdot(2^{|D|\cdot(2^{r+1}-1)})-(k+1)}$$

   many times.

Clearly, for $k = (2^{|D|\cdot(2^{r+1}-1)})$ we then get the least number of occurrences of $\mathfrak{M}(q(k))$, equal to $r\cdot(2^{r+1}-r)$. For indices $n \in \mathbb{N}$ such that $l(u) > k > 2^{r+1}-2$ then define u_n equal to the final member of the sequence $q(n)$. u then has the property that it's every connected subsequence of length at most $2^{r+1}-1$ then occurs at least $r\cdot(2^{r+1}-1)$ many times in $\mathfrak{A}$.

Denote now by $v(k)$ for $0 \leq k < 2^{|D|\cdot(2^{r+1}-1)}$ connected subsequences of u of length $2^{r+1}-1$ such that $v_0(k) = u_k$ and $v_{2^{r+1}-2}(k) = u_{k+2^{r+1}-2}$. For some i and j (without loss of generality, $i < j$), there must be then $\mathfrak{M}(v(i)) = \mathfrak{M}(v(j))$, as in $\mathfrak{A}$, there are at most $2^{|D|\cdot(2^{r+1}-1)}$ different weak markings of sequences of length at most $2^{r+1}-1$.

1. Assume $i+(2^{r+1}-1) < j$. Denote $s(\mathfrak{A}) \subset u$ the connected subsequence with the first element being u_i and the last element being u_{j-1}. Then $s(\mathfrak{A})$ indeed upholds the property desired by theorem's statement, that every connected subsequence of $c \subset s(\mathfrak{A})\_s(\mathfrak{A})$ such that $l(c) \leq 2^{r+1}-1$ occurs in $\mathfrak{A}$ at least $r\cdot(2^{r+1}-1)$ many times.

2. Assume $i+(2^{r+1}-1) \geq j$. Denote $z \subset u$ the connected subsequence with the first element being u_i and the last element being u_{j-1}. Let $s(\mathfrak{A})$ be created by that many concatenation of z with itself so that it be of length at least $2^{r+1}-1$. Again, theorem's statement holds for $s(\mathfrak{A})$.

Weak marking of every connected subsequence c of $s(\mathfrak{A})\_s(\mathfrak{A})$ such that $l(s(\mathfrak{A})) \leq 2^{r+1}-1$ then truly does occur in either case at least $r \cdot (2^{r+1}-1)$ many times in $\mathfrak{A}$ and the proof is thus complete. ***Quod Erat Demonstrandum***

Theorem 14 (Theorem 3 from [Fag75]). *Let D be a finite monadic language, $r \in \mathbb{N}^+$ and $\mathbb{A}$ a cycle of length at least*

$$w = r \cdot (2^{r+1}-1) \cdot 2^{|D| \cdot (2^{|D| \cdot (2^{r+1}-1)} + 2^{r+1} - 1)}.$$

Then, if $\mathbb{B}$ be created from structures $\mathbb{A}$ and $\mathscr{C}$ by cardinal sum, there is $a \in \mathbb{N}^+$ such that if $\mathscr{C}$ is a cycle of size divisible by a, then $\mathbb{A} \rightrightarrows_r^D \mathbb{B}$.

Proof. Let M be the set of all lengths of all sequences $s(\mathfrak{A})$ (as established in theorem 13) pertaining to some structure $\mathfrak{A}$ expanding $\mathbb{A}$ to signature $D \cup \{R\}$. Set a to be the least common multiple of all elements within M.

Let c be a sequence of length a such that $|\mathrm{rng}(c)| = a$. Consider now $\mathscr{C}$ of length ka and a connected sequence d denumerating $|\mathscr{C}|$ injectively, in such a manner that the successor of an element in d be also one of it's adjacent vertices. For each expansion $\mathfrak{A} \restriction \mathbb{A}$, we will find an expansion $\mathfrak{C} \restriction \mathscr{C}$ into $D \cup \{R\}$ such that there be a r-round ZZ system between $\mathfrak{A}$ and the cardinal sum of $\mathfrak{A}$ and $\mathfrak{C}$, thus proving the theorem. Choose a function f periodic in a, assigning vertices d_0 to d_{ka-1} subsets of D. Expand then $\mathscr{C}$ to $\mathfrak{C}$ so that for every $p \in |\mathscr{C}|$ be p's weak marking equal to $f(p)$. By theorem 12, $\mathfrak{A} \leftrightharpoons_r \mathfrak{B}$ and thus $\mathbb{A} \rightrightarrows_r^D \mathbb{B}$. ***Q.E.D.***

Theorem 15. *Non-connectedness of a graph is expressible in monadic existential second-order logic. Connectedness of a graph is expressible in dyadic existential second-order logic.*

Proof. Assume built-in only the binary reachability relation R. Then, if we have P a unary predicate, we may express non-connectedness as:

$$(\exists P)((\exists x)P(x) \,\&\, (\exists x)\neg P(x) \,\&\, (\forall x)(\forall y)(R(x,y) \rightarrow (P(x) \equiv P(y)))).$$

Connectedness may be then expressed using a binary relation $<$ as:

$$(\exists <)\Big(\bigwedge \mathtt{SPO}_{\mathrm{Max}} \,\&\, (\forall x)(\forall y)(x < y \,\&\, (\forall z)\neg(x < z < y) \rightarrow R(x,y))\Big),$$

where $\mathtt{SPO}_{\mathrm{Max}}$ is the theory of strict partial ordering $<$ with a greatest element. The second member of the outer conjunction says that y being a successor to x implies mutual reachability of these two points. ***Quod Erat Demonstrandum***

Theorem 16. *Acyclicity of a graph is expressible in monadic existential second-order logic and cyclicity of a graph is expressible in dyadic existential second-order logic.*

Proof. Follows easily from the definition of cyclicity and theorem 16. ***Q.E.D.***

Fagin-Hájek theorem can now be easily stated as a simple corollary of what has up to now been proven. All it requires is to find at least one class of structures expressible in monadic existential second-order logic, whose complementary class has not the same property. In [Fag75], non-connectedness is found to be of such a property and although not explicitly mentioned there, acyclicity follows by theorem 16. In [Háj75], outside of non-connectedness and acyclicity, non-planarity is also named to be of this property.

Theorem 17 (Fagin-Hájek theorem). *Non-connectedness of a graph is definable by a monadic existential second-order sentence in strong prenex normal form and thus is in monadic* **NP**, *whereas connectedness of a graph, although in dyadic* **NP**, *is not in monadic* **NP**. *Therefore, monadic* **NP** *sets are not closed under complementation.*

Proof. By theorem 14, there is a connected graph $\mathbb{A}$ and a non-connected graph $\mathbb{B}$ such that $\mathbb{A} \Rightarrow_r^D$ for arbitrarily large monadic D and $r \in \mathbb{N}^+$. Therefore, by theorem 11, if a monadic existential second-order sentence be satisfied by all connected graphs, it is also satisfied in some non-connected graph. The set of encodings of all cycles and the set of encodings of all connected graphs do not form monadic **NP** sets. ***Quod Erat Demonstrandum***

Résumé

At the end of the second chapter, we proved Fagin-Hájek theorem in the way it was originally done by Fagin. However self-contained as this method may be, it is notably difficult, utilising elementary yet very complicated combinatorial techniques and procedures. There are at least two other proofs of Fagin-Hájek theorem which evade the difficulties posed by Fagin's original method: first there is the proof by Fagin, Stockmeyer and Vardi published in [SV95] where the original theorem is also significantly generalised, having it's statement extended even to built-in languages richer than the one consisting simply of the binary reachability relation. The proof of the original theorem described therein, however, although simpler, is not that much self-contained, as it relies on a non-trivial equivalence between two kinds of generalised Ehrenfeucht-Fraïssé games, published in the article [AF90].

The second proof is due to Hájek in [Háj75], published in the same year as [Fag75]. Unlike both of the afore discussed proofs, it is not based on finitistic methods; instead it is non-standard, therefore reducing the finitary problem to a more easily resolvable task concerning infinite sets, elluding the technicalities of the problem's finitary version. Hájek's proof uses the theory of semisets, nowadays abandoned area, most broadly and completely treated in the book [VH72]. However, as Hájek himself notes in [Háj75], the same result can be achieved using techniques involving ultraproduct construction and thus the semisets are not necessary for the result's replication. The then following note that in order to achieve the same result, *one can... **(likely)** use the notion of partial isomorphisms...* further indicates that unlike the proof published in [SV95], this one was devised completely independently of the original result.

Bibliography

[AF90] Miklos Ajtai and Ronald Fagin. "Reachability is Harder for Directed Than for Undirected Graphs". In: *The Journal of Symbolic Logic* 55.1 (1990), pp. 113–150.

[Ass55] Günter Asser. "Das Repräsentenproblem in Prädikatenkalkül der ersten Stufe mit Identität". In: *Zeitschrift für mathematische Logik und Grundlagen der Mathematik* 1 (1955), pp. 252–253.

[BML41] Garrett Birkhoff and Saunders Mac Lane. *A Survey of Modern Algebra.* New York: Macmillan, 1941.

[BŠ86] Bohuslav Balcar and Petr Štěpánek. *Teorie množin.* Praha: Academia, 1986.

[Cur77] Haskell Brooks Curry. *Foundations of Mathematical Logic.* Courier Corporation, 1977.

[Ehr61] Andrzej Ehrenfeucht. "An Application of Games to the Completeness Problem for Formalized Theories". In: *Fundamenta Mathematicae* 49 (1961), pp. 129–141.

[Fag73] Ronald Fagin. "Contributions to the Model Theory of Finite Structures". PhD thesis. University of California, Berkeley, 1973.

[Fag74] Ronald Fagin. "Generalized First-Order Spectra, and Polynomial-Time Recognizable Sets". In: *Complexity of Computation: Proceedings of a Symposium in Applied Mathematics of the American Mathematical Society and the Society for industrial and Applied Mathematics held in New York City, April 18–19, 1973.* Ed. by Richard Manning Karp. Vol. 7. American Mathematical Society, Jan. 1974, pp. 43–73. ISBN: 978-0-8218-1327-0.

[Fag75] Ronald Fagin. "Monadic Generalized Spectra". In: *Zeitschrift für mathematische Logik und Grundlagen der Mathematik* 21 (1975), pp. 89–96.

[Fra53] Roland Fraïssé. "Sur quelques classifications des systèmes de relations". PhD thesis. University of Paris, 1953.

[Fra54] Roland Fraïssé. "Sur une nouvelle classification des systèmes de relations". In: *Publications Scientifique de l'Université d'Alger* I (1954).

[Grä07] Erich Grädel. "Finite Model Theory and Descriptive Complexity". In: *Finite Model Theory and It's Applications.* Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 125–130. ISBN: 978-3-540-68804-4.

[Háj75] Petr Hájek. "On Logics of Discovery". In: *Mathematical Foundations of Computer Science 1975, 4th Symposium, Mariánské Lázně, Czechoslovakia, September 1-5, 1975, Proceedings.* Ed. by Jiří Bečvář. Vol. 32. Lecture Notes in Computer Science. Springer, Jan. 1975, pp. 30–45.

[Hon16] Radek Honzík. *Introduction to Boolean algebras.* Lecture notes. Department of Logic, Faculty of Arts of Charles University. 2016.

[Imm99] Neil Immerman. *Descriptive Complexity.* Springer Verlag, 1999. ISBN: 0-387-98600-6.

[JS74] Neil Jones and Alan Selman. "Turing Machines and the Spectra of First-Order Sentences". In: *Journal of Symbolic Logic* 39 (1974), pp. 139–150.

[Kle67] Stephen Cole Kleene. *Mathematical Logic*. New York: John Wiley & Sons, Incorporated, 1967.

[Mar06] David Marker. *Model theory: an introduction*. Vol. 217. Springer Science & Business Media, 2006.

[Mlč22] Josef Mlček. *Pokročilá matematická logika*. Unpublished lecture notes created for a course of the same name, running regularly at Charles University. Version from: 2022.

[MM09] Arnaud Durand, Neil Jones, Johann Makowsky and Malika More. "Fifty Years of the Spectrum Problem: Survey and New Results." In: (2009). arXiv: 0907.5495 [math.LO].

[Ně90] Ladislav Procházka, Ladislav Bican, Tomáš Kepka, Petr Němec. *Algebra*. Academia, 1990. ISBN: 80-200-0301-0.

[Sch52] Heinrich Scholz. "Ein ungelöstes Problem in der symbolischen Logik". In: *The Journal of Symbolic Logic* 17 (1952), p. 160.

[Sho67] Joseph R. Shoenfield. *Mathematical Logic*. Addison-Wesley Publishing Company, 1967.

[Sip06] Michael Sipser. *Introduction to the Theory of Computation*. Boston, Massachusetts: Thomson Course Technology, a division of Thomson Learning, Incorporated, 2006. ISBN: -534-95097-3.

[Soc01] Antonín Sochor. *Klasická matematická logika*. Praha: Karolinum, publishing house of Charles University, 2001. ISBN: 80-246-0218-0.

[SV95] Ronald Fagin, Larry J. Stockmeyer and Moshe Y. Vardi. "On Monadic **NP** vs. Monadic co-**NP**". In: *The Journal of Symbolic Logic* 120.1 (1995), pp. 78–92. ISSN: 0890-5401.

[Šve02] Vítězslav Švejdar. *Logika: neúplnost, složitost a nutnost*. Praha: Academia, 2002. ISBN: 80-200-1005-X.

[Tar56] Alfred Tarski. "Contributions to the Theory of Models". In: *Journal of Symbolic Logic* 21.4 (1956), pp. 405–406.

[VH72] Petr Vopěnka and Petr Hájek. *The Theory of Semisets*. Studies in Logic. North-Holland Publishing Company, 1972. ISBN: 9780720422672.