ABSTRACT

Title of dissertation: MODEL THEORY AND COMPLEXITY THEORY

Walid Gomaa
Doctor of Philosophy, 2007

Dissertation directed by: Professor William Gasarch
Department of Computer Science
and
Professor David Kueker
Department of Mathematics

Descriptive complexity theory is a branch of complexity theory that views the hardness of a problem in terms of the complexity of expressing it in some logical formalism; among the resources considered are the number of object variables, quantifier depth, type, and alternation, sentences length (finite/infinite), etc.

In this field we have studied two problems: (i) expressibility in $\exists SO$ and (ii) the descriptive complexity of finite abelian groups. Inspired by Fagin's result that $NP = \exists SO$, we have developed a partial framework to investigate expressibility inside $\exists SO$ so as to have a finer look into NP. The framework uses combinatorics derived from second-order Ehrenfeucht-Fraïssé games and the notion of game types. Among the results obtained is that for any k, divisibility by k is not expressible by an $\exists SO$ sentence where (1) each second-order variable has arity at most 2, (2) the first-order part has at most 2 first-order variables, and (3) the first-order part has quantifier depth at most 3.

In the second project we have investigated the descriptive complexity of finite abelian groups. Using Ehrenfeucht-Fraïssé games we find upper and lower bounds on quantifier depth, quantifier alternations, and number of variables of a first-order sentence that distinguishes two finite abelian groups. Our main results are the following. Let G_1 and G_2 be a pair of non-isomorphic finite abelian groups, and let m be a number that divides one of the two groups' orders. Then the following hold: (1) there exists a first-order sentence φ that distinguishes G_1 and G_2 such that φ is existential, has quantifier depth $O(\log m)$, and has at most 5 variables and (2) if φ is a sentence that distinguishes G_1 and G_2 then φ must have quantifier depth $\Omega(\log m)$.

In infinitary model theory we have studied abstract elementary classes. We have defined Galois types over arbitrary subsets of the monster (large enough homogeneous model), have defined a simple notion of splitting, and have proved some properties of this notion such as invariance under isomorphism, monotonicity, reflexivity, existence of non-splitting extensions.

MODEL THEORY AND COMPLEXITY THEORY

by

Walid Gomaa

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2007

Advisory Committee:
Professor William Gasarch, Chair/Advisor
Professor David Kueker, Co-Chair/Co-Advisor
Professor Jonathan Katz
Professor Amol Deshpande
Professor Lawrence Washington

© Copyright by
Walid Gomaa
2007

ACKNOWLEDGEMENTS

I'd like to thank my advisor Professor David Kueker for the so valuable knowledge he taught me. He introduced me to the field of mathematical logic and in particular model theory around which my research centers. It is a very exciting and intellectually challenging research area. Working in this field has had a tremendous impact on my career and even on my view to every aspect of life. He has always made himself available for help and advice. It has been a pleasure to work with and learn from such an extraordinary individual.

I'd like to thank Professor Nick Roussopoulos with whom I have worked for many semesters as a teaching assistant which on one hand provided me with necessary funds to do my research and on the other hand get me to know this fine sophisticated man who used to give me valuable advice at critical times for me.

I'd like to thank my co-advisor Professor William Gasarch who suggested several ideas over which a large part of this dissertation is based. He also supported me to go to many conferences.

I owe my deepest thanks to my parents who have always stood by me and guided me through my career. Words cannot express the gratitude I owe them.

I'd like to thank my friends who greatly supported me especially in the transition to my life in the states; in particular I'd like to express my gratitude to Moustafa Youssef, Tamer ElSharnouby, and Tamer Nadeem. I'd like also to thank Mohamed Shawky, Mohamed Abdallah, Ahmed Sadek, Karim Sadik, Tarek Ghanem, Yasser Jaradat, Mohamed Farouk, Amr ElSherif and Mohamed Fahmi.

Table of Contents

Chapter 1

Introduction

1.1 Preliminary

A logical language consists of a set of symbols called the vocabulary along with formation rules for arranging these symbols into a well-formed formulas. For example, take first-order logic, its vocabulary consists of two parts: (i) a set of logical symbols that have fixed meanings and consists of a set of object variables $\{x_i \colon i \in \mathbb{N}\}$, the propositional connectives $\wedge, \vee, \neg$, and the quantifiers $\exists, \forall$ and (ii) non-logical symbols whose existence and meanings depend on the domain of study, for example in the graph domain there is a binary relation symbol that captures the edge relation; in general these symbols fall into three categories: function symbols for functions, relation symbols for relations, and constant symbols for the distinguished elements in the domain such as the identity element in groups. Well-formed formulas are defined inductively: start with atomic formulas then close under conjunction, disjunction, negation, existential, and universal quantification.

So far we have just described the syntactic structure of a logical langauge which seems to be merely nice arrangements of meaningless symbols. Here comes the driving force of semantics which imposes meanings and live over the dead symbols. Most often the semantic component eventually leads to giving truth valuations to sentences in the language.

Consider first-order logic with one non-logical symbol, a binary relation symbol. Consider the following sentence

$$\sigma \overset{def}{=} \forall x \forall y \exists z (x < y \rightarrow x < z < y) \tag{1.1}$$

Assume $<$ is interpreted as a total ordering. Then this sentence says that between any two distinct members of the domain, there exists a new element between them. In other words this asserts the density of the total ordering. When σ is interpreted over the rationals (the variables x, y, z take their values from $\mathbb{Q}$), σ is evaluated to true. However, when σ is interpreted over the integers it becomes false since the integers are scattered. As another example consider the following sentence

$$\sigma \overset{def}{=} \exists x \forall y (y \leq x) \tag{1.2}$$

This says that the total ordering has a last element. σ is false over the naturals, however, when evaluated over any finite ordered set or even over ω^*, the reverse ordering of the naturals, σ becomes true. When $<$ is interpreted as an edge relation in a graph, then this last sentence asserts that there is a vertex that is connected to every vertex in the graph.

This interplay between the syntactic structure represented by a set of sentences called the axioms and the semantic structure represented by the class of structures over which these sentences are interpreted and evaluated to true is the scope of study of model theory.

The research done in this thesis centers around *model theory.* My research spans both the applied and the pure aspects of model theory. On the application side we have done research in the areas of finite model theory and descriptive complexity theory. Whereas on the pure theoretical side we have been working in classification theory for abstract elementary classes.

Traditionally model theory studies classes of infinite structures. The interest in *finite model theory* started with Trakhtenbrot's result in 1950 stating that logical validity over finite models is not recursively enumerable, that is, completeness fails over finite structures (for a proof see [21]). There are currently two different threads of research in finite model theory: (i) the study of the expressive power of different logics over classes of finite structures, this research has strong connections with theoretical computer science in particular database theory and complexity theory and (ii) developing a classification/stability theory for classes of finite structures, this research is purely mathematical, still in its infancy, and as far as we know there have been no attempts to apply it to complexity theory, however, we strongly believe that the rich and wide variety of tools from classification/stability theory can provide deep insights into open problems in complexity theory.

The connection between finite model theory and complexity theory started in 1974 when R. Fagin proved his celebrated theorem that the class NP can be exactly captured by existential second-order logic [7]. This opened up a new area of research called *descriptive complexity.* As we know the purpose of *traditional complexity theory* is twofold: (i) to study the amount of computational resources needed to solve important computational problems and (ii) to classify the computational problems according to their hardness. The computational resources considered are (i) time and space as in the Turing machine-based model or (ii) the amount of hardware circuitry as in the circuit-based model. However, descriptive complexity theory investigates how hard it is to express a problem in some logical formalism and to classify the problems based on that. The resources considered are basically logical such as the number of object variables, quantifier depth, type, and alternation, sentences length (finite vs. infinite), recursive vs. non-recursive capabilities, etc.

Consider for example 3-colorability which is an NP-complete problem. It can be expressed by the following second-order sentence.

$$\psi \overset{def}{=} \exists R \exists B \exists G \, (\varphi \wedge \theta) \tag{1.3}$$

$$\varphi \overset{def}{=} \forall x \, ((R(x) \wedge \neg B(x) \wedge \neg G(x)) \vee \ldots) \tag{1.4}$$

$$\theta \overset{def}{=} \forall x \forall y \, ((R(x) \wedge R(y) \rightarrow \neg E(x, y)) \wedge \ldots) \tag{1.5}$$

ψ says that the set of vertices can be partitioned into three subsets: one colored R, one colored B, and one colored G (for red, blue, and green respectively). This partitioning must satisfy two properties: φ which asserts that this is a valid coloring (each vertex has exactly one color) and θ which asserts that it is a valid three coloring. So given a graph G, ψ is true on G if and only if G is 3-colorable. ψ as defined above belongs to monadic existential second-order logic; it is second-order since there are quantifications over relations and it is monadic since it quantifies just over sets (no quantification over relations of higher arities). It should be noted that computational resources do not match exactly with logical resources, for example, graph connectivity, a P problem, can not be expressed in monadic existential second-order logic, it needs more logical resources.

Several important complexity classes have nice logical characterizations [22]. For example, Fagin's result has been generalized in [26] to show that the whole of the polynomial hierarchy is exactly captured by second-order logic. Immerman showed in [17] that P is exactly captured with least fixpoint logic over the class of ordered structures ($<$ must be in the vocabulary). Hence the P vs. NP problem is equivalent to separating the two logics: existential second-order logic and least fixpoint logic with $<$. $PSpace$ was shown to be captured by partial fixpoint logic over the class of finite structures. NL was shown to be closed under complementation using transitive closure logic.

One of the most significant tools that finite model theory provides is the *Ehrenfeucht-Fraïssé* (EF) games. They were invented by Ehrenfeucht [6] based on work by Fraïssé [11]. An EF game for a particular logic $\mathcal{L}$ is a game-theoretic characterization for expressibility in $\mathcal{L}$. The game is played over two structures of the same kind (for example two graphs) between two players one of them is called the spoiler (or the $\exists$ player) and the other is called the duplicator (or the $\forall$ player). The game is played for r rounds for some positive integer r. At each round both players alternate choosing elements or sets of elements from the two structures. The goal of the duplicator is to show that the two structures can not be distinguished from each other within r rounds which roughly corresponds to saying that the two structures can not be distinguished by some proper sublogic of $\mathcal{L}$ that is defined based on the game parameters which is just r in our explanation here. Whereas the goal of the spoiler is to show that this can be done. If for every r, the duplicator has a winning strategy, then this shows that a certain class of structures is not definable in $\mathcal{L}$.

Consider the game played over the integers $\mathbb{Z}$ and the rationals $\mathbb{Q}$. We show that the spoiler can win in 3 moves (this is actually optimal). The spoiler starts by choosing an element $a_1 \in \mathbb{Z}$, let b_1 be the duplicator's response from $\mathbb{Q}$. At round 2, the spoiler chooses $a_2 \in \mathbb{Z}$ such that $a_2 = a_1 + 1$, let b_2 be the duplicator's response. At round 3, the spoiler chooses an element $b_3 \in \mathbb{Q}$ that lies between b_1 and b_2, the duplicator would then fail to respond with a corresponding element from $\mathbb{Z}$.

Consider the sentence in (1.1), obviously σ is true on the rationals and false on the integers, hence σ is a first-order sentence that distinguishes the rationals from the integers. Here we can see the close relationship between logical expressibility and game-theoretic characterization. The quantifier depth of σ is 3 which corresponds to 3 moves necessary for the spoiler to win the game. The two outermost quantifiers are universal corresponding to the first two moves of the spoiler, the last quantifier is existential corresponding to the spoiler changing the structure from which her last response is chosen, and finally the quantifier-free part corresponds to the spoiler using the density of the rationals to win the game.

1.2 Summary of Results

In Chapter 2, inspired by Fagin's result we develop a partial framework to investigate expressibility inside existential second-order logic so as to have a finer look into NP. This framework uses interesting combinatorics derived from second-order EF games and the notion of *game types*. A second-order EF game is played over two classes of structures of the same vocabulary where the duplicator has the additional advantage of first choosing the two structures over which the traditional first-order game is played. These games are used to characterize expressibility in second-order logic or sublogics of it. The notion of game types is based on the *locality* of first-order logic and extensions of it (for example extending with unary generalized quantifiers) to provide necessary and sufficient conditions for the duplicator to have a winning strategy. This in many cases avoids giving complicated combinatorial argument for an actual winning strategy for the duplicator.

Using this framework expressibility results are proved such as:

1. for any integer $k \geq 2$, divisibility by k is not expressible by an existential second-order sentence where the second-order variables have arity at most 2 and the first-order part has 2 first-order variables and quantifier depth 3, and

2. having one more first-order variable makes the same problem expressible and the parameter k induces a proper hierarchy with varying the number of binary second-order variables.

In Chapter 3, we investigate the descriptive complexity of finite abelian groups. Using EF games we find upper and lower bounds on quantifier depth, quantifier alternations, and number of variables of a first-order sentence that distinguishes two finite abelian groups. The main results are the following. Let G_1 and G_2 be a pair of non-isomorphic finite abelian groups, and let m be a number that divides one of the two groups' orders. Then the following hold:

1. there exists a first-order sentence φ that distinguishes G_1 and G_2 such that φ is existential, has quantifier depth $O(\log m)$, and has at most 5 variables, and

2. if φ is a sentence that distinguishes G_1 and G_2 then φ must have quantifier depth $\Omega(\log m)$.

These results are applied to

1. get bounds on the first-order distinguishability of dihedral groups,
2. to prove that on the class of finite groups both cyclicity and the closure of a single element are not first-order definable, and
3. give a different more accessible proof for the first-order undefinability of simplicity, nilpotency, and the normal closure of a single element on the class of finite groups (their undefinability were shown by A. Koponen and K. Luosto in an unpublished paper [19]).

1.3 Abstract Elementary Classes

Chapter 4 focuses on the rather different topic of *abstract elementary classes* (*AEC*'s) which deals exclusively with classes of infinite structures. The context of *AEC*'s was introduced by Shelah in the eighties [25], it encompasses much of current research in model theory. He embarked on the ambitious program of developing a *classification/stability theory* for this context. A class of structures $\mathscr{K} = (\mathbb{K}, \preceq_{\mathscr{K}})$ is an *AEC* if it satisfies the following axioms:

1. Closure under isomorphism
2. $\preceq_{\mathscr{K}}$ refines the substructure relation $\subseteq$

3. The coherence axiom

4. Closure of Tarski-Vaught chains

5. Downward Löwenheim-Skolem axiom (the existence of a Löwenheim-Skolem number)

However, as far as we know most of the current research assume three more properties: amalgamation, joint embedding, and the existence of arbitrarily large models. In most cases these properties are assumed in its full generality, however, restricted forms (up-to a particular cardinal) are assumed in some articles such as [27] and [16]. These additional properties guarantee the existence of a large enough strongly homogeneous model called the *monster*. The axiomatization of $AEC's$ as seen above is purely semantical, however, the *presentation theorem* proved by Shelah allows us to replace this entirely semantic description by a syntactic one. It shows that every AEC can be represented as a *pseudoelementary class* omitting a set of types. This theorem has the important consequence of allowing us to use the technology of *Ehrenfeucht-Mostowski models* which plays a crucial role in proving results about $AEC's$ especially under the assumption of categoricity. A proof of the theorem can be found in [3, 2].

Let λ be a cardinal (finite or infinite) and let $\mathscr{K}_\lambda = \{\mathcal{M} \in \mathscr{K} : |M| = \lambda\}$. Then classification theory aims at answering questions about $\mathscr{K}_\lambda / \cong$ of the following nature [12].

1. Is $\mathscr{K}_\lambda \neq \emptyset$?

2. Does $\mathscr{K}_\lambda \neq \emptyset$ imply that $\mathscr{K}_{\lambda^+} \neq \emptyset$?

3. If $\mathscr{K}$ is λ^+-categorical ($|\mathscr{K}_{\lambda^+}| = 1$ up-to isomorphism), does that imply it is λ-categorical? (downward transfer of categoricity)

4. If $\mathscr{K}$ is λ-categorical, does that imply it is λ^+-categorical? (upward transfer of categoricity)

5. What are the possible functions $\lambda \longmapsto |\mathscr{K}_\lambda|$?

6. Under what conditions on $\mathscr{K}$ it is possible to find a nice *independence* relation on subsets of every $\mathcal{M} \in \mathscr{K}$? (this is a generalization of linear independence in vector spaces or algebraic independence in fields)

Stability theory is the main technology used to develop a classification theory. For example, the study of the structure of models of a first-order theory was developed to provide classifications of those models. First-order stable classes behave very nicely and have a well-defined *dimension theory* based on an independence relation called *forking*.

The guiding conjecture for the development of classification theory for *AEC*'s is due to Shelah and states that if an *AEC* is categorical in some cardinal above the *Hanf number* (a characteristic cardinal for the class) then it is categorical in every cardinal above the Hanf number. This conjecture is still far from being proved and there is no known stability theory or even a categoricity theorem for *AEC*'s without some additional strong assumptions [13]. As far as we know most of the work that have been done so far assume that notions such as Galois types, stability, tameness, saturation, etc are defined over models in $\mathscr{K}$ or with respect to models in $\mathscr{K}$. The exception to this is the work done by T. Hyttinen and M. Kesälä in [16] and the followup work in [15]. The main concept in the latter work that distinguishes it from others is *finite character*. This states that if $\mathcal{A}, \mathcal{B} \in \mathscr{K}$ with $\mathcal{A} \subseteq \mathcal{B}$, then if for every $\bar{a} \in A$, the Galois type of $\bar{a}$ inside $\mathcal{A}$ coincides with its type inside $\mathcal{B}$, then $\mathcal{A} \preceq_{\mathscr{K}} \mathcal{B}$.

So far in our work we have defined Galois types over arbitrary subsets of the monster, have defined a simple notion of splitting, and have proved some properties of this notion such as invariance under isomorphism, monotonicity, reflexivity, existence of non-splitting extensions, its relation to the stability of the class, etc.

Chapter 2

Expressibility in Σ^1_1

Inspired by Fagin's result that $NP = \Sigma^1_1$, we have developed a partial framework to investigate expressibility inside Σ^1_1 so as to have a finer look into NP. The framework uses interesting combinatorics derived from second-order Ehrenfeucht-Fraïssé games and the notion of game types. Some of the results that have been proven within this framework are: (1) for any k, divisibility by k is not expressible by a Σ^1_1 sentence where (1.i) each second-order variable has arity at most 2, (1.ii) the first-order part has at most 2 first-order variables, and (1.iii) the first-order part has quantifier depth at most 3, (2) adding one more first-order variable makes the same problem expressible, and (3) inside this last logic the parameter k creates a proper hierarchy with varying the number of second-order variables.

2.1 Introduction

The birth of finite model theory is often identified with Trakhtenbrot's result from 1950 stating that logical validity over finite models is not recursively enumerable, that is, completeness fails over finite structures [21]. In 1974, R. Fagin proved his celebrated theorem that NP can be exactly captured by existential second-order logic [7]. This opened up a new area of research called descriptive complexity. It is a branch of complexity theory that views the hardness of problems in terms of the complexity of their logical expressiveness such as the number of object variables, quantifier depth, type, and alternation, sentences length (finite/infinite), etc.

Fagin's result has been generalized in [26] to show that the whole of the polynomial hierarchy is exactly captured by second-order logic.

Inspired by the above results we have developed a partial framework to investigate expressibility inside Σ^1_1. Currently this framework encompasses sublogics of Σ^1_1 defined as follows.

Definition 2.1.

1. Existential second-order logic*, or* Σ^1_1*, is defined to be the class of sentences of the form*

$$\exists X_1 \ldots \exists X_l \varphi \tag{2.1}$$

where the X_i*'s are second-order relational variables of arbitrary finite arities and* φ *is a first-order sentence.*

2. *Let* $mon\Sigma^1_1$ *be the sublogic of* Σ^1_1 *obtained by restricting the arities of the* X_i*'s to be at most* 1 *(hence the prefix mon).*

3. *Let* $bin\Sigma^1_1$ *be the sublogic of* Σ^1_1 *obtained by restricting the arities of the* X_i*'s to be at most* 2 *(hence the prefix bin). Note that any sentence in* $bin\Sigma^1_1$ *is equivalent to a sentence of the form*

$$\exists R_1 \ldots \exists R_n \exists S_1 \ldots \exists S_m \varphi \tag{2.2}$$

where the R_i*'s and the* S_i*'s are binary and unary second-order variables respectively. For simplicity of discussion we will assume that* $bin\Sigma^1_1$ *consists exactly* *of sentences of the form (2.2).*

4. *Let* $bin\Sigma_1^1(p,r)$ *be the sublogic of* $bin\Sigma_1^1$ *obtained by restricting* φ *to have at most* p *first-order variables and quantifier depth ar most* r. *Define* $mon\Sigma_1^1(p,r)$ *similarly.*

Within this framework we plan to study expressibility of some number-theoretic properties. In this chapter we started by studying divisibility.

Definition 2.2. *For every integer* $k \geq 2$, *let* DIV_k *denote the problem of deciding whether a positive integer is divisible by* k. *Let* $\overline{DIV_k}$ *denote the complement problem, that is non-divisibility by* k.

Example 2.1. *Consider* DIV_2 *which is the famous* $EVEN$ *problem. It was shown that* $EVEN$ *can not be expressible in first-order logic (e.g., see [21]). However,* $EVEN$ *can be expressed by the following* $bin\Sigma_1^1$ *sentence.*

$$\sigma \overset{def}{=} \exists R\,(\varphi_1(R) \wedge \varphi_2(R) \wedge \varphi_3(R)) \tag{2.3}$$

where

$$\varphi_1(R) \overset{def}{=} \forall x \neg R(x,x)$$

$$\varphi_2(R) \overset{def}{=} \forall x \forall y\,(R(x,y) \longleftrightarrow R(y,x))$$

$$\varphi_3(R) \overset{def}{=} \forall x \exists y\,(R(x,y) \wedge \forall z\,(R(x,z) \longrightarrow z = y))$$

Notice that σ *defines the class of simple finite graphs with isolated edges (*1*-regular graphs). The number of vertices in these graphs must be even.*

Notation 2.1. *Throughout the remaining part of this chapter if the variable* k *is* *mentioned free (unquantified) in a result, this indicates that the result holds for every value of k.*

Assuming the empty vocabulary we have proved the following results:

1. $DIV_k, \overline{DIV_k}$ are neither in $mon\Sigma_1^1$ nor in $mon\Pi_1^1$

2. $DIV_k \notin bin\Sigma_1^1(1, r)$ for any r

3. $DIV_k \notin bin\Sigma_1^1(2, 2)$ and $DIV_k \notin bin\Sigma_1^1(2, 3)$

4. $DIV_k \in bin\Sigma_1^1(3, 3)$. More specifically, given $\Gamma \subseteq bin\Sigma_1^1(3, 3)$ where every $\sigma \in \Gamma$ has at most l binary variables then $DIV_k \in \Gamma$ for every $k \leq (4^l - 1)$. Furthermore, $DIV_k \in \Gamma$ for only finitely-many k, hence DIV_k creates a proper hierarchy inside the logic $bin\Sigma_1^1(3, 3)$.

5. An immediate consequence of the above is that $mon\Sigma_1^1 \subset bin\Sigma_1^1$.

6. $DIV_k \notin bin\Sigma_1^1$ when the sizes of the interpretations of the binary variables are bounded from above by some linear function of the size of the universe.

Section 2.2 gives axiomatization of a type of colored graphs which will be the main structures throughout the rest of this chapter. Section 2.3 introduces the Ehrenfeucht-Fraïssé (EF) game. we define a specific version called $bin\Sigma_1^1(p, r)$-game which will be applied to study the expressibility of DIV_k in $bin\Sigma_1^1(p, r)$. In Section 2.4 we prove that DIV_k and its complement are neither in $mon\Sigma_1^1$ nor in $mon\Pi_1^1$. In Section 2.5, the notion of game types is defined which is a combinatorial concept based on the locality of first-order logic, it is used to provide necessary and sufficient conditions for winning EF-games without actually playing them. In Sections 2.6 through 2.9 we prove the other expressibility results mentioned above. Section 2.10 concludes the chapter with some insights for future work.

2.2 Colored Graphs

We study expressibility by sentences of the following form

$$\exists R_1 \ldots \exists R_{n'} \exists S_1 \ldots \exists S_{m'} \varphi \tag{2.4}$$

where the R_i's and S_i's are binary and unary second-order variables respectively and φ is a first-order sentence whose vocabulary is exactly the R_i's and the S_i's.

Such sentences will be modeled by first-order structures of the following form

$$G' = (V, U_1, \ldots, U_{m'}, E_1, \ldots, E_{n'})$$

V is a finite set of elements. The U_i's are unary relations over V, these represent the interpretations of the S_i's in (2.4). The E_i's are binary relations over V which represent the interpretations of the R_i's. Consider an element in V. There are $m = 2^{m'}$ different combinations of which unary relations hold for it and do not hold for it. Similarly, for a pair there are $n = 4^{n'}$ different combinations of which binary relations hold. Hence we can easily obtain a graph G where the vertices are m-colored (not necessarily properly) and the edges are n-colored (not necessarily properly). We denote this graph

$$G = (V, C_1, \ldots, C_m, D_1, \ldots, D_n) \tag{2.5}$$

where G is a complete undirected graph, each vertex has a self-edge, each C_i is a unary relation (for a vertex color), and each D_i is a binary relation (for an edge color). G must satisfy the following axioms:

$$\forall u \bigvee_{1 \leq i \leq m} C_i(u)$$

$$\forall u \left(C_i(u) \longrightarrow \bigwedge_{1 \leq j \leq m, j \neq i} \neg C_j(u) \right), \qquad for\ every\ 1 \leq i \leq m$$

$$\forall u \bigvee_{1 \leq i \leq n} D_i(u,u)$$

$$\forall u \left(D_i(u,u) \longrightarrow \bigwedge_{1 \leq j \leq n, j \neq i} \neg D_j(u,u) \right), \qquad for\ every\ 1 \leq i \leq n$$

$$\forall u \forall v \bigwedge_{1 \leq i \leq n} (D_i(u,v) \longleftrightarrow D_i(v,u))$$

$$\forall u \forall v \left(u \neq v \longrightarrow \bigvee_{1 \leq i \leq n} D_i(u,v) \right)$$

$$\forall u \forall v \left(u \neq v \wedge D_i(u,v) \longrightarrow \bigwedge_{1 \leq j \leq n, j \neq i} \neg D_j(u,v) \right) \qquad for\ every\ 1 \leq i \leq n$$

The first two axioms indicate that every vertex u must have a unique color from the color list $C_1, \ldots, C_m$. The third and fourth axioms indicate that the self-edge of every vertex u must have a unique color from the color list $D_1, \ldots, D_n$. The last three axioms indicate that the graph is undirected and every edge (u, v) must have a unique color from the color list $D_1, \ldots, D_n$. It can easily be observed that the axioms for self-edges can be combined into the last two axioms, however, they are separated since for the rest of this chapter they are treated differently from the other edges.

Notation 2.2.

1. *Let $\mathcal{G}_{m,n}$ be the class of graphs with exactly m vertex colors and n edge colors. Let $\mathcal{G} = \bigcup_{m,n} \mathcal{G}_{m,n}$.*

2. *Let $\mathscr{C}$ be the set of m vertex colors and let $\mathscr{D}$ be the set of n edge colors.*

2.3 Ehrenfeucht-Fraïssé Games

Ehrenfeucht-Fraïssé (EF) games are used to characterize expressibility in some logical formalism. In our context we apply it to study expressibility in $bin\Sigma_1^1(p, r)$ for positive integers p and r.

2.3.1 Pebble first-order EF-games

In this section we briefly review pebble first-order EF-games. A pebble first-order EF-game [21, 18] is played over two structures of the same kind, for example two linear orderings. There are two players: the spoiler denoted by $\mathcal{S}$ and the duplicator denoted by $\mathcal{D}$. The game has two parameters: the number of rounds r and the number of pebbles $p \leq r$. Intuitively, the goal of $\mathcal{S}$ is to show that the two structures can be distinguished in at most r steps using only p pebbles, whereas $\mathcal{D}$ wants to show that this can not be done.

Definition 2.3 (Partial isomorphism). *Let $\mathcal{A}$ and $\mathcal{B}$ be two first-order structures with vocabulary τ. Assume $\bar{a} = \langle a_1, \ldots, a_n \rangle \in A^n$ and $\bar{b} = \langle b_1, \ldots, b_n \rangle \in B^n$. We say that there is a* partial isomorphism *from $\bar{a}$ onto $\bar{b}$ if for every m, for every first-order quantifier-free formula $\varphi(x_1, \ldots, x_m)$ over τ, and for every $\{i_1, \ldots, i_m\} \subseteq \{1, \ldots, n\}$*

the following holds

$$\mathcal{A} \models \varphi(a_{i_1}, \ldots, a_{i_m}) \iff \mathcal{B} \models \varphi(b_{i_1}, \ldots, b_{i_m})$$

Given $\mathcal{A}$ and $\mathcal{B}$, the pebble EF-game goes as follows. The players start the game each having a fixed number of p pebbles. At each round $\mathcal{S}$ does the following: (i) she chooses an element x from one of the two structures and (ii) then she either removes a pebble that has been placed on a previously chosen element and places it on x or placing a new pebble, if she still has any, on x. $\mathcal{D}$ then responds to the challenge by choosing an element from the other structure and does the same pebbling so as to preserve the partial isomorphism among the pebbled elements chosen so far from $\mathcal{A}$ and $\mathcal{B}$. At the beginning the pebbles are not placed on any elements (we can assume having extra pebbles always placed on the distinguished elements of the structure such as the group identity, even before the game starts). Assume that at the end of the game p pebbles are placed on $\bar{a} = \langle a_1, \ldots, a_p \rangle$ from the structure $\mathcal{A}$ and correspondingly p pebbles are placed on $\bar{b} = \langle b_1, \ldots, b_p \rangle$ from the structure $\mathcal{B}$. Notice that these are in general subsets of the elements chosen during the course of the game. $\mathcal{D}$ wins the game if $\bar{a}$ and $\bar{b}$ are partially isomorphic, otherwise $\mathcal{S}$ wins.

Pebble first-order EF-games characterize expressibility in bounded variable logic. Let $\mathcal{L}^p$ denote first-order logic with at most p variables. For a formula $\varphi \in \mathcal{L}^p$, let $qr(\varphi)$ denote the quantifier rank (depth) of φ.

Definition 2.4 (**Elementary equivalence**). *Assume $\mathcal{A}$ and $\mathcal{B}$ are two structures over a vocabulary τ. We say that $\mathcal{A}$ and $\mathcal{B}$ are* (p, r)-elementarily equivalent, *denoted* *by $\mathcal{A} \equiv_r^p \mathcal{B}$ if and only if for every sentence $\varphi \in \mathcal{L}^p$ such that $qr(\varphi) \leq r$ we have*

$$\mathcal{A} \models \varphi \iff \mathcal{B} \models \varphi \tag{2.6}$$

The following theorem gives the relationship between pebble games and expressibility in $\mathcal{L}^p$.

Theorem 2.1. *The following are equivalent:*

i. $\mathcal{A} \equiv_r^p \mathcal{B}$

ii. *$\mathcal{D}$ has a winning strategy in the pebble first-order EF-game over $\mathcal{A}$ and $\mathcal{B}$ with r-rounds and p-pebbles*

This theorem basically says that no sentence in $\mathcal{L}^p$ of quantifier rank at most r can distinguish $\mathcal{A}$ and $\mathcal{B}$ if and only if the duplicator has a winning strategy in the EF-game over $\mathcal{A}$ and $\mathcal{B}$ with r rounds and p pebbles.

2.3.2 Second-order EF-games

As seen above the first-order game is played over two structures that are fixed apriori. In contrast the second-order game is played over a class of structures and consists of two phases: (i) the second-order phase played over a class of structures $\mathscr{K}$ where the duplicator gets to choose two structures $\mathcal{A} \in \mathscr{K}$ and $\mathcal{B} \in \overline{\mathscr{K}}$ (the complement of $\mathscr{K}$) and (ii) the first-order phase which is the regular pebble first-order game played over $\mathcal{A}'$ and $\mathcal{B}'$ where $\mathcal{A}'$ and $\mathcal{B}'$ are expansions of $\mathcal{A}$ and $\mathcal{B}$ as described below. These games are used to study expressibility in second-order logic.

The second-order game was introduced by Fagin in [8] and then modified in [1] to what is called the *Ajtai-Fagin* game (also called *monadic* Σ^1_1 game). In our context we slightly modify the Ajtai-Fagin game to a new game we call $bin\Sigma^1_1(p, r)$. The new game has four parameters m, n, p, and r and has the following rules.

1. $\mathcal{D}$ selects a member $\mathcal{A} \in \mathscr{K}$.

2. Using the domain of $\mathcal{A}$ as a set of vertices, $\mathcal{S}$ forms a complete undirected graph with each vertex has a self-edge.

3. $\mathcal{S}$ colors the vertices using colors from $\mathscr{C}$ such that each vertex has exactly one color. She then colors the edges using colors from $\mathscr{D}$ such that each edge has exactly one color. Let $\mathcal{A}'$ be the new expanded colored structure.

4. $\mathcal{D}$ selects a member $\mathcal{B} \in \overline{\mathscr{K}}$.

5. Using the domain of $\mathcal{B}$ as a set of vertices, $\mathcal{D}$ forms a complete undirected graph with each vertex has a self-edge.

6. $\mathcal{D}$ colors the vertices from $\mathscr{C}$ such that each vertex has exactly one color. She then colors the edges from $\mathscr{D}$ such that each edge has exactly one color. Let $\mathcal{B}'$ be the new expanded colored structure.

7. $\mathcal{S}$ and $\mathcal{D}$ play a pebble first-order game over $\mathcal{A}'$ and $\mathcal{B}'$ with parameters r rounds and p pebbles.

This new game is used to study expressibility in $bin\Sigma^1_1(p, r)$. The relation is indicated in the following theorem whose proof is very similar to that of Theorem 4.5 in [1].

Theorem 2.2. *Let $\mathscr{K}$ be a class of structures of the same vocabulary. Then $\mathscr{K}$ is $bin\Sigma^1_1(p,r)$ if and only if there are positive integers m, n, p and r such that $\mathcal{S}$ has a winning strategy in the $bin\Sigma^1_1(p,r)$-game with parameters m, n, p and r.*

Remark 2.1.

1. *If the coloring is restricted to the vertices (no edge coloring), then we would call the resulting game $mon\Sigma^1_1(p,r)$, this is actually a pebbled version of the Ajtai-Fagin game.*

2. *In the definition of the $bin\Sigma^1_1(p,r)$-game, the ordering of the coloring of the vertices and/or edges (by either of the players) does not matter since the ordering of the corresponding second-order existential quantifiers is irrelevant as long as it does not alternate with universal quantifiers.*

3. *Notice that in the rules of the $bin\Sigma^1_1(p,r)$-game, the spoiler has to color the vertices and the edges of $\mathcal{A}$ before she knows what the other structure $\mathcal{B}$ is or how it will be colored by the duplicator. However, this does not make the game harder for her since if $\mathscr{K} \in bin\Sigma^1_1(p,r)$, then the coloring is predetermined completely by the sentence that defines $\mathscr{K}$.*

4. *In the following discussion we will always assume, unless otherwise stated, classes of structures over the empty vocabulary (the base language does not contain any non-logical symbols) so the structure is just a domain of elements; however, relations are defined over the domains during the course of the second-order EF-game. More specifically, the pebble first-order games are played over structures in $\mathcal{G}$.*

2.4 $\mathbf{DIV_k}, \overline{\mathbf{DIV_k}} \notin \mathbf{mon\Sigma_1^1(p, r)}$

Theorem 2.3. *$DIV_k \notin mon\Sigma_1^1(p, r)$ for any positive integers p and r.*

Proof. We will show that for large enough graphs $\mathcal{D}$ has a winning strategy in the $mon\Sigma_1^1(r, r)$-game. Fix $k \geq 2$. Assume m vertex colors. $\mathcal{D}$ starts by choosing a graph G such that $|G| \pmod{k} = 0$ and $|G| \geq mr$. $\mathcal{S}$ then colors the vertices of G using the given m colors. By the pigeonhole principle there must be at least r vertices having the same color $c \in \mathscr{C}$, let Γ be the set of all such vertices. $\mathcal{D}$ then chooses a graph $G' = (G \cup \{w\})$ with a new vertex w and does the following: (i) color $G \subseteq G'$ exactly as $\mathcal{S}$ did and (ii) color w with c. Let $\Gamma' = (\Gamma \cup \{w\})$. Now the first-order phase of the EF-game with r rounds. Assume the $(i+1)^{st}$ round of the game $(i + 1 \leq r)$ and assume $\langle u_1, \ldots, u_i \rangle \subseteq G$ and $\langle v_1, \ldots, v_i \rangle \subseteq G'$ have been chosen such that for every $1 \leq j \leq i$, u_j and v_j have exactly the same color. Assume $\mathcal{S}$ chooses $u_{i+1} \in G$. If $u_{i+1} \notin \Gamma$, then $\mathcal{D}$ responds with the corresponding vertex in G' $(\notin \Gamma')$. If $u_{i+1} \in \Gamma$ then

- if $u_{i+1} = u_j$ for some $j \leq i$, then $\mathcal{D}$ responds with v_j,
- otherwise $\mathcal{D}$ responds with an arbitrary $v_{i+1} \in \Gamma'$ that has not been chosen before, this is possible since $|\Gamma'| \geq r$.

The case when $\mathcal{S}$ chooses $v_{i+1} \in G'$ is symmetric. □

Theorem 2.4. *$\overline{DIV_k} \notin mon\Sigma_1^1(p, r)$ for any positive integers p and r.*

Proof. The proof is very similar to that of Theorem 2.3. $\mathcal{D}$ starts the game by choosing a graph G such that $|G| \pmod{k} \neq 0$ and $|G| \geq mr$. $\mathcal{S}$ does her coloring and then $\mathcal{D}$ responds by choosing a graph $G' = (G \cup W)$, where W is a new set of vertices such that $|G'| \pmod{k} = 0$. $\mathcal{D}$ colors all the vertices of W with c and let $\Gamma' = (\Gamma \cup W)$. The game then proceeds exactly as in Theorem 2.3. □

Corollary 2.1.

1. $DIV_k \notin mon\Pi^1_1$

2. $\overline{DIV_k} \notin mon\Pi^1_1$

Proof. Follows directly from Theorems 2.3 and 2.4. □

2.5 Game Types

The definition of game types given in this section is inspired by a similar one given in [20].

Definition 2.5 (Isomorphism types). *Let $u, v, w \in G \in \mathcal{G}$.*

1. *Define the* isomorphism type *of u in G as*

$$I(u; G) = \langle c, d \rangle, \qquad c \in \mathscr{C} \text{ and } d \in \mathscr{D} \tag{2.7}$$

where c is the color of u and d is the color of its self-edge.

2. *Define the* isomorphism type *of the pair u, v in G as*

$$I(u, v; G) = \langle I(u; G), I(v; G), d, eq(u, v) \rangle, \qquad d \in \mathscr{D} \tag{2.8}$$

where d is the color of the edge (u, v) and $eq(u, v)$ is true if they are the same vertex otherwise false.

3. *Define the* isomorphism type *of the triple u, v, w in G as*

$$\begin{aligned} I(u,v,w;G) = \langle & I(u;G), I(v;G), I(w;G), \\ & I(u,v;G), I(u,w;G), I(v,w;G), eq(u,v), eq(u,w), eq(v,w)\rangle \end{aligned} \tag{2.9}$$

Remark 2.2. *The isomorphism type of any set of vertices corresponds to the first-order quantifier-free type of these vertices in G over the empty set of parameters.*

Definition 2.6 (**Game types**)**.** *Let $u \in G \in \mathcal{G}$.*

1. *Define the* $(1,r)$-game type of u inside G *as*

$$\zeta_{1,r}(u;G) = I(u;G) \tag{2.10}$$

2. *Define the* $(2,r)$-game type of u inside G *inductively as*

$$\begin{aligned} &\zeta_{2,1}(u;G) = I(u;G) \\ &\zeta_{2,r}(u;G) = \langle I(u;G), \{\langle I(u,v;G), \zeta_{2,r-1}(v,G)\rangle : v \in G\}\rangle \end{aligned} \tag{2.11}$$

3. *Define the* $(3,r)$-game type of u inside G *inductively as*

$$\begin{aligned} &\zeta_{3,1}(u;G) = I(u;G) \\ &\zeta'_{3,1}(u,v;G) = I(u,v;G) \\ &\zeta'_{3,r}(u,v;G) = \langle I(u,v;G), \{\langle I(u,v,w;G), \zeta_{3,r-1}(w;G)\rangle : w \in G\}\rangle \\ &\zeta_{3,r}(u;G) = \big\langle I(u;G), \big\{\big\langle I(u,v;G), \zeta'_{3,r-1}(u,v;G), \zeta_{3,r-1}(v;G)\big\rangle : v \in G\big\}\big\rangle \end{aligned} \tag{2.12}$$

where ζ' is a helper function and can be thought of as the game type of edges.

4. *For every $1 \leq p \leq 3$ define the (p, r)*-game type *of G as*

$$\zeta_{p,r}(G) = \{\zeta_{p,r}(u; G) \colon u \in G\} \tag{2.13}$$

Remark 2.3. *The (p, r)-game type of a vertex u corresponds to the first-order type of u in G over the empty set of parameters where every formula in that type has at most p variables and has quantifier rank at most r.*

The intuition behind these definitions of isomorphism and game types is the following: given $G, G' \in \mathcal{G}_{m,n}$ and given $u \in G, v \in G'$ such that $\zeta_{p,r}(u; G) = \zeta_{p,r}(v; G')$, then $\mathcal{D}$ has a winning strategy in the r-round first-order game with p pebbles which starts by placing pebbles on u and v. One can see this by induction, as $\mathcal{D}$ can maintain the invariant that the corresponding pebbled vertices have always the same game type [20]. If furthermore we have the stronger assumption that $\zeta_{p,r}(G) = \zeta_{p,r}(G')$, then $\mathcal{D}$ can always win no matter how the game starts.

The following proposition from [20] states the relationship between game types and first-order expressibility.

Proposition 2.1. *Assume $G, G' \in \mathcal{G}_{m,n}$. Then $\zeta_{p,r}(G) = \zeta_{p,r}(G')$ if and only if for every first-order sentence $\sigma \in \mathcal{L}^p$ such that $qr(\sigma) \leq r$ it is the case that $G \models \sigma \iff G' \models \sigma$.*

Notation 2.3.

1. *We will omit the argument G from isomorphism types and game types when understood from the context.*

2. *Fix m and n for vertex and edge colors respectively. Let $\Lambda(p, r; G)$ denote the maximum number of possible (p, r)-game types of graphs in $\mathcal{G}_{m,n}$ and let $\Lambda(p, r; u)$ denote the maximum number of possible (p, r)-game types of vertices in such graphs.*

2.6 $\mathbf{DIV_k \notin bin\Sigma^1_1(1, r)}$ and $\mathbf{DIV_k \notin bin\Sigma^1_1(2, 2)}$

We show that $DIV_k \notin bin\Sigma^1_1(1, r)$ and $DIV_k \notin bin\Sigma^1_1(2, 2)$ by looking at the $(1, r)$- and $(2, 2)$-game types of graphs in $\mathcal{G}$.

Lemma 2.1. *Assume m vertex colors and n edge colors. Then $\Lambda(1, r; u) \leq mn$ and $\Lambda(1, r; G) \leq 2^{mn}$.*

Proof. Assume some vertex u. From Definition 2.6 we need only to count the number of isomorphism types of u which is at most mn. Since the game type of any $G \in \mathcal{G}_{m,n}$ is determined by the game types of its single vertices, then $\Lambda(1, r; G) \leq 2^{mn}$ (counting all possible subsets of game types of single vertices). □

Lemma 2.2. *Let $G \in \mathcal{G}_{m,n}$. Then there exists $G' \in \mathcal{G}_{m,n}$ such that $|G'| = |G| + 1$ and $\zeta_{1,r}(G') = \zeta_{1,r}(G)$.*

Proof. Choose an arbitrary $u \in G$. Add to G a new vertex v, color it and its self-edge exactly as u's, and color its edges to the vertices of G arbitrarily. Let G' be the new graph. Clearly, $\zeta_{1,r}(G') = \zeta_{1,r}(G)$. □

As a direct consequence of this lemma and Proposition 2.1 we have the following inexpressibility result.

Theorem 2.5. *$DIV_k \notin bin\Sigma^1_1(1,r)$*

Next we consider $(2,2)$-game types.

Lemma 2.3. *Assume m vertex colors and n edge colors. Then $\Lambda(2,2;u) \leq (mn)2^{(mn^2)}$ and $\Lambda(2,2;G) \leq 2^{\Lambda(2,2;u)}$.*

Proof. Given a vertex u, the $(2,2)$-game type of u is determined by: (i) its isomorphism type, (ii) the isomorphism type of any other vertex v, and (iii) the isomorphism type of the edge (u,v). There are (mn) possible vertex and self-edge colors for u, (mn) vertex and self-edge colors for v, and n possible colors for the edge (u,v). Hence there are at most a total of (mn^2) possible combinations of colors for v and (u,v) of which there are at most 2^{mn^2} possible subsets that can be associated with u. Therefore, $\Lambda(2,2;u) \leq (mn)2^{mn^2}$. As mentioned above the game type of any $G \in \mathcal{G}_{m,n}$ is determined by the set of game types of its single vertices, hence $\Lambda(2,2;G) \leq 2^{\Lambda(2,2;u)}$. □

Lemma 2.4. *Let $G \in \mathcal{G}_{m,n}$. Assume $|G| > \Lambda(2,2;u)$. Then there exists $G' \in \mathcal{G}_{m,n}$ such that $|G'| = |G| + 1$ and $\zeta_{2,2}(G') = \zeta_{2,2}(G)$.*

Proof. From Lemma 2.3, there must be $u_1, u_2 \in G$ that have the same $(2,2)$-game type. Add to G a new vertex v, color it and its self-edge exactly as u_1. Connect v to every vertex in G. For every $w \in G$ such that $w \neq u_1$, use the color of the edge (u_1, w) to color the edge (v, w). Use the color of the edge (u_1, u_2) to color (v, u_1). Let G' be the new graph. It is easy to check that $\zeta_{2,2}(v; G') = \zeta_{2,2}(u_1; G)$ and for every $w \in G$, $\zeta_{2,2}(w; G) = \zeta_{2,2}(w; G')$. Hence, $\zeta_{2,2}(G') = \zeta_{2,2}(G)$. □

As a direct consequence of this lemma we have the following inexpressibility result.

Theorem 2.6. *$DIV_k \notin bin\Sigma^1_1(2,2)$*

2.7 $\mathbf{DIV_k \notin bin\Sigma^1_1(2,3)}$

We show that $DIV_k \notin bin\Sigma^1_1(2,3)$ by looking at the $(2,3)$-game types of graphs in $\mathcal{G}$.

Remark 2.4. *Assume $G \in \mathcal{G}$ and let $u \in G$. Then $\zeta_{2,3}(u;G)$ can be characterized by the set of all paths in G of length 2 starting from u. This includes paths of the form uvu (going from u to v then back to u). Actually as we will see below these latter kind of paths is the main reason for the inexpressibility in $bin\Sigma^1_1(2,3)$. Given one such path uvw (two or all vertices may be identical) we will represent it by the tuple*

$$t = (c_1c_2c_3, d_1d_2d_3, e_1e_2)$$

where the first triple represents the colors of the vertices $u, v,$ and w respectively, the second triple represents the colors of their self-edges, and the last pair represents the colors of the edges uv and vw respectively. In the following discussion the $(2,3)$-game type of a single vertex u will be taken to be the collection of all possible such tuples. So we can say things like $t \in \zeta_{2,3}(u)$. Sometimes we will need to ignore the vertex and self-edge colors when they do not play any role in the discussion. In such cases we consider $t = (e_1e_2) \in \zeta_{2,3}(u)$.

Lemma 2.5. *Assume m vertex colors and n edge colors. Then* $\Lambda(2,3;u) \leq (mn)2^{n\Lambda(2,2;u)}$ *and* $\Lambda(2,3;G) \leq 2^{\Lambda(2,3;u)}$.

Proof. Given the recursive nature of the definition of game types, the $(2,3)$-game type of a single vertex u is determined by (i) its isomorphism type which is represented by the first multiplicand (mn) and (ii) all possible combinations of the pairs: $\langle$the isomorphism type of (u,v), the $(2,2)$-game type of v $\rangle$ for every vertex $v \in G$. There are $n\Lambda(2,2;u)$ such pairs (excluding the isomorphism type of u for it is already counted in (i) and the isomorphism type of v for it is already counted in $\Lambda(2,2;u)$), hence all possible subsets of such pairs is given by the multiplicand $2^{n\Lambda(2,2;u)}$. The upper bound on $\Lambda(2,3;G)$ is clear. □

Lemma 2.6. *Let $G \in \mathcal{G}_{m,n}$. Assume $|G| > \Lambda(2,3;u)$. Then there exists $G' \in \mathcal{G}_{m,n}$ such that $|G'| = |G| + 1$ and $\zeta_{2,3}(G') = \zeta_{2,3}(G)$.*

Proof. By Lemma 2.5 there must be two vertices $u_1, u_2 \in G$ such that $\zeta_{2,3}(u_1) = \zeta_{2,3}(u_2) = \gamma$. Add a new vertex v to G. Color v and its self-edge exactly as u_1's. Connect v to every other vertex in G. For every $w \in G$ such that $w \neq u_1$, use the color of the edge (u_1, w) to color the edge (v, w). Finally, use the color of (u_1, u_2) to color (v, u_1). Let G' be the newly constructed graph. As already mentioned in Remark 2.4, for every edge emanating from u_1 of color e it must be the case that $(ee) \in \zeta_{2,3}(u_1; G)$. This corresponds to putting the first pebble p_1 on u_1, the second p_2 on v, where (u_1, v) has color e, and then removing p_1 and reinserting it onto u_1. Another way through which (ee) can be in $\zeta_{2,3}(u_1; G)$ is that there is a path in G of distinct vertices u_1ww' of color ee. Actually the addition of v as done above will create these latter monochromatic paths starting from v for every color e of an edge emanating from v. Such monochromatic paths of distinct vertices that start from u_1 may not exist, however, u_1 can not be distinguished from v using them since there are only two pebbles, hence $\zeta_{2,3}(u_1;G) = \zeta_{2,3}(u_1;G') = \zeta_{2,3}(v;G')$. It is also obvious that for any other $w \in G$, it is maintained that $\zeta_{2,3}(w;G) = \zeta_{2,3}(w;G')$. Hence, $\zeta_{2,3}(G') = \zeta_{2,3}(G)$. □

As a direct consequence of this lemma we have the following inexpressibility result.

Theorem 2.7. *$DIV_k \notin bin\Sigma_1^1(2,3)$*

2.8 $\mathbf{DIV_k \in bin\Sigma_1^1(3,3)}$

In this section we show that $DIV_k \in bin\Sigma_1^1(3,3)$ by looking at the $(3,3)$-game types of graphs in $\mathcal{G}$. From the proofs one could extract out the actual defining sentence. We will do this in the case of $k = 2$.

Remark 2.5. *Assume $G \in \mathcal{G}$ and let $u \in G$. Then $\zeta_{3,3}(u;G)$ can be characterized by the set of all paths in G of length 2 starting from u. Given one such path uvw we will represent it by the tuple*

$$t = (c_1c_2c_3, d_1d_2d_3, e_1e_2, \neg eq(u,w))$$

where the first triple represents the colors of the vertices u, v, w respectively, the second triple represents the colors of their self-edges, e_1e_2 represents the colors of the edges uv, and vw respectively, and finally $\neg eq(u,w)$ represents the truth value of *whether u and w are not identical, it is assigned either t for true or f for false. Notice that the existence of three pebbles enables the spoiler to overcome the problem raised in the proof of Lemma 2.6 and caused her to lose the EF game, namely the inability to distinguish between monochromatic paths of the form uvu and monochromatic paths of the form uvw where $u \neq w$. Actually, as we will see below, this distinction is the main reason for successful expressibility of DIV_k in $bin\Sigma_1^1(3,3)$.*

Definition 2.7 (**Symmetric game types**). *Let γ be a $(3,3)$-game type of a vertex $u \in G \in \mathcal{G}_{m,n}$. Let $\mathscr{C}$ be the set of m vertex colors and let $\mathscr{D}$ be the set of n edge colors. Assume $k \leq n$.*

1. *γ is called* k-symmetric *if the following hold:*
   (a) *there exist $c \in \mathscr{C}$ and $d \in \mathscr{D}$ such that if $(c_1c_2c_3, d_1d_2d_3, e_1e_2, *) \in \gamma$, ($*$ means 'do not care') then $c_1 = c_2 = c_3 = c$ and $d_1 = d_2 = d_3 = d$ (so γ is monochromatic with respect to the vertex and self-edge colors)*
   (b) *there exists $D \subseteq \mathscr{D}$ such that $|D| = k$ and for all distinct $e, e' \in \mathscr{D}$, $(ccc, ddd, ee', t), (ccc, ddd, e'e, t) \in \gamma$*
   (c) *if $(ccc, ddd, ee', t), (ccc, ddd, e'e, t) \in \gamma$ and $e \neq e'$ then it must be the case that $e, e' \in D$*
2. *γ is called* fully symmetric *if γ is n-symmetric.*
3. *A graph $G \in \mathcal{G}_{m,n}$ is called k-symmetric if all vertices in G have the same $(3,3)$-game type γ where γ is k-symmetric.*

Notation 2.4. *Most often in the following discussion we will only consider game types $\zeta_{3,3}(u)$ that are monochromatic with respect to the vertex and self-edge colors and/or be concerned only with paths of length 2 of distinct vertices starting from u. For simplicity in such cases, $\zeta_{3,3}(u)$ will be viewed as the collection of pairs (dd') that represent the colors along the path of length 2 starting from u.*

Let G be a graph. Let $\Delta(G)$ denote the maximum degree of G and let $\chi'(G)$ denote its edge chromatic number. The following theorem gives bounds for χ'.

Theorem 2.8 (Vizing 1964, p.119 in [5])**.**

$$\Delta(G) \leq \chi'(G) \leq \Delta(G) + 1$$

Vizing's theorem divides the finite graphs into two classes based on their edge chromatic number. Those with $\chi' = \Delta$ are called *class I*, and those with $\chi' = \Delta + 1$ are called *class II* [5]. The following lemma applies this classification to complete graphs.

Lemma 2.7 (Theorem 4.1 in [10])**.** *Consider the complete graph K_n. If n is even, then it is class I, otherwise it is class II.*

Lemma 2.8. *Let $G \in \mathcal{G}_{m,n}$ be fully symmetric of minimum size k. Then $n + 1 \leq k \leq n + 2$.*

Proof. Since there are n distinct colors, then $k \geq n + 1$. If n is odd, then let $k = n + 1$. Since k is even, then by Lemma 2.7 we have $\chi'(K_{n+1}) = n$. If n is even, let $k = n+2$. Again by Lemma 2.7, $\chi'(K_{n+2}) = n+1$. Add a new color c' to the list of given n colors and use the new list to get a proper edge coloring of K_{n+2}. Choose a color c arbitrarily from the original list, and for every edge of color c' change its color to c. □

Remark 2.6. *Let $G \in \mathcal{G}_{m,n}$ be fully symmetric. Let $\gamma = \zeta_{3,3}(u)$ for any $u \in G$. Let $d \in \mathscr{D}$ and assume that $(dd) \notin \gamma$. Then it must be the case that $|G| \pmod 2 = 0$. Otherwise either there exists some $u \in G$ with two edges incident on it of color d, hence $(dd) \in \gamma$ which contradicts the assumption or u has no edge incident on it of color d which contradicts the definition of G being fully symmetric.*

Lemma 2.9. *Let k be an even positive integer. Then there exist a pair of positive integers (m, n) and a $(3,3)$-game type Γ for graphs such that for any $G \in \mathcal{G}_{m,n}$ the following holds: $\zeta_{3,3}(G) = \Gamma$ implies that $|G| = bk$ for some integer $b \geq 1$.*

Proof. We will build Γ to be monochromatic with respect to the vertex color and the self-edge color, hence $m = 1$. Let d be the self-edge color. Assume $k = 2j$. Construct symmetric vertex game types $\gamma_0, \ldots, \gamma_{j-1}$ such that $\gamma_i = \{(d_{\gamma_i}, d), (d, d_{\gamma_i}), (d, d)\}$ where $d_{\gamma_i} \neq d$ and is unique for every $i < j$ (each pair in γ_i represents the colors of some path of length 2 starting from the vertex). Let $D = \{d_{i,i+1 \pmod j} : i < j\}$ be a collection of colors such that: (i) if $j = 1$, then $d_{0,0} = d$ and D will just represent the color of self-edges, (ii) if $j = 2$, then $d_{0,1} = d_{1,0}$, and (iii) if $j \geq 2$, then $d \notin D$ and $d_{\gamma_i} \notin D$ for every i.

For every $i < j$, let H_i be a 2-symmetric graph such that (i) for every $u \in H_i$, $\zeta_{3,3}(u) = \gamma_i$, hence $|H_i|$ must be even since $(d_{\gamma_i}, d_{\gamma_i}) \notin \gamma_i$ (see Remark 2.6) and (ii) for every i, i', $|H_i| = |H_{i'}|$. Connect all the graphs H_i's and let H denote the resulting graph. For every i and for every $u \in H_i$ choose a unique $v_u \in H_{(i+1) \pmod j}$ and use

$d_{i,(i+1) \pmod j}$ to color the edge (u, v_u) (in case $j = 1$, then $H = H_0$ and $v_u = u$ and this is just coloring the self-edge of u). For all the remaining uncolored edges use d to color them. Hence for any $i < j$, we have $(d_{i,(i+1) \pmod j}, d_{i,(i+1) \pmod j}) \notin \zeta_{3,3}(u; H)$ for any $u \in H$.

We can easily notice that: (i) for every i, all vertices of the subgraph H_i have the same $(3, 3)$-game type inside H, let δ_i denote this type, (ii) δ_i is an extension of γ_i, (iii) for all distinct i, i', we have $\delta_i \neq \delta_{i'}$ ($\delta_i \Delta \delta_{i'} \supseteq \{(d_{\gamma_i}, d), (d_{\gamma_{i'}}, d)\}$), and (iv) each δ_i is 2-symmetric with respect to the two colors d_{γ_i} and d. Let $n = |\{d_{\gamma_i} \colon i < j\}| + |\{d_{i,(i+1) \pmod j} \colon i < j\}| + 1 = 2j + 1$ (the last 1 is for the color d). Let $\Gamma = \{\delta_i \colon i < j\}$.

Let $G \in \mathcal{G}_{m,n}$ such that $\zeta_{3,3}(G) = \Gamma$. Each $\gamma_i \subseteq \delta_i$, which represents the 2-symmetric part of δ_i, must be realized inside G by a subgraph H_i such that $|H_i| \pmod 2 = 0$. Notice that for every $i, i' < j$, $(d_{i,(i+1) \pmod j}, d_{i,(i+1) \pmod j}) \notin \delta_{i'}$, hence all $H_i's$ must have the same size (the edges $d_{i,(i+1) \pmod j}$ may be thought of as creating one-to-one maps between the H_i's so they are forced to have the same size). Therefore, $|G| = 2bj = bk$ for some positive integer b. So $(1, 2j + 1) = (1, k + 1)$ and Γ satisfy the conclusion of the lemma. □

From this lemma we can immediately derive the following expressibility result.

Theorem 2.9. *Let k be an even positive integer. Then $DIV_k \in bin\Sigma^1_1(3, 3)$. More specifically, DIV_k can be expressed by a sentence of the following form*

$$\exists R_1 \ldots \exists R_l \varphi$$

where φ is a first-order sentence with 3 first-order variables and quantifier depth 3.

Each R_i is a binary second-order variable and $l \leq \lceil \log_4 (k+1) \rceil$.

Proof. Let Γ be the game type obtained in Lemma 2.9. We will show that $\mathcal{S}$ has a winning strategy in the $bin\Sigma_1^1(3,3)$ game over the class of structures of cardinalities divisible by k. Assume $\mathcal{D}$ starts the game by choosing a structure $\mathcal{A}$ such that $|A| \pmod{k} = 0$. Let $\mathcal{S}$ colors $\mathcal{A}$ to get a graph $G \in \mathcal{G}$ such that $\zeta_{3,3}(G) = \Gamma$. $\mathcal{D}$ has then two possible responses: (i) choosing a structure $\mathcal{B}$ and coloring it to obtain $G' \in \mathcal{G}$ such that $\zeta_{3,3}(G') = \Gamma$, but then by Lemma 2.9 it must be the case that $|G'| \pmod{k} = 0$ and hence $\mathcal{D}$ loses the game at its second-order phase or (ii) choosing a structure $\mathcal{B}$ such that $|B| \pmod{k} \neq 0$ and color it to obtain $G' \in \mathcal{G}$ with $\zeta_{3,3}(G') = \Gamma'$ but again by Lemma 2.9 it must be the case that $\Gamma \neq \Gamma'$ hence by Proposition 2.1, $\mathcal{D}$ loses the game at its first-order phase. So in any case $\mathcal{S}$ wins the game, hence $DIV_k \in bin\Sigma_1^1(3,3)$. The upper bound for l is obtained from the value of n derived in the proof of Lemma 2.9 and by realizing that each binary second-order variable contributes exactly 4 new colors. □

In the introduction we gave a sentence that defines DIV_2. In the following example we will use the proof of Lemma 2.9 to show how this sentence can be derived systematically.

Example 2.2. *Consider divisibility by 2, call this problem $EVEN$. We need two edge colors d_1 and d_2 and one vertex color c. In the second-order phase of the EF game, $\mathcal{D}$ will first choose G_1 which is just a set of unconnected vertices with $|G_1| \pmod{2} = 0$. $\mathcal{S}$ will then convert G into a complete graph with all self-edges, let G_1' denote the new graph. $\mathcal{S}$ colors G_1' as follows: (i) use c to color all the vertices, (ii)* *use d_1 to color all the self-edges, (iii) for every distinct pair of vertices $u_i, v_i \in G'_1$, use d_2 to color the edge (u_i, v_i), and (iv) use d_1 to color all the remaining edges. This coloring implies that every $u \in G'_1$ has exactly one edge of color d_2 incident on it, hence d_2 corresponds to d_{γ_i} in the proof of Lemma 2.9. G'_1 can be viewed as a 1-regular graph (a graph with isolated edges) by looking exclusively at the edges of color d_2. It can be easily checked that all the vertices in G'_1 have the same game type $\gamma \supseteq \{(d_1d_2, t), (d_2d_1, t), (d_1d_1, t)\}$ (ignoring the vertex and self-edge colors and considering only paths of length 2 with distinct vertices). Next $\mathcal{D}$ chooses a set of unconnected vertices G_2 with $|G_2| \pmod 2 = 1$. $\mathcal{D}$ converts G_2 into G'_2, a complete graph with all self-edges, and then tries to color it so as to have the same $(3,3)$-game type as G'_1. Since $(d_2d_2) \notin \gamma$, then by Remark 2.6, this is impossible, in other words G'_2 can not be converted into a 1-regular graph. There must exist some vertex $u \in G'_2$ such that either $(d_2d_2) \in \zeta_{3,3}(u; G'_2)$ or $(d_2d_1) \notin \zeta_{3,3}(u; G'_2)$. Hence, $\mathcal{S}$ can win the first-order phase of the game by playing the differentiating path using her 3 pebbles. In the following we construct a sentence $\sigma \in bin\Sigma^1_1(3,3)$ that defines EVEN*

$\varphi_1(R) \overset{def}{=} \forall x \neg R(x,x)$ *coloring the self-edges of G'_1 with c*

$\varphi_2(R) \overset{def}{=} \forall x \forall y\, (R(x,y) \longleftrightarrow R(y,x))$ *G'_1 is undirected*

$\varphi_3(R) \overset{def}{=} \forall x \exists y\, (R(x,y) \wedge \forall z\, (R(x,z) \longrightarrow z = y))$ *the d_2 coloring of edges in G'_1*

$$\sigma \overset{def}{=} \exists R\, (\varphi_1(R) \wedge \varphi_2(R) \wedge \varphi_3(R)) \tag{2.14}$$

Remark 2.7. *From Example 2.2, it is clear that 1-regular graphs can be used to characterize divisibility by 2. This observation can only be locally generalized for divisibility by even numbers greater than 2 to characterize the evenness of the sub-*

graphs H_i's constructed in the proof of Lemma 2.9. However, across different H_i's this becomes no longer valid in our construction since each H_i has its own unique color d_{γ_i}.

Next we turn to expressibility of divisibility by odd numbers.

Lemma 2.10. *Let $k \neq 1$ be an odd positive integer. Then there exist a pair of positive integers (m, n) and a $(3,3)$-game type Γ for graphs such that for any $G \in \mathcal{G}_{m,n}$ the following holds: $\zeta_{3,3}(G) = \Gamma$ implies that $|G| = bk$ for some integer $b \geq 1$.*

Proof. We will build Γ to be monochromatic with respect to the vertex color and the self-edge color, hence $m = 1$. Assume $k = 2j + 1$ for $j \geq 1$. Let Γ' be the game type Γ constructed in the proof of Lemma 2.9. Let $H \in \mathcal{G}_{m,n}$ be the graph constructed in the proof of Lemma 2.9 such that H is constructed exactly from the subgraphs $H_0, \dots, H_{j-1}$ with $|H_i| = 2b$ for some positive integer b.

Let $u_0, \dots, u_{b-1}$ be new vertices, connect them together and to every vertex in H. Use d to color all the edges between the u_i's. For each $i < j$ choose an arbitrary set of vertices V_i such that (i) $V_i \subseteq H_i$, (ii) $|V_i| = b$, and (iii) for every $w, w' \in V_i$, the edge (w, w') is colored d. For every $i < j$ and for every $i' < b$, choose a unique $w_{u_{i'}} \in V_i$, and use $d_{\gamma_{(i+1) \pmod j}}$ to color the edge $(u_{i'}, w_{u_{i'}})$. Use d to color the remaining uncolored edges from the u_i's to H. Call the new graph H' and notice that $H' \in \mathcal{G}_{m,n}$ where $n = 2j + 1$ is the number of colors used to color the edges of H'.

Notice the following: (i) for each color d_{γ_i}, u_i has an edge of that color incident on it, (ii) all the u_i's have the same $(3,3)$-game type inside H', let ρ denote that game type, (iii) $(d_{\gamma_i}, d_{\gamma_i}) \notin \rho$ for every $i < j$, however, $(d_{\gamma_i}, d_{\gamma_{(i+1) \pmod j}}) \in \rho$, and (iv) $(d, d) \in \rho$. Now look at the new emerging game types inside H'. For every $i < j$, δ_i no longer exists, but is broken into two new game types: (i) δ_i^0 which is the game type of every vertex in V_i and (ii) δ_i^1 which is the game type of every vertex in $H_i \backslash V_i$. Each vertex u_i has the new game type ρ. An important observation is that for every $u \in H'$, $(d_{\gamma_i}, d_{\gamma_i}) \notin \zeta_{3,3}(u)$ for every $i < j$. Let

$$\Gamma = \{\delta_i^0 \colon i < j\} \cup \{\delta_i^1 \colon i < j\} \cup \{\rho\}$$

Let $G \in \mathcal{G}_{m,n}$ be such that $\zeta_{3,3}(G) = \Gamma$. Notice that for every vertex $v \in G$ with $\zeta_{3,3}(v) = \delta_i^0$, there must exist exactly one vertex w_v such that $\zeta_{3,3}(w_v) = \delta_i^1$ and the edge (v, w_v) is colored d_{γ_i}. The converse also holds for vertices of game type δ_i^1. Hence there is a one-to-one correspondence between $\{u \in G \colon \zeta_{3,3}(u) = \delta_i^0\}$ and $\{u \in G \colon \zeta_{3,3}(u) = \delta_i^1\}$, therefore $|\{u \in G \colon \zeta_{3,3}(u) = \delta_i^0 \textit{ or } \zeta_{3,3}(u) = \delta_i^1\}| = 2b'$ for some positive integer $b' \geq 1$. Let W_i denote this last set of vertices. Similarly, we can show that (see also the proof of Lemma 2.9) there is a one-to-one correspondence between W_i and $W_{i'}$ for all $i, i' < j$. Hence, $|\bigcup\{W_i \colon i < j\}| = 2b'j$. Then any $u \in G \backslash \bigcup\{W_i \colon i < j\}$ must be of game type ρ.

Let $T_i = \{u \in G \colon \zeta_{3,3}(u) = \delta_i^0\}$. Note that all the T_i's must have the same size. Let $P = \{u \in G \colon \zeta_{3,3}(u) = \rho\}$. From the construction of H' it must be the case that every $u \in T_i$ uniquely determines a distinct $v_u \in P$ such that (u, v_u) is colored $d_{\gamma_{(i+1) \pmod j}}$ (since $(d_{\gamma_{(i+1) \pmod j}}, d_{\gamma_{(i+1) \pmod j}}) \notin \delta_i^0$). Hence $|T_i| \leq |P|$. Similarly, every $v \in P$ uniquely determines a vertex $w_v \in T_i$ such that (v, w_v) is colored $d_{\gamma_{(i+1) \pmod j}}$ (since $(d_{\gamma_{(i+1) \pmod j}}, d_{\gamma_{(i+1) \pmod j}}) \notin \rho$). Hence $|P| \leq |T_i|$. Therefore,

$|P| = |T_i| = b'$. Now we count the number of vertices in G. $|G| = |\bigcup\{W_i \colon i < j\}| + |P| = 2b'j + b' = b'(2j+1) = b'k$. Hence, $(1, 2j+1) = (1, k)$ and Γ are as desired. $\square$

From Lemmas 2.9 and 2.10 we can derive the following general result.

Lemma 2.11. *Fix a positive integer $k \neq 1$. Let $m = 1$ and $n = k+1$. Then there exits a $(3,3)$-game type Γ for graphs in $\mathcal{G}_{m,n}$ such that for any $G \in \mathcal{G}_{m,n}$ the following holds: $\zeta_{3,3}(G) = \Gamma$ implies that $|G| = bk$ for some integer $b \geq 1$.*

This directly implies the following expressibility result.

Theorem 2.10. *Let $k \neq 1$ be a positive integer. Then $DIV_k \in bin\Sigma_1^1(3,3)$. More specifically, DIV_k can be expressed by a sentence of the following form*

$$\exists R_1 \ldots \exists R_l \varphi$$

where φ is a first-order sentence with 3 first-order variables and quantifier depth 3. Each R_i is a binary second-order variable and $l \leq \lceil \log_4 (k+1) \rceil$.

Proof. Similar to the proof of Theorem 2.9. $\square$

Corollary 2.2. $mon\Sigma_1^1 \subset bin\Sigma_1^1$

Proof. This follows directly from the inexpressibility result in Theorem 2.3 and the expressibility result in Theorem 2.10. $\square$

Lemma 2.12. *Let l_1, l_2 be two non-negative integers. Define $\Theta \subseteq bin\Sigma_1^1(3,3)$ that consists exactly of sentences that have at most l_1, l_2 unary and binary second-order variables respectively. Then $DIV_k \in \Theta$ for only finitely many k.*

Proof. Let m, n be the corresponding vertex and edge colors respectively. There are at most finitely many $(3,3)$-game types for graphs in $\mathcal{G}_{m,n}$. Assume the conclusion does not hold, then there are two distinct positive integers k_1, k_2 that can be distinguished by the same $(3,3)$-game type. But this implies that $\mathcal{D}$ can win the $bin\Sigma_1^1(3,3)$ game by choosing a structure of cardinality k such that exactly one of k_1 and k_2 is a factor of k. This is a contradiction. □

Theorem 2.10 and Lemma 2.12 imply that DIV_k creates a proper hierarchy into $bin\Sigma_1^1(3,3)$.

2.9 Bounding the Binary Relation Variables

The following theorem gives an inexpressibility result for DIV_k in $bin\Sigma_1^1$ when the sizes of the interpretations of the binary relation variables are bounded.

Theorem 2.11. *Let $\sigma \in bin\Sigma_1^1$ be of the following form*

$$\exists R_1^{\leq f(l)} \dots \exists R_t^{\leq f(l)} \exists S_1 \dots \exists S_s \varphi$$

where $f(l) < \frac{l}{2t} - \frac{r2^s}{2t}$, where l is the size of any structure that models this sentence and r is the quantifier depth of φ. Then DIV_k can not be expressed by σ.

Proof. We show $\mathcal{D}$ has a winning strategy in the second-order EF game with r rounds in the first-order phase (assume the number of pebbles $p = r$). $\mathcal{D}$ starts by choosing a complete uncolored graph G with all self-edges such that

$$|G| \pmod{k} = 0 \tag{2.15}$$

$$|G| > r2^s + 2tf(|G|) \tag{2.16}$$

There are a total of $m = 2^s$ vertex colors. For the edges it is easier to directly handle each R_i separately than to consider the colors resulting from their combinations. $\mathcal{S}$ does the following with G: (i) color the vertices using the given m colors and (ii) construct the edge sets $E_1, \ldots, E_t$ among the vertices of G such that $|E_i| \leq f(|G|)$ for each i. From 2.16, there must be at least $r2^s$ vertices with degree 0, that is there is no edge from any of the E_i's that is incident on any of these vertices. Then by the pigeonhole principle there must be at least r of those vertices that are monochromatic, let their color be c. Let Γ be the collection of vertices in G that are colored c and with degree 0, then $|\Gamma| \geq r$. In order for the inequality in 2.16 to make sense it must be the case that $f(|G|) < \frac{|G|}{2t} - \frac{r2^s}{2t}$ as given in the theorem hypothesis. $\mathcal{D}$ then chooses a graph $G' = (G \cup \{w\})$ with a new vertex w and does the following: (i) color the vertices of $G \subseteq G'$ exactly as $\mathcal{S}$ did, (ii) color w with c, (iii) construct the edge sets $E_1, \ldots, E_t$ among the vertices of $G \subseteq G'$ exactly as $\mathcal{S}$ did, and (iv) leave the vertex w unconnected to any other vertex. In the first-order phase of the game $\mathcal{D}$ can win by following a similar strategy to that described in the proof of Theorem 2.3. □

2.10 Conclusion and Future Work

In this chapter we have provided a partial framework for the study of expressibility in Σ_1^1 which exactly captures the complexity class NP. This framework uses interesting combinatorics based on second-order EF-games and the notion of game types. We have studied the expressibility of DIV_k in different sublogics of Σ_1^1 getting inexpressibility results until expressibility is obtained inside $bin\Sigma_1^1(3,3)$. Based on k, DIV_k creates a proper hierarchy inside this sublogic. In the future we plan to pursue research in the following points:

1. Finding tight lower/upper bounds for the DIV_k hierarchy in $bin\Sigma_1^1(3,3)$. This is mainly a combinatorial problem and helps understanding game types specially for future plans when using second-order variables with higher arities.

2. Study the expressibility of $\overline{DIV_k}$ in $bin\Sigma_1^1(3,3)$.

3. Study natural extensions of $bin\Sigma_1^1(3,3)$ inside Σ_1^1 within the framework developed above. The parameters (logical resources) used in the abovementioned research, and hence in future extensions, are the following: (i) the arity of the second-order variables, (ii) the second-order quantifier depth, (iii) the number of first-order variables, and (iv) the first-order quantifier depth. Other parameters may also be studied such as the number of alternations of first-order quantifiers and also parameters that arise from the interleaving of first- and second-order quantifiers such as depth and alternation, however, this may require a dramatic change in the rules of the EF games. we plan to use number-theoretic properties for the study of expressibility such as primeness, number and sizes of equivalence classes of a definable equivalence relation, whether two definable subsets of a structure form an amicable number, etc. The main goals of this study are: (i) create proper hierarchies into sublogics of Σ_1^1 and into Σ_1^1 itself, hence giving more insight into NP and (ii) the study of expressibility of some interesting number-theoretic properties for its own sake.

4. Extending the above to Π_1^1 and the whole of second-order logic, hence essentially looking into the whole polynomial hierarchy.

Chapter 3

Descriptive Complexity of Finite Abelian Groups

We investigate the descriptive complexity of finite abelian groups. Using Ehrenfeucht-Fraïssé games we find upper and lower bounds on quantifier depth, quantifier alternations, and number of variables of a first-order sentence that distinguishes two finite abelian groups. Our main results are the following. Let G_1 and G_2 be a pair of non-isomorphic finite abelian groups, and let m be a number that divides one of the two groups' orders. Then the following hold: (1) there exists a first-order sentence φ that distinguishes G_1 and G_2 such that φ is existential, has quantifier depth $O(\log m)$, and has at most 5 variables and (2) if φ is a sentence that distinguishes G_1 and G_2 then φ must have quantifier depth $\Omega(\log m)$. These results are applied to (1) get bounds on the first-order distinguishability of dihedral groups, (2) to prove that on the class of finite groups both cyclicity and the closure of a single element are not first-order definable, and (3) give a different proof for the first-order undefinability of simplicity, nilpotency, and the normal closure of a single element on the class of finite groups (their undefinability were shown by A. Koponen and K. Luosto in an unpublished paper).

3.1 Introduction

In this chapter we investigate the descriptive complexity of finite abelian groups. Descriptive complexity is that branch of complexity theory that views the hardness of problems in terms of the complexity of their logical expressiveness such as the number of object variables, quantifier depth, type, and alternation, and sentences length (finite/infinite).

To the author's best knowledge there has been no work exploring the quantitative bounds on the logical resources needed for distinguishing finite groups. However, definability of some group theoretic notions have been studied before: simplicity ([14, 19, 9, 28]), nilpotency [19, 4], solvability [4, 19, 29], and the normal closure of a single element [19].

All of the results mentioned above use the following vocabulary for groups, as will we.

Definition 3.1. *Let $\mathcal{L}_G$ be a first-order language whose vocabulary contains the ternary relation symbol R (for the group operation) and the constant symbol e (for the group identity). Equality is considered as a logical symbol.*

We study the distinguishability of non-isomorphic finite abelian groups. Our main results are the following. Let G_1 and G_2 be a pair of non-isomorphic finite abelian groups, then there exists a number m that divides the order of one of the two groups (in the particular case of cyclic groups m would be the smallest divisor of exactly one of the two groups orders) such that

1. There exists a first-order sentence φ that distinguishes G_1 and G_2 (that is,

true on one and false on the other) such that φ is existential, has quantifier depth $O(\log m)$, and has at most 5 variables.

2. If φ is a sentence that distinguishes G_1 and G_2, then φ must have quantifier depth $\Omega(\log m)$.

We will apply these results to:

1. get bounds on the first-order distinguishability of dihedral groups exploiting the close relationship between elementary equivalence of groups of residues and elementary equivalence of dihedral groups,
2. show the first-order undefinability of the closure of a single element over the class of finite groups, and
3. show the first-order undefinability of cyclicity.

First-order undefinability on the class of finite groups of simplicity, nilpotency, and the normal closure of an element have been proved in [19]. However, the proofs use model-theoretic techniques that may not be accessible to many people. We will give simpler proofs for the same results using the distinguishability bounds obtained for finite abelian groups.

The basic tool used in our analysis is *Ehrenfeucht-Fraïssé* (*EF*) games. It is a game-theoretic characterization of expressibility in first-order logic. In our context the game is played over two groups for a finite number of rounds between two players, one of them is called the *spoiler* whose aim is to break the similarity between the two groups and the *duplicator* whose aim is to emphasize the similarity between them.

If the spoiler has a winning strategy, then a first-order sentence that distinguishes the two groups can be derived from this strategy as will be seen below.

Section 2 introduces EF games, defines them formally and shows their relation to first-order definability. Basic group- and game-theoretic definitions and examples are given in Section 3. In Section 4, EF games are applied to the groups $\mathbb{Z}_p$ and $\mathbb{Z}_q$ for prime numbers p and q to find bounds on the quantifier depth of a distinguishing first-order sentence. In Section 5, an extended version of EF games (using pebbles) is applied to the same groups to find bounds on the number of variables in a distinguishing first-order sentence. In Section 6, the game is applied to groups modulo any number. In Section 7 bounds are obtained for any finite abelian groups. In Section 8 we use the above bounds to get definability results on the following group-theoretic notions: cyclicity, simplicity, nilpotency, the closure of a single element, and dihedral groups. In Section 9 we state some of the open problems to look at.

3.2 Ehrenfeucht-Fraïssé Games

As described above EF games are used as a tool to get upper and/or lower bounds on logical expressibility. An EF-game [21, 18] is played over two structures of the same kind, for example two linear orderings. There are two players: the spoiler denoted by $\mathcal{S}$ and the duplicator denoted by $\mathcal{D}$. The game has k rounds, for some non-negative integer k. Intuitively, the goal of $\mathcal{S}$ is to show that the two structures can be distinguished in at most k steps, whereas $\mathcal{D}$ wants to show that this can not be done.

Definition 3.2 (Partial isomorphism). *Let $\mathcal{A}$ and $\mathcal{B}$ be two first-order structures with vocabulary τ. Assume $\bar{a} = \langle a_1, \dots, a_n \rangle \in A^n$ and $\bar{b} = \langle b_1, \dots, b_n \rangle \in B^n$. We say that there is a* partial isomorphism *from $\bar{a}$ onto $\bar{b}$ if for every m, for every quantifier-free formula $\varphi(x_1, \dots, x_m)$ over τ, and for every multiset $\{i_1, \dots, i_m\} \subseteq \{1, \dots, n\}$ the following holds*

$$\mathcal{A} \models \varphi(a_{i_1}, \dots, a_{i_m}) \iff \mathcal{B} \models \varphi(b_{i_1}, \dots, b_{i_m})$$

If $\mathcal{A}$ and $\mathcal{B}$ are groups, then partial isomorphism basically means that for every multiset $\{i_1, i_2, i_3\} \subseteq \{1, \dots, n\}$

$$\mathcal{A} \models R(a_{i_1}, a_{i_2}, a_{i_3}) \iff \mathcal{B} \models R(b_{i_1}, b_{i_2}, b_{i_3})$$

We now describe the game over $\mathcal{A}$ and $\mathcal{B}$. At each round of the game $\mathcal{S}$ starts by choosing an element from one of the two structures then $\mathcal{D}$ responds to the challenge by choosing an element from the other structure so as to preserve the partial isomorphism among the elements chosen so far from $\mathcal{A}$ and $\mathcal{B}$. Assume after k rounds the elements chosen from $\mathcal{A}$ are $\bar{a} = \langle a_1, \dots, a_k \rangle$ and those chosen from $\mathcal{B}$ are $\bar{b} = \langle b_1, \dots, b_k \rangle$, if $\bar{a}$ and $\bar{b}$ are partially isomorphic then $\mathcal{D}$ wins, otherwise $\mathcal{S}$ wins.

Notation 3.1. *Let $EF_m(\mathcal{A}, \mathcal{B}) \in \mathcal{S}$ denote that the spoiler has a winning strategy in the m-round EF-game over the structures $\mathcal{A}$ and $\mathcal{B}$, similarly for $EF_m(\mathcal{A}, \mathcal{B}) \in \mathcal{D}$.*

Definition 3.3. *[23] Let φ be a first-order formula. Define the* alternation number *of φ, $alt(\varphi)$, as the maximum number of quantifier alternations over all possible* *sequences of nested quantifiers inside φ under the assumption that φ is reduced to its negation normal form, i.e., all negations are assumed to occur only in front of atomic subformulas.*

For example, $alt(\exists x \forall y\ (x \leq y)) = 1$. For simplicity in the following discussion, we will always assume formulas in prenex normal form (it is known that every first-order formula is equivalent to one in prenex form). Let $qr(\varphi)$ denote the quantifier rank of φ. In the following we give a restricted notion of elementary equivalence between two structures.

Definition 3.4. *Let $\mathcal{A}$ and $\mathcal{B}$ be two structures over a vocabulary τ. We say that $\mathcal{A}$ and $\mathcal{B}$ are* n-elementarily equivalent*, denoted by $\mathcal{A} \equiv_n \mathcal{B}$, if and only if for every sentence φ over τ such that $qr(\varphi) \leq n$, we have*

$$\mathcal{A} \models \varphi \iff \mathcal{B} \models \varphi \tag{3.1}$$

The following theorem gives the relationship between EF-games and first-order expressibility.

Theorem 3.1 (Ehrenfeucht-Fraïssé)**.** *The following are equivalent:*

1. $\mathcal{A} \equiv_n \mathcal{B}$
2. $EF_n(\mathcal{A}, \mathcal{B}) \in \mathcal{D}$

This theorem basically says that no sentence of quantifier rank at most n can distinguish $\mathcal{A}$ and $\mathcal{B}$ if and only if the duplicator has a winning strategy in the n-round EF-game over $\mathcal{A}$ and $\mathcal{B}$.

If $\mathcal{A}$ and $\mathcal{B}$ are distinguishable, then from the actual spoiler's strategy we can know more about the sentence that distinguishes them. The following result relates the alternation number of the distinguishing sentence to the number of times $\mathcal{S}$ alternates her moves between the two structures in her winning strategy (this is based on Lemma 2.3 in [23]).

Lemma 3.1. *Assume $\mathcal{S}$ has a winning strategy in the n-round EF-game over structures $\mathcal{A}$ and $\mathcal{B}$. Assume in her winning strategy $\mathcal{S}$ makes m move alternations between the two structures ($m < n$). Then there exists a first-order sentence φ of quantifier rank at most n that distinguishes the two structures such that $alt(\varphi) \leq m$.*

3.3 The Group $\mathbb{Z}_n$

In this Section we present basic definitions and results that apply to $\mathbb{Z}_n$ for every n. In Section 3.4 we study the case when n is prime then we generalize to all n in Section 3.6. $\mathbb{Z}_n$ is defined as an $\mathcal{L}_G$-structure as follows.

Definition 3.5. *Let $n \in \mathbb{N}\backslash\{0\}$. Then $\mathbb{Z}_n = (\{0, \ldots, n-1\}, S, 0)$, where S is a ternary relation that interprets R, defined as follows*

$$S(x, y, z) \iff x + y \equiv z \pmod{n}$$

and 0 interprets e is the group additive identity.

Remark 3.1. *Since we consider the group addition as a relation rather than a function, we can not express equations like $3x + y \equiv z \pmod{n}$ using an atomic formula (that is, using one instance of R). So the following are the only possible* *forms of congruence equations that can be captured by the addition relation inside $\mathbb{Z}_n$.*

$$x + y \equiv z \pmod{n}$$

$$2x \equiv z \pmod{n}$$

$$x + y \equiv 0 \pmod{n}$$

$$2x \equiv 0 \pmod{n}$$

where x, y, z are distinct nonzero elements. The cases left out are:

- $x \equiv 0 \pmod{n}$*: 0 is a distinguished element, so it is automatically chosen before the EF-game starts.*

- $x \equiv y \pmod{n}$*: as mentioned above equality is a logical symbol, so $\mathcal{S}$ re-choosing the same element will dictate $\mathcal{D}$ to respond similarly. As far as the addition relation is concerned, re-choosing the same element will not help the spoiler to win the game.*

The following will define a weak notion of independence inside the group $\mathbb{Z}_n$ that will be used later to analyze winning strategies in EF-games.

Definition 3.6. *Let $X = \{x_1, \ldots, x_m\} \subseteq \mathbb{Z}_n \backslash \{0\}$.*

(i) We say that X is independent with respect to $\mathbb{Z}_n$*, or simply n-*independent*, if for every $x, y \in X$ and for every $z \in (X \cup \{0\}) \backslash \{x, y\}$, the following holds*

$$x + y \not\equiv z \pmod{n}$$

(ii) *A* basis *of $\mathbb{Z}_n$ is any smallest maximal subset of non-zero elements of $\mathbb{Z}_n$ that are n-independent. We denote a basis of $\mathbb{Z}_n$ by $\mathbb{I}_n$. Given some basis $\mathbb{I}_n$, by definition every element $c \in \mathbb{Z}_n$ is dependent on some elements of $\mathbb{I}_n$, that is either $c \equiv a + b \pmod{n}$, $c + a \equiv b \pmod{n}$, or $2c \equiv a \pmod{n}$ for some $a, b \in (\mathbb{I}_n \cup \{0\})$. So a basis can be thought of as a minimal subset of elements that can* generate *the whole group in the same sense that the element c mentioned above is generated.*

(iii) *If X is not independent with respect to $\mathbb{Z}_n$, then we say that it is* dependent with respect to $\mathbb{Z}_n$ *or simply* n-dependent*. Note this means that there exist $x, y \in X$ and $z \in (X \cup \{0\}) \backslash \{x, y\}$ such that $x + y \equiv z \pmod{n}$.*

(iv) *If X is dependent and there are* exactly *$k \leq m$ different triples (x, y, z) of which this last condition holds, then X is said to be* n-dependent with k degrees of dependency*, or shortly* (n, m, k)-dependent*. If there are $k \geq m$ such triples, then we just say X is (n, m, m)-dependent or* totally dependent*.*

In the following we define an operator $\mathscr{G}$, that takes as input a subset of $\mathbb{Z}_n$ and produces as output a subset of $\mathbb{Z}_n$ that contains exactly all the possible elements that can be generated from the input in the sense of 'generating' given in Definition 3.6.ii.

Definition 3.7. *Let $\mathcal{P}(.)$ denote the power set. Define the following* generating operator

$$\mathscr{G} : \mathcal{P}(\mathbb{Z}_n) \rightarrow \mathcal{P}(\mathbb{Z}_n)$$

given X define $Y = \mathscr{G}(X)$ as the minimal set such that the following hold (let $X' = (X \cup \{0\})$):

i. for every $y \in \mathbb{Z}_n$, if $2y \equiv x$ for some $x \in X'$, then we have $y \in Y$

ii. for every $x_1, x_2 \in X'$ we have $(x_1 + x_2) \in Y$

iii. for every $x_1, x_2 \in X'$, we have $(x_1 - x_2) \in Y$

iv. These are exactly the only ways of populating Y with elements

Now we give an example that illustrates the concepts given in the previous definitions.

Example 3.1.

1. *Let $X = \{1, 3, 5\} \subseteq \mathbb{Z}_{14}$. Using Definition 3.7 we calculate $\mathscr{G}(X)$ as follows. We have $(X \cup \{0\}) \subseteq \mathscr{G}(X)$ by part (ii) of the definition, $\{2, 6, 10\} \subseteq \mathscr{G}(X)$ by part (ii), $\{7\} \subseteq \mathscr{G}(X)$ by part (i), $\{4, 8\} \subseteq \mathscr{G}(X)$ by part (ii), and $\{9, 11, 12, 13\} \subseteq \mathscr{G}(X)$ by part (iii). The union of all these sets gives $\mathscr{G}(X) = \mathbb{Z}_{14}$. By applying $\mathscr{G}$ to every subset of X of cardinality 2 we can easily notice that: $5 \notin \mathscr{G}(\{1, 3\})$, $3 \notin \mathscr{G}(\{1, 5\})$, and $1 \notin \mathscr{G}(\{3, 5\})$. Hence X is an independent set that generates the whole group. It can be easily checked for any independent $X' \subseteq \mathbb{Z}_{14}$ with $|X'| = 2$ that X' is not maximally independent, hence X is a basis for $\mathbb{Z}_{14}$ and the size of any basis of $\mathbb{Z}_{14}$ is 3.*

2. *Let $C = \{1, 5, 6, 10\} \subseteq \mathbb{Z}_{14}$. From above we know that $\{1, 5\}$ is independent. Note that $1 + 5 \equiv 6$ and $5 + 5 \equiv 10$, these are the only possible equations that*

hold among the elements of C, hence C is dependent with degree 2, in other words, it is $(14, 4, 2)$-dependent.

3. *Let $D = \{1, 2, 4, 8\} \subseteq \mathbb{Z}_{14}$. Note that $1 + 1 \equiv 2, 2 + 2 \equiv 4, 4 + 4 \equiv 8$, and $8 + 8 \equiv 2$, hence D is $(14, 4, 4)$-dependent*

The following important theorem gives a lower bound on the size of a group basis. This result will be used later in proofs for finding lower bounds on the number of moves required by the spoiler to win an EF-game.

Theorem 3.2. $|\mathbb{I}_n| = \Omega(\sqrt{n})$

Proof. Let $X = \{x_1, \ldots, x_m\} \subseteq \mathbb{Z}_n \backslash \{0\}$. We want to find an upper bound on $|\mathscr{G}(X)|$. From Definition 3.7 assuming the sets generated by (i), (ii), and (iii) are mutually exclusive, we have.

$$|\mathscr{G}(X)| \leq (m + 1) + \binom{m+1}{2} + \binom{m+1}{2}$$

$$|\mathscr{G}(X)| \leq m^2 + 2m + 1$$

Assume X is a basis, then

$$n \leq m^2 + 2m + 1$$

Hence $m = \Omega(\sqrt{n})$. □

Example 3.2.

1. *From Example 3.1, we have $\mathbb{I}_{14} = \{1, 3, 5\}$ and $|\mathbb{I}_{14}| = 3 = \lfloor\sqrt{14}\rfloor$.*

2. *If p is prime, then $\mathbb{I}_p = \{1, 3, \ldots, \frac{p-1}{2}\}$ and $|\mathbb{I}_p| = \lceil\frac{p-1}{4}\rceil$. We will not use this result hence we omit the proof.*

Next we define the notion of a *binder* which is the main tool used later to analyze winning strategies in EF-games and in particular obtaining bounds on the number of moves in a winning strategy. Given two elements $a, b \in \mathbb{Z}_n$, a binder of length l between them can be thought of as a path from a to b where traversing the path here is done through the addition relation rather than traveling along the edges as is the case in graphs. The path consists of l points (including a, b) such that the set of all points on that path is either $(n, l, l-1)$-dependent or (n, l, l)-dependent; in the latter case we may think of it as a cycle. So basically a binder shows how to reach b from a inside $\mathbb{Z}_n$ using only the equations given in Remark 3.1 as the only way of generating new points on the way from a to b. Actually, the same set of points can be considered as a path between any two of them; the order is just imposed to comply with the order of choosing elements in an EF-game. Here is the formal definition.

Definition 3.8. *Let $x, y \in \mathbb{Z}_n \backslash \{0\}$. We say that there exists a* binder *t from x to y of length l in $\mathbb{Z}_n$ if one the following holds:*

1. *$l = 1$: either $x \equiv y$ or $2x \equiv y \equiv 0$ (in which case there is a path from x to 0)*

2. *$l = 2$: $x \not\equiv y$ and at least one of the following holds (possible ways to get from*

x to y using only the equations in Remark 3.1):

$$2x \equiv y$$

$$2y \equiv x$$

$$x + y \equiv 0$$

3. *$l = k + 2$, $k > 0$: $x \not\equiv y$ and there must exist $\bar{z} = \langle z_1, \ldots, z_k \rangle \in \mathbb{Z}_n^k$ of distinct elements (the order is not important except later when we apply EF-games) such that the following hold:*

   (a) *$x, y \notin \bar{z}$,*

   (b) *$U = \{x, z_1, \ldots, z_k, y\}$ is either $(n, k+2, k+1)$-dependent or $(n, k+2, k+2)$-dependent (note that if U is $(n, k+2, k+1)$-dependent, then by Definition 3.6, it is not $(n, k+2, k+2)$-dependent),*

   (c) *if U is $(n, k+2, k+1)$-dependent, then the binder is called an* open binder*; in this case there must not exist any proper open sub-binder of t from x to y, that is there is no proper subset of U that forms an open binder from x to y, and*

   (d) *if U is $(n, k+2, k+2)$-dependent, then the binder is called a* closed binder*; in this case there must not exist any proper closed sub-binder of t from x to y.*

The following notation will be adopted throughout the remaining part of this chapter.

Notation 3.2.

1. *A "binder", without any qualifier, will be used to refer to either an open binder or an unspecified one, the context will provide the right choice.*

2. *A binder t between x and y will be represented by the tuple $\langle x, z_1, \ldots, z_k, y\rangle$.*

3. *The length of a binder t will be denoted by $|t|$*

Definition 3.9. *Let $x, y \in \mathbb{Z}_n$. Let $t = \langle x, z_1, \ldots, z_k, y\rangle$ be a binder from x to y of length $k+2$, $k \geq 0$. Define the* signature *of t as the set*

$$\mathscr{S}_t = \{(a, b, c) \colon a, b \in t \text{ and } c \in (t \cup \{0\}) \text{ and } S(a, b, c)\}$$

Remark 3.2. *In the following discussion we will ignore commutativity in defining $\mathscr{S}_t$, that is if $a + b \equiv c$, then either $(a, b, c) \in \mathscr{S}_t$ or $(b, a, c) \in \mathscr{S}_t$ but not both.*

Example 3.3. *Consider the following inside $\mathbb{Z}_{13}$.*

1. *Let $t_1 = \langle 1, 2, 4, 8\rangle$. Then t is an open binder of length 4 between 1 and 8 with signature $\mathscr{S}_{t_1} = \{(1, 1, 2), (2, 2, 4), (4, 4, 8)\}$. It can be easily checked that these are the only relations that hold among the elements of t_1.*

2. *Let $t_2 = \langle 1, 2, 3, 4, 8\rangle$. Then t_2 is a closed binder of length 5 between 1 and 8 with signature $\mathscr{S}_{t_2} = \mathscr{S}_{t_1} \cup \{(8, 8, 3), (1, 2, 3)\}$.*

3. *Consider $t_3 = \langle 2, 11\rangle$, an open binder of length 2 between 2 and 11, with signature $\mathscr{S}_{t_3} = \{(2, 11, 0)\}$*

Lemma 3.2. *Let $x > 1$ be a positive integer such that $x \geq 2^n$. Let t be an open binder between 1 and x inside the group $(\mathbb{N}, +)$ (or inside $\mathbb{Z}_u$ for large enough u, however, all the elements of t lie between 1 and x inclusively). Then $|t| \geq (n+1)$.*

Proof. Without loss of generality assume that $x = 2^n$. The only possible equations that can be applied to reach x from 1 are: $x + y = z$ and $2y = z$. Given $x < y$, the latter equation is at least as fast as the former, hence the fastest possible way to reach x is to double the step, therefore need $\log_2^x = n$ steps which implies that $|t| \geq (n+1)$. □

Next we define the notion of isomorphism between two binders. The isomorphism is basically determined by the binder's length and the signature.

Definition 3.10. *Let $t_1 = \langle x, \bar{z}_1, y \rangle$ be a binder from x to y of length l_1 inside $\mathbb{Z}_p$. Let $t_2 = \langle x', \bar{z}_2, y' \rangle$ be a binder from x' to y' of length l_2 inside $\mathbb{Z}_q$. We say that t_1 and t_2 are* isomorphic, *denoted by $t_1 \cong t_2$, if and only if $l_1 = l_2$ and there exists a bijection $f\colon (t_1 \cup \{0\}) \longrightarrow (t_2 \cup \{0\})$ satisfying*

- *$f(x) = x'$ and $f(y) = y'$*
- *$f(\bar{z}_1) = \bar{z}_2$ (order-preserving)*
- *$f(0) = 0$*
- *for every $a, b \in t_1$ and $c \in (t_1 \cup \{0\})$, the following holds: $S_p(a,b,c) \iff S_q(f(a), f(b), f(c))$ (where S_p is the addition relation modulo p)*

Example 3.4. *Let $t_1 = \langle 2, 5, 3, 10 \rangle$ be a closed binder of length 4 inside $\mathbb{Z}_{13}$. Its signature $\mathscr{S}_{t_1} = \{(2,3,5), (5,5,10), (3,10,0), (5,10,2)\}$. Let $t_2 = \langle 3, 7, 4, 14 \rangle$ be a closed* *binder of length* 4 *inside* $\mathbb{Z}_{18}$. *Its signature is* $\mathscr{S}_{t_2} = \{(3,4,7),(7,7,14),(4,14,0),(7,14,3)\}$. *It can be easily checked that* $t_1 \cong t_2$.

3.4 $\mathbb{Z}_p$: p is Prime

In this section we apply EF-games to the groups $\mathbb{Z}_p$ for prime numbers $p \geq 3$. Note that $2x \equiv 0 \pmod{p}$ has no non-zero solution, hence the equations in Remark 3.1 can be shortened as indicated in the following.

Remark 3.3. *Given p is prime and the fact that addition is treated as a ternary relation, the following are the only possible forms of relevant congruence equations that can be captured by the addition relation inside* $\mathbb{Z}_p$.

$$\begin{aligned} x + y &\equiv z \pmod{p} \\ 2x &\equiv z \pmod{p} \\ x + y &\equiv 0 \pmod{p} \end{aligned}$$

where x, y, z *are nonzero distinct elements.*

Remark 3.4. *Note that for any prime p, the group* $\mathbb{Z}_p$ *contains the closed binder* $t = \langle 1, p-2, p-1 \rangle$ *that has the signature* $\mathscr{S}_t = \{(1,p-2,p-1),(1,p-1,0),(p-1,p-1,p-2)\}$. *So closed binders in general do not uniquely identify their groups.*

For the remaining part of this section we will always assume that p and q are two different primes with $p < q$.

In the following we apply EF-games over the groups $\mathbb{Z}_p$ and $\mathbb{Z}_q$ to get bounds on the number of steps required by the spoiler to win the game and hence bounds on the quantifier complexity of a first order sentence that distinguishes the two groups. It turned out that $\Theta(\log p)$ is a tight bound. The winning strategy for $\mathcal{S}$ is basically to choose all of her elements from $\mathbb{Z}_p$ to form a system of congruence equations that are only solvable modulo p, in other words the elements chosen by $\mathcal{S}$ form a closed binder inside $\mathbb{Z}_p$ whilst it is impossible for $\mathcal{D}$ to get an isomorphic copy inside $\mathbb{Z}_q$.

3.4.1 Lower bound for $EF(\mathbb{Z}_p, \mathbb{Z}_q) \in \mathcal{S}$

The following lemma gives a lower bound on the length of a closed binder that uniquely characterizes its own group.

Lemma 3.3. *Let $2^n < p < 2^{n+1}$ for some positive integer n. Let t be a closed binder of length m inside $\mathbb{Z}_p$ that does not have an isomorphic copy inside $\mathbb{Z}_q$ for any prime $q \neq p$. Then it must be the case that $m \geq (n+1)$.*

Proof. Since $\mathbb{Z}_p$ is a field, we can assume that $1 \in t$ (if not, multiply t by x^{-1} for some $x \in t$ to get an isomorphic copy that contains 1). Let $s = \max\{z \colon z \in t\}$ (the maximum is computed modulo $\mathbb{N}$). View t as a closed binder from 1 to s, hence t can be broken into two different open binders from 1 to s; in other words s is reachable from 1 through two different open paths using only the elements of t. Let t_1 and t_2 be these two open binders. Since t uniquely characterizes $\mathbb{Z}_p$ among all groups of prime order, t_1 and t_2 can be represented by two congruence equations that have solutions modulo prime r if and only if $r = p$.

$$y \equiv ax \pmod{p} \tag{3.2}$$

$$x \equiv by \pmod{p} \tag{3.3}$$

where $a, b \in (\mathbb{Z}_p \backslash \{0\})$ are constants and $b \equiv a^{-1} \pmod p$ and $(x, y) = (1, s)$ is a solution to this system.

Equation 3.2 gives the relationship between 1 and s as it is modulo $\mathbb{N}$, hence a can actually be taken to have the value s. Whereas Equation 3.3 gives the relationship between 1 and s that is unique to $\mathbb{Z}_p$ among all groups of prime order. So t_1 is the straightforward way to go from 1 to s as would be done modulo $\mathbb{N}$, whereas t_2 is a shortcut path between the two points exploiting the cyclicity of $\mathbb{Z}_p$. Partition $(\mathbb{Z}_p \backslash \{0\})$ into two halves: $A = \{1, \ldots, \frac{p-1}{2}\}$ and $B = \{\frac{p+1}{2}, \ldots, p-1\}$. From the hypothesis we have $p > 2^n$, hence $\frac{p-1}{2} \geq 2^{n-1}$, hence $2^{n-1} \in A$.

Claim I: There exists an element z such that $z \in (t \cap B)$.

Proof of Claim I: Assume not. Given t_1 and t_2 as described above the following must hold for some $z_1, z_2, z_3 \in \ (A \cap t)$

$$z_1 + z_2 \neq z_3$$

$$z_1 + z_2 \equiv z_3 \pmod p$$

where the first inequality holds modulo $\mathbb{N}$. Hence, $z_1 + z_2 \geq p$, which is impossible since the largest element in A is $\frac{p-1}{2}$. $\square_{Claim\ I}$

Since $2^{n-1} \in A$, by Lemma 3.2 we have $|A \cap t_1| \geq n$. By Claim I we have $|B \cap t| \geq 1$, hence $|t| \geq (n+1)$. $\square$

The following theorem gives a lower bound on the number of moves needed by $\mathcal{S}$ to win an EF-game.

Theorem 3.3. *Let $2^n < p < 2^{n+1}$ for some positive integer n. Assume $p < q$. If $EF_m(\mathbb{Z}_p, \mathbb{Z}_q) \in \mathcal{S}$, then it must be the case that $m \geq (n+1)$.*

Proof. Assume $EF_m(\mathbb{Z}_p, \mathbb{Z}_q) \in \mathcal{S}$. We can assume that m is minimal, that is $EF_{m-1}(\mathbb{Z}_p, \mathbb{Z}_q) \in \mathcal{D}$. Let $\mathcal{G}$ denote an m-round EF-game played over $\mathbb{Z}_p$ and $\mathbb{Z}_q$ in which $\mathcal{S}$ has played a fixed winning strategy. Assume that $\mathcal{D}$ has played her best strategy in $\mathcal{G}$. Let $s_1 = \langle a_1, \ldots, a_m \rangle \subseteq \mathbb{Z}_p$ and $s_2 = \langle b_1, \ldots, b_m \rangle \subseteq \mathbb{Z}_q$ be the elements chosen by the players during the course of $\mathcal{G}$. It can easily be verified that the following three cases cover all the possible ways by which $\mathcal{S}$ can win $\mathcal{G}$.

Case i: $\mathcal{S}$ chooses a_m such that she creates a binder $t_{a_1 a_m}$ of length m inside $\mathbb{Z}_p$ that satisfies $t_{a_1 a_m} \ncong t_{b_1 b_m}$. Then it must be the case that exactly one of the two binders is closed (note that since $t_{a_1 a_m}$ is a binder, $\mathcal{D}$ is forced to play exactly one particular point b_m). Hence by Lemma 3.3, $m \geq (n+1)$.

Case ii: $\mathcal{S}$ chooses b_m to be independent from $\langle b_1, \ldots, b_{m-1} \rangle$, that is $b_m \notin \mathscr{G}(\{b_1, \ldots, b_{m-1}\})$, however, $\mathcal{D}$ is forced to choose a point $a_m \in \mathscr{G}(\{a_1, \ldots, a_{m-1}\})$, that is every point in $\mathbb{Z}_p$ belongs to $\mathscr{G}(\{a_1, \ldots, a_{m-1}\})$, hence $\{a_1, \ldots, a_{m-1}\}$ contains a basis for $\mathbb{Z}_p$. By Theorem 3.2, $m = \Omega(\sqrt{p}) = \Omega(2^{n/2})$.

Case iii: $\mathcal{S}$ chooses $b_m \in \mathscr{G}(\{b_1, \ldots, b_{m-1}\})$ and $\mathcal{D}$ has to choose $a_m \in \mathscr{G}(\{a_1, \ldots, a_{m-1}\})$ (or vice versa) such that the following hold: (i) there is no binder from b_1 to b_m (hence also no binder from a_1 to a_m, otherwise either one of the above two cases applies and we are done) and (ii) there exists a minimal set $U \subseteq (s_2 \backslash \{b_m\})$ such that $b_m \in \mathscr{G}(U)$ and $b_m \notin \mathscr{G}(s_2 \backslash (U \cup \{b_m\}))$, however, given $U' = \{a_i \in s_1 \colon b_i \in U\}$, it holds that $a_m \in \mathscr{G}(U')$ and $a_m \in \mathscr{G}(s_1 \backslash (U'' \cup \{a_m\}))$ for non-empty $U'' \subseteq U'$ (that is a_m depends on more previously chosen elements than b_m does). Let k be maximal such that $b_k \notin \mathscr{G}(\{b_1, \ldots, b_{k-1}\})$ but $b_l \in \mathscr{G}(\{b_1, \ldots, b_{l-1}\})$ for every $k < l \leq m$. Note that it must be the case that $k > 1$, otherwise s_2 forms an open binder from b_1 to b_m which contradicts our assumption. Let $A = \{a_1, \ldots, a_{k-1}\}$ and $B = \{a_k, \ldots, a_m\}$. Let $C = \mathbb{Z}_p \backslash \mathscr{G}(A)$.

Let $\mathbb{E}$ denote the system of equations inside $\mathbb{Z}_p$ that capture the dependency of each element chosen at the l^{th} round on previously chosen elements for $k < l \leq m$. Let the variable x_i in $\mathbb{E}$ represent the element chosen at the i^{th} round. Let

$$\mathbb{E}_m = \{\mathcal{E} \in \mathbb{E} \colon \mathcal{E} \textit{ is an equation that contains the variable } x_m\} \tag{3.4}$$

By the way $\mathcal{S}$ won the game, $\mathbb{E}_m$ must contain 2 or more of the following equations:

$$x_m \equiv x_{i_1} + x_{i_2} \pmod{p} \tag{3.5}$$

$$x_m \equiv x_{i_3} - x_{i_4} \pmod{p} \tag{3.6}$$

$$2x_m \equiv x_{i_5} \pmod{p} \tag{3.7}$$

$$x_m + x_{i_6} \equiv 0 \pmod{p} \tag{3.8}$$

Replace each variable x_i in $\mathbb{E}$ such that $i < k$ (variables representing elements from A) by its actual value, then reduce $\mathbb{E}$ accordingly (solve for the maximum possible number of variables). Let $\mathbb{E}'$ denote the new reduced system. If $\mathbb{E}'$ is completely determined (all of its variables have definite values), then round k, where the elements played are independent of A, is redundant, hence $\mathcal{S}$ could have won $\mathcal{G}$ in $(m-1)$ rounds which is a contradiction. By the same reasoning (that round k is not redundant), there must exist some relation between x_k and x_m that can be derived from $\mathbb{E}'$

$$a_1 x_m + a_2 x_k \equiv a_3 \pmod{p} \tag{3.9}$$

where $a_1, a_2 \in (\mathbb{Z}_p \backslash \{0\})$ and $a_3 \in \mathbb{Z}_p$. By the way $\mathcal{S}$ won the game, derive another different equation

$$b_1 x_m + b_2 x_k \equiv b_3 \pmod{p} \tag{3.10}$$

where $b_1 \in (\mathbb{Z}_p \backslash \{0\})$ and $b_2, b_3 \in \mathbb{Z}_p$. There are two subcases:

Subcase iii.i: $\mathcal{S}$ played $a_k \in \mathbb{Z}_p$: Since $\mathcal{D}$ lost the game, Equations 3.9 and 3.10 have no non-zero solutions in $\mathbb{Z}_q$. Hence, $\mathcal{S}$ could have won $\mathcal{G}$ by playing all of her elements from $\mathbb{Z}_p$. This has two implications: (i) if there exists $j < k$ such that x_j does not appear in $\mathbb{E}$, then the j^{th} round is redundant and $\mathcal{S}$ could have won in $(m-1)$ rounds which is a contradiction, so all elements of A must be represented by variables in $\mathbb{E}$ and (ii) if $\mathcal{S}$ played all of her elements from $\mathbb{Z}_p$, then the order of her choices is irrelevant. Choose an arbitrary $j < k$, and assume a new game $\mathcal{G}'$ in which $\mathcal{S}$ has played the following strategy: (i) for rounds 1 through $(j-1)$, $\mathcal{S}$ plays $\langle a_1, \ldots, a_{j-1} \rangle$, (ii) for rounds j through $(m-1)$, $\mathcal{S}$ plays $\langle a_{j+1}, \ldots, a_m \rangle$, and finally (iii) at the m^{th} round, $\mathcal{S}$ plays a_j. Clearly, $\mathcal{S}$ wins $\mathcal{G}'$ at the m^{th} round but not before that. Let

$$\mathbb{E}_m^{-j} = \{\mathcal{E} \in \mathbb{E}_m \colon \mathcal{E} \textit{ does not contain the variable } x_j\}$$

It must be the case that: (i) $\mathbb{E}_m^{-j} \subset \mathbb{E}_m$, otherwise $\mathcal{S}$ won in $(m-1)$ steps and (ii) $|\mathbb{E}_m^{j}| \geq 2$ where $\mathbb{E}_m^{j} = \mathbb{E}_m \backslash \mathbb{E}_m^{-j}$, otherwise $\mathcal{S}$ does not win in m steps. Given Equations 3.5 through 3.8, $\mathbb{E}_m^{j}$ contains exactly 2 equations (more than 2 is either redundant, will give zero solutions, or equality between elements). Based on which pair of equations $\mathbb{E}_m^{j}$ consists of, we have the following cases.

1. Assume $\mathbb{E}_m^j$ contains the following equations.

$$x_m \equiv x_j + x_{i_1} \pmod p$$
$$2x_m \equiv x_j \pmod p$$

   From these two equations derive

$$x_m + x_{i_1} \equiv 0 \pmod p \tag{3.11}$$

   Since $i_1 < m$, this last equation holds also modulo q. Now imagine $\mathcal{G}'$ at the m^{th} round and it is the duplicator turn. $\mathcal{D}$ can choose x_j that satisfies $x_j \equiv x_m - x_{i_1} \pmod q$. Given that Equation 3.11 holds in $\mathbb{Z}_q$, then $2x_m \equiv x_j \pmod q$ holds. Hence, $\mathbb{E}_m^j$ has non-zero solutions in $\mathbb{Z}_q$ which is a contradiction.

2. Assume $\mathbb{E}_m^j$ contains the following equations.

$$x_m \equiv x_j + x_{i_1} \pmod p \tag{3.12}$$
$$x_m \equiv x_{i_2} - x_j \pmod p \tag{3.13}$$

   From these derive

$$2x_m \equiv x_{i_1} + x_{i_2} \pmod p \tag{3.14}$$

   If this last equation holds in $\mathbb{Z}_q$, then the previous case applies and we are done. So assume that it does not hold in $\mathbb{Z}_q$. Assume Equation 3.12 fails in $\mathbb{Z}_q$ (the case where Equation 3.13 fails is similar). We show that $\mathcal{S}$ can win the game in $(m-1)$ rounds which contradicts our initial assumption. Assume the following strategy for the spoiler: (i) for rounds 1 through $(m-3)$, $\mathcal{S}$ plays $s_1 \backslash \{a_j, a_{i_1}, a_{i_2}\}$ such that a_m is played at the $(m-3)^{rd}$ round, then (ii) based on $\mathcal{D}$'s response at the $(m-3)^{rd}$ round we have the following:

(a) if $\mathcal{D}$ plays b_m (her last choice in the original game $\mathcal{G}$), then $\mathcal{S}$ wins by playing a_j and a_{i_1} and the game is up,

(b) if $\mathcal{D}$ plays an element d such that $2d \equiv b_{i_1} + b_{i_2} \pmod{q}$, then $\mathcal{S}$ wins by playing a_{i_1} and a_{i_2} and the game is up (otherwise, $\mathcal{D}$ could have won the m-round game $\mathcal{G}$ by playing d at the $(m-1)^{st}$ round)

(c) if $\mathcal{D}$ plays an element d' that is different from the two previous cases, then

- if $a_m \in \mathscr{G}(\{a_1, \ldots, a_{m-1}\} \backslash \{a_j\})$, then $\mathcal{S}$ wins by playing a_{i_1} and a_{i_2} and the game is up,
- otherwise, $\mathcal{S}$ wins by playing a_j and either of a_{i_1} or a_{i_2} but not both and the game is up

3. Any other valid pair of equations (does not yield zero elements or equality of different elements) constituting $\mathbb{E}_m^j$ falls into either one of the previous two cases.

Subcase iii.ii: $\mathcal{S}$ played $b_k \in \mathbb{Z}_p$: Assume $m = O(n)$. Then from the proof of Theorem 3.2 it must be the case that $|\mathscr{G}(A)| = O(n^2)$, hence $|C| = \Omega(2^n - n^2)$. Since all the elements played after the k^{th} round are dependent on previous elements, it follows that: (i) starting from the k^{th} round $\mathcal{S}$ can exclusively choose all of her elements from $\mathbb{Z}_q$ and (ii) no matter how $\mathcal{D}$ reacts at the k^{th} round $\mathcal{S}$ wins by following exactly the same strategy starting from the $(k+1)^{st}$ round, that is by playing $\langle b_{k+1}, \ldots, b_m \rangle$. Hence for every $y \in C$, the congruence system $\mathbb{E}$ holds in $\mathbb{Z}_p$ if x_k is replaced by y. Now look at Equations 3.9 and 3.10. If $a_3 \equiv b_3 \equiv 0$, then B must contain a closed binder, hence $m \geq (n+1)$. Otherwise, these two equations will give definite unique solutions for x_k and x_m which is a contradiction for $|C| > 1$. □

This allows us to give a lower bound on the quantifier complexity of a first-order sentence that distinguishes $\mathbb{Z}_p$ and $\mathbb{Z}_q$.

Corollary 3.1. *Assume $2^n < p < 2^{n+1}$ for some positive integer n. Assume $p < q$. Then for any $\mathcal{L}_G$-sentence φ that distinguishes $\mathbb{Z}_p$ and $\mathbb{Z}_q$ it must be the case that $qr(\varphi) \geq (n+1)$*

Proof. Follows directly from Theorem 3.1 and Theorem 3.3. □

Remark 3.5. *The lower bound obtained in Corollary 3.1 is optimal for it is achievable for at least a class of primes that includes the Mersenne primes (see Section 3.4.3 for details).*

3.4.2 Upper bound for $EF(\mathbb{Z}_p, \mathbb{Z}_q) \in \mathcal{S}$

In this section we show that $2n$ is an upper bound for the number of moves needed by the spoiler to win the game. First, we show that every group $\mathbb{Z}_p$ contains a closed binder that uniquely characterizes it. The length of this closed binder is logarithmic in the group order.

Lemma 3.4. *Assume $2^n < p < 2^{n+1}$ for some positive integer n. Then $\mathbb{Z}_p$ can be uniquely identified among all groups of prime order by a closed binder $\mathcal{C}_p$ inside it. Furthermore, $|\mathcal{C}_p| \leq 2n$.*

Proof. Write p in binary radix

$$p = 2^{i_k} + \ldots + 2^{i_1} + 1 \tag{3.15}$$

where $1 \leq i_1 < \ldots < i_k = n$. Let $\mathbb{E}_1$ denote the following set of congruence equations

$$\begin{gathered} x_2 \equiv 2x_1 \pmod{p} \\ x_3 \equiv 2x_2 \pmod{p} \\ \vdots \\ x_{i_k+1} \equiv 2x_{i_k} \pmod{p} \end{gathered}$$

Since $i_k = n$, then $|\{x_1, \ldots, x_{i_k+1}\}| = n + 1$. From the above system we can derive

$$x_h \equiv 2^{h-1}x_1 \pmod{p} \tag{3.16}$$

for $2 \leq h \leq i_k + 1$. Let $\mathbb{E}_2$ denote the following congruence equation

$$(x_{i_1+1} + \ldots + x_{i_k+1}) + x_2 \equiv x_1 \pmod{p}$$

From 3.16 into this last equation we get

$$\left(2^{i_1}x_1 + \ldots + 2^{i_k}x_1\right) + 2x_1 \equiv x_1 \pmod{p}$$

$$\left(2^{i_1} + \ldots + 2^{i_k} + 1\right) x_1 \equiv 0 \pmod{p}$$

$$px_1 \equiv 0 \pmod{p} \tag{3.17}$$

Any element in $(\mathbb{Z}_p \backslash \{0\})$ can be a solution to this last equation. On the other hand it is clear that the equation

$$px_1 \equiv 0 \pmod{q}$$

does not have a non-zero solution for any prime $q \neq p$. Hence, the congruence system $(\mathbb{E}_1 \cup \mathbb{E}_2)$ uniquely characterizes the group $\mathbb{Z}_p$ among all groups of prime order.

The only remaining thing to do in order to obtain a valid closed binder is to break $\mathbb{E}_2$ into an equivalent set of congruence equations that conform to the equation forms given in Remark (3.3). This can be easily done by introducing a new set of variables as follows.

$$\begin{aligned}
&x_{i_1+1} + x_{i_2+1} \equiv y_1 \pmod{p} \\
&y_1 + x_{i_3+1} \equiv y_2 \pmod{p} \\
&\qquad\vdots \\
&y_{k-2} + x_{i_k+1} \equiv y_{k-1} \pmod{p} \\
&y_{k-1} + x_2 \equiv x_1 \pmod{p}
\end{aligned}$$

$(k-1)$ new variables were introduced. From Equation 3.15 and given the hypothesis $p < 2^{n+1}$ we have $k \leq n$, hence $|\{y_1, \ldots, y_{k-1}\}| \leq n-1$.

So we have constructed a closed binder $\mathcal{C}_p$ whose points are $\{x_1, \ldots, x_{i_k+1}, y_1 \ldots, y_{k-1}\}$ (note that from its very construction any proper subset of these points does not form a closed binder). $|\mathcal{C}_p| \leq n+1+n-1 = 2n$. The set of congruence equations $(\mathbb{E}_1 \cup \mathbb{E}_2)$ determines the signature of $\mathcal{C}_p$. □

Notice that the previous proof gives an actual winning strategy for the spoiler as follows. The spoiler would first realize $\mathbb{E}_1$ by choosing $a_1 = 1, a_2 = 2, \ldots, a_{n+1} = 2^{i_k}$. Then she would realize $\mathbb{E}_2$ by choosing $b_1 = 2^{i_1} + 2^{i_2}, b_2 = b_1 + 2^{i_3}, \ldots, b_{k-1} = b_{k-2} + 2^{i_k}$. As a direct consequence of this lemma we have an upper bound on the number of moves required by $\mathcal{S}$ to win an EF-game. This is given in the following theorem.

Theorem 3.4. *Assume $2^n < p < 2^{n+1}$ for some positive integer n. Assume $p < q$. Then there exists $m \leq 2n$ such that $EF_m(\mathbb{Z}_p, \mathbb{Z}_q) \in \mathcal{S}$.*

Proof. From Lemma 3.4, $\mathcal{S}$ can win by playing the closed binder $\mathcal{C}_p$. □

From the lower and upper bounds given above we can conclude the following corollary.

Corollary 3.2. *Assume $2^n < p < 2^{n+1}$ for some positive integer n. Assume $p < q$. Then the following hold.*

1. *If $EF_m(\mathbb{Z}_p, \mathbb{Z}_q) \in \mathcal{S}$, then it must be the case that $m \geq (n + 1)$.*

2. *There exists $m \leq 2n$ such that $EF_m(\mathbb{Z}_p, \mathbb{Z}_q) \in \mathcal{S}$. Furthermore, $\mathcal{S}$ can win by choosing all of her points from $\mathbb{Z}_p$ that construct the closed binder $\mathcal{C}_p$.*

From this follows directly the corresponding expressibility result.

Corollary 3.3. *Assume $2^n < p < 2^{n+1}$ for some positive integer n. Assume $p < q$. Then the following hold.*

1. *If φ is an $\mathcal{L}_G$-sentence distinguishing $\mathbb{Z}_p$ and $\mathbb{Z}_q$, then it must be the case that $qr(\varphi) \geq (n + 1)$.*

2. *There exists an existential $\mathcal{L}_G$-sentence φ distinguishing $\mathbb{Z}_p$ and $\mathbb{Z}_q$ such that $qr(\varphi) \leq 2n$.*

Proof. The quantifier rank bounds follow directly from Corollary 3.2. From the same corollary, $\mathcal{S}$ can win within these bounds by choosing all of her points from $\mathbb{Z}_p$ during the course of the game (no alternation between the two groups), hence $alt(\varphi) = 0$, therefore φ is existential. □

It is an open question whether this lower/upper bounds gap can get closer. As will be seen below in Section 3.4.3, the lower bound of $(n + 1)$ is optimal. We believe that the upper bound of $2n$ is optimal too.

From the proof of Lemma 3.4, we can actually construct the sentence that distinguishes $\mathbb{Z}_p$ and $\mathbb{Z}_q$. Assume that $2^n < p < 2^{n+1}$. Assume $p < q$. Remember that from the proof of this lemma, $|\mathbb{E}_1| = n+1$ and $|\mathbb{E}_2| = n-1$. The distinguishing sentence is as follows.

$$\begin{gathered}\exists x_1 \cdots \exists x_{i_k+1} \exists y_1 \cdots \exists y_{k-1} (R(x_1, x_1, x_2) \wedge \cdots \wedge R(x_{i_k}, x_{i_k}, x_{i_k+1}) \\ \wedge R(x_{i_1+1}, x_{i_2+1}, y_1) \wedge R(y_1, x_{i_3+1}, y_2) \wedge \cdots \wedge R(y_{k-2}, x_{i_k+1}, y_{k-1}) \qquad (3.18) \\ \wedge R(y_{k-1}, x_2, x_1))\end{gathered}$$

3.4.3 Some general examples

In the following we show that for some classes of primes the lower bound obtained above is achievable and hence an optimal one.

Theorem 3.5. *Let $p = 2^n - 1$ be a Mersenne prime. Then $EF_n(\mathbb{Z}_p, \mathbb{Z}_q) \in \mathcal{S}$.*

Proof. Consider the following system of congruence equations

$$x_2 \equiv 2x_1 \pmod p$$

$$x_3 \equiv 2x_2 \pmod p$$

$$\vdots$$

$$x_n \equiv 2x_{n-1} \pmod p$$

$$x_1 \equiv 2x_n \pmod p$$

By substitution derive

$$x_1 \equiv 2^n x_1 \pmod p$$

$$(2^n - 1)x_1 \equiv 0 \pmod p$$

$x_1 \equiv 1$ is a solution to this equation, however, since q is prime, the system has no non-zero solution in $\mathbb{Z}_q$. So $\mathcal{S}$ can win in just n (note that $2^{n-1} < p < 2^n$) steps by playing $x_1 \equiv 1, x_2 \equiv 2, \ldots, x_n \equiv 2^{n-1}$ from $\mathbb{Z}_p$. $\square$

Corollary 3.4. *Let $p = 2^n - 1$ be a Mersenne prime. Assume $p < q$. Then there exists an $\mathcal{L}_G$-existential sentence distinguishing $\mathbb{Z}_p$ and $\mathbb{Z}_q$ with $qr(\varphi) = n$.*

The following theorem gives the same result for a more general class of prime numbers.

Theorem 3.6. *Assume $p = 2^{i-1} + 2^{j-1} - 2^{k-1}$ for some positive integers i, j, k. Let $n = max\{i, j, k\}$. Then $EF_n(\mathbb{Z}_p, \mathbb{Z}_q) \in \mathcal{S}$.*

Proof. Consider the following system of congruence equations

$$x_2 \equiv 2x_1 \pmod{p}$$

$$x_3 \equiv 2x_2 \pmod{p}$$

$$\vdots$$

$$x_n \equiv 2x_{n-1} \pmod{p}$$

$$x_i + x_j \equiv x_k \pmod{p}$$

From this system derive

$$x_i \equiv 2^{i-1}x_1 \pmod{p}$$

$$x_j \equiv 2^{j-1}x_1 \pmod{p}$$

$$x_k \equiv 2^{k-1}x_1 \pmod{p}$$

Substituting in the last equation get

$$(2^{i-1} + 2^{j-1} - 2^{k-1})x_1 \equiv 0 \pmod{p}$$

$x_1 \equiv 1$ is a solution to this equation, however, since q is prime, the system has no non-zero solution in $\mathbb{Z}_q$. So $\mathcal{S}$ can win in just n steps by choosing $x_1 \equiv 1, x_2 \equiv 2, \ldots, x_n \equiv 2^{n-1}$ from $\mathbb{Z}_p$. □

Corollary 3.5. *Assume $p = 2^{i-1} + 2^{j-1} - 2^{k-1}$ for some positive integers i, j, k. Let $n = max\{i, j, k\}$. Then there exists an $\mathcal{L}_G$-existential sentence distinguishing $\mathbb{Z}_p$ and $\mathbb{Z}_q$ with $qr(\varphi) = n$.*

3.5 Pebble EF-Games

In this section we describe an extended version of EF-games called pebble EF-games. Assume a positive integer k. The players start the game each having a fixed number of k pebbles ($k \leq n$ for number of rounds n). At each round $\mathcal{S}$ does either one of the following (i) removing a pebble that has been placed on a previously chosen element and placing it on a new element or (ii) placing a new pebble, if she still has any, on a new element. $\mathcal{D}$ must act correspondingly on the other structure. At the beginning the pebbles are not placed on any elements (we can assume having extra pebbles always placed on the distinguished elements of the structures such as the group identity even before the game starts). Assume at the end of the game that k pebbles are placed on $\bar{a} = \langle a_1, \ldots, a_k \rangle$ from the structure $\mathcal{A}$ and correspondingly k pebbles are placed on $\bar{b} = \langle b_1, \ldots, b_k \rangle$ from the structure $\mathcal{B}$. Since $k \leq n$, these tuples are in general subsets of the elements chosen during the course of the game. Then $\mathcal{D}$ wins the game if $\bar{a}$ and $\bar{b}$ are partially isomorphic, otherwise $\mathcal{S}$ wins.

Notation 3.3.

1. *An n-round pebble EF-game with k pebbles over the structures $\mathcal{A}$ and $\mathcal{B}$ will be denoted $pEF_n^k(\mathcal{A}, \mathcal{B})$.*

2. *Let $\mathcal{L}_G^k$ be the restriction of $\mathcal{L}_G$ to formulas with at most k variables.*

Definition 3.11. *Assume $\mathcal{A}$ and $\mathcal{B}$ are two structures over a vocabulary τ. We say that $\mathcal{A}$ and $\mathcal{B}$ are* (n, k)-elementarily equivalent*, denoted by $\mathcal{A} \equiv_n^k \mathcal{B}$ if and only if* *for every first-order τ-sentence φ such that φ has at most k variables and $qr(\varphi) \leq n$ the following holds:*

$$\mathcal{A} \models \varphi \iff \mathcal{B} \models \varphi \tag{3.19}$$

Pebble games characterize expressibility in finite variable first-order logic as indicated in the following theorem.

Theorem 3.7. *The following are equivalent:*

1. $\mathcal{A} \equiv_n^k \mathcal{B}$

2. $pEF_n^k(\mathcal{A}, \mathcal{B}) \in \mathcal{D}$

The following theorem gives an upper bound for the number of pebbles required for $\mathcal{S}$ to win an EF-game over $\mathbb{Z}_p$ and $\mathbb{Z}_q$.

Theorem 3.8. *Let $2^n < p < 2^{n+1}$ for some positive integer n. Assume $p < q$. Then there exists a positive integer $m \leq 2n$ such that $pEF_m^5(\mathbb{Z}_p, \mathbb{Z}_q) \in \mathcal{S}$.*

Proof. From Theorem 3.4, there exists $m \leq 2n$ such that $EF_m(\mathbb{Z}_p, \mathbb{Z}_q) \in \mathcal{S}$, and the spoiler can win by playing the closed binder $\mathcal{C}_p$, hence all of her choices are from $\mathbb{Z}_p$. Now we describe how $\mathcal{S}$ can play $\mathcal{C}_p$ using only 5 pebbles in order to win the game. From Lemma 3.4, the elements of $\mathcal{C}_p$ are the set $\{x_1, \ldots, x_{i_k+1}, y_1, \ldots, y_{k-1}\}$. The equations in this lemma are used to guide $\mathcal{S}$'s strategy.

In the first 2 rounds $\mathcal{S}$ puts two of her pebbles on x_1, x_2; these pebbles will not be removed till the end of the game. Assume $\mathcal{D}$'s corresponding pebbles are on y_1, y_2. Note that only y_1 can be arbitrary for it must be the case that $y_2 \equiv 2y_1$

(mod q) and it will remain the only arbitrarily chosen element till the end of the game. In the 3^{rd} and 4^{th} rounds $\mathcal{S}$ places two new pebbles on x_3, x_4. In the 5^{th} round $\mathcal{S}$ removes the pebble on x_3 and places it on x_5 and on the 6^{th} round $\mathcal{S}$ removes the pebble on x_4 and places it on x_6. This sequencing forces $\mathcal{D}$ to choose particular fixed elements after the first round, more specifically $y_i \equiv 2y_{i-1} \pmod{q}$. $\mathcal{S}$ pursues this alternation of pebbles until putting a pebble on x_{i_1+1}.

This last pebble is fixed temporarily and $\mathcal{S}$ then uses the pebble on x_{i_1} and the 5^{th} pebble (the one not yet used) to continue its alternation (successively doubling the elements) until a pebble is placed on x_{i_2+1}. $\mathcal{S}$ then removes the pebble on x_{i_2} and places it on y_1 (remember $x_{i_1+1} + x_{i_2+1} \equiv y_1 \pmod{p}$). $\mathcal{S}$ uses the two pebbles on x_{i_1+1}, x_{i_2+1} to continue her choices until placing a pebble on x_{i_3+1}. $\mathcal{S}$ then removes the pebble on x_{i_3} and puts it on y_2 ($y_1 + x_{i_3+1} \equiv y_2 \pmod{p}$). $\mathcal{S}$ then uses the two pebbles on x_{i_3+1}, y_1 to continue her choices (doubling the elements starting from x_{i_3+1}) until putting a pebble on x_{i_4+1}. $\mathcal{S}$ pursues this pebble placing strategy until having 3 pebbles on $y_{k-2}, x_{i_k+1}, y_{k-1}$ (see Lemma 3.4). The game then terminates and $\mathcal{S}$ wins since $y_{k-1} + x_2 \equiv x_1 \pmod{p}$ (these elements have pebbles on them) whereas the corresponding pebbles in $\mathbb{Z}_q$ fail to satisfy the same equation modulo q. □

A direct expressibility consequence of the above theorem is the following corollary.

Corollary 3.6. *Assume* $2^n < p < 2^{n+1}$ *for some positive integer* n*. Assume* $p < q$*. Then the following hold.*

1. *If φ is an $\mathcal{L}_G$-sentence distinguishing $\mathbb{Z}_p$ and $\mathbb{Z}_q$, then it must be the case that $qr(\varphi) \geq n$.*

2. *There exists an $\mathcal{L}_G^5$-existential sentence distinguishing $\mathbb{Z}_p$ and $\mathbb{Z}_q$ with $qr(\varphi) \leq 2n$.*

Proof. Follows directly from Theorem 3.7 and Theorem 3.8. □

3.6 $\mathbb{Z}_u$: u is Integer

In this section we will extend the previous results to groups of residue classes modulo any number.

Notation 3.4.

1. *u, v are positive integers with $u < v$.*

2. *Let $H_f \leq \mathbb{Z}_u$ denote that H_f is a subgroup of $\mathbb{Z}_u$ of order f. If H_f is a proper subgroup, then we use the notation $H_f < \mathbb{Z}_u$.*

3. *Let $divisor(u) = \{f\colon f \mid u\}$.*

The following famous theorem will help us analyzing $EF(\mathbb{Z}_u, \mathbb{Z}_v)$.

Theorem 3.9 (Fact 1.3.9 in [24]). *Let $H_f \leq \mathbb{Z}_u$. Then the following hold.*

1. *H_f is cyclic and $f|u$*

2. *for each $e \in divisor(u)$, $\mathbb{Z}_u$ has exactly one subgroup of order e, namely, $\left\langle \frac{u}{e} \right\rangle$*

It is an easy fact that any finite cyclic group of order f is isomorphic to $\mathbb{Z}_f$, hence we can talk about H_f and $\mathbb{Z}_f$ interchangeably.

Remark 3.6. *In the following we will use a slightly modified definition of closed binders. In the original definition a closed binder was not supposed to contain any proper sub-binder that is also closed. However, in the following this condition will be applied only to closed binders that uniquely identify their own groups among smaller subgroups. More precisely, if t is a closed binder inside $\mathbb{Z}_u$ such that t uniquely identifies this group among its proper subgroups (that is, there does not exist any $t' \cong t$ inside any $H_f < \mathbb{Z}_u$), then t does not contain any proper closed sub-binder that uniquely identifies $\mathbb{Z}_u$ among its proper subgroups. For example, consider the group $\mathbb{Z}_8$ and consider the closed binder $t = \langle 1, 2, 4 \rangle$. It is easy to see that t uniquely distinguishes $\mathbb{Z}_8$ from $\mathbb{Z}_2$ and $\mathbb{Z}_4$. Clearly, t contains the closed sub-binders $\langle 4 \rangle$ and $\langle 2, 4 \rangle$, however, they do have isomorphic copies inside $\mathbb{Z}_2$ and $\mathbb{Z}_4$ respectively.*

Lemma 3.5. *Let t be a closed binder inside $\mathbb{Z}_u$. Then t has an isomorphic copy inside $\mathbb{Z}_v$ for every v such that $u \in divisor(v)$.*

Proof. Fix v and let $d = v/u$. Assume $x + y \equiv z \pmod{u}$ represents some triple in the signature of t. Multiply by d to get a valid equation $dx + dy \equiv dz \pmod{v}$. Let t' be the result of multiplying modulo v every element of t by d, then $t' \cong t$ and is a closed binder inside $\mathbb{Z}_v$. An important thing to note is that all the elements of t' belong to $H_u \leq \mathbb{Z}_v$, where $H_u \cong \mathbb{Z}_u$. □

The following lemma gives a lower bound on the length of a closed binder that uniquely characterizes $\mathbb{Z}_u$ among its subgroups.

Lemma 3.6. *Assume $2^n \leq u < 2^{n+1}$ for some positive integer n. Let t be a closed binder inside $\mathbb{Z}_u$ such that t has no isomorphic copy inside any $H_f < \mathbb{Z}_u$. Then it* *must be the case that $|t| \geq n$.*

Proof. Since t is not a closed binder inside any $H_f < \mathbb{Z}_u$, there must exist some $x \in t$ such that $x \notin \bigcup_{H_f < \mathbb{Z}_u} H_f$. So there is no $y \in (\mathbb{Z}_u \backslash \{0\})$ such that $xy \equiv 0 \pmod{u}$, hence x is a unit inside the ring $\mathbb{Z}_u$ (that is x has a multiplicative inverse). Multiply modulo u every element in t by x^{-1} to get an isomorphic copy t' that contains 1. Now we can proceed by applying the same argument as in Lemma 3.3 except that we need a slight change in the partition of the group into the two sets A and B when u is even (this actually is the source of the n vs. $(n+1)$ bounds given in the two lemmas). If u is even, then define $A = \{1, \ldots, \frac{p}{2} - 1\}$ and $B = \{\frac{p}{2}, \ldots, p-1\}$. Given this partition it might be the case that (for example, when $u = 2^n$) $2^{n-1} \notin A$. Hence only $(n-1)$ elements of t are guaranteed to come from A, in addition to at least one element from B making a total of at least n elements comprising the binder t. □

Remark 3.7. *The bound obtained in Lemma 3.6 is optimal for consider $u = 2^n$ and consider the closed binder $t = \langle 1, 2, 4, \ldots, 2^{n-1} \rangle$. It is easy to check that t is a closed binder inside $\mathbb{Z}_u$ and that it does not have an isomorphic copy inside $\mathbb{Z}_{2^l}$ for any $l \leq (n-1)$.*

Lemma 3.7. *Let t be a closed binder inside $\mathbb{Z}_u$ such that t has no isomorphic copy inside any $H_f < \mathbb{Z}_u$. Then t has no isomorphic copy inside $\mathbb{Z}_v$ for any v such that $u \notin divisor(v)$.*

Proof. If $v \in divisor(u)$, then the conclusion holds trivially by the hypothesis of the lemma. So assume $v \notin divisor(u)$. Let $d = gcd(u, v)$. Since $u \notin divisor(v)$, it must be the case that $d < u$. Assume $u = dl_1$ and $v = dl_2$. By way of contradiction assume there exists t' inside $\mathbb{Z}_v$ such that $t \cong t'$. Then t' must result from t by multiplying modulo v every element of t by l_2. Hence, all the elements of t' belong to the subgroup of $\mathbb{Z}_v$ generated by $l_2 = \frac{v}{d}$. This subgroup has order d. Hence t has an isomorphic copy inside $\mathbb{Z}_d$ which is a contradiction to the hypothesis of the lemma that t uniquely characterizes $\mathbb{Z}_u$ among all its proper subgroups. □

The following lemma gives a lower bound for the length of a distinguishing closed binder.

Lemma 3.8. *Let $f = min\{f' \colon f' \in (divisor(u) \triangle divisor(v))\}$. Assume $2^n \leq f < 2^{n+1}$ for some positive integer n. Let t be a closed binder that distinguishes $\mathbb{Z}_u$ from $\mathbb{Z}_v$ (that is, t has an isomorphic copy in exactly one of the two groups). Then it must be the case that $|t| \geq n$.*

***Proof*.** Without loss of generality assume that t is a closed binder inside $\mathbb{Z}_u$. Let e be minimal such that t has an isomorphic copy inside $\mathbb{Z}_e$. By Lemma 3.7 it must be the case that $e \in divisor(u)$. Since t has no isomorphic copy in $\mathbb{Z}_v$, by Lemma 3.5 $e \notin divisor(v)$. Hence $e \in (divisor(u) \Delta divisor(v))$. Given the minimality of f, then by Lemma 3.6 it must be the case that $|t| \geq n$. □

Now we are ready to give a lower bound on the number of moves needed by $\mathcal{S}$ to win the $EF(\mathbb{Z}_u, \mathbb{Z}_v)$.

Theorem 3.10. *Let $f = min\{f' \colon f' \in (divisor(u) \triangle divisor(v))\}$. Assume $2^n \leq f < 2^{n+1}$ for some positive integer n. If $EF_m(\mathbb{Z}_u, \mathbb{Z}_v) \in \mathcal{S}$, then it must be the case that $m \geq n$.*

Proof. Using the same argument as of Theorem 3.3, it can be shown that playing a distinguishing closed binder is the shortest possible strategy for $\mathcal{S}$ to win the game. Let t be such a binder. Then by Lemma 3.8, $|t| \geq n$. □

Remark 3.8. *The lower bound obtained in Theorem 3.10 is optimal. Let $v = 2^n$ for some positive integer n. Assume $u = 2^{n-1}$. Then $v = min\{f \colon f \in (divisor(u) \Delta divisor(v))\}$. Consider the closed binder $t = \langle 1, 2, 4, \ldots, 2^{n-1} \rangle$. Then by Remark 3.7, t is a winning tuple for $\mathcal{S}$.*

The next task is to find an upper bound on the number of steps needed by $\mathcal{S}$ to win the game. First, we construct a distinguishing closed binder in the following lemma whose proof is similar to that of Lemma 3.4.

Lemma 3.9. *Assume $2^n \leq u < 2^{n+1}$. Then there exists a closed binder $\mathcal{C}_u$ inside $\mathbb{Z}_u$ such that $\mathcal{C}_u$ has no isomorphic copy inside any $H_f < \mathbb{Z}_u$. Furthermore, $|\mathcal{C}_u| \leq 2n$.*

Proof. Write u in binary radix

$$u = 2^{i_k} + \cdots + 2^{i_1} \tag{3.20}$$

where $0 \leq i_1 < \cdots < i_k = n$. Let $\mathbb{E}_1$ denote the following set of congruence equations

$$\begin{gathered} x_2 \equiv 2x_1 \pmod{u} \\ x_3 \equiv 2x_2 \pmod{u} \\ \vdots \\ x_{i_k+1} \equiv 2x_{i_k} \pmod{u} \end{gathered}$$

Since $i_k = n$, $|\{x_1, \ldots, x_{i_k+1}\}| = n+1$. Let $\mathbb{E}_2$ denote the following congruence equation

$$(x_{i_1+1} + \cdots + x_{i_k+1}) \equiv 0 \pmod{u} \tag{3.21}$$

From $\mathbb{E}_1$ in the last equation we have

$$\begin{aligned} \left(2^{i_1}x_1 + \cdots + 2^{i_k}x_1\right) &\equiv 0 \pmod{u} \\ \left(2^{i_1} + \cdots + 2^{i_k}\right)x_1 &\equiv 0 \pmod{u} \\ ux_1 &\equiv 0 \pmod{u} \end{aligned} \tag{3.22}$$

$x_1 = 1$ is a solution to this last equation. However, $1 \notin H_f$ for any $H_f < \mathbb{Z}_u$. Hence, $(\mathbb{E}_1 \cup \mathbb{E}_2)$ represent the desired closed binder. The only remaining thing to do is to break $\mathbb{E}_2$ into an equivalent set of congruence equations that conform to the equation forms given in Remark (3.1). This can be easily done by introducing a new set of variables as follows.

$$\begin{aligned} &x_{i_1+1} + x_{i_2+1} \equiv y_1 \pmod{u} \\ &y_1 + x_{i_3+1} \equiv y_2 \pmod{u} \\ &\qquad\vdots \\ &y_{k-2} + x_{i_k+1} \equiv 0 \pmod{u} \end{aligned}$$

$(k-2)$ new variables were introduced. From Equation 3.20, we have $k \leq (n+1)$ (the upper bound is reached when $u = \sum_{0 \leq i \leq n} 2^i$), hence $|\{y_1, \ldots, y_{k-2}\}| \leq (n-1)$.

So we have constructed a closed binder $\mathcal{C}_u$ whose points are $\{x_1, \ldots, x_{i_k+1}, y_1 \ldots, y_{k-2}\}$.

This binder uniquely identifies $\mathbb{Z}_u$ among its proper subgroups. $|\mathcal{C}_u| \leq n+1+n-1 = 2n$. The set of congruence equations $(\mathbb{E}_1 \cup \mathbb{E}_2)$ determines the signature of $\mathcal{C}_u$. □

The following theorem gives an upper bound on the number of rounds needed by $\mathcal{S}$ to win $EF(\mathbb{Z}_u, \mathbb{Z}_v)$.

Theorem 3.11. *Let $f = min\{f' \colon f' \in (divisor(u) \bigtriangleup divisor(v))\}$. Assume $2^n \leq f < 2^{n+1}$ for some positive integer n. Then there exists $m \leq 2n$ such that $pEF^5_m(\mathbb{Z}_u, \mathbb{Z}_v) \in \mathcal{S}$.*

Proof. Without loss of generality assume $f \in divisor(u)$. $\mathcal{S}$ plays the closed binder $\mathcal{C}_f$, constructed in the proof of Lemma 3.9, inside $\mathbb{Z}_u$. By Lemma 3.7, $\mathcal{C}_f$ has no isomorphic copy inside $\mathbb{Z}_v$, hence $\mathcal{C}_f$ is a winning strategy for $\mathcal{S}$. From Lemma 3.9, $|\mathcal{C}_f| \leq 2n$. By an argument similar to that of Theorem 3.8 we can show that $\mathcal{S}$ needs at most 5 pebbles to realize $\mathcal{C}_f$. □

Now we combine Theorem 3.10 and Theorem 3.11 into one theorem.

Theorem 3.12. *Let $f = min\{f' \colon f' \in (divisor(u) \bigtriangleup divisor(v))\}$. Assume $2^n \leq f < 2^{n+1}$. Then the following hold.*

1. *If $EF_m(\mathbb{Z}_u, \mathbb{Z}_v) \in \mathcal{S}$, then it must be the case that $m \geq n$. This lower bound is optimal.*

2. *There exists $m \leq 2n$ such that $pEF^5_m(\mathbb{Z}_u, \mathbb{Z}_v) \in \mathcal{S}$. Furthermore, in her winning strategy $\mathcal{S}$ can choose all of her points from exactly one of the two groups.*

The direct expressibility consequence of the above game-theoretic bounds is given in the following corollary.

Corollary 3.7. *Assume two finite cyclic groups G and G'. Let $f = min\{f' \colon f' \in (divisor(|G|) \bigtriangleup divisor(|G'|))\}$. Assume $2^n \leq f < 2^{n+1}$. Then the following hold.*

1. *If φ is an $\mathcal{L}_G$-sentence distinguishing G and G', then it must be the case that $qr(\varphi) \geq n$. This lower bound is optimal.*
2. *There exists an existential $\mathcal{L}_G^5$-sentence φ distinguishing G and G' such that $qr(\varphi) \leq 2n$.*

3.7 Abelian Finite Groups

In this section we generalize the previous results to the class of abelian finite groups. The following is the basic theorem about the construction of these groups.

Theorem 3.13 (Frobenius-Stickelberger[24]). *An abelian group G is finite if and only if it is a direct product of finitely many cyclic groups with prime-power orders.*

This leads to the following expressibility result.

Corollary 3.8. *Assume two non-isomorphic finite abelian groups G and G'. Then there exists a positive integer f that satisfies the following.*

1. *f divides the order of one of the two groups (it may divide the orders of both groups).*
2. *Assume $2^n \leq f < 2^{n+1}$. If φ is an $\mathcal{L}_G$-sentence distinguishing G and G', then it must be the case that $qr(\varphi) \geq n$. This lower bound is optimal.*

3. There exists an existential $\mathcal{L}_G^5$-sentence φ distinguishing G and G' such that $qr(\varphi) \leq 2n$.

Proof. Since G and G' are finite abelian groups, then by Theorem 3.13

$$G \cong \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_r}$$

$$G' \cong \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_s}$$

The notion of binder is still well-defined in this more general context of finite abelian groups. Hence, using a similar argument to that of Theorem 3.3, it can be shown that playing a distinguishing closed binder is the shortest possible strategy for $\mathcal{S}$ to win the EF game. Note that the individual components of any tuple resulting from a direct product are independent from each other, that is there is no particular relation that ties them together, hence we can reduce the $EF(G, G')$ to $EF(\mathbb{Z}_{m_i}, \mathbb{Z}_{n_i})$.

Let $M = \{m_1, \ldots, m_r\}$ and let $N = \{n_1, \ldots, n_s\}$. Note that $\mathbb{Z}_{l_1} \oplus \mathbb{Z}_{l_2} \cong \mathbb{Z}_{l_2} \oplus \mathbb{Z}_{l_1}$ by the mapping that takes $(a \pmod{l_1}, b \pmod{l_2})$ to $(b \pmod{l_2}, a \pmod{l_1})$. Hence given $G \ncong G'$ it must be the case that $M \neq N$. Choose minimal f such that: (i) $f \in (M \Delta N)$ and (ii) there is no $u \in (M \cup N)$ such that $f \in divisor(u)$. Assume $f = m_j$. The $EF(G, G')$-game is now reduced to a game over $\mathbb{Z}_f$ and $\mathbb{Z}_{f'}$ where $f \notin divisor(f')$ by projecting over the j^{th} component, that is $\mathcal{S}$ always chooses her elements from G that are isomorphic to $(0, \ldots, 0, a, 0, \ldots, 0)$ where $a \in \mathbb{Z}_f$ and lies in the j^{th} position. □

3.8 Other Expressibility Results

In this section we apply the results obtained above to study expressibility of some group-theoretic notions. First, we remind the reader of some of the definitions.

Definition 3.12. *1. The* dihedral *group D_n is the symmetry group of an n-sided regular polygon. $|D_n| = 2n$ where it contains n rotations and n reflections. Dihedral groups are an example of a non-abelian group.*

2. A group is simple, *if it is non-trivial and has no non-trivial proper normal subgroups.*

3. A group is nilpotent *if its lower central series converges to the trivial subgroup after a finite number of steps of application of the commutator operator.*

4. The normal closure *of an element $g \in G$ is the smallest normal subgroup of G containing g.*

Assume $g \in G$. Let $o(g)$ denote $|\langle g \rangle|$. The following lemma shows an interesting relationship between elementary equivalence of dihedral groups and elementary equivalence of groups of residue classe.

Lemma 3.10. $D_m \equiv_l D_n \iff \mathbb{Z}_m \equiv_l \mathbb{Z}_n$

Proof. $|D_m| = 2m$ and the group is generated by two elements g_1, h_1 where $o(g_1) = 2$ and $o(h_1) = m$. Similarly, D_n is generated by g_2, h_2 where $o(g_2) = 2$ and $o(h_2) = n$. The right-to-left direction is Lemma 4.3 in [19]. Now assume $D_m \equiv_l D_n$, need to show $\mathbb{Z}_m \equiv_l \mathbb{Z}_n$. From Theorem 3.1, need to show $EF_l(\mathbb{Z}_m, \mathbb{Z}_n) \in \mathcal{D}$. While playing the game over $\mathbb{Z}_m$ and $\mathbb{Z}_n$, another l-round fictitious game is played over D_m and D_n in which the duplicator uses her winning strategy as described in the proof of Lemma 4.3 in [19]. Suppose $\mathcal{S}$ chooses $j \in \mathbb{Z}_m$. This corresponds to her choosing $h_1^j \in D_m$ in the fictitious game. Then $\mathcal{D}$ would respond with $h_2^k \in D_n$ for some $k \in \{0, \ldots, n-1\}$. Then in the real game $\mathcal{D}$ responds by playing $k \in \mathbb{Z}_n$. If $\mathcal{S}$ chooses $j \in \mathbb{Z}_n$, one plays in a similar way.

Suppose in the real game the players have chosen the elements $\langle a_1, \ldots, a_l \rangle \in \mathbb{Z}_m$ and $\langle b_1, \ldots, b_l \rangle \in \mathbb{Z}_n$. Let the corresponding elements chosen in the fictitious game be $\langle a'_1, \ldots, a'_l \rangle \in D_m$ and $\langle b'_1, \ldots, b'_l \rangle \in D_n$. $\mathcal{D}$ wins the fictitious game, hence $a'_{i_1} a'_{i_2} = a'_{i_3} \iff b'_{i_1} b'_{i_2} = b'_{i_3}$. We need to show that $a_{i_1} + a_{i_2} \equiv a_{i_3} \pmod{m} \iff b_{i_1} + b_{i_2} \equiv b_{i_3} \pmod{n}$.

$$a_{i_1} + a_{i_2} \equiv a_{i_3} \pmod{m} \iff h_1^{a_{i_1}} h_1^{a_{i_2}} = h_1^{a_{i_3}} \iff a'_{i_1} a'_{i_2} = a'_{i_3} \iff$$
$$b'_{i_1} b'_{i_2} = b'_{i_3} \iff h_2^{b_{i_1}} h_2^{b_{i_2}} = h_2^{b_{i_3}} \iff b_{i_1} + b_{i_2} \equiv b_{i_3} \pmod{n}$$

□

From the previous lemma and the bounds obtained above for distinguishing of $\mathbb{Z}_m$ and $\mathbb{Z}_n$ we can obtain similar bounds for D_m and D_n as indicated in the following theorem.

Theorem 3.14. *Let $f = min\{f' \colon f' \in (divisor(m) \bigtriangleup divisor(n))\}$. Assume $2^l \leq f < 2^{l+1}$. Then the following hold.*

1. *If φ is an $\mathcal{L}_G$-sentence distinguishing D_m and D_n, then it must be the case that $qr(\varphi) \geq l$. This lower bound is optimal*

2. *There exists an existential $\mathcal{L}_G^5$-sentence φ distinguishing D_m and D_n such that $qr(\varphi) \leq 2l$.*

Proof. Follows directly from Lemma 3.10 and Corollary 3.7. □

In the following we present a sequence of undefinability results that follow from the expressibility bounds obtained above (some of them have already been proved in [19] using model-theoretic techniques).

Theorem 3.15. *The closure of a single element is not first-order definable on the class of finite groups.*

Proof. By way of contradiction assume there exists an $\mathcal{L}_G$-formula $\varphi(x, y)$ that defines the closure of y. Assume $qr(\varphi) = k$. Let $p \geq 2^{k+3}$ be a prime. Let $n = pq$ for $q > p$ is also a prime. Consider the two groups $\mathbb{Z}_p$ and $\mathbb{Z}_n$. From Corollary 3.7, we have $\mathbb{Z}_p \equiv_{k+2} \mathbb{Z}_n$. Then there exists an element $g \in \mathbb{Z}_p \backslash \{0\}$ such that $(\mathbb{Z}_p, g) \equiv_{k+1} (\mathbb{Z}_n, q)$. The closure of g in $\mathbb{Z}_p$ is the whole group whereas the closure of q in $\mathbb{Z}_n$ is a subgroup $H \cong \mathbb{Z}_p$. Hence

$$\mathbb{Z}_p \models \forall x \varphi(x, g) \textit{ and } \mathbb{Z}_n \not\models \forall x \varphi(x, q)$$

$qr(\forall x \varphi(x, y)) = k + 1$ hence we get a contradiction since $(\mathbb{Z}_p, g) \equiv_{k+1} (\mathbb{Z}_n, q)$. □

Theorem 3.16. *Simplicity is not first-order definable on the class of finite groups.*

Proof. By way of contradiction assume that simplicity is definable by a first-order $\mathcal{L}_G$-sentence σ. Assume $qr(\sigma) = k$. Let p be a prime number such that $p \geq 2^{k+1}$. Consider the groups $\mathbb{Z}_p$ and $\mathbb{Z}_{p^2}$. From Corollary 3.7 we have $\mathbb{Z}_p \equiv_k \mathbb{Z}_{p^2}$. It can be easily checked that $\mathbb{Z}_p$ is simple whereas $\mathbb{Z}_{p^2}$ is not hence $\mathbb{Z}_p \models \sigma$ and $\mathbb{Z}_{p^2} \not\models \sigma$ which is a contradiction. □

Theorem 3.17. *Cyclicity is not first-order definable on the class of finite groups.*

Proof. By way of contradiction assume that cyclicity is definable by a first-order $\mathcal{L}_G$-sentence σ. Assume $qr(\sigma) = k$. Let p be a prime number such that $p \geq 2^{k+1}$. Consider the groups $G = \mathbb{Z}_p$ and $H = \mathbb{Z}_p \times \mathbb{Z}_p$. From Corollary 3.8, we have $G \equiv_k H$. It is easy to check that G is cyclic and H is not (since p and p are not coprimes), hence $G \models \sigma$ and $H \not\models \sigma$ which is a contradiction. □

Theorem 3.18. *Nilpotency is not first-order definable on the class of finite groups.*

Proof. By way of contradiction assume that nilpotency is definable by a first-order $\mathcal{L}_G$-sentence σ. Assume $qr(\sigma) < k$. Consider the dihedral groups D_{2^k} and $D_{p \cdot 2^k}$ where $p > 2^k$ is prime. From Theorem 3.14, we have $D_{2^k} \equiv_{k-1} D_{p \cdot 2^k}$. D_{2^k} is nilpotent whereas $D_{p \cdot 2^k}$ is not (D_n is nilpotent if and only if n is a power of 2). Hence $D_{2^k} \models \sigma$ and $D_{p \cdot 2^k} \not\models \sigma$ which is a contradiction. □

Theorem 3.19. *The normal closure of a single element is not first-order definable on the class of finite groups*

Proof. By way of contradiction assume there is an $\mathcal{L}_G$-formula $\varphi(x, y)$ that defines the normal closure of y. Assume $qr(\varphi) = k$. Let p be a prime such that $p \geq 2^{k+3}$. Consider the two groups $\mathbb{Z}_p$ and $\mathbb{Z}_{p^2}$. From Corollary 3.7 we have $\mathbb{Z}_p \equiv_{k+2} \mathbb{Z}_{p^2}$, hence there exists $g \in \mathbb{Z}_p \backslash \{0\}$ such that $(\mathbb{Z}_p, g) \equiv_{k+1} (\mathbb{Z}_{p^2}, p)$. The normal closure of g in $\mathbb{Z}_p$ is the whole group and that of p in $\mathbb{Z}_{p^2}$ is $G \cong \mathbb{Z}_p$. Hence

$$\mathbb{Z}_p \models \forall x \varphi(x, g) \textit{ and } \mathbb{Z}_{p^2} \not\models \forall x \varphi(x, p)$$

$qr(\forall x \varphi(x, y)) = k + 1$, hence we get a contradiction. □

3.9 Open Problems

The following are still open for further research.

1. Can the lower/upper bounds of $n/2n$ on the quantifier rank of a distinguishing sentence (for groups of residue classes and dihedral groups) be improved? We have already shown that n is an optimal lower bound and we believe that the upper bound is also optimal.

2. Can the upper bound of 5 on the number of object variables in a distinguishing sentence be improved?

3. Investigate the complexity-theoretic consequences of these expressibility results.

4. Generalize the results to all finite groups (we have already started here with dihedral groups).

5. Study the first-order expressibility of infinite groups.

6. Use other formalisms such as fixed-point logic, infinitary logics, second-order logic, allowing for generalized quantifiers, etc.

Chapter 4

Abstract Elementary Classes

4.1 Basic Definitions

Definition 4.1 (**Abstract elementary classes**). *Assume a vocabulary τ. Let $\mathscr{K} = (\mathbb{K}, \preceq_{\mathscr{K}})$ be a partial ordering with domain $\mathbb{K}$ of τ-structures. Then $\mathscr{K}$ is an abstract elementary class if it satisfies the following axioms.*

1. *Closure under isomorphism:*

   (a) *Let $\mathcal{M} \in \mathscr{K}$. Assume a τ-structure $\mathcal{N}$ such that $\mathcal{M} \cong \mathcal{N}$, then $\mathcal{N} \in \mathscr{K}$.*

   (b) *Let $\mathcal{M}_1, \mathcal{M}_2, \mathcal{N}_1, \mathcal{N}_2 \in \mathscr{K}$. Assume $f_l \colon \mathcal{M}_l \cong \mathcal{N}_l$ for $l = 1, 2$ such that $f_1 \subseteq f_2$. If $\mathcal{M}_1 \preceq_{\mathscr{K}} \mathcal{M}_2$, then $\mathcal{N}_1 \preceq_{\mathscr{K}} \mathcal{N}_2$.*

2. *Refining the substructure relation: Let $\mathcal{M}, \mathcal{N} \in \mathscr{K}$. If $\mathcal{M} \preceq_{\mathscr{K}} \mathcal{N}$, then $\mathcal{M} \subseteq \mathcal{N}$.*

3. *Closure under Tarski-Vaught Chains: Let $\langle \mathcal{M}_i \colon i < \delta \rangle$ be an increasing continuous $\preceq_{\mathscr{K}}$-chain of models from $\mathscr{K}$, then*

   (a) *$\bigcup_{i<\delta} \mathcal{M}_i \in \mathscr{K}$*

   (b) *for every $j < \delta$, $\mathcal{M}_j \preceq_{\mathscr{K}} \bigcup_{i<\delta} \mathcal{M}_i$*

   (c) *if for every $j < \delta$, $\mathcal{M}_j \preceq_{\mathscr{K}} \mathcal{N}$ for some $\mathcal{N} \in \mathscr{K}$, then $\bigcup_{i<\delta} \mathcal{M}_i \preceq_{\mathscr{K}} \mathcal{N}$*

4. *Coherence: Let $\mathcal{M}_0, \mathcal{M}_1, \mathcal{M}_2 \in \mathscr{K}$ such that $\mathcal{M}_0 \preceq_{\mathscr{K}} \mathcal{M}_2$, $\mathcal{M}_1 \preceq_{\mathscr{K}} \mathcal{M}_2$, and $\mathcal{M}_0 \subseteq \mathcal{M}_1$, then $\mathcal{M}_0 \preceq_{\mathscr{K}} \mathcal{M}_1$.*

5. *Downward Löwenheim-Skolem axiom: There is a Löwenheim-Skolem number for $\mathscr{K}$ denoted $LSK(\mathscr{K})$ which is the minimal cardinal κ such that for every $\mathcal{N} \in \mathscr{K}$ and $A \subseteq N$, there exists $\mathcal{M} \in \mathscr{K}$ such that $A \subseteq M \preceq_{\mathscr{K}} \mathcal{N}$ and $|M| = |A| + \kappa$.*

The relation $\preceq_{\mathscr{K}}$ yields a natural notion of *$\mathscr{K}$-embedding* $f\colon \mathcal{M} \longrightarrow \mathcal{N}$ which satisfies $f(\mathcal{M}) \preceq_{\mathscr{K}} \mathcal{N}$.

Remark 4.1. 1. *Let $\mathcal{M}, \mathcal{N} \in \mathscr{K}$. Assume a $\mathscr{K}$-embedding $f\colon \mathcal{M} \longrightarrow \mathcal{N}$. Then by Definition (4.1).2, f is an isomorphism from $\mathcal{M}$ onto $f(\mathcal{M})$, in other words $\mathscr{K}$-embedding refines the isomorphism function.*

2. *Assume $\mathcal{M}, \mathcal{N} \in \mathscr{K}$ such that $\mathcal{M} \preceq_{\mathscr{K}} \mathcal{N}$. Let f be an automorphism of $\mathcal{N}$. Let $\mathcal{M}' = f(\mathcal{M})$. Then by Definition (4.1).1 it must be the case that $\mathcal{M}' \in \mathscr{K}$ and $\mathcal{M}' \preceq_{\mathscr{K}} \mathcal{N}$.*

Definition 4.2 (Amalgamation). 1. *Let $\mathcal{M} \in \mathscr{K}$. We say that $\mathcal{M}$ is an* amalgamation base *if for every $\mathcal{M}_1, \mathcal{M}_2 \in \mathscr{K}$ and for every $\preceq_{\mathscr{K}}$-embeddings $f_i\colon \mathcal{M} \longrightarrow \mathcal{M}_i$ for $i = 1, 2$, there is a model $\mathcal{M}^* \in \mathscr{K}$ called* the amalgam *and $\preceq_{\mathscr{K}}$-embeddings $g_i\colon \mathcal{M}_i \longrightarrow \mathcal{M}^*$ for $i = 1, 2$ such that $(g_1 \circ f_1) \restriction \mathcal{M} = (g_2 \circ f_2) \restriction \mathcal{M}$.*

2. *We say that $\mathscr{K}$ has the* amalgamation property (AP) *if every $\mathcal{M} \in \mathscr{K}$ is an amalgamation base.*

In most applications of the *AP* we take $\mathcal{M} \preceq_{\mathscr{K}} \mathcal{M}_i$, that is $f_i = id$ and we take $\mathcal{M}^*$ to be a $\preceq_{\mathscr{K}}$-extension of either $\mathcal{M}_1$ or $\mathcal{M}_2$, that is either g_1 or g_2 is the identity. In first-order model theory the *AP* follows directly from *compactness* and it allows (along with the joint embedding property defined below) the identification (in a suitable monster model) of a *syntactic type* (the description of a point by the formulas it satisfies) with an *orbit* under the automorphism group of this monster model [2].

Definition 4.3 (**Joint embedding**). *We say that $\mathscr{K}$ has the* joint embedding property *(JEP) if for every $\mathcal{M}_1, \mathcal{M}_2 \in \mathscr{K}$ there exists $\mathcal{M}^* \in \mathscr{K}$ and $\preceq_{\mathscr{K}}$-embeddings $g_i \colon \mathcal{M}_i \longrightarrow \mathcal{M}^*$ for $i = 1, 2$.*

Assumption 4.1. *Unless otherwise stated, we will always assume the following.*

1. *$\mathscr{K}$ has the amalgamation property.*

2. *$\mathscr{K}$ has the joint embedding property.*

3. *$\mathscr{K}$ has arbitrarily large models.*

These properties imply that $\mathscr{K}$ has no maximal models.

Definition 4.4 (**Model homogeneous**). 1. *Assume a cardinal $\lambda > LSK(\mathscr{K})$. Let $\mathcal{N} \in \mathscr{K}$. We say that $\mathcal{N}$ is* λ-model homogeneous *if the following holds: assume $\mathcal{M}, \mathcal{M}' \in \mathscr{K}$ such that $\mathcal{M} \preceq_{\mathscr{K}} \mathcal{M}'$ and $|M|, |M'| < \lambda$, if there is a $\mathscr{K}$-embedding $f \colon \mathcal{M} \longrightarrow \mathcal{N}$, then there exists a $\mathscr{K}$-embedding $f' \colon \mathcal{M}' \longrightarrow \mathcal{N}$ such that $f \subseteq f'$. We also allow $\mathcal{M}$ to be empty, hence any $\mathcal{M}' \in \mathscr{K}$ of cardinality less than λ $\mathscr{K}$-embeds into $\mathcal{N}$.*

2. *We say that $\mathcal{N}$ is* strongly λ-model homogeneous *if (i) $\mathcal{N}$ is λ-model homogeneous and (ii) for every $\mathcal{M}, \mathcal{M}' \in \mathscr{K}$ such that $\mathcal{M}, \mathcal{M}' \preceq_{\mathscr{K}} \mathcal{N}$, and $|M|, |M'| < \lambda$, if $f\colon \mathcal{M} \cong \mathcal{M}'$, then f can be extended to an automorphism of $\mathcal{N}$.*

Remark 4.2. *Assume $\mathcal{N} \in \mathscr{K}$ is strongly λ-model homogeneous for $\lambda > LSK(\mathscr{K})$. Let $\mathcal{M} \in \mathscr{K}$ be such that $\mathcal{M} \subseteq \mathcal{N}$ and $|M| < \lambda$. Then $\mathcal{M} \preceq_{\mathscr{K}} \mathcal{N}$.*

By repeated application of AP and JEP we can construct homogeneous models. In addition if $\mathscr{K}$ has arbitrarily large models, that is Assumption 4.1 holds, we can construct a large strongly λ^*-homogeneous model called the *monster*. The monster model has two properties: (i) it has power λ^* where λ^* is strongly inaccessible cardinal and (ii) it must be strongly λ^*-model homogeneous. The existence of the monster allows us to assume that *all models of power less than λ lie inside it.* We will denote the monster as $\mathfrak{C}$ and will always assume working inside it.

Lemma 4.1 (**Uniqueness of homogeneous models**). *Let $\mathcal{N}, \mathcal{N}' \in \mathscr{K}$ such that $|N| = |N'| = \mu$. Assume $\mathcal{N}, \mathcal{N}'$ are μ-model homogeneous, then $\mathcal{N} \cong \mathcal{N}'$.*

Proof. Write $\mathcal{N}$ as the limit of a continuous $\preceq_{\mathscr{K}}$-increasing sequence of models $\langle \mathcal{N}_i \colon i < \mu \rangle$, where $|N_i| < \mu$. Similarly, write $\mathcal{N}'$ as the limit of $\langle \mathcal{N}'_i \colon i < \mu \rangle$. By a back-and-forth argument we define an increasing sequence of $\mathscr{K}$-embeddings $\langle f_i \colon i < \mu \rangle$ whose limit is an isomorphism from $\mathcal{N}$ onto $\mathcal{N}'$.

Base case: Consider $\mathcal{N}_0$. By μ-model homogeneity of $\mathcal{N}'$, there exists a $\mathscr{K}$-embedding $f_0 \colon \mathcal{N}_0 \longrightarrow \mathcal{N}'$.

Odd successor stage: Let $\alpha = \beta + (2k + 1)$ where β is a limit ordinal or 0 and k

is a non-negative integer. Let $\gamma = \beta + 2k$. Assume f_γ has been constructed with $\mathcal{M} = dom(f_\gamma)$ and $\mathcal{M}' = ran(f_\gamma)$ such that $\mathcal{M} \preceq_{\mathscr{K}} \mathcal{N}$, $\mathcal{M}' \preceq_{\mathscr{K}} \mathcal{N}'$, and $\mathcal{N}_{\beta+k} \subseteq \mathcal{M}$. Notice that f_γ^{-1} is a $\mathscr{K}$-embedding from $\mathcal{M}'$ into $\mathcal{N}$. We want to construct a $\mathscr{K}$-embedding f_α from a small strong substructure of $\mathcal{N}$ into $\mathcal{N}'$ such that $f_\gamma \subseteq f_\alpha$ and $\mathcal{N}'_{\beta+k} \subseteq ran(f_\alpha)$. If $\mathcal{N}'_{\beta+k} \subseteq \mathcal{M}'$, then we are done by letting $f_\alpha = f_\gamma$. Otherwise, by *the downward Löwenheim-Skolem axiom* find $\mathcal{M}'' \preceq_{\mathscr{K}} \mathcal{N}'$ such that $|M''| < \mu$ and $\big(\mathcal{M}' \cup \mathcal{N}'_{\beta+k}\big) \subseteq \mathcal{M}''$. We have $\mathcal{M}' \preceq_{\mathscr{K}} \mathcal{N}'$, $\mathcal{M}'' \preceq_{\mathscr{K}} \mathcal{N}'$, and $\mathcal{M}' \subseteq \mathcal{M}''$ (since both are included in $\mathcal{N}'$), hence by *the coherence axiom* we have $\mathcal{M}' \preceq_{\mathscr{K}} \mathcal{M}''$. By μ-model homogeneity of $\mathcal{N}$, f_γ^{-1} can be extended to a $\mathscr{K}$-embedding $h\colon \mathcal{M}'' \longrightarrow \mathcal{N}$. Let $f_\alpha = h^{-1}$.

Even successor stage: Let $\alpha = \beta + 2k$ where β is a limit ordinal or 0 and k is a positive integer. Let $\gamma = \beta + (2k-1)$. Assume f_γ has been constructed with $\mathcal{M} = dom(f_\gamma)$ and $\mathcal{M}' = ran(f_\gamma)$ such that $\mathcal{M} \preceq_{\mathscr{K}} \mathcal{N}$, $\mathcal{M}' \preceq_{\mathscr{K}} \mathcal{N}'$, and $\mathcal{N}'_{\beta+(k-1)} \subseteq \mathcal{M}'$. We want to construct a $\mathscr{K}$-embedding f_α from a small strong substructure of $\mathcal{N}$ into $\mathcal{N}'$ such that $f_\gamma \subseteq f_\alpha$ and $\mathcal{N}_{\beta+k} \subseteq dom(f_\alpha)$. The argument then is very similar to the odd successor case.

Limit case: Let $\delta < \mu$ be a limit ordinal. Then let $f_\delta = \bigcup_{\alpha<\delta} f_\alpha$. Then by construction we have $\mathcal{N}_\delta \subseteq dom(f_\delta)$ and $\mathcal{N}'_\delta \subseteq ran(f_\delta)$. $\square_{Induction}$

Let $f_\mu = \bigcup_{\alpha<\mu} f_\alpha$, then $f_\mu\colon \mathcal{N} \cong \mathcal{N}'$. □

4.2 Examples of AEC's

The following example is based on that given in Chapter 6 of [2].

Example 4.1. *Let Q be the quantifier 'there exist uncountably many'. Let ψ be a sentence in $\mathcal{L}_{\omega_1\omega}(Q)$ in a countable vocabulary and let $\mathcal{L}^*$ be the smallest countable fragment of $\mathcal{L}_{\omega_1\omega}(Q)$ containing ψ ($\mathcal{L}^*$ contains all the quantifier-free formulas and is first-order closed). Define $\mathscr{K} = (\mathbb{K}, \preceq_{\mathscr{K}})$ such that $\mathbb{K}$ is exactly the class of models of ψ and for every $\mathcal{M}, \mathcal{N} \in \mathscr{K}$, $\mathcal{M} \preceq_{\mathscr{K}} \mathcal{N}$ if the following hold:*

1. *$\mathcal{M} \preceq_{\mathcal{L}^*} \mathcal{N}$ (elementary substructure with respect to the language $\mathcal{L}^*$)*

2. *for every $\mathcal{L}^*$-formula $\varphi(x, \bar{y})$ and for every $\bar{b} \in M$, if $\mathcal{M} \models \neg Qx\varphi(x, \bar{b})$, then $\varphi(\mathcal{M}, \bar{b}) = \varphi(\mathcal{N}, \bar{b})$*

We will show that $\mathscr{K}$ is an AEC with Löwenheim-Skolem number $\aleph_1$.

1. *Assume $\mathcal{M}, \mathcal{N}_1, \mathcal{N}_2, \mathcal{N}_3 \in \mathscr{K}$. It is clear that $\mathcal{M} \preceq_{\mathscr{K}} \mathcal{M}$, hence $\preceq_{\mathscr{K}}$ is reflexive. Assume $\mathcal{N}_1 \preceq_{\mathscr{K}} \mathcal{N}_2 \preceq_{\mathscr{K}} \mathcal{N}_3$. This implies $\mathcal{N}_1 \preceq_{\mathcal{L}^*} \mathcal{N}_2 \preceq_{\mathcal{L}^*} \mathcal{N}_3$. Hence, $\mathcal{N}_1 \preceq_{\mathcal{L}^*} \mathcal{N}_3$ by transitivity of $\preceq_{\mathcal{L}^*}$. Let $\bar{b} \in N_1$ and let $\varphi(x, \bar{y}) \in \mathcal{L}^*$. Assume $\mathcal{N}_1 \models \neg Qx\varphi(x, \bar{b})$. Since $\mathcal{N}_1 \preceq_{\mathscr{K}} \mathcal{N}_2$, we have $\varphi(\mathcal{N}_1, \bar{b}) = \varphi(\mathcal{N}_2, \bar{b})$, hence $\mathcal{N}_2 \models \neg Qx\varphi(x, \bar{b})$. Since $\mathcal{N}_2 \preceq_{\mathscr{K}} \mathcal{N}_3$, we have $\varphi(\mathcal{N}_2, \bar{b}) = \varphi(\mathcal{N}_3, \bar{b})$. So $\varphi(\mathcal{N}_1, \bar{b}) = \varphi(\mathcal{N}_3, \bar{b})$. This indicates that $\mathcal{N}_1 \preceq_{\mathscr{K}} \mathcal{N}_3$, and therefore $\preceq_{\mathscr{K}}$ is transitive. It is clear that $\preceq_{\mathscr{K}}$ is antisymmetric (since $\preceq_{\mathcal{L}^*}$ is). Hence, $\preceq_{\mathscr{K}}$ is a partial ordering.*

2. *Let $\mathcal{M}, \mathcal{N} \in \mathscr{K}$ such that $\mathcal{M} \preceq_{\mathscr{K}} \mathcal{N}$. Then $\mathcal{M} \preceq_{\mathcal{L}^*} \mathcal{N}$, hence $\mathcal{M} \subseteq \mathcal{N}$.*

3. *Assume $\overline{\mathcal{M}} = \langle \mathcal{M}_i \colon i < \delta \rangle$ is a continuous $\preceq_{\mathscr{K}}$-increasing chain of models from $\mathscr{K}$. Let $\mathcal{M}_\delta = \bigcup \{\mathcal{M}_i \colon i < \delta\}$.*

- *By the definition of $\mathscr{K}$, $\mathcal{M}_i \models \psi$ for every $i < \delta$. Hence $\mathcal{M}_\delta \models \psi$, therefore $\mathcal{M}_\delta \in \mathscr{K}$.*

- *Fix some $i < \delta$ and let α be the least limit ordinal such that $i < \alpha \leq \delta$. It is clear that $\mathcal{M}_i \preceq_{\mathcal{L}^*} \mathcal{M}_\delta$ (using the Tarski-Vaught test). Let $\varphi(x, \bar{y}) \in \mathcal{L}^*$ and assume $\bar{b} \in M_i$ such that $\mathcal{M}_i \models \neg Qx\varphi(x, \bar{b})$. BWOC assume $\varphi(\mathcal{M}_i, \bar{b}) \neq \varphi(\mathcal{M}_\alpha, \bar{b})$. Then $\varphi(\mathcal{M}_i, \bar{b}) \neq \varphi(\mathcal{M}_j, \bar{b})$ for $i < j < \alpha$ and j is a successor ordinal. Given the choice of α, there are only finite number of points between i and j. Hence, by transitivity of $\preceq_{\mathscr{K}}$ it must be the case that $\mathcal{M}_i \preceq_{\mathscr{K}} \mathcal{M}_j$ which is a contradiction. Therefore, $\varphi(\mathcal{M}_i, \bar{b}) = \varphi(\mathcal{M}_\alpha, \bar{b})$. Repeating this argument inductively over $\overline{\mathcal{M}}$, we can show that $\mathcal{M}_i \preceq_{\mathscr{K}} \mathcal{M}_\delta$.*

- *Assume some $\mathcal{N} \in \mathscr{K}$ such that $\mathcal{M}_i \preceq_{\mathscr{K}} \mathcal{N}$ for every $i < \delta$. Then $\mathcal{M}_i \preceq_{\mathcal{L}^*} \mathcal{N}$, hence by the Tarski-Vaught test and the continuity of the chain we have $\mathcal{M}_\delta \preceq_{\mathcal{L}^*} \mathcal{N}$. Assume $\mathcal{M}_\delta \models \neg Qx\varphi(x, \bar{b})$. Since $\overline{M}$ is continuous, there exists $\alpha < \delta$ such that $\varphi(\mathcal{M}_\alpha, \bar{b}) = \varphi(\mathcal{M}_\delta, \bar{b})$. Given $\mathcal{M}_\alpha \preceq_{\mathscr{K}} \mathcal{N}$, then $\varphi(\mathcal{M}_\alpha, \bar{b}) = \varphi(\mathcal{N}, \bar{b})$. Hence, $\varphi(\mathcal{M}_\delta, \bar{b}) = \varphi(\mathcal{N}, \bar{b})$ which implies $\mathcal{M}_\delta \preceq_{\mathscr{K}} \mathcal{N}$.*

4. *Let $\mathcal{M}_1, \mathcal{M}_2, \mathcal{N} \in \mathscr{K}$ such that $\mathcal{M}_1 \preceq_{\mathscr{K}} \mathcal{N}$, $\mathcal{M}_2 \preceq_{\mathscr{K}} \mathcal{N}$, and $\mathcal{M}_1 \subseteq \mathcal{M}_2$. It is easy to conclude the coherence of $\preceq_{\mathcal{L}^*}$, hence $\mathcal{M}_1 \preceq_{\mathcal{L}^*} \mathcal{M}_2$. Let $\bar{b} \in M_1$ and assume $\mathcal{M}_1 \models \neg Qx\varphi(x, \bar{b})$. Since $\mathcal{M}_1 \preceq_{\mathscr{K}} \mathcal{N}$ then $\varphi(\mathcal{M}_1, \bar{b}) = \varphi(\mathcal{N}, \bar{b})$. We have $\mathcal{M}_1 \preceq_{\mathcal{L}^*} \mathcal{M}_2$, hence $\mathcal{M}_2 \models \neg Qx\varphi(x, \bar{b})$ and given $\mathcal{M}_2 \preceq_{\mathscr{K}} \mathcal{N}$ we have $\varphi(\mathcal{M}_2, \bar{b}) = \varphi(\mathcal{N}, \bar{b})$. Therefore, $\varphi(\mathcal{M}_1, \bar{b}) = \varphi(\mathcal{M}_2, \bar{b})$ and $\mathcal{M}_1 \preceq_{\mathscr{K}} \mathcal{M}_2$.*

Hence $\mathscr{K}$ has the coherence property.

5. *$LSK(\mathscr{K}) = \aleph_1$ follows from: (i) $\mathcal{L}^*$ is countable, (ii) downward Löwenhiem-Skolem theorem for $\mathcal{L}^*$, and (iii) the existence of the quantifier Q in the language which asserts the existence of uncountably many realizations.*

The following example is due to David Kueker.

Example 4.2. *Let the vocabulary $\tau = \{P\}$ where P is a unary relation symbol. Define $\mathscr{K} = (\mathbb{K}, \preceq_{\mathscr{K}})$ as follows:*

$$\mathbb{K} = \{\mathcal{M}\colon |P^{\mathcal{M}}| = \aleph_0 \textit{ and } |(\neg P)^{\mathcal{M}}| \geq \aleph_0\}$$

Let $\mathcal{M}, \mathcal{N} \in \mathbb{K}$, then $\mathcal{M} \preceq_{\mathscr{K}} \mathcal{N}$ if

1. $\mathcal{M} \subseteq \mathcal{N}$

2. $P^{\mathcal{M}} = P^{\mathcal{N}}$

It can be easily checked that $\mathscr{K}$ is an AEC. However, if $\preceq_{\mathscr{K}}$ is redefined to be the regular elementary substructure relation $\preceq$, then $\mathscr{K}$ will fail to be an AEC because of the violation of the Tarski-Vaught chains axiom. Let $\langle \mathcal{M}_i\colon i < \aleph_1\rangle$ be a $\preceq$-elementary increasing chain of models from $\mathscr{K}$, where at each step i, a new element is added to $P^{\mathcal{M}_i}$. Let $\mathcal{M} = \bigcup_{i<\aleph_1} \mathcal{M}_i$, then $|P^{\mathcal{M}}| = \aleph_1$, hence $\mathcal{M} \notin \mathscr{K}$.

4.3 Presentation Theorem

The presentation theorem allows us to replace the entirely semantic description of *AEC*'s by a syntactic one [3]. It shows that every *AEC* can be represented as a *pseudoelementary class* omitting a set of types. This theorem has an important consequence of allowing us to use the technology of *Ehrenfeucht-Mostowski models* which plays a crucial role in proving results about $AEC's$ especially under the assumption of categoricity. The proof is basically a generalization of the Fraïssé construction of countable structures.

Theorem 4.1 (**Presentation theorem**). *Let $\mathscr{K}$ be an abstract elementary class in vocabulary τ. Let κ be an infinite cardinal. Assume $LSK(\mathscr{K}) = \kappa$ with $|\tau| \leq \kappa$. Then there exists a vocabulary τ' extending τ with cardinality κ, a first-order τ'-theory T', and a set Γ of first-order pure τ'-types (without parameters) with cardinality at most 2^κ such that*

i.

$$\mathscr{K} = \{\mathcal{M}' \restriction \tau \colon \mathcal{M}' \models T' \textit{ and } \mathcal{M}' \textit{ omits } \Gamma\}$$

ii. let $\mathcal{M}', \mathcal{N}'$ be τ'-structures such that

- $\mathcal{M}' \subseteq \mathcal{N}'$
- $\mathcal{M}', \mathcal{N}' \models T'$
- $\mathcal{M}', \mathcal{N}'$ *omit* Γ

then

$$\mathcal{M}' \restriction \tau \preceq_{\mathscr{K}} \mathcal{N}' \restriction \tau$$

Proof. Let

$$\tau' = \tau \cup \{F^n_i \colon i < \kappa, n < \omega \; and \; F^n_i \; is \; an \; n-ary \; function \; symbol\}$$

Then τ' extends τ and $|\tau'| = \kappa$. Let $T' = \{\exists x x = x\}$, that is the theory T' just asserts that its models are non-empty. For any τ'-structure $\mathcal{M}' \models T'$ we always assume the following partial interpretation of the new function symbols

$$\forall n < \omega \colon \forall \bar{a} \in M', \bar{a} = \langle a_0, \ldots, a_{n-1} \rangle : \forall\, i < n \colon (F_i^n)^{\mathcal{M}'}(\bar{a}) = a_i$$

Let $\mathcal{M} \in \mathscr{K}$ with $|\mathcal{M}| \geq \kappa$, let $\mathcal{M}'$ be an arbitrary expansion of $\mathcal{M}$ to a τ'-structure. Let $n \in \omega$, let $\bar{a} \in M'$ with $|\bar{a}| = n$. Let

$$M'_{\bar{a}} = \{(F_i^n)^{\mathcal{M}'}(\bar{a}) \colon i < \kappa\}$$

Notice that $\bar{a} \in M'_{\bar{a}}$ by the partial interpretation of the function symbols given above. It is also important to notice that $\mathcal{M}'_{\bar{a}}$ may neither be a τ'-structure nor a τ-structure (τ may contain other functions). Let $qf - tp(\bar{a})$ denote the pure τ'-quantifier free type of $\bar{a}$. Let

$$\Gamma = \{qf - tp(\bar{a}) \colon either\ \mathcal{M}'_{\bar{a}} \restriction \tau \notin \mathscr{K}\ or\ for\ some\ \bar{b} \subseteq \bar{a},$$

$$\mathcal{M}'_{\bar{b}} \restriction \tau \not\leq_{\mathscr{K}} \mathcal{M}'_{\bar{a}} \restriction \tau\}$$

Since $|\tau'| = \kappa$, then $|\Gamma| \leq 2^\kappa$.

<u>claim I:</u> T' and Γ satisfy part (i)

<u>proof of claim I:</u> $\Longleftarrow$: Let $\mathcal{N} \in \{\mathcal{M}' \restriction \tau \colon \mathcal{M}' \models T'\ and\ \mathcal{M}'\ omits\ \Gamma\}$, need to show that $\mathcal{N} \in \mathscr{K}$. Let $\mathcal{N}'$ denote its τ' expansion. Since $\mathcal{N}'$ omits Γ, then for every $\bar{a} \in \mathcal{N}'$ it is the case that $\mathcal{N}'_{\bar{a}} \restriction \tau \in \mathscr{K}$. Write $\mathcal{N}$ as the direct limit of all these finitely generated subsets $\mathcal{N}'_{\bar{a}}$. Then by the union of chains axiom we have $\mathcal{N}' \restriction \tau \in \mathscr{K}$.

$\Longrightarrow$: Let $\mathcal{N} \in \mathscr{K}$. We need to show that $\mathcal{N} \in \{\mathcal{M}' \restriction \tau \colon \mathcal{M}' \models T' \textit{ and } \mathcal{M}' \textit{ omits } \Gamma\}$. We will construct $\mathcal{N}'$, a τ' expansion of $\mathcal{N}$, such that $\mathcal{N}' \models T'$ and $\mathcal{N}'$ omits Γ. So basically all we have to do is to get a proper interpretations of the functions F_i^n. Consider a finite $A \subseteq \mathcal{N}$, we define by induction on $|A|$, $\preceq_{\mathscr{K}}$- substructures of $\mathcal{N}$.

Base case: let $\mathcal{N}_\emptyset \preceq_{\mathscr{K}} \mathcal{N}$ be arbitrary with $|\mathcal{N}_\emptyset| = \kappa$. Let $\mathcal{N}'_\emptyset$ be the τ' expansion of $\mathcal{N}_\emptyset$ by interpreting the function symbols in $\tau' \backslash \tau$ as follows: let $\{(F_i^0)^{\mathcal{N}'_\emptyset} \colon i < \kappa\}$ enumerate all the elements in $\mathcal{N}_\emptyset$ and for every $0 < n < \omega$ and $i < \kappa$ interpret F_i^n arbitrarily. Since $\mathcal{N}'_\emptyset \restriction \tau = \mathcal{N}_\emptyset \in \mathscr{K}$, then $\mathcal{N}'_\emptyset$ omits Γ.

Inductive step: Let $B \subseteq \mathcal{N}$ with $|B| = n+1$. Let $\mathcal{N}_B \preceq_{\mathscr{K}} \mathcal{N}$ with $|\mathcal{N}_B| = \kappa$ and $\mathcal{N}_B \supseteq \mathcal{N}_A$ for all $A \subsetneq B$ (can find such $\mathcal{N}_B$ by the Löwenheim-Skolem axiom). Let $\mathcal{N}'_B$ be the τ' expansion of $\mathcal{N}_B$ by interpreting the function symbols in $\tau' \backslash \tau$ as follows: (i) let $\{(F_i^{n+1})^{\mathcal{N}'_B}(B) \colon i < \kappa\}$ enumerate all the elements of $\mathcal{N}_B$ such that the value of the function applied to any ordering of B has the same value, (ii) for every $n+1 < m < \omega$ and $i < \kappa$ interpret F_i^m arbitrarily, and (iii) for $m < n+1$ interpret F_i^m as given by the inductive hypothesis. Since $\mathcal{N}'_B \restriction \tau = \mathcal{N}_B \in \mathscr{K}$, then $\mathcal{N}'_B$ omits Γ. $\square_{induction}$

Let $\mathcal{N}'$ be the direct limit of $\mathcal{N}'_B$ for all finite $B \subseteq \mathcal{N}$. Note that all the symbols in $\tau' \backslash \tau$ are interpreted in $\mathcal{N}'$. It is easy to see that $\mathcal{N}'$ is a τ' expansion of $\mathcal{N}$ and $\mathcal{N}'$ omits Γ. $\square_{ClaimI}$

Claim II: T' and Γ satisfy part (ii)

Proof of claim II: Let $\mathcal{M}', \mathcal{N}'$ be τ' structures such that $\mathcal{M}' \subseteq \mathcal{N}'$ and $\mathcal{M}', \mathcal{N}' \models T'$ and $\mathcal{M}', \mathcal{N}'$ omit Γ. From part (i), we have $\mathcal{M} = \mathcal{M}' \restriction \tau \in \mathscr{K}$ and $\mathcal{N} = \mathcal{N}' \restriction \tau \in \mathscr{K}$. So we need to show $\mathcal{M} \preceq_{\mathscr{K}} \mathcal{N}$. Write $\mathcal{M}'$ as the direct limit of $\mathcal{M}'_{\bar{a}}$ for finite tuples $\bar{a} \in M'$ (using $(F_i^n)^{\mathcal{M}'}$). Since $\mathcal{M}'$ omits Γ, $\mathcal{M}_{\bar{a}} = \mathcal{M}'_{\bar{a}} \restriction \tau \in \mathscr{K}$ and from the proof of Claim I, $\mathcal{M}_{\bar{a}} \preceq_{\mathscr{K}} \mathcal{M}$ (by the union of chains axiom). Write $\mathcal{N}'$ as the direct limit of $\mathcal{N}'_{\bar{b}}$ for finite tuples $\bar{b} \in N'$ such that for $\bar{b} \in M'$ we have $\mathcal{N}'_{\bar{b}} = \mathcal{M}'_{\bar{b}}$ (this is true since $\mathcal{M}' \subseteq \mathcal{N}'$ hence for every $i < \kappa, n < \omega$ and for every $\bar{c} \in M'$ such that $|\bar{c}| = n$, $(F_i^n)^{\mathcal{M}'}(\bar{c}) = (F_i^n)^{\mathcal{N}'}(\bar{c})$). Since $\mathcal{N}'$ omits Γ, $\mathcal{N}_{\bar{b}} = \mathcal{N}'_{\bar{b}} \restriction \tau \in \mathscr{K}$ and from the proof of Claim I, $\mathcal{N}_{\bar{b}} \preceq_{\mathscr{K}} \mathcal{N}$. So for every $\bar{a} \in M$, we have $\mathcal{M}_{\bar{a}} \in \mathscr{K}$ and $\mathcal{M}_{\bar{a}} \preceq_{\mathscr{K}} \mathcal{N}$ hence by the union of chains axiom the direct limit of all $\mathcal{M}_{\bar{a}}$'s is $\preceq_{\mathscr{K}}$-substructure of $\mathcal{N}$ hence $\mathcal{M} \preceq_{\mathscr{K}} \mathcal{N}$. $\Box_{ClaimII}$ $\Box$

4.4 Galois Types over Arbitrary Sets

Notation 4.1. *1. If $X \subseteq \mathfrak{C}$ then $\overline{X}$ will denote $\mathfrak{C} \backslash X$.*

2. *Let $X \subseteq \mathfrak{C}$. Then $f \in Aut_X(\mathfrak{C})$ means that f is an automorphism of the monster that fixes X pointwise. If $X = \emptyset$, we just write $f \in Aut(\mathfrak{C})$.*

3. *Let f be a unary function. Let $\bar{a} = (a_0, \ldots, a_{n-1}) \in \mathfrak{C}$ and let $\bar{b} = (b_0, \ldots, b_{n-1}) \in \mathfrak{C}$. Then $f(\bar{a}) = \bar{b}$ means that for every $i < n$, $f(a_i) = b_i$.*

4. *Let $\mathbb{Z}$ denote the ordered integers, $\mathbb{Q}$ the ordered rationals, and $\mathbb{R}$ the ordered reals.*

The following defines Galois types over arbitrary small subsets of the monster.

Definition 4.5. *1. Let $\bar{a} \in \mathfrak{C}$ be a finite tuple. Define the* Galois type *of $\bar{a}$ over*

A inside $\mathfrak{C}$ as

$$tp^g(\bar{a}/A) = \{\bar{b} \in \mathfrak{C}, |\bar{b}| = |\bar{a}| \colon \textit{there exists } f \in Aut_A(\mathfrak{C}) \textit{ such that } f(\bar{a}) = \bar{b}\} \tag{4.1}$$

that is $tp^g(\bar{a}/A)$ is the orbit *of $\bar{a}$ under the pointwise stabilizer of A assuming the action of the automorphism group of $\mathfrak{C}$.*

2. *Assume $\mathcal{M} \in \mathscr{K}$. Let $\bar{a} \in M$ and $A \subseteq M$. Define the* Galois type *of $\bar{a}$ over A inside $\mathcal{M}$ as*

$$tp^g(\bar{a}/A, \mathcal{M}) = \{\bar{b} \in M, |\bar{b}| = |\bar{a}| \colon \textit{there exists } f \in Aut_A(\mathcal{M}) \textit{ such that } f(\bar{a}) = \bar{b}\} \tag{4.2}$$

that is $tp^g(\bar{a}/A, \mathcal{M})$ is the orbit *of $\bar{a}$ under the pointwise stabilizer of A assuming the action of the automorphism group of $\mathcal{M}$.*

Notation 4.2. 1. *Assume $A \subseteq \mathfrak{C}$. Let $\mathscr{S}_n(A)$ denote the class of Galois-types of arity n over A inside the monster. Let $\mathscr{S}(A) = \bigcup_{n \in \omega} \mathscr{S}_n(A)$.*

2. *Let $\mathcal{M} \in \mathscr{K}$. Assume $A \subseteq M$. Let $\mathscr{S}_n(A, \mathcal{M})$ denote the class of Galois-types of arity n over A inside $\mathcal{M}$. Let $\mathscr{S}(A, \mathcal{M}) = \bigcup_{n \in \omega} \mathscr{S}_n(A, \mathcal{M})$.*

Definition 4.6. *Let $p \in \mathscr{S}(A)$. Assume $q \in \mathscr{S}(B)$ where $A \subseteq B$. We say that q is an* extension *of p over B if for every $a \in \mathfrak{C}$, if $a \models q$ then $a \models p$. In other words if $p = tp^g(b/A)$ and $a \models q$ then there exists $f \in Aut_A(\mathfrak{C})$ such that $f(a) = b$.*

Example 4.3. *Let $\mathscr{K}$ be the class of dense linear orderings without endpoints under the elementary substructure relation. Then $\mathscr{K}$ is an AEC since it is first-order* *axiomatizable. Let $a, b \in \mathbb{Q}$ such that $a < b$. Then by the transitivity of $\mathbb{Q}$ we have $|\mathscr{S}_1(ab, \mathbb{Q})| = 3$, namely, $p_1 = \{x \in \mathbb{Q} \colon x < a\}, p_2 = \{x \in \mathbb{Q} \colon a < x < b\}$, and $p_3 = \{x \in \mathbb{Q} \colon b < x\}$.*

Remark 4.3. *Let $\mathscr{K}$ be an AEC. Let $\mathcal{M}, \mathcal{N} \in \mathscr{K}$ such that $\mathcal{M} \preceq_{\mathscr{K}} \mathcal{N}$. Let $a \in M$ and $A \subseteq M$. It might be the case that $tp^g(a/A, \mathcal{M}) \neq tp^g(a/A, \mathcal{N})$. This is illustrated in the next example.*

Example 4.4. *Let $\tau = \{R\}$, where R is a binary relation symbol. Let $\mathscr{K}$ be the class of τ structures with $\preceq_{\mathscr{K}}$ taken to be the substructure relation. Clearly, $\mathscr{K}$ is an AEC. Let $\mathcal{M}, \mathcal{N} \in \mathscr{K}$ such that the following hold:*

1. *$\mathcal{M} \subseteq \mathcal{N}$*

2. *there are $a, b \in M$ such that $\mathcal{M} \models R(a, b)$ and for every $x, y \in M$, $\mathcal{M} \models R(x, y)$ implies that $x = a$ and $y = b$*

3. *there exists $c \in N \backslash M$ such that $\mathcal{N} \models R(b, c)$ and $\mathcal{N} \models R(c, a)$ and for every $x, y \in N$, $\mathcal{N} \models R(x, y)$ implies either $(x, y) = (a, b)$ or $(x, y) = (b, c)$ or $(x, y) = (c, a)$*

Then $tp^g(a/\emptyset, \mathcal{M}) = \{a\}$, however, $tp^g(a/\emptyset, \mathcal{N}) = \{a, b, c\}$ by the automorphism of $\mathcal{N}$ that takes a to b and b to c and c to a.

4.4.1 Galois Splitting

Next we define the notion of splitting.

Definition 4.7. *1. Let $q \in \mathscr{S}(B)$. Let $A \subseteq B$. Then we say that q* does not split over *A if $q \restriction A = q$. Equivalently, we say that $q \restriction A$* does not split over *B if $q \restriction A$ has exactly one extension to a type over B.*

2. Let $p \in \mathscr{S}(A)$. Let $Z \subseteq p$. We say that p does not self-split over *Z if p has exactly one extension to a type over $A \cup Z$.*

3. Let $\mathcal{M} \in \mathscr{K}$ and let $A \subseteq B \subseteq M$. Let $q \in \mathscr{S}(B, \mathcal{M})$. Then we say that q does not split over *A inside $\mathcal{M}$ if $q \restriction A = q$. Equivalently, we say that $q \restriction A$* does not split over *B inside $\mathcal{M}$ if $q \restriction A$ has exactly one extension to a type over B inside $\mathcal{M}$.*

4. Let $\mathcal{M} \in \mathscr{K}$ and let $A \subseteq M$. Assume $p \in \mathscr{S}(A, \mathcal{M})$ and let $Z \subseteq p$. We say that p does not self-split over *Z if p has exactly one extension to a type over $A \cup Z$ inside $\mathcal{M}$.*

Let $p = q \restriction A$ and assume $q \backslash B \neq \emptyset$. Assume that there exists an element $a \in B \backslash A$ such that $a \models p$. Then p splits over B, even if $q = p \backslash B$ (p splits into at least two types: q and $tp^g(a/B)$ which has a as its only element).

Assumption 4.2. *In the following if $p \in \mathscr{S}(A)$ and p splits/does not split over B then, unless otherwise stated, it will always be assumed that $p \cap B = \emptyset$.*

Example 4.5. *Back to Example 4.3. Let $c \in \mathbb{Q}$. Consider the following three cases for the relative position of c with respect to a and b and consider the type p_2.*

1. $c < a$: p_2 does not split over c

2. $a < c < b$: p_2 self-splits over c into two types: $p_2' = \{x\colon a < x < c\}$ and $p_2'' = \{x\colon c < x < b\}$

3. $b < c$: p_2 does not split over c

Example 4.6. *Assume a language $\mathcal{L} = \{E\}$ where E is a binary relation symbol. Let T be the first-order complete theory saying that E is an equivalence relation with exactly two equivalence classes each has infinite cardinality. Let $\mathscr{K}$ be the class of models of T with $\preceq$ as the strong substructure relation, then $\mathscr{K}$ is an AEC. Assume the two classes in $\mathfrak{C}$ are C_1 and C_2. Let $A \subsetneq C_1$ and let $a \in C_1 \backslash A$. Assume $p = tp^g(a/A)$. Then clearly, $p = C_1 \backslash A$. Assume $b \in C_1 \backslash (A \cup \{a\})$ and assume $d \in C_2$. Then*

1. p does not self-split over b, that is $tp^g(a/Ab) = p \backslash \{b\} = C_1 \backslash (A \cup \{b\})$.

2. p does not split over d, that is $tp^g(a/Ad) = p$.

4.4.2 Basic properties of splitting

The following theorem shows that non-splitting is invariant under isomorphism.

Theorem 4.2 (Invariance under isomorphism I). *Let $A \subseteq B \subseteq \mathfrak{C}$. Let $f \in Aut(\mathfrak{C})$. Assume $p \in \mathscr{S}(A)$. Then p does not split over B if and only if $f(p)$ does not split over $f(B)$.*

Proof. Assume that $p \cap B = \emptyset$. Assume p does not split over B, then we need to show $f(p)$ does not split over $f(B)$. Let $A' = f(A), B' = f(B), p' = f(p)$.

Claim I: $p' \in \mathscr{S}(A')$.

Proof of Claim I: Let $a', b' \in p'$ and let $a = f^{-1}(a'), b = f^{-1}(b')$, then $a, b \models p$, hence there exists $g \in Aut_A(\mathfrak{C})$ such that $g(a) = b$. Consider the function $h = f \circ g \circ f^{-1}$. Then

$$A' \xmapsto{f^{-1}} A \xmapsto{g} A \xmapsto{f} A'$$

hence $h \in Aut_{A'}(\mathfrak{C})$. And

$$a' \xmapsto{f^{-1}} a \xmapsto{g} b \xmapsto{f} b'$$

so $h(a') = b'$, hence a', b' realize the same type over A'. $\square_{ClaimI}$

Since f is a permutation, $p' \cap B' = \emptyset$.

Claim II: $p' \in \mathscr{S}(B')$ (hence p' does not split over B')

Proof of Claim II: Let $c', d' \models p'$ (from Claim I, we have $p' = tp^g(c'/A') = tp^g(d'/A')$). Let $c = f^{-1}(c')$ and $d = f^{-1}(d')$, then $tp^g(c/B) = tp^g(d/B)$ since p does not split over B, hence there exists $h_1 \in Aut_B(\mathfrak{C})$ such tht $h_1(c) = d$. Consider the function $h_2 = f \circ h_1 \circ f^{-1}$

$$B' \xmapsto{f^{-1}} B \xmapsto{h_1} B \xmapsto{f} B'$$

so $h_2 \in Aut_{B'}(\mathfrak{C})$

$$c' \xmapsto{f^{-1}} c \xmapsto{h_1} d \xmapsto{f} d'$$

so $h_2(c') = d'$, hence c', d' realize the same type over B'. $\square_{ClaimII}$

Now assume p' does not split over B', then need to show p does not split over B. The proof is very similar to the previous direction. $\square$

The following theorem shows that non-self splitting is invariant under isomorphism.

Theorem 4.3 (**Invariance under isomorphism II**)**.** *Let $p \in \mathscr{S}(A)$ and let $B \subseteq p$. Assume $f \in Aut(\mathfrak{C})$. Then p does not self-split over B if and only if $f(p)$ does not self-split over f(B).*

Proof. Let $p' = f(p)$. Assume p does not self-split over B, so we need to show p' does not self-split over $f(B)$. Let $Z = A \cup B$ and let $Z' = f(Z) = f(A) \cup f(B)$. p does not self-split over B, hence p has exactly one extension to a type over Z, let this type be q so $q = p\backslash B$. Let $q' = f(q)$, then $q' = p'\backslash f(B)$. By an argument similar to that in Theorem 4.2, it can be shown that $p' \in \mathscr{S}(f(A))$. So it remains to show that $q' \in \mathscr{S}(Z')$ and hence q' is the only extension of p' to a type over Z'. Let $a', b' \in q'$, let $a = f^{-1}(a'), b = f^{-1}(b')$, then $a, b \models q$, hence there exists $g \in Aut_Z(\mathfrak{C})$ such that $g(a) = b$. Consider $h = f \circ g \circ f^{-1}$.

$$Z' \xmapsto{f^{-1}} Z \xmapsto{g} Z \xmapsto{f} Z'$$

then $h \in Aut_{Z'}(\mathfrak{C})$.

$$a' \xmapsto{f^{-1}} a \xmapsto{g} b \xmapsto{f} b'$$

so $h(a') = b'$, hence a', b' realize the same type over Z'.

Proof in the other direction is similar. □

Theorem 4.4 (**Monotonicity**)**.** *Let $p \in \mathscr{S}(A)$. Let $A \subseteq B$. Assume p does not split over B. Then p does not split over any Z such that $A \subseteq Z \subseteq B$.*

Proof. Follows directly from the definition of non-splitting. □

However, non-self splitting is not monotonic as indicated by the following example.

Example 4.7. *Consider Example 4.3. Let $c \in \mathbb{Q}$ such that $a < c < b$. Let $A = \{x\colon a < x \leq c\}$. Then p_2 does not self-split over A since it has exactly one extension to a type over Aab, namely $\{x\colon c < x < b\}$. However, p_2 self-splits over $c \in A$ into two types $\{x\colon a < x < c\}$ and $\{x\colon c < x < b\}$ hence non-self splitting is not monotonic.*

The following result shows a reflexivity behavior of splitting.

Theorem 4.5 (Reflexivity). *Let $p = tp^g(a/A)$. Then p splits over b if and only if p splits over any $b' \models tp^g(b/A)$.*

Proof. Let $b' \models tp^g(b/A)$, then there exists $f \in Aut_A(\mathfrak{C})$ such that $f(b) = b'$. Let $a' = f(a)$, then $tp^g(a/A) = tp^g(a'/A)$. By Theorem 4.2, $tp^g(a/A)$ splits over b if and only if $tp^g(f(a)/f(A))$ splits over $f(b)$ if and only if $tp^g(a'/A)$ splits over b' if and only if $tp^g(a/A)$ splits over b'. □

Example 4.8. *Consider the language $\mathcal{L} = \{R, S_1, S_2\}$ where R is a binary relation symbol and each of S_1 and S_2 is a unary relation symbol. Let T be a first-order complete theory that contains the following sentences*

1. *T does not have finite models*

2. *S_1 contains exactly two elements*

3. *S_2 contains exactly two elements*

4. there are exactly 4 elements x_0, x_1, y_0, y_1 such that the following hold

- *$S_1(x_0)$ and $S_1(x_1)$*
- *$S_2(y_0)$ and $S_2(y_1)$*
- *$R(x_0, y_0)$ and $R(y_0, x_1)$*
- *$R(x_1, y_1)$ and $R(y_1, x_0)$*
- *R is interpreted on the remaining elements (all elements except x_0, x_1, y_0, y_1) as a scattered linear ordering with a left endpoint and no right endpoint (so for countable structures this is simply the order type of the natural numbers)*
- *The above is exactly the interpretation of R.*

Let $\mathscr{K}$ be the class of models of T with $\preceq_{\mathscr{K}}$ taken to be the the elementary substructure relation, then $\mathscr{K}$ is an AEC. Let $\mathcal{A} \in \mathscr{K}$, let $a_0, a_1, b_0, b_1 \in A$ be the interpretations of x_0, x_1, y_0, y_1 respectively. Let $A' = A \backslash \{a_0, a_1, b_0, b_1\}$. Clearly, A' is rigid, that is for any automorphism f of $\mathcal{A}$, f fixes A' pointwise. Note also that $(A' \cap S_1^{\mathcal{A}}) = \emptyset$ and $(A' \cap S_2^{\mathcal{A}}) = \emptyset$. Let $p_1 = tp^g(a_0/\emptyset, \mathcal{A})$ and $p_2 = tp^g(b_0/\emptyset, \mathcal{A})$. Then $p_1 = \{a_0, a_1\}$ and $p_2 = \{b_0, b_1\}$, all witnessed by an automorphism f of $\mathcal{A}$ where $f(A') = id_{A'}, f(a_0) = a_1, f(a_1) = a_0, f(b_0) = b_1, f(b_1) = b_0$.

<u>Claim I:</u> p_1 splits over b_0

<u>Proof of Claim I:</u> Assume p_1 does not split over b_0, so there exists $f \in Aut_{b_0}(\mathcal{A})$ such that $f(a_0) = a_1$. Hence $R(a_0, b_0)$ implies $R(f(a_0), f(b_0)) = R(a_1, b_0)$ which is a contradiction. $\square_{ClaimI}$

By a similar argument can show that p_1 splits over $b_1 \models tp^g(b_0/\emptyset)$.

Corollary 4.1. *Assume $tp^g(a/A)$ does not split over b. Then $tp^g(a/A)$ does not split over $tp^g(b/A)$. Hence, $tp^g(a/A) = tp^g(a/A \cup tp^g(b/A))$.*

***Proof*.** Let $tp^g(b/A)$ be enumerated as $B = \langle b_i \colon i < \kappa \rangle$. We prove the conclusion by induction over $\alpha < \kappa$.

Base case: $tp^g(a/A)$ does not split over b, hence by Theorem 4.5, $tp^g(a/A)$ does not split over b_0.

Successor stage: assume $tp^g(a/A)$ does not split over $\langle b_i \colon i \leq \alpha \rangle$, hence by the definition of non-splitting $tp^g(a/A) = tp^g(a/A \cup \{b_i \colon i \leq \alpha\})$. $tp^g(a/A)$ does not split over b, so by Theorem 4.5, $tp^g(a/A)$ does not split over $b_{\alpha+1}$, hence $tp^g(a/A \cup \{b_i \colon i \leq \alpha\})$ does not split over $b_{\alpha+1}$, then $tp^g(a/A) = tp^g(a/A \cup \{b_i \colon i \leq \alpha + 1\})$, $tp^g(a/A)$ does not split over $\langle b_i \colon i \leq \alpha + 1 \rangle$.

Limit stage: Let $\delta < \kappa$ be a limit ordinal and assume that $tp^g(a/A)$ does not split over $\langle b_i \colon i < \delta \rangle$, hence $tp^g(a/A) = tp^g(a/A \cup \{b_i \colon i < \delta\})$. $tp^g(a/A)$ does not split over b, hence $tp^g(a/A)$ does not split over b_δ, hence $tp^g(a/A \cup \{b_i \colon i < \delta\})$ does not split over b_δ, hence $tp^g(a/A)$ does not split over $\langle b_i \colon i \leq \delta \rangle$. $\square_{Induction}$ $\square$

The following several results show some *compactness* behavior of splitting. The first one is a direct consequence of the reflexivity property.

Lemma 4.2. *Let $B \subsetneq tp^g(b/A)$. Assume $tp^g(a/A)$ splits over B. Then $tp^g(a/A)$ splits over b.*

***Proof*.** Assume that $tp^g(a/A)$ does not split over b, then by Corollary 4.1, $tp^g(a/A)$

does not split over $tp^g(b/A)$, hence by monotonicity, $tp^g(a/A)$ does not split over B which contradicts the hypothesis. □

Lemma 4.3. *Assume $tp^g(a/A)$ splits over Z. Assume that there exist two elements in Z realizing the same type over A. Then $tp^g(a/A)$ splits over some $Z' \subsetneq Z$.*

***Proof*.** Let

$$\Gamma = \{p \in \mathscr{S}(A)\colon p \textit{ is realized by some element in } Z\}$$

For every $p \in \Gamma$, assume some $a_p \in Z$ such that $a_p \models p$ (chosen arbitrarily from all the elements in Z realizing p). Let $Z' = \{a_p\colon p \in \Gamma\}$. There are two elements in Z realizing the same type over A, hence $Z' \subsetneq Z$. Apply Corollary 4.2 for every type in Γ with representative in Z', then we have $tp^g(a/A)$ splits over Z'. □

Then it directly follows.

Theorem 4.6. *Let $p \in \mathscr{S}(A)$. Assume p splits over Z. Then p splits over $B \subseteq Z$ where every element in B realizes a unique type in $\mathscr{S}(A)$.*

Next we define the notion of stability.

Definition 4.8 (Stability). *Let κ be an infinite cardinal. We say that $\mathscr{K}$* is κ-stable *if for every $A \subseteq \mathfrak{C}$ such that $|A| \leq \kappa$, it holds that $|\mathscr{S}(A)| \leq \kappa$.*

Assuming stability we can get a stronger compactness result where the cardinality of the splitting set is bounded by the cardinality of the type domain. This is given in the following theorem.

Theorem 4.7. *Assume $\mathscr{K}$ is μ-stable. Let $p \in \mathscr{S}(A)$ with $|A| \leq \mu$. Assume p splits over Z. Then p splits over $Z' \subseteq Z$ with $|Z'| \leq \mu$.*

Proof. If $|Z| \leq \mu$, then the conclusion trivially follows. So assume $|Z| > \mu$. Let Z' be the set constructed in the proof of Lemma 4.3. $\mathscr{K}$ is μ-stable and $|A| \leq \mu$, so $|\mathscr{S}(A)| \leq \mu$, hence $|Z'| \leq \mu$. By Lemma 4.3, p splits over Z'. □

The following result indicates that stability implies the existence of non-splitting types.

Theorem 4.8 (Existence of non-splitting types). *Assume $\mathscr{K}$ is μ-stable. Let $p \in \mathscr{S}(A)$ with $|A| = \mu$. Then there exists $B \supseteq A$ with $|B| = \mu$ and $q \in \mathscr{S}(B)$ such that $q \restriction A = p$ and q does not split over any Z such that $B \subseteq Z \subseteq \mathfrak{C}$. (so p has an extension that does not split over any subset of the monster)*

Proof. By way of contradiction assume that the conclusion does not hold. We will show that this contradicts the μ-stability of $\mathscr{K}$. Let κ be minimal such that $2^\kappa > \mu$. We will inductively construct a perfect binary tree of depth κ where each node corresponds to a pair (r, A), where r is a type with domain A and $|A| = \mu$.

Base case: Let $(p_0, A_0) = (p, A)$ be the root of the tree.

Successor stage: Let $\alpha \in 2^{<\kappa}$ and assume (p_α, A_α) at the node corresponding to α ($|A_\alpha| = \mu$ and $p_\alpha \restriction A = p$). From our assumption, there exists $Z \supseteq A_\alpha$ such that p_α splits over Z, hence from Theorem 4.7, p_α splits over $Z' \subseteq Z$ with $|Z'| = \mu$. Let r_1, r_2 be two types resulting from that splitting ($r_1, r_2 \in \mathscr{S}(Z')$). Let $(p_{\alpha^\wedge 0}, A_{\alpha^\wedge 0}) = (r_1, Z')$ and $(p_{\alpha^\wedge 1}, A_{\alpha^\wedge 1}) = (r_2, Z')$.

Limit stage: Let δ be a limit ordinal with $|\delta| < \kappa$, let $\alpha \in 2^\delta$ and assume that for every $i < \delta$, $(p_{\alpha|i}, A_{\alpha|i})$ has been found at the node corresponding to $\alpha|i$ such that $|A_{\alpha|i}| = \mu$ and $p_{\alpha|i} \restriction A = p$. Let $A_\alpha = \bigcup_{i<\delta} A_{\alpha|i}$, hence $|A_\alpha| = \mu$. Let p_α be some extension of p to a type over A_α, hence (p_α, A_α) corresponds to the node α $\quad \square_{construction}$

Let $A = \bigcup_{\alpha<\kappa} \bigcup_{\nu\in 2^\alpha} A_\nu$, then $|A| = \mu$. Hence we can extend each p_ν to a type over A. Then $|\mathscr{S}(A)| > \mu$ which contradicts the μ-stability of $\mathscr{K}$. □

4.5 Open Problems

In the future we plan to pursue several research paths:

1. Getting a deeper understanding of the splitting relation defined above and see whether a well-behaved independence relation can be defined based on it.

2. Based on the previous point, trying to develop a dimension theory for *AEC*'s starting with strong assumptions such as adding some sort of syntactic component to the definition of the class.

3. Investigate infinitary logic characterization of *AEC*'s.

4. Assume $\mathscr{K}$ has the amalgamation property (AP) at the cardinal κ, does that imply $\mathscr{K}$ has AP at κ^+ (upward transfer of amalgamation)? Is there a *Hanf number* for amalgamation, that is, a threshold cardinal after which the answer to the first question changes?

5. Studying the difference in behavior between *AEC*'s that are well-founded (do not contain infinite descending chains) and those that are not.

6. Studying the implications of the existence of a prime model (or prime over a set) in $\mathscr{K}$.

7. Investigating the conjecture: if $\mathscr{K}$ is χ-tame, then $\mathscr{K}$ is χ'-tame for some $\chi' < Hanf(\mathscr{K})$.

Bibliography

[1] M. Ajtai and R. Fagin. Reachability is harder for directed than for undirected finite graphs. *The Journal of Symbolic Logic*, 55(1), 1990.

[2] J. Baldwin. *Abstract Elementary Classes.* Monograph, in preparation. Available at http://www.math.uic.edu/ jbaldwin/model.html.

[3] J. Baldwin. Ehrenfeucht-Mostowski models in abstract elementary classes. *Classes,Logic and Its Applications, ed. Yi Zhang, Contemporary Mathematics*, 380:1–17, 2003.

[4] X. Caicedo. Finite model theory and computational complexity. *Apuntes matematicos 32, Universidad de los Andes*, 1995.

[5] R. Diestel. *Graph Theory.* Springer, 2006.

[6] A. Ehrenfeucht. An application of games to the completeness problem for formalized theories. *Fundamenta Mathematicae*, 49:129–141, 1961.

[7] R. Fagin. Generalized first-order spectra and polynomial-time recognizable sets. In R. Karp, editor, *Complexity of Computation*, volume 7, pages 43–73. SIAM-AMS, 1974.

[8] R. Fagin. Monadic generalized spectra. *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik*, 21:89–96, 1975.

[9] U. Felgner. Pseudo-endliche gruppen. In *Proceedings of the 8th Easter Conference on Model Theory*, pages 82–96, 1990.

[10] S. Fiorini and R. J. Wilson. *Edge-colourings of graphs.* Pitman, 1977.

[11] R. Fraïssé. Sur quelques classifications des systèmes de relations. *Université d'Alger, Publications Scientifiques, Série A*, 1:35–182, 1954.

[12] R. Grossberg. Classification theory for abstract elementary classes. *Contemporary Mathematics*, 302, 2002.

[13] R. Grossberg and M. VanDieren. Galois-stability in tame abstract elementary classes. *Journal of Mathematical Logic*, 6(1):25–49, 2006.

[14] W. Hodges. *Model Theory.* Cambridge University Press, 1993.

[15] T. Hyttinen and M. Kesälä. Categoricity transfer in simple finitary abstract elementary classes. 2005. Available at http://mathstat.helsinki.fi/logic/people/meeri.kesala/SimpleFinitaryAEC.pdf.

[16] T. Hyttinen and M. Kesälä. Independence in finitary abstract elementary classes. 2005. To appear in Annals of Pure and Applied Logic.

[17] N. Immerman. Relational queries computable in polynomial time. *Information and control*, 68:86–104, 1986.

[18] N. Immerman. *Descriptive Complexity.* Springer, 1998.

[19] A. Koponen and K. Luosto. Definability of group theoretic notions. Manuscript, 2000.

[20] M. Koucký, C. Lautemann, S. Poloczek, and D. Thérien. Circuit lower bounds via Ehrenfeucht-Fraïssé games. *IEEE Conference on Computational Complexity*, pages 190–201, 2006.

[21] L. Libkin. *Elements of Finite Model Theory.* Springer, 2004.

[22] L. Libkin and J. Nurmonen. Counting and locality over finite structures A survey. In *Generalized quantifiers and computatiion*, volume 1754 of *LNCS*, pages 18–50. Springer, 2000.

[23] O. Pikhurko and O. Verbitsky. Descriptive complexity of finite structures: Saving the quantifier rank. *The Journal of Symbolic Logic*, 70(2), 2005.

[24] D. Robinson. *A Course in the Theory of Groups.* Springer, 1995.

[25] S. Shelah. Classification of non-elementary classes II, Abstract elementary classes. *Lecture notes in mathematics*, 1292:419–497, 1987.

[26] L. Stockmeyer. The polynomial-time hierarchy. *Theoretical Computer Science*, 3:1–22, 1977.

[27] M. VanDieren. Categoricity in abstract elementary classes with no maximal models. *Annals of Pure and Applied Logic*, 141:108–147, 2006.

[28] J. Wilson. On simple pseudofinite groups. *Journal of the London Mathematical Society*, 2(51):471–490, 1995.

[29] J. Wilson. Finite axiomatisability of finite soluble groups. *Journal of the London Mathematical Society*, 74(3):566–582, 2006.