Model Theory and Complexity Theory

Walid Gomaa

Supervised by

Prof. William Gasarch and Prof. David Kueker

Outline

I. Introduction and basic definitions

II. Expressibility in existential second-order logic

III. Descriptive complexity of abelian finite groups

IV. Classification theory in abstract elementary classes

I. Descriptive Complexity

- **Traditional complexity theory** classifies problems based on time,space, or hardware resources
- **Descriptive complexity** classifies problems based on how hard it is to express the problem in some logical formalism
- Example: 3-colorability ($\in NPC$)

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

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

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

Descriptive Complexity Cont'd

- Virtually all traditional complexity classes can be captured by logical formalisms
- Examples
  - $NP = \Sigma^1_1$ and hence $coNP = \Pi^1_1$ [Fagin 74]
  - $PH = SO$ [Stockmeyer 77]
  - $P = (LFP+ <)$ [Immerman 86], hence

$$P = NP \iff (LFP+ <) = \Sigma^1_1$$

  - $PSpace = (PFP+ <)$
  - It has been shown using transitive closure logic that $NL = coNL$
  - $TC^0 = FOC(<, +, \times)$ [Bar and Imm 90]

Logical Resources

3-colorability revisited

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

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

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

i. How many object variables? ($2FO$ and $3SO$)

ii. Types/semantics of quantifiers (FO and monadic $\exists SO$)

iii. Quantifier rank ($3SO$ and $2FO$)

iv. Alternation of quantifiers (0 FO and 0 SO)

v. Length of sentences: finite/infinite (finite)

Definitions

Let φ be a first-order formula.

- **Quantifier rank** $qr(\varphi)$: the maximum length of any nested sequence of quantifiers inside φ
- **Alternation number** $alt(\varphi)$: the maximum number of quantifier alternations over any sequence of nested quantifiers inside φ assuming φ is reduced to its negation normal form

Ehrenfeucht-Fraïssé Games

- Two players: Spoiler $\mathcal{S}$ and Duplicator $\mathcal{D}$
- Played over two structures $\mathcal{A}$ and $\mathcal{B}$ of the same kind
- r rounds of the game
- Round i:
  - $\mathcal{S}$ selects either $a_i \in A$ or $b_i \in B$
  - $\mathcal{D}$ responds by $b_i \in B$ or $a_i \in A$ respectively such that $\langle a_j : j \leq i \rangle \cong \langle b_j : j \leq i \rangle$, **if possible**
- $\mathcal{D}$ wins if $\langle a_j : j \leq r \rangle \cong \langle b_j : j \leq r \rangle$, otherwise $\mathcal{S}$ wins
- Intuitively, the goal of $\mathcal{S}$ is to show that the two structures can be distinguished in at most r steps, whereas $\mathcal{D}$'s goal is to show that this can not be done

Notation

- $\mathcal{A} \equiv_r \mathcal{B}$: $\mathcal{A}$ and $\mathcal{B}$ agree on all FO sentences σ such that $qr(\sigma) \leq r$
- $EF_r(\mathcal{A}, \mathcal{B}) \in \mathcal{S}$: the spoiler has a winning strategy in the r-round EF game. Similarly for $EF_r(\mathcal{A}, \mathcal{B}) \in \mathcal{D}$

The EF Theorem

Theorem 1. *The following are equivalent:*

1. $\mathcal{A} \equiv_r \mathcal{B}$
2. $EF_r(\mathcal{A}, \mathcal{B}) \in \mathcal{D}$

Pebble EF Games

- Each player starts with a fixed set of $p \leq r$ pebbles
- Round i
  - $\mathcal{S}$ selects either $a_i \in A$ or $b_i \in B$, let x denote her choice
  - She either (i) removes a pebble that has been placed on a previously chosen element and places it on x or (ii) places a new pebble, if she still has any, on x
  - $\mathcal{D}$ acts correspondingly on the other structure.
- $\mathcal{D}$ wins if $\langle a_{i_1}, \ldots, a_{i_p} \rangle \cong \langle b_{i_1}, \ldots, b_{i_p} \rangle$, otherwise $\mathcal{S}$ wins

Notation

- $\mathcal{A} \equiv_r^p \mathcal{B}$: $\mathcal{A}$ and $\mathcal{B}$ agree on all FO-sentences σ such that $qr(\sigma) \leq r$ and σ has at most p object variables

- $pEF_r^p(\mathcal{A}, \mathcal{B}) \in \mathcal{S}$: the spoiler has a winning strategy in the pebble EF-game with r rounds and p pebbles. Similarly for $pEF_r^p(\mathcal{A}, \mathcal{B}) \in \mathcal{D}$

The pebble EF Theorem

Theorem 2. *The following are equivalent:*

1. $\mathcal{A} \equiv_r^p \mathcal{B}$
2. $pEF_r^p(\mathcal{A}, \mathcal{B}) \in \mathcal{D}$

II. Expressibility in Σ_1^1

- Σ_1^1 consists exactly of

$$\exists X_1 \cdots \exists X_n \varphi$$

  where X_i is SO variable and φ is FO sentence

- Inspired by Fagin's result $NP = \Sigma_1^1$, we have developed a partial framework to investigate expressibility inside Σ_1^1

- Main goal is to have a finer look into NP

Outline

- Problem studied is DIV_k: divisibility by $k \geq 2$
- Framework uses combinatorics derived from SO EF-games and the notion of *game types*
- Work is basically done over the sublogic $bin\Sigma^1_1(p, r)$:
  - $arity(X_i) \leq 2$
  - $qr(\varphi) \leq r$
  - φ has at most p FO variables
- $arity(X_i) = 1 \Longrightarrow mon\Sigma^1_1(p, r)$

Example: DIV_2

It is known $DIV_2 \notin FO$. However, It can be expressed by the following $bin\Sigma_1^1$ sentence.

$$\sigma \overset{def}{=} \exists R\left(\varphi_1(R) \land \varphi_2(R) \land \varphi_3(R)\right)$$

$$where$$

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

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

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

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

Colored Graphs

Let $$\sigma \stackrel{def}{=} \exists R_1 \cdots \exists R_{n'} \exists S_1 \cdots \exists S_{m'} \varphi$$

- **Models** of σ are colored complete self-edged graph

$$G = (V, C_1, \ldots, C_m, D_1, \ldots, D_n)$$

- $m = 2^{m'}$ vertex colors induced by the S_i's

$$color(u) = (S_1(u), \ldots, S_{m'}(u))$$

- $n = 4^{n'}$ edge colors induced by the R_i's

$$color(u, v) = ((R_1(u, v), R_1(v, u)), \ldots, (R_{n'}(u, v), R_{n'}(v, u)))$$

- Let $\mathcal{G}_{m,n}$ be the class of graphs with m, n vertex and edge colors.

$bin\Sigma_1^1(p, r)$ EF-games

- Game has 4 parameters:
  - number of vertex colors m
  - number of edge colors n
  - number of FO rounds r
  - number of pebbles p

- Played over two classes of structures:
  $\mathscr{K} = \{G \in \mathcal{G}_{m,n} \colon |G| \equiv 0 \pmod{k}\}$
  $\overline{\mathscr{K}} = \{G \in \mathcal{G}_{m,n} \colon |G| \not\equiv 0 \pmod{k}\}$

$bin\Sigma_1^1(p,r)$ EF-games Cont'd

Rules of the game:

1. $\mathcal{D}$ chooses a number s
2. $\mathcal{S}$ chooses $G \in \mathscr{K}$ such that $|G| \geq s$
3. $\mathcal{D}$ chooses $G' \in \overline{\mathscr{K}}$
4. $\mathcal{S}$ and $\mathcal{D}$ play pEF-game over G, G' for r rounds with p pebbles

Theorem 3. *The following are equivalent*

1. $DIV_k \in bin\Sigma_1^1(p,r)$
2. $EF(\mathscr{K}, \overline{\mathscr{K}}) \in \mathcal{S}$

Game Types

- Notion based on the *locality* of first-order logic
- Small neighborhoods of points in the two structures can determine who can guarantee a winning strategy
- Provide sufficient and necessary conditions of who has a winning strategy without actually playing the game

Main Results

1. $DIV_k, \overline{DIV_k}$ are neither in $mon\Sigma_1^1$ nor in $mon\Pi_1^1$
2. $DIV_k \notin bin\Sigma_1^1(2,2)$ and $DIV_k \notin bin\Sigma_1^1(2,3)$
3. $DIV_k \in bin\Sigma_1^1(3,3)$.
4. Let $\Gamma = \{\sigma \in bin\Sigma_1^1(3,3) \colon \sigma\ has\ \leq\ l\ binary\ variables\}$, then $DIV_k \in \Gamma$ for every $k \leq (4^l - 1)$.
5. Furthermore, $DIV_k \in \Gamma$ for only finitely-many k.

Main Results Cont'd

6. Hence DIV_k creates a proper hierarchy inside the logic $bin\Sigma^1_1(3,3)$.

7. An immediate consequence of the above is that $mon\Sigma^1_1 \subset bin\Sigma^1_1$.

8. $DIV_k \notin bin\Sigma^1_1$ when the sizes of the interpretations of the binary variables are bounded from above by some linear function of the size of the universe.

Open Problems

1. Finding tight lower/upper bounds for the DIV_k hierarchy in $bin\Sigma_1^1(3,3)$.

2. Get a lower bound on the expressibility of $\overline{DIV_k}$ in Σ_1^1.

3. Study natural extensions of $bin\Sigma_1^1(3,3)$ inside Σ_1^1 within the framework developed above. The main goal is to get separation results among n-$ary\Sigma_1^1$ sublogics using expressibiltiy of number-theoretic properties such as primeness.

Open Problems Cont'd

4. Investigate expressibility inside Π^1_1 to get separation results among n-$ary\Pi^1_1$ sublogics

5. Get separation results between n-$ary\Sigma^1_1$ logics and n-$ary\Pi^1_1$ logics

6. Investigate the whole of SOL and consequently the whole of the polynomial hierarchy

7. Complexity-theoretic consequences of the above

III. Descriptive Comp. of Abelian Finite Groups

We want to answer the following two questions.

1. Given two AFG's G and G', want to find a logical sentence that distinguishes between them?

2. How complex can this sentence be (lower/upper bounds)?

Abelian Finite Groups Cont'd

- We answer these questions in FOL, hence commit to
  - finite length formulas
  - first-order quantifiers
  - $+$ as a ternary relation
- Analysis done in 3 stages
  1. groups of residue classes with prime orders
  2. groups of residue classes with arbitrary orders (include all cyclic groups)
  3. finite abelian groups

Main Results

Theorem 4. *Let G_1 and G_2 be a pair of non-isomorphic finite abelian groups. Then there exists a number f such that the following hold:*

1. *f divides at least one of the two groups' orders*
2. *If φ is a sentence that distinguishes G_1 and G_2 then φ must have quantifier depth $\Omega(\log f)$.*
3. *There exists a first-order sentence φ that distinguishes G_1 and G_2 such that φ is existential, has quantifier depth $O(\log f)$, and has at most 5 variables.*

Main Results Cont'd

- Let D_n denote the *dihedral group* of order $2n$ (n rotations + n reflections)
- Exploiting the close relationship between elementary equivalence of $\mathbb{Z}_n$'s and elementary equivalence of D_n's

Theorem 5. *Let D_m and D_n be dihedral groups, and let $f = min(divisor(m) \Delta divisor(n))$. Then the following hold:*

1. *If φ is a sentence that distinguishes D_m and D_n then φ must have quantifier depth $\Omega(\log f)$.*
2. *There exists a first-order sentence φ that distinguishes D_m and D_n such that φ is existential, has quantifier depth $O(\log f)$, and has at most 5 variables.*

Main Results Cont'd

Consequences of the above bounds are the first-order undefinability of some group-theoretic notions.

Theorem 6.

1. *Cyclicity is not first-order definable over the class of finite groups*
2. *The closure of a single element is not first-order definable over the class of finite groups*

Main Results Cont'd

Theorem 7.

1. *Simplicity is not first-order definable over the class of finite groups (known)*

2. *Nilpotency is not first-order definable over the class of finite groups (known)*

3. *Normal closure of a single element is not first-order definable over the class of finite groups (known)*

Open Problems

1. Can the concrete lower/upper on the quantifier rank of a distinguishing sentence (for $\mathbb{Z}_n$'s and D_n's) be improved? We have already shown that the lower bound is optimal 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.

Open Problems Cont’d

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.

IV. Abstract Elementary Classes

- A generalization of FO model theory
- $\mathscr{K} = (\mathbb{K}, \preceq_{\mathscr{K}})$ is a class of models $\mathscr{K}$ of the same vocabulary that are partially ordered
- $\mathscr{K}$ satisfies a finite set of purely semantical axioms like closure under isomorphism and closure under unions of chains
- Example: the class of all ordinals is an AEC: it is neither definable in FO-logic nor in $\mathcal{L}_{\infty,\infty}$, the class of dense linear orderings, any class of structures of a FO theory

Classification Theory for AEC's

Given $\mathscr{K}$ want to answer questions about $\mathscr{K}_\lambda/\cong$:

1. Is $\mathscr{K}_\lambda \neq \emptyset$?
2. Does $\mathscr{K}_\lambda \neq \emptyset$ imply $\mathscr{K}_{\lambda^+} \neq \emptyset$?
3. If $\mathscr{K}$ is λ^+-categorical, does this imply $\mathscr{K}$ is λ-categorical?
4. If $\mathscr{K}$ is λ-categorical, does this imply $\mathscr{K}$ is λ^+-categorical?
5. What are the possible functions $\lambda \mapsto |\mathscr{K}_\lambda|$?
6. Under what conditions on $\mathscr{K}$ is it possible to find a nice dependence relation among the subsets of $\mathcal{M} \in \mathscr{K}$?