On Canonical Forms of Complete Problems via First-order Projections

Nerio Borges
Departamento de Matemáticas
Universidad Simón Bolívar
Caracas, Venezuela
nborges@usb.ve

Blai Bonet
Departamento de Computación
Universidad Simón Bolívar
Caracas, Venezuela
bonet@ldc.usb.ve

June 22, 2007

Abstract

The class of problems complete for NP via first-order reductions is known to be characterized by existential second-order sentences of a fixed form. All such sentences are built around the so-called generalized IS-form of the sentence that defines IndependentSet. This result can also be understood as that every sentence that defines a NP-complete problem P can be decomposed in two disjuncts such that the first one characterizes a fragment of P as hard as IndependentSet and the second the rest of P. That is, a decomposition that divides every such sentence into a a "quotient and residue" modulo IndependentSet.

In this paper, we show that this result can be generalized over a wide collection of complexity classes, including the so-called nice classes. Moreover, we show that such decomposition can be done for any complete problem with respect to the given class, and that two such decompositions are non-equivalent in general. Interestingly, our results are based on simple and well-known properties of first-order reductions.

Keywords: Finite Model Theory, Complexity Theory, First-Order Reductions, Canonical Forms

1 Introduction

Descriptive complexity studies the interplay between complexity theory, finite model theory and mathematical logic. Since its inception in 1974 [3], descriptive complexity has been able to characterize all major complexity classes in term of logical languages independent of any computational model, thus suggesting that the computational complexity of languages is a property intrinsic to them and not an accidental consequence of our choice for the computational model.

In descriptive complexity, problems are understood as sets of (finite) models which are described by logical formulae over given vocabularies. Reductions between problems correspond to logical relations between the set of models that characterize the problems. As important as the notion of polynomial many-one reductions in structural complexity, there is the notion of first-order reductions in descriptive complexity, and among such, the first-order projections (fops). A fop is a very weak type of polynomial-time reduction whose study have provided interesting results such as that common NP-complete problems like SAT, CLIQUE and others remain complete via fop reductions, and that such NP-complete problems can be described by logical sentences in a *canonical form* [2, 5].

In this paper we continue the study of the syntactic aspects of complete problems via fop reductions extending the work of Medina and Immerman [7, 6]. In particular, we provide a general characterization of complete problems via fops for a large collection of complexity classes that cover well beyond just NP, including classes like P, PSPACE, Σ_n^p and Π_n^p, and others. Interestingly, our results rely on very general assumptions and tools already known in the field.

The paper is organized as follows. In Sect. 2, we give standard definitions and known results which provide the theoretical framework of the paper and make it self contained. Sect. 3 contains our main result, namely the generalization of the Medina-Immerman result, together with relevant remarks and some examples. Later, Sect. 4 shows a general result about the existence of non-isomorphic problems via fop reductions, which implies that our canonical form is indeed minimal. Finally, Sect. 5 concludes with a brief summary and directions for future work.

2 Preliminaries

2.1 Logics, Finite Models, and Decision Problems

A logical vocabulary is a tuple $\tau = \langle R_1^{a_1}, \ldots, R_r^{a_r}, c_1, \ldots, c_s, f_1^{r_1}, \ldots, f_t^{r_t} \rangle$ where the R_js are relational symbols of arity a_j, c_is are constant symbols, and the f_ks are r_k-ary functional symbols. A structure for τ, also referred as τ-structure or just structure if τ is clear from context, is a tuple $\mathcal{A} = \langle |\mathcal{A}|, R_1^{\mathcal{A}}, \ldots, R_r^{\mathcal{A}}, c_1^{\mathcal{A}}, \ldots, c_s^{\mathcal{A}}, f_1^{\mathcal{A}}, \ldots, f_t^{\mathcal{A}} \rangle$ where

- $|\mathcal{A}|$ is the universe (or domain) of $\mathcal{A}$,
- $R_j^{\mathcal{A}} \subseteq |\mathcal{A}|^{a_j}$ is a a_j-ary relation over $|\mathcal{A}|$,
- $c_j \in |\mathcal{A}|$ is an element of the universe, and
- $f_k^{\mathcal{A}} : |\mathcal{A}|^{r_k} \to |\mathcal{A}|$ is a total r_k-ary function over $|\mathcal{A}|$.

For vocabulary τ, STRUC[τ] denotes the class of all finite structures, i.e. those whose universe is an initial segment $\{0, 1, \ldots, n-1\}$ of $\mathbb{N}$.

In addition to above logical symbols, we also have the *numerical* relational symbols '=', '$\leq$', 'BIT' and 'suc', and constants '0' and 'max', which are assumed to belong to each vocabulary, and have *fixed interpretations* on every structure $\mathcal{A}$:

- $=$ and $\leq$ are interpreted as the usual equality and order on $\mathbb{N}$,
- $\mathcal{A} \models \mathrm{BIT}(i, j)$ iff the j-th bit in the binary representation of i is 1,
- $\mathcal{A} \models \mathrm{suc}(x, y)$ iff y is the successor of x in the usual order on $\mathbb{N}$, and
- 0 and max denote the least and greatest element in $|\mathcal{A}|$.

If $\mathcal{L}$ denotes a logic, the language $\mathcal{L}[\tau]$ is the set of all well-formed formulae of $\mathcal{L}$ over the vocabulary τ. A numerical formula in $\mathcal{L}[\tau]$ is a formula with only numerical symbols. For example, SO$\exists[\tau]$ is the set of all second-order formulae of form $\exists Q_1 \cdots \exists Q_n \Phi$ where the Q_is are relational variables and Φ is a first-order formula over over vocabulary τ. As usual, FO denotes first-order logic and SO denotes second-order logic.

A formula with no free variables is a sentence. For sentence $\varphi \in \mathcal{L}[\tau]$, the class of all finite models that satisfy φ is denoted as $\mathrm{MOD}[\varphi]$. For fixed τ, it is possible to code every finite τ-structures into a sequence of bits, i.e. a binary string, using a map $\mathrm{MOD}[\tau] \rightsquigarrow \{0,1\}^*$. Hence, a collection of finite models can be represented as a collection of strings, or language.

In descriptive complexity, a decision problem P is characterized by a subset of models from $\mathrm{STRUC}[\tau]$ for some fixed τ. For example, the problem CLIQUE can be characterized by structures $\mathcal{A} = \langle |\mathcal{A}|, E^{\mathcal{A}}, k^{\mathcal{A}} \rangle$ over the vocabulary $\tau = \langle E^2, k \rangle$, where E is a binary relational symbol and k is a constant, such that $G = (|\mathcal{A}|, E^{\mathcal{A}})$ makes up an undirected graph and $k^{\mathcal{A}} \in \{0, \dots, |\mathcal{A}| - 1\}$ denotes the size of a clique in G. Such models are typically characterized by a sentence Ψ over some fragment $\mathcal{L}$. The problem CLIQUE, for example, can be characterized with a SO$\exists$ sentence over τ [3]; see below.

2.2 First-Order Queries, Fops, and Duals

Let τ and σ be two vocabularies where $\sigma = \langle R_1^{a_1}, \dots, R_r^{a_r}, c_1, \dots, c_s \rangle$ has no functional symbols (from now on, we only consider vocabularies with no functional symbols). Let $k \geq 1$ and consider the tuple $I = \langle \varphi_0, \dots, \varphi_r, \psi_1, \dots, \psi_s \rangle$ of $r+s+1$ first-order formulae in $\mathrm{FO}[\tau]$ of form $\varphi_0(x_1, \dots, x_k)$, $\varphi_i(x_1, \dots, x_{ka_i})$ and $\psi_j(x_1, \dots, x_k) = (x_1 = c'_{j_1} \wedge \cdots \wedge x_k = c'_{j_k})$ where the c'_{j_i}s are constant symbols from τ (possibly with repetitions). That is, φ_0 has at most k free variables among $x_1, \dots, x_k$, φ_i has at most ka_i free variables among $x_1, \dots, x_{ka_i}$, and ψ_j denotes a tuple in $\{c' : c' \in \tau\}^k$.

Such tuple defines a mapping $\mathcal{A} \rightsquigarrow I(\mathcal{A})$, called a *first-order query* of arity k, from τ-structures into σ-structures given by:

- the universe $|I(\mathcal{A})| \doteq \{(u_1, \dots, u_k) \in |A|^k : \mathcal{A} \vDash \varphi_0(u_1, \dots, u_k)\}$ is ordered lexicographically,
- the relations are $R_i^{I(\mathcal{A})} \doteq \{(\bar{u}_1, \dots, \bar{u}_{a_i}) \in |\mathcal{A}|^{ka_i} : \mathcal{A} \vDash \varphi_i(\bar{u}_1, \dots, \bar{u}_{a_i})\}$,
- the constants are $c_j^{I(\mathcal{A})} \doteq \bar{u}$ for the unique $\bar{u}$ with $\mathcal{A} \vDash \varphi_0(\bar{u}) \wedge \psi_j(\bar{u})$.

Furthermore, if for $T \subseteq \mathrm{STRUC}[\tau]$ and $S \subseteq \mathrm{STRUC}[\sigma]$, it is true that $\mathcal{A} \in T$ iff $I(\mathcal{A}) \in S$, then I is called a *first-order reduction* from T to S.

A first-order query is called a *first-order projection* (fop) if φ_0 is numerical and each φ_i has form:

$$\varphi_j(\bar{x}) \;\equiv\; \alpha_0(\bar{x}) \;\vee\; (\alpha_1(\bar{x}) \wedge \lambda_1(\bar{x})) \;\vee\; \cdots \;\vee\; (\alpha_r(\bar{x}) \wedge \lambda_r(\bar{x}))$$

where the α_is are numerical and mutually exclusive, and each λ_i is a τ-literal. Projections are typically denoted by the letter p. If p is a reduction from Π to Ψ, we write $p : \Pi \leq_{fop} \Psi$, and if Π is complete via $\leq_{fop}$ reductions we say that Π is $\leq_{fop}$-complete.

Projections have interesting properties. For example, projections are a special case of Valiant's non-uniform projections [10]. For our purposes, we are interested in the fact that for each projection p there is a first-order sentence $\beta_p \in \mathrm{FO}[\sigma]$ that characterizes the image of p, i.e. $\mathcal{B} \vDash \beta_p$ iff $\mathcal{B} = p(\mathcal{A})$ for some $\mathcal{A} \in \mathrm{STRUC}[\tau]$. The sentence β_p is called the *characteristic sentence* of p [1].

Finally, there is a syntactic operator associated to a first-order query that plays a fundamental role in our results. For a first-order query $I : \mathrm{STRUC}[\tau] \to \mathrm{STRUC}[\sigma]$, the *dual operator* $\widehat{I}$ maps formulae in $\mathcal{L}[\sigma]$ to formulae in $\mathcal{L}[\tau]$ in such a way that

$$\mathcal{A} \vDash \widehat{I}(\theta) \quad \text{if and only if} \quad I(\mathcal{A}) \vDash \theta$$

for all $\theta \in \mathcal{L}[\sigma]$ and $\mathcal{A} \in \mathrm{STRUC}[\tau]$ [5, Sect. 3.2].

2.3 Complexity Classes

For a family $\mathcal{F}$ of proper complexity functions [9], we consider the complexity classes $\mathrm{TIME}(\mathcal{F}) = \cup_{f\in\mathcal{F}}\mathrm{TIME}(f)$, and similarly for non-deterministic time and space. A complexity class $\mathbf{C}$ defined by $\mathcal{F}$ is *nice* if it has a universal problem of the form

$$U_{\mathbf{C}} = \{\langle M_i, \omega, 1^t\rangle : M_i \text{ accepts } \omega \text{ within } f_i(t) \text{ resources}\}$$

where $L(M_i) \in \mathbf{C}$ and $f_i \in \mathcal{F}$ bounds the resources of M_i. Some well-known classes that are nice are L, NL, P, NP and PSPACE. Allender et al. [1] showed that if Π is $\leq_{fop}$-complete for a nice class $\mathbf{C}$, then it is complete via injective fops of arity at least 2. The following properties are shown easily:

Proposition 1 *Let $\mathbf{C}$ be a complexity class defined by family $\mathcal{F}$. Then, (a) if $\mathbf{C}$ is a deterministic class and $\mathcal{F}$ is closed under sums, then $\mathbf{C}$ is closed under finite unions; (b) if $\mathbf{C}$ is a nondeterministic class and $\mathcal{F}$ is such that for every $f, g \in \mathcal{F}$ there is $h \in \mathcal{F}$ with $f, g \leq h$, then $\mathbf{C}$ is closed under finite unions; (c) if $\mathbf{C}$ is closed under finite unions and $\mathbf{C}$ is captured by logic $\mathcal{L}$, then $\mathcal{L}$ is closed under disjunctions.*

The nice classes L, NL, P, NP and PSPACE are known to be characterized by SO-DetKrom, SO-Krom, SO-Horn, SO$\exists$ and SO+TC respectively [4, 5]. Additionally, Σ^p_k and Π^p_k are characterized by SO$\exists\forall\cdots Q_k$ and SO$\forall\exists\cdots Q'_k$ sentences where $Q_k = \exists, Q'_k = \forall$ if k is odd, and $Q_k = \forall, Q'_k = \exists$ if k is even. Thus, by the proposition, all these logical fragments are closed under disjunctions, and also under conjunctions with first-order formulae. We will make use of these facts later.

3 Canonical Forms of Complete Problems

Medina and Immerman characterized $\leq_{fop}$-complete problems for NP syntactically using the IndependentSet problem. This problem consists of checking whether an input graph G has an independent set of size k. IndependentSet is known to be complete for NP under different notions of reductions, and in particular, under fop reductions [7]. IndependentSet in characterized by the following SO$\exists[\tau]$ sentence, for $\tau = \langle E^2, k\rangle$:

$$\Psi_{IS} \;=\; (\exists f \in \mathrm{Inj})(\forall x, y)\big[x \neq y \,\wedge\, f_x \leq k \,\wedge\, f_y \leq k \,\rightarrow\, \neg E(x,y)\big] \tag{1}$$

where '$f \in \mathrm{Inj}$' means that f is a total and 1-1 function, i.e. an ordering of the elements of the universe, and f_x denotes $f(x)$. Although it seems that (1) quantifies over a functional variable, f is indeed a relational variable such that f_x is the unique element such that $f(x, f_x)$. The condition $f \in \mathrm{Inj}$ is easily defined in first-order logic. Observe that the only second-order variable in (1) is f which is existentially quantified.

Theorem 2 ([7]) *Let $L \subseteq STRUC[\sigma]$ be a NP problem characterized by $\Psi \in \mathcal{L}[\sigma]$ where $\sigma = \langle Q^1\rangle$ is the vocabulary of binary strings. Then, a problem L is NP-complete via $\leq_{fop}$ reductions iff there is an injective fop $p : STRUC[\langle E^2, k\rangle] \rightarrow STRUC[\sigma]$ such that*

$$\Psi \;\equiv\; (\beta_p \,\wedge\, \Upsilon_{IS}) \,\vee\, (\neg\beta_p \,\wedge\, \Lambda) \tag{2}$$

where $\beta_p \in FO[\sigma]$ is the characteristic sentence of p, $\Upsilon_{IS} \in SO\exists[\sigma]$ is a generalized IS-form *[7], and Λ is a $SO\exists[\sigma]$ sentence.*

Intuitively, this result says that if sentence Ψ characterizes a $\leq_{fop}$-complete problem L for NP, then it can be decomposed in two disjuncts $\Psi = \Psi_{IS} \vee \Psi_{rest}$ such that MOD$[\Psi_{IS}]$ is $\leq_{fop}$-complete for NP and MOD$[\Psi_{rest}]$ equals the "rest" of L which is not necessarily complete.

Our main contribution is to show that above result can be generalized over a wide collection of complexity classes, including the nice classes, and that such decomposition can be done modulo any $\leq_{fop}$-complete problem for the given class. Moreover, we also show two such decompositions are not in general equivalent.

The main obstacle for such generalization is to take care of the sentence Υ_{IS} for classes different than NP. As it will be shown, we do not have to consider each different class in isolation, since the corresponding Υ sentences will be the duals of the sentence Ψ that characterize the complete problem.

Let us first define the relation $\cong_\Pi$ over STRUC$[\tau]$ with respect to a given problem $\Pi \subseteq$ STRUC$[\tau]$. For structures $\mathcal{A}$ and $\mathcal{B}$, define

$$\mathcal{A} \cong_\Pi \mathcal{B} \quad \text{iff} \quad (\mathcal{A} \in \Pi \Leftrightarrow \mathcal{B} \in \Pi)\,. \tag{3}$$

Clearly, $\cong_\Pi$ is an equivalence relation that partitions STRUC$[\tau]$ into Π and its complement.

By using dual operators and the equivalence relation, we are able to show the following generalization of Theorem 2. In the following, τ and σ refer to any two vocabularies.

Theorem 3 (Main) *Let* $\mathbf{C}$ *be a complexity class captured by fragment* $\mathcal{L}$ *closed under disjunctions and closed under conjunctions with FO. Let* $\Pi \subseteq STRUC[\tau]$ *be a* $\leq_{fop}$*-complete problem for* $\mathbf{C}$ *characterized by* $\Psi \in \mathcal{L}[\tau]$*, and* B *a problem over vocabulary* σ*. Then,* B *is* $\leq_{fop}$*-complete for* $\mathbf{C}$ *if and only if there is a fop* $p : STRUC[\tau] \to STRUC[\sigma]$ *such that for all* $\mathcal{B} \in STRUC[\sigma]$*:*

$$\mathcal{B} \in B \quad \textit{iff} \quad \mathcal{B} \models (\beta_p \wedge \widehat{I}(\Psi)) \vee (\neg\beta_p \wedge \Lambda) \tag{4}$$

where

(*a*) $\beta_p \in FO[\sigma]$ *is the characteristic of* p*, i.e.* $\mathcal{B} \models \beta_p$ *iff* $\mathcal{B} \in p(STRUC[\tau])$*,*

(*b*) $\Lambda \in \mathcal{L}[\sigma]$*, and*

(*c*) $I : STRUC[\sigma] \to STRUC[\tau]$ *is a first-order query such that for all* $\mathcal{A} \in STRUC[\tau]$*,* $I(p(\mathcal{A})) \cong_\Pi \mathcal{A}$*.*

Proof: For the necessity, assume that B is $\leq_{fop}$-complete for $\mathbf{C}$; i.e. B is characterized by some sentence $\Lambda \in \mathcal{L}[\sigma]$ and there is $p : \Pi \leq_{fop} B$. For $\mathcal{B} \in B$ we consider the two cases whether $\mathcal{B} \notin p(\text{STRUC}[\tau])$ or not. For the first case, $\mathcal{B} \models \neg\beta_p \wedge \Lambda$. For the second case, $\mathcal{B} \models \beta_p$ and

$$\begin{array}{ll}
\mathcal{B} = p(\mathcal{A}) & \text{(for some } \mathcal{A} \in \text{STRUC}[\tau] \text{ by } (a))\\
\quad\Longrightarrow\quad \mathcal{A} \in \Pi & \text{(since } p \text{ is reduction)}\\
\quad\Longrightarrow\quad \mathcal{A} \models \Psi & (\Psi \text{ characterizes } \Pi)\\
\quad\Longrightarrow\quad I(p(\mathcal{A})) \models \Psi & \text{(by condition } (c))\\
\quad\Longrightarrow\quad p(\mathcal{A}) \models \widehat{I}(\Psi) & \text{(def. of dual of } I)\,.
\end{array}$$

Therefore, $\mathcal{B} \in B \implies \mathcal{B} \models (\beta_p \wedge \widehat{I}(\Psi)) \vee (\neg\beta_p \wedge \Lambda)$. Now, let $\mathcal{B} \in \mathrm{STRUC}[\sigma]$ be such that $\mathcal{B} \models (\beta_p \wedge \widehat{I}(\Psi)) \vee (\neg\beta_p \wedge \Lambda)$. If $\mathcal{B} \models \Lambda$, then $\mathcal{B} \in B$. Otherwise,

$$\begin{aligned}
&\mathcal{B} \models \beta_p \wedge \widehat{I}(\Psi) \\
&\implies \mathcal{B} = p(\mathcal{A}) \text{ and } p(\mathcal{A}) \models \widehat{I}(\Psi) && \text{(for some } \mathcal{A} \in \mathrm{STRUC}[\tau]) \\
&\implies I(p(\mathcal{A})) \models \Psi && \text{(def. of dual)} \\
&\implies \mathcal{A} \models \Psi && \text{(by } (c)) \\
&\implies \mathcal{A} \in \Pi && (\Psi \text{ characterizes } \Pi) \\
&\implies \mathcal{B} \in B && \text{(since } p \text{ is reduction)}\,.
\end{aligned}$$

It remains to show that there are first-order queries satisfying (c). Since Π is complete, there is a fop $I : \mathrm{STRUC}[\sigma] \to \mathrm{STRUC}[\tau]$ that reduces $p(\Pi)$ to Π. Note that $p(\Pi) \subseteq B$ since p is also a reduction. For $\mathcal{A} \in \mathrm{STRUC}[\tau]$, observe

$$\begin{gathered}
\mathcal{A} \in \Pi \;\Rightarrow\; p(\mathcal{A}) \in p(\Pi) \;\Rightarrow\; I(p(\mathcal{A})) \in \Pi\,, \\
I(p(\mathcal{A})) \in \Pi \;\Rightarrow\; p(\mathcal{A}) \in p(\Pi) \;\Rightarrow\; p(\mathcal{A}) \in B \Rightarrow \mathcal{A} \in \Pi\,.
\end{gathered}$$

Thus, $I : p(\Pi) \leq_{fop} \Pi$ satisfies $\mathcal{A} \in \Pi$ iff $I(p(\mathcal{A})) \in \Pi$; i.e. $\mathcal{A} \cong_\Pi I(p(\mathcal{A}))$.

For the sufficiency, assume there is a fop $p : \mathrm{STRUC}[\tau] \to \mathrm{STRUC}[\sigma]$ such that (4) holds for all $\mathcal{B} \in \mathrm{STRUC}[\sigma]$. We need to show that B is complete for $\mathbf{C}$. The inclusion $B \in \mathbf{C}$ is direct from the closure properties on $\mathcal{L}$. For the hardness, we show that p is indeed a reduction from Π to B. For $\mathcal{A} \in \mathrm{STRUC}[\tau]$, we have $p(\mathcal{A}) \models \beta_p$. If $\mathcal{A} \in \Pi$, then

$$\mathcal{A} \models \Psi \;\Rightarrow\; I(p(\mathcal{A})) \models \Psi \;\Rightarrow\; p(\mathcal{A}) \models \widehat{I}(\Psi) \;\Rightarrow\; p(\mathcal{A}) \in B\,.$$

On the other hand, if $p(\mathcal{A}) \in B$, then

$$p(\mathcal{A}) \models \beta_p \;\Rightarrow\; p(\mathcal{A}) \models \widehat{I}(\Psi) \;\Rightarrow\; I(p(\mathcal{A})) \models \Psi \;\Rightarrow\; \mathcal{A} \models \Psi \;\Rightarrow\; \mathcal{A} \in \Pi\,.$$

Thus, $\mathcal{A} \in \Pi$ iff $p(\mathcal{A}) \in B$, p is a reduction, and B is complete. □

Corollary 4 *The theorem holds if the first-order query I is the reduction $I : p(\Pi) \leq_{fop} \Pi$ which exists since Π is complete.*

Moreover, a first-order query J satisfying (c) is essentially equivalent (with respect to Ψ) to the reduction $I : p(\Pi) \leq_{fop} \Pi$. Indeed, for such J and a finite σ-structure $\mathcal{B} = p(\mathcal{A})$ for $\mathcal{A} \in \mathrm{STRUC}[\tau]$,

$$\mathcal{B} \models \widehat{J}(\Psi) \iff J(\mathcal{B}) \models \Psi \iff \mathcal{A} \models \Psi \iff I(\mathcal{B}) \models \Psi \iff \mathcal{B} \models \widehat{I}(\Psi)\,.$$

If we consider nice complexity classes, then the fop p can be assumed to be injective by a result of Allender et. al [1].

Corollary 5 *For nice classes, the fop $p : STRUC[\tau] \to STRUC[\sigma]$ can be assumed to be injective.*

To see that Theorem 2 is equivalent to Corollary 5 when $\mathbf{C} = \mathrm{NP}$, let $\tau = \langle E^2, k\rangle$ and $\sigma = \langle Q^1 \rangle$ be the vocabularies for graphs and binary strings respectively, and consider a problem $L \subseteq \mathrm{STRUC}[\sigma]$ complete for NP characterized by Ψ_L. According to Theorem 2,

$$\Psi_L \;\equiv\; (\beta_p \wedge \Upsilon_{IS}) \vee (\neg\beta_p \wedge \Lambda)$$

where p : IndependentSet $\to L$ is a first-order projection and Λ is a SO$\exists$ sentence. On the other hand, according to Corollary 5, Ψ_L also satisfies

$$\Psi_L \;\equiv\; (\beta_p \wedge \widehat{I}(\Psi_{IS})) \vee (\neg\beta_p \wedge \Lambda')\,.$$

As shown before, Υ_{IS} and $\widehat{I}(\Psi_{IS})$ are equivalent on $p(\mathrm{STRUC}[\tau])$, and thus Λ and Λ' must be equivalent on $\mathrm{STRUC}[\sigma] \cap \mathrm{MOD}[\neg\beta]$.

3.1 Examples

Consider Clique $\subseteq \mathrm{STRUC}[\tau = \langle E^2, k\rangle]$ characterized by the SO$\exists$ sentence

$$\Psi_{CL} \;=\; (\exists f \in \mathrm{Inj})(\forall x, y)\big[x \neq y \;\wedge\; f_x \leq k \;\wedge\; f_y \leq k \;\to\; E(x,y)\big]\,.$$

For $\sigma = \tau$, it is not hard to see that IndependentSet can be reduced to Clique using the fop $p = \lambda_{xy}\langle\varphi_0, \varphi_1, \psi\rangle$, of arity 1, where

$$\varphi_0(x) \;=\; \mathit{true}\,, \quad \varphi_1(x,y) \;=\; \neg E(x,y)\,, \quad \psi(x) \;=\; (x = k)\,.$$

Clearly, if $\mathcal{A} = \langle|\mathcal{A}|, E^{\mathcal{A}}, k^{\mathcal{A}}\rangle$, then $|p(\mathcal{A})| = |\mathcal{A}|$, $E^{p(\mathcal{A})} = |\mathcal{A}|^2 \setminus E^{\mathcal{A}}$ and $k^{p(\mathcal{A})} = k^{\mathcal{A}}$. Therefore, $p(p(\mathcal{A})) = \mathcal{A}$ for all $\mathcal{A} \in \mathrm{STRUC}[\tau]$, and hence

$$p(p(\mathcal{A})) \in \textsc{IndependentSet} \quad \text{iff} \quad \mathcal{A} \in \textsc{IndependentSet}\,.$$

Furthermore, $\beta_p = \mathit{true}$ and since Clique is also known to be NP-complete with respect to $\leq_{fop}$ reductions, we have

$$\Psi_{CL} \;\equiv\; (\beta_p \;\wedge\; \widehat{p}(\Psi_{IS})) \;\vee\; (\neg\beta_p \;\wedge\; \Gamma) \;=\; \widehat{p}(\Psi_{IS})\,.$$

Conversely, beginning with the observation tha $\beta_p = \mathit{true}$ and $\widehat{p}(\Psi_{IS}) = \Psi_{CL}$ we can conclude, by Theorem 3, that Clique is $\leq_{fop}$-complete for NP. We call this formulation of Clique as its canonical form with respect to IndependentSet. In this example, the formula Ψ_{CL} was already in its canonical form with respect to IndependentSet.

For a second example, consider the problem SubGraphIso defined by tuples $\langle G, G'\rangle$ such that the graph G contains a subgraph isomorphic to graph G'. Such tuples can be expressed with the vocabulary $\sigma = \langle F^2, H^2, k\rangle$ where F and H define the edges of G and G', and the constant k defines the initial segment $\{0, \ldots, k-1\}$ for the edges of G'. Among other things, instances of SubGraphIso are identified with structures $\mathcal{B}$ in which $H^{\mathcal{B}} \subseteq \{0, \ldots, k-1\}^2$. SubGraphIso is defined by the SO$\exists$ sentence Ψ_{SG}

$$(\exists f \in \mathrm{Inj})(\forall x, y)\big[x \neq y \;\wedge\; f_x < k \;\wedge\; f_y < k \;\to\; (H(f_x, f_y) \to F(x,y))\big]\,.$$

A fop reduction p from Clique into SubGraphIso outputs $\langle G, K_k, k\rangle$ on input $\langle G, k\rangle$. The fop is $p = \langle\varphi_0, \varphi_1, \varphi_2, \psi\rangle$ given by

$$\varphi_0 \;=\; \mathit{true}\,,\; \varphi_1 \;=\; E(x,y)\,,\; \varphi_2 \;=\; (x < k \wedge y < k)\,,\; \psi \;=\; (x = k)\,.$$

The characteristic sentence of p is

$$\beta_p \;=\; x < k \wedge y < k \to F(x,y)\,.$$

The reduction $I : p(\textsc{Clique}) \leq_{fop} \textsc{Clique}$ given by $I = \langle\varphi_0 = \mathit{true}, \varphi_1 = F(x,y)\rangle$ satisfies $\mathcal{B} \in p(\textsc{Clique})$ if and only if $I(\mathcal{B}) \in \textsc{Clique}$ for all $\mathcal{B}$. Since Ψ_{SG} is equivalent to $(\beta_p \wedge \widehat{I}(\Psi_{CL})) \vee (\neg\beta_p \wedge \Psi_{SG})$, then, by Corollary 5, SubGraphIso is complete for NP via $\leq_{fop}$ reductions.

Finally, other classes that satisfies the conditions of Corollary 5 are L, NL, P, PSPACE, and all Σ_k^p and Π_k^p.

4 Non-Isomorphic Complete Problems for Nice Classes

The next result is a more general version of one already known for NP [7]. The proof is analogous to the NP case. Among other things. it implies that we cannot get rid of the disjunction in Corollary 5.

Theorem 6 *If* $\mathbf{C}$ *is a nice complexity class, then there are two* $\mathbf{C}$*-complete problems that are not fop-isomorphic.*

Proof: Let $\Gamma \subseteq \{0,1\}^*$ be a $\leq_{fop}$-complete problem for $\mathbf{C}$, and define $\Gamma' = \{\omega 0, \omega 1 : \omega \in \Gamma\}$. It is easy to see that Γ' is complete via fops; e.g. define the projection $p : \mathrm{STRUC}[\tau = \langle S^1 \rangle] \rightarrow \mathrm{STRUC}[\sigma = \langle T^1 \rangle]$, of arity 2, as $p = \langle \varphi_0(x,y), \varphi_1(x,y) \rangle$ where $\varphi_0(x,y) = (x = 0) \vee (x = 1 \wedge y = 0)$ gives the domain of $p(\mathcal{A})$ and $\varphi_1(x,y) = (x = 0 \wedge S(y)) \vee (x = 1 \wedge y = 0)$ gives $T^{p(\mathcal{A})}$. Thus, for $\mathcal{A}$ with domain $|\mathcal{A}| = \{0, \dots, n-1\}$, φ_0 defines

$$|p(\mathcal{A})| \ = \ \{(0,y) : 0 \leq y < n\} \ \cup \ \{(1,0)\}\,.$$

Formula φ_1 identifies the n bits of $\mathcal{A}$ with the tuples $(0,x)$ and assigns "value" 1 to the tuple $(1,0)$. Observe that the order induced in $p(\mathcal{A})$ is $(0,0) < (0,1) < \cdots < (0,n-1) < (1,0)$. Therefore, $\omega \in \Gamma$ iff $p(\omega) \in \Gamma'$ which shows that Γ' is complete.

Since $\mathbf{C}$ is a nice complexity class, there is a fop $p : \mathrm{STRUC}[\tau] \rightarrow \mathrm{STRUC}[\sigma]$ that is injective, of arity $k \geq 2$, that reduces Γ to Γ'. We will show that p cannot be onto by showing that if $\omega \in \Gamma$, then either $\omega 0 \notin p(\Gamma)$ or $\omega 1 \notin p(\Gamma)$.

Consider the formula $\varphi(\bar{x})$ that defines the interpretation of T in the structure $p(\mathcal{A})$ of form

$$\varphi(\bar{x}) \ = \ \alpha_0(\bar{x}) \ \vee \ (\alpha_1(\bar{x}) \wedge \lambda_1(\bar{x})) \ \vee \cdots \vee \ (\alpha_r(\bar{x}) \wedge \lambda_r(\bar{x}))\,.$$

We are going to show $w0 \in p(\Gamma) \implies w1 \notin p(\Gamma)$. Suppose that $|\omega 0| = n + 1$ and that $\omega 0 = p(\omega')$ for some $\omega' \in \Gamma$ represented by the structure $\mathcal{A}$. Each bit in $\omega 0$ corresponds to a k-tuple in $p(\mathcal{A})$, i.e. $\omega 0 \sim \bar{u}_0 \bar{u}_2 \dots \bar{u}_n$ where $\bar{u}_j$ is 1 iff $\omega' \vDash \varphi(\bar{u}_j)$. Since $\bar{u}_n \sim 0$, $\omega' \nvDash \alpha_0(\bar{u}_n)$. Consider the two cases whether $\omega' \vDash \alpha_\ell(\bar{u}_n)$ for some $1 \leq \ell \leq r$, or not.

In the latter case, we can conclude that $\omega'' \nvDash \alpha_\ell(\bar{u}_n)$ for every $\omega'' \in \{0,1\}^{|w|}$ and $1 \leq \ell \leq r$ since α_ℓ, being a numerical formula, obtains a value that only depends on the size of its input; thus, $\omega 1 \notin p(\Gamma)$.

In the former case, $\omega' \vDash \alpha_\ell(\bar{u}_n)$, for some unique ℓ, and $\omega' \nvDash \lambda_\ell(\bar{u}_n)$ since $\bar{u}_n \sim 0$. Thus, since $\lambda_\ell(\bar{u}_n)$ is a literal, some bit of ω' determines the value 0 for $\bar{u}_n$. On the other hand, observe that

$$\omega' \in \Gamma \iff p(\omega') = \omega 0 \in \Gamma' \iff \omega \in \Gamma$$

where the first equivalence follows since p is a reduction, and the second by construction of Γ'. Furthermore, being p injective, implies that each bit in ω' determines one bit in ω. Therefore, there is a bit in ω' that determines two bits in $\omega 0$: one bit in ω and the rightmost 0. If $\omega 1$ were in $p(\Gamma)$, then the same bit in the preimage of $\omega 1$ would determine the same bit in ω and the rightmost 1, this time in an inconsistent manner. Therefore, $\omega 1 \notin p(\Gamma)$. $\square$

5 Conclusions

We have extended the canonical form proposed by Medina and Immerman to all complexity classes characterized by fragments $\mathcal{L}$ closed under disjunctions, and under conjunctions with FO. Although, Medina and Immerman's method could be generalized to other nice classes beyond NP, it requires the formulation of "generalized" sentences. Our method, on the other hand, circumvent this problem by considering the dual operator. Additionally, it is not clear how Medina and Immerman's method could be used to find canonical forms with respect to problems that are not "graph" problems, or on classes that do not have complete problems based on explicit graphs, e.g. PSPACE.

As for the near future, we are currently working on syntactic operators that preserve completeness via fops for general complexity classes. This subject is also addressed by Medina [6] where syntactic operators $I : \mathcal{L}[\tau] \to \mathcal{L}[\sigma]$, that map formulae into formulae, are defined such that if Ψ characterizes a NP-complete problem, then so is $I(\Psi)$. We think that as inverse images play a fundamental role in (mathematical) analysis, inverse images of syntactic transformations are worth to explore. In our case, we look for operators I such that if $I(\Psi)$ defines a complete problem, then Ψ also defines a complete problem; Nijjar also mention that such transformations are worth exploring [8]. We believe that such operators could be use to establish completeness of problems in an easier way.

References

[1] E. Allender, J. Balcázar, and N. Immerman. A first-order isomorphism theorem. *SIAM Journal of Computing*, 26(2):555–567, 1997.

[2] E. Dahlhaus. Reduction to NP-complete problems by interpretations. *Lecture Notes in Computer Science*, pages 357–365, 1984.

[3] R. Fagin. Generalized first-order spectra and polynomial-time recognizable sets. In R. Karp, editor, *SIAM-AMS Proc. 7*, pages 27–41, 1974.

[4] E. Gradel. Capturing complexity classes by fragments of second-order logic. *Theoretical Computer Science*, 101:35–57, 1992.

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

[6] J. A. Medina. *A Descriptive Approach to The Class NP.* PhD thesis, University of Massachusetts, Amherst, 1997.

[7] J. A. Medina and N. Immerman. A syntactic characterization of NP-completeness. In *Proc. IEEE Symp. Logic in Computer Science*, pages 241–250, 1994.

[8] P. Nijjar. An attempt to automate np-hardness reductions via SO$\exists$ logic. Master's thesis, Waterloo University, Ontario, Canada, 2004.

[9] C. Papadimitriou. *Computational Complexity.* Addison-Wesley, 1994.

[10] L. Valiant. Reducibility by algebraic projections. *L'Ensignment Mathématique*, 28:253–268, 1982.