Hiérarchies de définissabilité logique au second ordre

Arnaud Durand

Remerciements

Je suis très heureux de pouvoir remercier ici Etienne Grandjean. Sans sa culture et son expérience, sans les nombreux conseils et encouragements qu'il m'a prodigués, j'ose à peine imaginer où en serait ce travail aujourd'hui. Il a consacré à m'écouter et à me lire un nombre considérable d'heures, m'orientant invariablement par ses questions et ses remarques dans la meilleure direction. En outre, sa bienveillance et sa gentillesse ont rendu idéales les conditions dans lesqueslles cette thèse s'est déroulée. Enfin, peut être parce que sa passion et son enthousiasme sont communicatifs, il a su éveiller en moi un intérêt pour la recherche que je ne soupçonnais pas et pour cela, je lui dois beaucoup.

I am very grateful to Clemens Lautemann for the interest he takes to my work since now two years. I am very honoured that he and Erich Grädel have accepted to write a report on this thesis.

Ma reconnaissance va aussi à Michel de Rougemont pour avoir accepté d'être rapporteur sur cette thèse et pour les nombreuses remarques qu'il m'a suggérées.

Je suis très honoré de la présence de Patrice Enjalbert, Stéphane Grumbach, Jacques Stern, Patrick Dehornoy et Friedrich Wehrung dans ce jury. Ces deux derniers, par leurs enseignements de maîtrise de mathématiques, sont à l'origine de ma curiosité pour le monde étrange (et passionnant) de la complexité.

Alors que je n'étais encore qu'en D.E.A., Ionona Ranaivoson a accepté de travailler d'égal à égal avec moi. De notre collaboration sont issues un grand nombre des idées de cette thèse. Je le remercie sincèrement.

Enfin, j'aimerais terminer en exprimant ma profonde gratitude envers tous ceux qui, gens de Caen ou d'ailleurs, chercheurs, secrétaires ou amis, ont contribué d'une façon ou d'une autre à l'aboutissement de ce travail.

Il y a parmi nous des magiciens et des magiciennes,
mais personne ne le sait...
L'Arioste

A mes parents
A Anne et Séverine

A Christophe

Table des matières

Introduction

0.1 Complexité descriptive et complexité algorithmique

Définir un ensemble de structures (entiers, mots, graphes, structures algébriques, bases de données, ...) c'est, la plupart du temps, exhiber une propriété caractéristique de cet ensemble que l'on exprime ensuite dans un langage particulier, souvent un langage logique. Plus précisement, si P est un ensemble de structures et $\mathcal{L}$ une logique, P sera dit définissable dans $\mathcal{L}$ s'il existe une formule φ de $\mathcal{L}$ "vraie" dans chaque structure de P et fausse partout ailleurs. Mais, commençons par quelques exemples.

Soit $G = \langle V, E \rangle$ un graphe fini non orienté, c'est à dire, la donnée d'un ensemble fini V et d'une relation symétrique $E \subseteq V \times V$ sur les couples d'éléments de V. Dans, la suite tout graphe sera supposé non-orienté.[1]

1. Un tel graphe est de degré borné par un entier fixé k (on dira qu'il est k-borné) si tout x de V est en relation par E avec au plus k éléments distincts de V. La formule φ :

$$\forall x \exists y_1 \exists y_2 \ldots \exists y_k \forall z \; R(x,z) \rightarrow \bigvee_{i=1}^{k} z = y_i$$

est vérifiée par tout graphe k-borné. Réciproquement, toute structure vérifiant φ est k-bornée. φ est donc une "description" logique des structures vérifiants cette propriété.

2. Un graphe est dit 3-*colorable* si ses sommets peuvent être coloriés à l'aide de trois couleurs différentes, mettons *noir, rouge, blanc*, de façon à ce que deux points quelconques reliés entre eux ne portent jamais la même couleur. Autrement dit, l'ensemble des éléments d'un tel graphe peut être partitionné en trois sous-ensembles U_n, U_r et U_b de telle sorte qu'aucun d'eux ne contiennent deux sommets en relation par E. Ceci peut alors s'exprimer par :

1. Quoique se voulant informelle, cette présentation n'en utilise pas moins quelques termes de logique et de théorie des modèles. Le lecteur ignorant cette terminologie est invité à se reporter au chapitre suivant.

$$\exists U_n \exists U_r \exists U_b \quad \forall x \ [U_n(x) \vee U_r(x) \vee U_b(x)] \wedge$$
$$[\neg(U_n(x) \wedge U_r(x)) \wedge \neg(U_n(x) \wedge U_b(x)) \wedge \neg(U_r(x) \wedge U_b(x))] \wedge$$
$$\forall y \bigwedge_{i=n,r,b} [U_i(x) \wedge U_i(y) \rightarrow \neg E(x,y)].$$

3. Un graphe est *connexe* si entre deux sommets quelconques x, y de V il existe toujours un chemin, i.e. un ensemble de points $\{x_1, x_2, \ldots, x_n\}$ tel que, pour tout $i \leq n$, on a $E(x_i, x_{i+1})$ avec $x = x_1$ et $y = x_n$. Si l'on cherche à "capturer" cette classe, on ne peut exprimer directement ce qui vient d'être dit pour la simple et bonne raison que l'on ne connait pas, à l'avance, la longueur du chemin reliant x à y (sauf à posséder dans notre formalisme un opérateur $\Delta_E(x,y)$: "il existe un chemin entre x et y par la relation E"). On remarque alors la chose suivante: un graphe G est connexe si et seulement si pour toute partition de ses sommets en deux sous-ensembles U et $\overline{U}$, il existe au moins deux éléments $u \in U$, $\overline{u} \in \overline{U}$ vérifiants $E(u, \overline{u})$. Ceci s'exprime facilement par :

$$\forall U \ \exists u \exists \overline{u} \quad U(u) \wedge \neg U(\overline{u}) \wedge E(u, \overline{u}).$$

Replongeons nous dans ce qui vient d'être dit et examinons une à une les formules définissant les différentes classes de structures. Le premier exemple présente le cas de figure le plus simple. La formule, dont tous les quantificateurs portent sur les individus, est dite du *premier ordre* et utilise $k+2$ variables.

La propriété suivante, la 3-colorabilité, a nécessité l'introduction de quantificateurs existentiels portant sur des prédicats unaires (encore appelés monadiques). Mais "nécessité" est-il le mot adéquat? n'aurait-on pu, en réfléchissant un peu plus, trouver une définition de la 3-colorabilité dans la logique du premier ordre? la réponse est ... NON. Ceci est rigoureusement impossible. La nouvelle logique obtenue par enrichissement du premier ordre est donc strictement plus expressive que cette dernière. Elle porte le nom de *logique existentielle monadique du second ordre*.

Pour définir la connexité, une quantification *universelle* portant sur un symbole de relation unaire a été utilisée. Là encore, la question se pose : le premier ordre ou le second ordre existentiel monadique auraient-ils suffi? la réponse est toujours NON ([Fag75a]).

De ces exemples classiques, une certaine notion de complexité se dégage : celle des ressources[2] mises en jeu dans l'expression d'une propriété donnée. L'étude de ces ressources s'appelle la complexité *descriptive*.

2. Bien entendu, ces ressources peuvent se mesurer de mille et une manières : nombre de variables ou nombre de quantificateurs universels au premier ordre; forme et/ou alternance des quantificateurs au second-ordre, arité et/ou nombre de prédicats utilisés ...

Seuls les modèles finis des formules considérées nous intéresseront ici. Cette restriction prend tout son sens, à coup sur, avec l'explosion de l'informatique théorique et la mise à jour de liens surprenants entre la complexité descriptive d'une propriété donnée et sa complexité algorithmique, c'est à dire les ressources en temps ou mémoire demandées par un calcul qui décide si celle ci est vraie.

Un des premiers "ponts" entre ces deux domaines apparaît à travers la notion de caractérisation logique des classes de complexité. Formellement, si $\mathcal{C}$ est une classe de complexité et $\mathcal{L}$ une logique, on dit que $\mathcal{L}$ *caractérise* $\mathcal{C}$ si pour tout ensemble de structures P de $\mathcal{C}$, il existe une formule Φ_P dans $\mathcal{L}$ dont les modèles sont exactement les éléments de P. De plus, la caractérisation est *exacte* si l'ensemble des modèles de toute formule Φ de $\mathcal{L}$ est aussi dans $\mathcal{C}$.

On note par Σ_1^1 la logique existentielle du second ordre. En d'autres mots, une formule Φ appartient à Σ_1^1 si elle est de la forme

$$\exists R_1 \ldots \exists R_k \; \varphi,$$

où les R_i désignent des symboles de relations ou de fonctions d'arités quelconques et où φ est du premier-ordre. En codant dans cette logique le calcul d'une machine de Turing fonctionnant en temps polynomial non-déterministe (i.e. dans NP), Fagin ([Fag74]) donne un des premiers résultats de caractérisation (par généralisation d'un résultat un peu plus ancien de Jones et Selman [JS74]). Il établit par là-même la stricte équivalence entre deux problèmes, toujours non résolus, d'origines différentes; l'un de théorie des modèles finis, dit problème d'Asser généralisé ([Ass55]), qui s'interroge sur l'éventuelle clôture par complémentaire de Σ_1^1; l'autre, beaucoup plus connu et provenant de la théorie de la complexité, qui cherche à savoir si $NP = co\text{-}NP$.

Plus tard, Lynch puis Grandjean vont raffiner le théorème de Fagin en mettant à jour de nouveaux liens entre polynôme de complexité en temps et ressources logique nécessaire.

Lynch ([Lyn82, Lyn92]), tout d'abord, va prouver que tout ensemble de structures accepté en temps n^d par une machine de Turing non-déterministe est l'ensemble des modèles finis d'une formule Σ_1^1 dont tous les prédicats du second ordre sont d'arités au plus d (en supposant toutefois qu'une addition si $d \geq 1$, ou seulement une relation successeur si $d \geq 2$, est prédéfinie sur le domaine des structures).

Grandjean ([Gra84, Gra85]), quelques temps après, démontre pour tout $d \geq 2$ que si un ensemble de structures est décidé en temps $O(n^d)$ sur machine RAM non-déterministe, on peut trouver une formule Σ_1^1 qui le définit, dont la partie du premier ordre est restreinte à d quantificateurs universels et dont les prédicats apparaissant au second-ordre sont des symboles de fonctions d'arité au plus d. Il établit de plus la réciproque de ce résultat. Pour le cas $d \geq 1$ ([Gra90c]), il redonne dans un premier temps une caractérisation identique mais pour des ensembles d'entiers seulement (correspondant à des structures finies de signature vide). Enfin, en introduisant un nouveau modèle de calcul et en supposant un codage différent des structures en entrée, il définit une nouvelle

notion de temps linéaire sur machine RAM ([Gra94b, Gra96]) que lui et F. Olive caractérisent exactement aussi d'un point de vue logique ([GO94]). Mais nous y reviendrons plus tard.

Un grand nombre de classes de complexité ont fait l'objet d'une caractérisation logique, exacte ou non. En vrac, citons pour les plus importantes : P, le temps polynomial déterministe, $NLOGSPACE$, l'espace logarithmique non-déterministe , $PSPACE$, l'espace polynomial, $NEXPTIME$, le temps exponentiel non-déterministe (pour un survol de ce domaine, voir [Imm89]).

0.2 Contenu de la thèse

Comme le lecteur aura pu le deviner, au regard de l'insistance dont nous avons fait preuve jusqu'à maintenant, la logique existentielle du second-ordre, Σ^1_1, va jouer dans toute cette thèse un rôle central. C'est à l'étude du pouvoir d'expression de certains de ses fragments que nous allons nous consacrer. Un *fragment* de Σ^1_1 est une sous-classe de formule de cette logique définie le plus souvent par des conditions portant sur l'arité et/ou le nombre des prédicats quantifiés (appelés prédicats du second ordre), ou sur la forme du préfixe en quantificateurs du premier ordre. Soient $\mathcal{S}$ une signature et $\Phi \in \Sigma^1_1$,

$$\Phi : \exists R_1 \ldots \exists R_k \ \varphi(\mathcal{S}, R_1, \ldots, R_k)$$

où φ est du premier-ordre de signature $\mathcal{S} \cup \{R_1, \ldots, R_k\}$. On appelle $Func^\omega_1(\mathcal{S})$ (resp. $BIN(\mathcal{S})$) la classe des structures définissables par une formule Φ de Σ^1_1, comme ci-dessus, où chaque R_i est un symbole de fonction unaire (resp. où $k = 1$ et R_1, l'unique symbole quantifié, est un prédicat relationnel binaire). Lorsque l'on cherche à capturer des ensembles d'entiers ou de graphes (i.e. quand la signature de "l'entrée" $\mathcal{S}$ est vide ou restreinte à un seul symbole de relation binaire), il est intéressant de constater que rares sont les ensembles définis naturellement qui ne semblent être ni dans $Func^\omega_1(\mathcal{S})$, ni dans $BIN(\mathcal{S})$.

Le premier résultat significatif de cette thèse est d'établir (cf. chapitre 2) que, pour toute signature $\mathcal{S}$, on a :

$$Func^\omega_1(\mathcal{S}) \subseteq BIN(\mathcal{S}).$$

De plus, nous prouvons (chap. 5) que si $\mathcal{S}$ contient au moins un symbole de prédicat binaire, alors l'inclusion est stricte (l'inclusion stricte est obtenue en montrant que l'ensemble des graphes dont le nombre d'arêtes est pair est dans $BIN(\mathcal{S})$ mais pas dans $Func^\omega_1(\mathcal{S})$ [3]). Trouver une propriété sur les graphes (décidable dans P, NP, $co-NP$ ou $PSPACE$) qui ne soit définissable par aucune formule de Σ^1_1 dont le second-ordre ne contienne qu'un seul symbole de relation binaire est, à ce jour, une question ouverte.

3. la borne inférieure est prouvé à l'aide d'un résultat d'Ajtai [Ajt83]

On améliore ensuite notre résultat de plusieurs manières :

1. En examinant la preuve de l'inclusion ci-dessus, on s'aperçoit que la relation R_1 (existentiellement quantifiée) est de degré extérieur borné par une constante k dépendant uniquement du nombre de fonctions. Comme l'inclusion inverse est vraie (une relation de degré extérieur k peut être "simulée" par $k+1$ fonctions), on obtient alors une égalité de classes d'exprimabilité.

   Dans la suite, lorsqu'on limitera les interprétations possibles d'un symbole binaire R_1 aux graphes de degré extérieur borné par une certaine constante k, on dira que R_1 est un prédicat *k-borné*.

2. L'inclusion ci-dessus est toujours vraie lorsque l'on impose à la relation binaire R_1 d'être : un ordre partiel ou une relation symétrique ou encore une relation bipartite (symétrique ou non-symétrique). De plus, si on suppose que les fonctions unaires sont bijectives, on peut alors imposer que la relation R_1 soit de degré extérieur et intérieur bornés par une constante (dépendant du nombre de bijections). Dans ce cas, la réciproque est vraie elle aussi.

3. Pour chaque formule de Σ_1^1 dont la partie du second ordre est restreinte à un nombre quelconque de symboles de fonctions unaires, il est possible, comme précédemment, de trouver une autre formule avec un seul prédicat binaire h-borné au second ordre (h dépendant de k) qui lui est logiquement équivalente sur les structures finies et qui, de plus, a le même nombre d de quantificateurs universels au premier ordre. Ce résultat, valable pour tout entier d, va nous permettre, dans le cas $d = 1$ de donner une nouvelle caractérisation exacte du temps linéaire non-déterministe sur machine RAM.

De nombreux corollaires de ces résultats sont présentés tout au long de cette thèse. Certains concernent d'autres problèmes de définissabilité, d'autres des questions d'indécidabilité dans les logiques préfixielles.

Dans la dernière partie de la thèse, on prouve un théorème de hiérarchie stricte à partir d'un lemme "de transfert". Ce théorème qui ne concerne que la définissabilité d'ensembles d'entiers prend en compte aussi bien l'arité des prédicats mis en jeu que le nombre de quantificateurs universels. Enfin, on aborde des questions de définissabilité au premier ordre.

Plusieurs parties de cette thèse sont publiées ou soumises à publication. Elles sont donc, de ce fait, en anglais.

0.3 Quelques idées sur la méthode

Intéressons nous, à nouveau, au premier résultat de cette thèse. L'inclusion,

$$Func_1^{\omega}(\mathcal{S}) \subseteq BIN(\mathcal{S}),$$

se prouve principalement en construisant pour toute structure $\langle Dom, f_1, \ldots, f_k \rangle$ (où les f_i sont des fonctions unaires) un graphe orienté $\langle Dom, R \rangle$ qui va, en quelque sorte, "simuler" la structure $\langle Dom, f_1, \ldots, f_k \rangle$ (pourvu que Dom soit de taille n assez grande).

La méthode utilisée pour construire de tels graphes est relativement simple. De plus, son caractère modulaire et uniforme a permis que se développent, petit à petit, de nombreuses variantes; certaines suffisamment puissantes pour nous permettre de prouver finalement la plupart des résultats des chapitres 2, 3 et 4.

Il a donc semblé intéressant de tenter de dessiner ici les grandes lignes de cete méthode. La situation est la suivante: on dispose d'un domaine Dom de taille n et de k fonctions f_1, ..., f_k définies sur celui-ci. On construit alors notre relation binaire R sur Dom en deux temps. Tout d'abord une phase de mise en forme du domaine (i.e. de "représentation" du domaine puis de "transport" de l'information) est nécessaire. Ce travail, préalable à tout codage, sera exactement le même quelles que soient les fonctions f_i . Ensuite seulement, la relation R sera complétée, en tirant profit au maximum de la première étape, pour simuler les fonctions.

0.3.1 Représenter le domaine

Soient A et B deux sous-ensembles[4] disjoints de Dom de taille au moins $\sqrt{n}$. On fabrique, par R, une injection de Dom vers $A \times B$ en associant à chaque élément y du domaine une unique paire de représentant (a, b). Ceci se fait en créant les arcs (y, a) et (y, b) pour la relation R. Implicitement, ceci va nous permettre de considérer $A \times B$ comme une "copie" de Dom. En renouvelant cette opération un grand nombre de fois avec d'autres sous-ensembles du domaine (ce qui est toujours possible lorsque n est suffisamment grand), on obtient alors plusieurs "copies" de celui-ci.

Le schema 0.1 illustre ce que nous venons de dire. L'union des paires de sous-ensembles représentant le domaine est appelée "zone de représentation".

Une telle idée qui consiste à projeter le domaine sur des sous-ensembles assez grands de celui-ci n'est absolument pas nouvelle. On la retrouve par exemple, plus ou moins explicitement, dans certaines preuves d'indécidabilité de théories logiques. Dans le cadre des modèles finis, une de ses premières applications est due à E. Grandjean ([Gra90c]). C'est l'influence de ce travail que l'on sentira ici.

4. On ne dit pas ici comment l'on procède pour distinguer des sous-ensembles du domaine. En s'aidant de la relation R, cette phase est bien souvent assez facile à réaliser

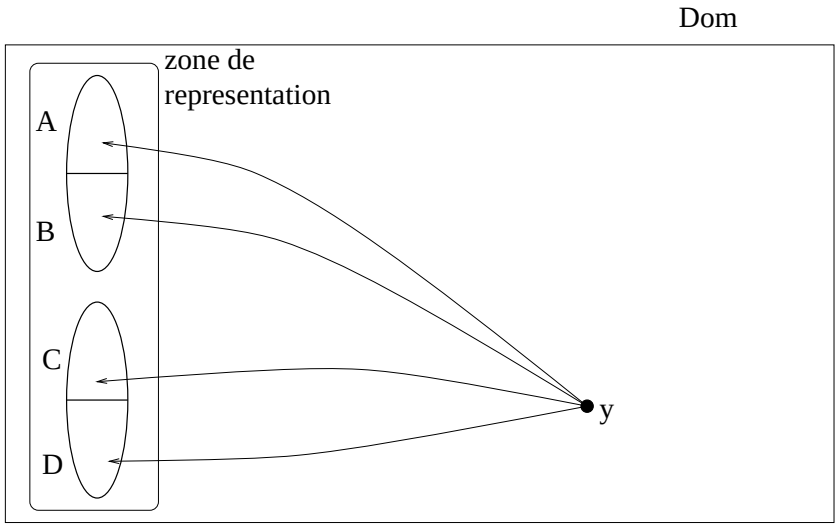

FIG. 0.1 - *représenter le domaine*

0.3.2 "Transporter" l'information

Une fois la première étape réalisée, il apparaît vite malaisé de manipuler directement les représentants des éléments du domaine pour simuler les fonctions. L'idée alors est de mettre en bijection, toujours par R, les sous-ensembles de la zone de représentation avec d'autres sous-ensembles du domaine.

Plaçons nous dans le cas où Dom est représenté sur $A \times B$ seulement. Soient $U, V \subseteq Dom$ disjoints (et disjoints de A et B) et de même cardinalité que A et B. A tout couple (a, b) de $A \times B$, on associe un unique couple (u, v) de $U \times V$ en ajoutant les arcs (a, u) et (b, v) à la relation R. En suivant alors les arcs de représentation (de Dom vers $A \times B$) puis les nouveaux arcs, dits de bijection de $A \times B$ vers $U \times V$, tout élément y de Dom se trouve alors en relation avec un unique couple (u, v) de $U \times V$.

Dans la pratique, les choses seront un peu plus compliquées. Les différents sous-ensembles de la zone de représentation seront mis en correspondance bijective avec un nombre parfois important d'autres sous-ensembles du domaine. Sous-ensembles que l'on regroupe en k parties appelées "zones de codage" et numérotées de 1 à k. De plus, les correspondances bijectives que l'on construit seront bien souvent des compositions de bijections élémentaires passant par des sous-ensembles intermédiaires. On parlera alors, non plus simplement d'arcs, mais de chemins d'arcs de bijection (cf. figure 0.2).

Il nous reste à voir comment l'on peut exploiter la construction que nous venons de faire pour simuler les k fonctions unaires de départ, $f_1, \ldots, f_k$. L'idée principale consiste maintenant à utiliser les différentes zones de codage. C'est dans la première de ces zones

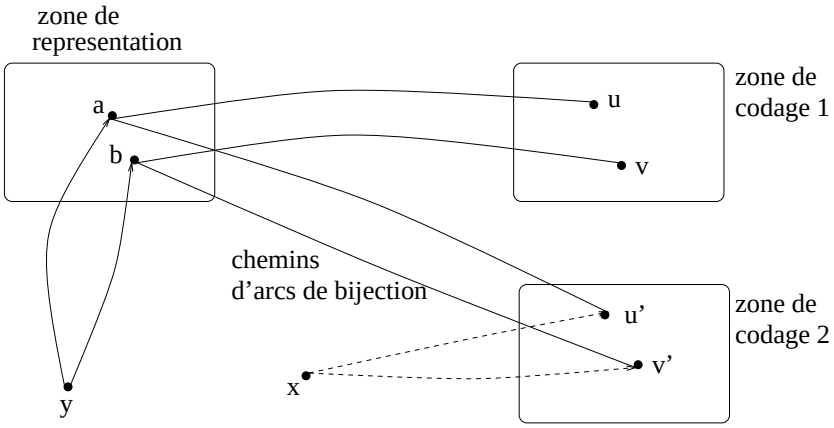

FIG. 0.2 - *schéma général de la relation binaire R (et aperçu du codage de $f_2(x) = y$)*

que l'on codera la fonction f_1, dans la deuxieme que l'on codera f_2 etc[5]...

Soient x, y tels que $f_i(x) = y$; on procédera alors presque toujours comme suit: on lit le representant (a, b) de y dans la zone de representation[6]; de (a, b), on suit les chemins d'arcs de bijection jusqu'à un couple (u, v) de la zone de codage n^o i; on ajoute à la relation R les arcs (x, u) et (x, v) (voir figure 0.2.

5. d'un certain point de vue la zone de représentation n'est, elle aussi, rien d'autre qu'une zone de codage particulière (de numéro 0) correspondant à la fonction f_0 égale à l'identité

6. on suppose que ce représentant est unique, ou que tous les représentants sont, en quelque sorte, équivalents

Chapitre 1

Notations

1.1 Formulas

A *signature* $\mathcal{S} = \{S_1, \ldots, S_l\}$ is a finite set of relation or function symbols each with a fixed arity j_i. We will always consider that $\mathcal{S}$ contains the equality sign "=".
Let $t_1, t_2, \ldots, t_{j_i}, t_{j_{i+1}}$ be some variable. A $\mathcal{S}$-*atom* is an expression of the form:

- $S_i(t_1, t_2, \ldots, t_{j_i})$ where S_i is a relation symbol in $\mathcal{S}$
- $S_i(t_1, t_2, \ldots, t_{j_i}) = t_{j_{i+1}}$ where S_i is a function symbol in $\mathcal{S}$.

A *first-order* formula of signature $\mathcal{S}$ (a **FO** formula for short) is built inductively with the following rules:

- An $\mathcal{S}$-atom is a formula
- Let ϕ and ψ be formulas then $\neg\phi$, $\phi \wedge \psi$, $\phi \vee \psi$, $\phi \rightarrow \psi$, $\phi \leftrightarrow \psi$, $\forall x \phi$, $\exists x \phi$ are formulas.

A formula $\Psi(S_1, \ldots, S_l)$ is an *existential second-order* formula of signature $\mathcal{S}$ (i.e. is a Σ_1^1-formula) if it is of the form

$$\exists R_1 \ldots \exists R_k \ \psi(S_1, \ldots, S_l, R_1, \ldots, R_k)$$

where

- $\mathcal{R} = \{R_1, \ldots, R_k\}$ is a finite set of relation or function symbol disjoint with $\mathcal{S}$.
- $\psi(S_1, \ldots, S_l, R_1, \ldots, R_k)$ is a first-order formula of signature $\mathcal{S} \cup \mathcal{R}$.

1.2 Finite structures, models and characterization

We suppose that the reader has some familiarity with the notions of *interpretation* and of *model* of a first-order formula (see [LdR93, EFT89]).

Let $\mathcal{S} = \{S_1, \ldots, S_l\}$ be a signature. A finite $\mathcal{S}$-structure $\mathcal{M} = \langle Dom, S_1^{\mathcal{M}}, \ldots, S_l^{\mathcal{M}} \rangle$ consists in a finite universe Dom and in an interpretation $S_1^{\mathcal{M}}, \ldots, S_l^{\mathcal{M}}$ on Dom of the symbols of $\mathcal{S}$. Most of the time we will not make distinction in notation between a symbol and its interpretation. We will often write $\mathcal{M} = \langle Dom, \mathcal{S} \rangle$ and say that $\mathcal{M}$ is an $\mathcal{S}$-structure. The expression $\mathcal{M} \models \Psi(\mathcal{S})$ is used to say that the structure $\mathcal{M}$ is a model of $\Psi(\mathcal{S})$.

Now let $\mathcal{R} = \{R_1, \ldots, R_k\}$ be another set of symbols which is disjoint with $\mathcal{S}$. An *expansion* of $\mathcal{M}$ over $\mathcal{R}$ is an $\mathcal{S} \cup \mathcal{R}$-structure

$$\mathcal{M}' = \langle Dom, S_1, \ldots, S_l, R_1, \ldots, R_k \rangle.$$

Let $\Psi(S_1, \ldots, S_l)$ be the following Σ_1^1 formula:

$$\exists R_1 \ldots \exists R_k \ \psi(S_1, \ldots, S_l, R_1, \ldots, R_k)$$

A finite model of $\Psi(\mathcal{S})$ is some $\mathcal{S}$-structure $\mathcal{M}$ which has an expansion over $\mathcal{R}$ which satisfies $\psi(\mathcal{S}, \mathcal{R})$.

If ϕ is a formula, the expression $\mathcal{M} \models \phi$ is used to say that the structure $\mathcal{M}$ is a model of ϕ.

A formula ϕ *characterizes* (or, equivalently, *defines*) a set C of $\mathcal{S}$-structures, if for every $\mathcal{S}$-structure $\mathcal{M}$ it holds that

$$\mathcal{M} \in C \iff \mathcal{M} \models \phi$$

1.3 Generalized Spectra

The *generalized spectrum* of $\Psi(\mathcal{S})$, denoted

$$GenSp(\Psi(\mathcal{S}))$$

is the set of finite models of $\Psi(\mathcal{S})$. When $\mathcal{S}$ is empty this set is called the *spectrum* of Ψ and is denoted by $Sp(\Psi)$.

According to which kind of symbol occurs in second-order part of formulas, in other words according to which kind of symbol $\mathcal{R}$ is made of, we introduce new notations. Let

$$Rel_j^i(\mathcal{S}) \quad (\text{resp. } Func_j^i(\mathcal{S}))$$

be the class of generalized spectra of formulas whose second-order part is restricted to at most i relation (resp. function) symbols of arity at most j. We set

$$Rel_j^\omega(\mathcal{S}) = \bigcup_{i\geq 1} Rel_j^i(\mathcal{S}), \quad Func_j^\omega(\mathcal{S}) = \bigcup_{i\geq 0} Func_j^i.$$

Two classes of generalized spectra will be of particular interest here: $Func_1^\omega(\mathcal{S})$ when $\mathcal{R}$ is a set of unary function symbols, $Rel_2^1(\mathcal{S})$ when $\mathcal{R} = \{R\}$ contains only one binary relation symbol R.

$Rel_2^1(\mathcal{S})$ is sometimes called $BIN(\mathcal{S})$ (as a direct reference to second-order part of formulas). We will do the same here.

1.4 Semantical restrictions on the binary relation R

Let's consider the case when only one binary relation symbol R appears in second-order part of formulas. We will be interested in adding semantical restrictions to this binary relation R. More precisely, let C be a set of graphs, a set S of $\mathcal{S}$-structure is definable in (is in, for short)

$$C(\mathcal{S})$$

if there exists a first-order formula $\psi(\mathcal{S}, R)$ s.t.

$$\mathcal{M} = \langle Dom, \mathcal{S}\rangle \in S \iff \text{ there exists } R \in C \text{ s.t. } \langle Dom, \mathcal{S}, R\rangle \models \psi(\mathcal{S}, R)$$

When all interpretations of a symbol R in a formula Ψ are required to belong to a class C, R is said to be a C-symbol.

We will be interested in the following classes of graphs (the list is not exhaustive):

Sym: the class of all symmetric graphs.

Acy: the class of all acyclic graphs.

Sym–Bip: the class of all symmetric bipartite graphs.

Dir–Bip: the class of all directed bipartite graphs (see chapter 3 for a precise definition of these two later classes).

h–Deg^+: the class of all directed graph of outdegree bounded by h (where h is a fixed positive integer.)

h–Deg^-: the class of all directed graph of indegree bounded by h.

h–$Deg^\pm$: the class of all directed graph of indegree and outdegree bounded by h.

$PartOrd$: the class of all partial orders.

$\neg Refl$: the class of all irreflexive graphs.

1.5 More logic

A first-order formula ϕ is said to be in a *prenex normal form* if and only if it is in the form of

$$Q_1 x_1 \ldots Q_n x_n \ \varphi$$

where every Q_i is either $\forall$ or $\exists$ and φ is a quantifier free formula.

Let ϕ be first-order. Let $\Delta(x)$ be a formula with only one free variable x. We define the *relativization* ϕ^Δ for ϕ by induction on the construction of formulas as follows: if ϕ is atomic, then $\phi^\Delta = \phi$; else $(\neg\phi)^\Delta = \phi^\Delta$, $(\phi_1 \wedge \phi_2)^\Delta = \phi_1^\Delta \wedge \phi_2^\Delta$. $(\exists x \phi)^\Delta$ (also denoted $(\exists x \Delta(x))\phi^\Delta$) becomes $\exists x(\Delta(x) \wedge \phi^\Delta)$ and $(\forall x \phi)^\Delta$ (also denoted $(\forall x \Delta(x))\phi^\Delta$) becomes $\forall x(\Delta(x) \rightarrow \phi^\Delta)$.

Chapitre 2

Unary functions vs. one binary relation

The aim of this chapter is mainly to show that on finite structures every existential second-order sentence with the second-order quantifiers ranging over unary functions is equivalent to an existential second-order sentence with a single second-order quantifier ranging over binary relations. Some kind of reciprocal result is also true by considering binary relations whose outdegree is bounded by a given integer h . Let $Deg^+(\mathcal{S}) = \bigcup_{h>0} h\text{–}Deg^+(\mathcal{S})$. The main result can be stated as follows:

Theorem 2.1 *With the definitions given above:*

$$Func_1^{\omega}(\mathcal{S}) = Deg^+(\mathcal{S})$$

The right to left inclusion of the above theorem is obviously the most difficult part and is established by the next proposition.

Proposition 2.2 *Let $\mathcal{S}$ be any signature. Let Φ be a first-order formula of type $\mathcal{S} \cup \{f_1, \ldots, f_k\}$ where $\{f_1, \ldots, f_k\}$ is a set of unary function symbols. Then, there exists a f.o. formula Φ' of type $\mathcal{S} \cup \{R\}$ where R is a $(2k+4)$–Deg^+ binary relation symbol s.t. for all structures $\mathcal{M} = \langle Dom, \mathcal{S} \rangle$, with large enough cardinality*

$$\mathcal{M} \models \exists f_1 \ldots \exists f_k \quad \Phi \iff \mathcal{M} \models \exists R \quad \Phi'.$$

A proof of this result is given for $\mathcal{S} = \emptyset$ (i.e. for the spectra case). The general case is no more complicated except in notations. The converse inclusion of theorem 2.1 is easier. We demonstrated it in section 2.2..

In section 2.3, we generalize the right to left inclusion of theorem 2.1 by showing that, for every integer d and every signature $\mathcal{S}$:

$$Func_d^{\omega}(\mathcal{S}) \subseteq Rel_{d+1}^1(\mathcal{S}).$$

In other words, we show that any number of d-ary functions can be "simulated" by only one $d+1$-ary relation. The proof is similar to that of proposition 2.2 and will only be sketched.

Finally, as an application of our main result, we settle a question raised by M.More [Mor94a, Mor94b] concerning images of spectra under polynomials of $\mathbb{Q}[X]$.

2.1 Proof of proposition 2.2

General outline of the proof

In the following, we will only consider structures with large enough cardinalities.

We construct three objects:

- a mapping red, which maps every structure $\mathcal{F} = \langle Dom, f_1, f_2, \ldots, f_k \rangle$ to a structure $red(\mathcal{F}) = \langle Dom, R \rangle$ on the same domain,
- a first-order formula Ψ over $\{R\}$ with $2k+3$ free variables $u_1, v_1, \ldots, u_k, v_k, a, b, c$,
- for every f.o formula Φ over $\{f_1, \ldots, f_k\}$ a f.o formula Φ^* over $\{R\}$ (with the same free variables as Ψ) such that:
  1. For all $\mathcal{F}$, there are $u_1, v_1, \ldots, a, b, c$ s.t. $(red(\mathcal{F}), u_1, v_1, \ldots, a, b, c) \models \Psi$,
  2. If $(\mathcal{G}, u_1, v_1, \ldots, a, b, c) \models \Psi$, for a $\{R\}$-structure $\mathcal{G}$ and $u_1, v_1, \ldots, a, b, c \in \mathcal{G}$, then there is a structure $\mathcal{F} = \langle Dom, f_1, f_2, \ldots, f_k \rangle$ s.t. $\mathcal{G} = red(\mathcal{F})$
  3. $\mathcal{F} \models \Phi \iff (red(\mathcal{F}), u_1, v_1, \ldots, a, b, c) \models \Phi^*$

The expected Φ' will be $\exists u_1 \exists v_1 \ldots \exists a \exists b \exists c \; \Psi \wedge \Phi^*$

2.1.1 The reduction of the models

Assume $\mathcal{F} = \langle Dom, f_1, f_2, \ldots, f_k \rangle$ where Dom is of cardinality n. As mentioned above, we construct a digraph $red(\mathcal{F}) = \langle Dom, R \rangle$ which encodes $\mathcal{F}$.

Our construction is in two parts. The first one is completely independent of the original structure $\mathcal{F}$ and would be exactly the same for all structures of size n. We will take into account structure $\mathcal{F}$ only in the second part.

Let $u_1, v_1, \ldots, u_k, v_k, a, b, c$ be $2k+3$ distinct fixed elements of Dom. With these points we define respectively $2k+3$ subsets $U_1, V_1, \ldots, U_k, V_k, A, B, C$ of Dom by (e.g. for U_1):

$$\text{for all } x \in Dom \backslash \{u_1, \ldots, c\}, \qquad x \in U_1 \iff R(x, u_1).$$

We suppose that $U_1, V_1, \ldots, U_k, V_k, A, B, C$ are pairwise disjoint (in fact we shall take $|U_i| = |V_i| = |A| = |B| = |C| \geq \lceil \sqrt{n} \rceil$).

($\bullet$) We represent Dom in $A \times B$ by associating injectively by R a pair (a_y, b_y) of $A \times B$ to each element y of Dom (arrows pr_1 and pr_2 in fig.1 and fig.2).

(••) We define a bijection from each set $U_1, V_1, \ldots, A, B$ to C (arrows bij of R in fig.1 and fig.2). This ends the first part of the construction.

Now, let us show how we encode $f_i(x) = y$: first, we read the representation (a_y, b_y) of y in $A \times B$ induced by step (•). Then, from (a_y, b_y), we follow bijections of step (••) to a (unique) pair $(u_{i,y}, v_{i,y})$ of $U_i \times V_i$ (U_i, V_i are two sets which correspond to the function f_i). Finally, we associate x by R to $u_{i,y}$ and $v_{i,y}$ (arrows f_i^1 and f_i^2 in fig.1 and fig.2).

In fig.1, we give the corresponding construction for three points x, y, z such that $f_1(x) = y$ and $f_2(x) = z$ and show how B is defined by b (recall that $x \in B \iff R(x, b)$).

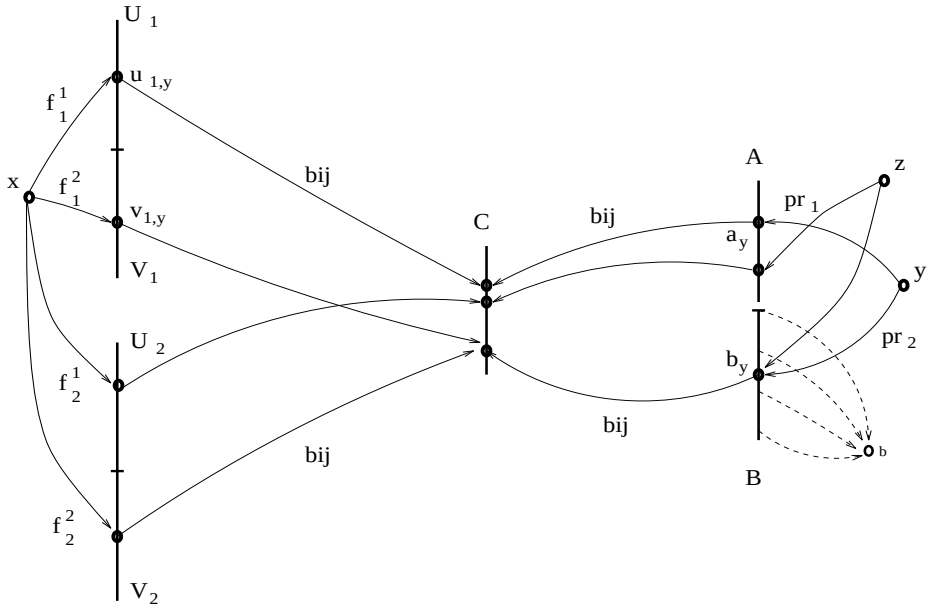

fig.1: the arrows (both full lines and dotted lines) represent relation R.

Remark 1 If two elements x_1, x_2 of Dom have the same image y under f_i, they will be associated by R to the same pair $(u_{i,y}, v_{i,y})$ of $U_i \times V_i$.

Remark 2 It is easy to see that the digraph $\mathcal{G}$ has an outdegree bounded by $2k + 4$ where k is the number of functions of $\mathcal{F}$ (outdegree $2k + 4$ is obtained for elements in $U_1, V_1, \ldots, A, B$).

2.1.2 The reduction of the formulas

Without loss of generality assume that all the atomic formulas in φ have one of the forms $f_i(u) = v$ or $u = v$ where u and v are variables. The formula Ψ is:

$$\Delta(u_1, v_1, \ldots, b, c) \wedge \Psi_0 \wedge \Psi_1 \wedge \Psi_2 \wedge \Psi_3 \wedge \Psi_4$$

where $\Delta(u_1, v_1, \ldots, b, c)$ expresses that:

- $u_1, v_1, \ldots, a, b, c$ are pairwise distinct,
- for all u, v belonging to $\{u_1, v_1, \ldots, a, b, c\}$ we have $\neg R(u, v)$,

and $\Psi_0, \ldots, \Psi_4$ are defined below.

Let $U_1(x)$ abbreviate $R(x, u_1)$,..., $C(x)$ abbreviate $R(x, c)$.

$$\Psi_0 : \forall x \ [(U_1(x) \to \neg V_1(x)) \wedge (U_1(x) \to \neg U_2(x)) \wedge \ldots \wedge (B(x) \to \neg C(x))]$$

"The subsets $U_1, V_1, \ldots, A, B, C$ are pairwise disjoint"

Remark $\Delta(u_1, v_1, \ldots, a, b, c)$ implies that $\{u_1, v_1, \ldots, a, b, c\}$ and $U_1 \cup V_1 \cup \ldots \cup A \cup B \cup C$ are disjoint.

We set $\Psi_1 = \bigwedge_{X \in \{U_1, V_1, \ldots, A, B\}} \Psi_{1,X}$ where:

$$\begin{aligned} \Psi_{1,X} : \ & (\forall \gamma C(\gamma)) \ (\exists! x X(x)) \quad R(x, \gamma) \\ & \wedge (\forall x X(x)) \ (\exists! \gamma C(\gamma)) \quad R(x, \gamma) \end{aligned}$$

"R is a one-one correspondence from each set $U_1, V_1, \ldots, A, B$ to C"

$$\begin{aligned} \Psi_2 : & \forall x \ (\exists \alpha A(\alpha)) \ (\exists \beta B(\beta)) \ (\forall \alpha' A(\alpha')) \ (\forall \beta' B(\beta')) \\ & [(R(x, \alpha') \wedge R(x, \beta')) \leftrightarrow (\alpha' = \alpha \wedge \beta' = \beta)] \end{aligned}$$

"Each element x of the domain is associated by R to a unique pair (a, b) of $A \times B$"

$$\begin{aligned} \Psi_3 : \quad & (\forall \alpha A(\alpha)) \ (\forall \beta B(\beta)) \ \forall x \ \forall y \\ & [(R(x, \alpha) \wedge R(x, \beta) \wedge R(y, \alpha) \wedge R(y, \beta)) \to x = y] \end{aligned}$$

"The above construction (from the domain to $A \times B$) is an injection"

We set $\Psi_4 = \bigwedge_{i=1}^{k} \Psi_4^i$ where:

$$\begin{aligned} \Psi_4^i : & \forall x (\exists u U_i(u)) \ (\exists v V_i(v)) \ (\forall u' U_i(u')) \ (\forall v' V_i(v')) \\ & [(R(x, u') \wedge R(x, v')) \leftrightarrow (u' = u \wedge v' = v)] \end{aligned}$$

"each element x of the domain is associated by R to exactly one pair (u, v) of $U_i \times V_i$"

We obtain Φ^* from Φ by replacing each sub-formula of the form $f_i(x) = y$ by the following formula $(*)_i(x, y)$ (see fig.1) :

$$\begin{aligned} (\exists \alpha A(\alpha) \ & (\exists \beta B(\beta)) (\exists \gamma_1 C(\gamma_1)) \ (\exists \gamma_2 C(\gamma_2)) \ (\exists u U_i(u)) \ (\exists v V_i(v)) \\ & [R(y, \alpha) \wedge R(y, \beta) \wedge R(\alpha, \gamma_1) \wedge R(\beta, \gamma_2) \\ & \wedge R(u, \gamma_1) \wedge R(v, \gamma_2) \wedge R(x, u) \wedge R(x, v)]. \end{aligned}$$

2.1.3 Some remarks about formulas

$\Psi_0, \ldots, \Psi_4$ describe syntactically the constraints to be satisfied by the digraph $\mathcal{G} = red(\mathcal{F})$. Nevertheless we have to verify there is no hidden difficulty and those constraints are, in some sense, unambiguous. First, it is easy to see that there is no "double-use" possible. To show this, we will describe all kinds of edges between two points. Note that an element of A (or $B, C, \ldots, U_i, V_i$ or one of the "constants" $a, b, c, \ldots, u_i, v_i$) is also an element of the domain and then is concerned by formulas Ψ_2, Ψ_3, Ψ_4 as such an element. Let x, y be two elements of Dom such that $R(x, y)$ holds. Concerning y we obtain exactly one of the following four cases:

- If y is one of the "constants" $u_1, v_1, \ldots, a, b, c$, then $R(x, y)$ defines x as an element of one of the subsets $U_1, V_1, \ldots, A, B, C$, respectively (denoted def in fig.3).
- If $y \in C$, then $R(x, y)$ is an edge of bijection described by Ψ_1 (denoted bij in fig.3 e.g if $x \in A$ then bij is the bijection $A \to C$).
- If $y \in (A \cup B)$, then $R(x, y)$ means y is one of the two projections of x in $A \times B$ (denoted pr_1 or pr_2 in fig.3) described by $\Psi_2 \wedge \Psi_3$.
- If $y \in (U_i \cup V_i)$ for a certain i, then $R(x, y)$ means y is one of the two representatives projections of the image of x by f_i in $U_i \times V_i$ (denoted f_i^1 or f_i^2 in fig.3) described by Ψ_4.

Remark Constants $u_1, v_1, \ldots, a, b, c$, are also elements of Dom. Then they are represented in $A \times B$ (arrows pr_1, pr_2 in fig.1) and in $U_i \times V_i$ (arrows f_i^j in fig.1). Let us consider u_1. We can easily make a difference between the definition of the subset U_1 (edges of the form $R(., u_1)$) and the representation of u_1 in a subset (edges of the form $R(u_1, .)$). Figure 2 shows, as an example, all edges which are adjacent to the subset C:

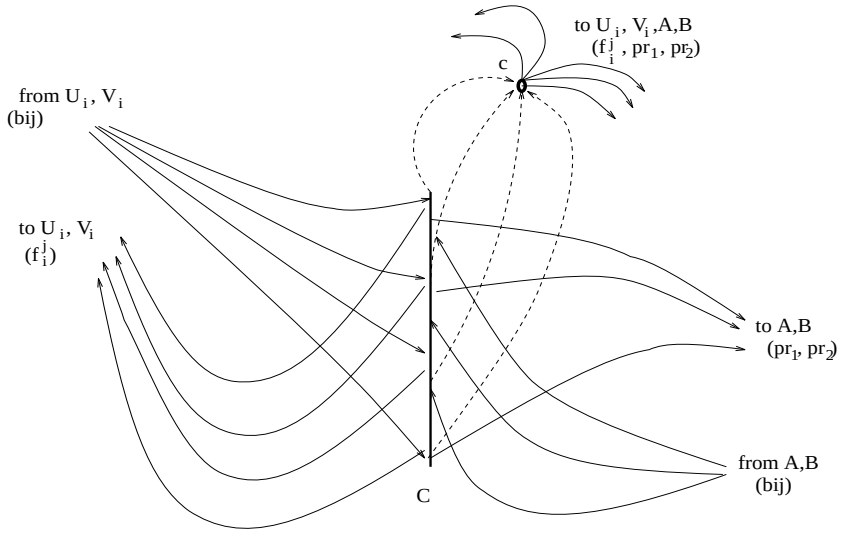

fig.2

Let Rem denote $Dom \backslash \{U_1, V_1, \ldots, A, B, C\}$ (in particular constants $a, b, c, \ldots, u_i,$

v_i are in Rem. Fig.3 describes the unique meaning of each arrow $R(x,y)$ according to the respective sets $(U_1, V_1, \ldots, A, B, C)$ of its endpoints x and y. We will also distinguish the case where y is one of the constants $u_1, v_1, \ldots, a, b, c$.

c							def	
b						def		
a					def			
v_2				def				
u_2			def					
v_1		def						
u_1	def							
C	bij	bij	bij	bij	bij	bij		
B	pr_2	pr_2	pr_2	pr_2	pr_2	pr_2	pr_2	pr_2
A	pr_1	pr_1	pr_1	pr_1	pr_1	pr_1	pr_1	pr_1
V_2	f_2^2	f_2^2	f_2^2	f_2^2	f_2^2	f_2^2	f_2^2	f_2^2
U_2	f_2^1	f_2^1	f_2^1	f_2^1	f_2^1	f_2^1	f_2^1	f_2^1
V_1	f_1^2	f_1^2	f_1^2	f_1^2	f_1^2	f_1^2	f_1^2	f_1^2
U_1	f_1^1	f_1^1	f_1^1	f_1^1	f_1^1	f_1^1	f_1^1	f_1^1
$\uparrow y, x \rightarrow$	U_1	V_1	U_2	V_2	A	B	C	Rem

fig.3

2.1.4 Cardinality conditions

We explain here why we have considered only large enough n.

- Conditions Ψ_1, Ψ_2, Ψ_3 (which express the existence of bijections or injections between some sets) imply $m = |A| = |B| = |C| = |U_i| = |V_i|$ for i=1,...,k and $m^2 \geq |Dom| = n$.
- On the other hand $\Psi_0 \wedge \Delta(u_1, v_1, \ldots, a, b, c)$ implies:
$$m \times (2k+3) + 2k + 3 \leq n$$

For example those inequations are satisfied by $m = \lceil \sqrt{n} \rceil$ for any $n \geq (2k+4)^2$.

2.1.5 Proof of proposition 2.2

Let $\mathcal{G} = \langle Dom, R \rangle$ be a model of Φ'. Then, there are $u_1, v_1, \ldots, a, b, c \in \mathcal{G}$ and a functional structure $\mathcal{F} = \langle Dom, f_1, \ldots, f_k \rangle$ on the same domain such that for $i = 1, \ldots, k$ and $x, y \in Dom$:

$$\mathcal{F} \models f_i(x) = y \iff (\mathcal{G}, u_1, \ldots, b, c) \models (*_i)(x, y) \qquad (*).$$

Clearly each f_i is a well-defined function because $(\mathcal{G}, u_1, \ldots, b, c) \models \Psi$ implies $(\mathcal{G}, u_1, \ldots, b, c) \models \forall x\ \exists! y\ (*_i)(x, y)$. $\mathcal{F}$ satisfies Φ because $(\mathcal{G}, u_1, \ldots, b, c) \models \Phi^*$ and because of equivalence $(*)$.

Conversely, let $\mathcal{F} = \langle Dom, f_1, \ldots, f_k \rangle$ be a structure of cardinality n such that $n \geq h_k = (2k+4)^2$. Let $red(\mathcal{F}) = \langle Dom, R \rangle$ be its associated digraph. By construction, there are $u_1, v_1, \ldots, a, b, c \in red(\mathcal{F})$ s.t. $(red(\mathcal{F}), u_1, \ldots, b, c) \models \Psi$ and Equivalence $(*)$ holds. So if $\mathcal{F} \models \Phi$ then $red(\mathcal{F}) \models \Phi'$. $\square$

Remark In this proof, only $\mathcal{S}$-structures with large enough domain were considered. This restriction was not essential since a first-order description of "small" models of Φ can be added in conjunction with Φ'.

As an immediate corollary of proposition 2.2, we obtain :

Corollary 2.3 *For all signatures $\mathcal{S}$:*

$$Func_1^{\omega}(\mathcal{S}) \subseteq Deg^{+}(\mathcal{S}) \subseteq BIN(\mathcal{S}).$$

The second inclusion comes from the fact that the property to be a digraph of outdegree bounded by k (for a given k) is easily first-order definable.

2.2 A converse result

The converse part of theorem 2.1 is implied by the proposition below.

Proposition 2.4 *Let $\mathcal{S}$ be any signature. Let Φ be a prenex first-order formula of type $\mathcal{S} \cup \{R\}$ where R is a k-Deg^{+} binary relation symbol. Then, there exists a f.o. formula Φ' of type $\mathcal{S} \cup \{f_0, f_1, \ldots, f_k\}$ where $\{f_0, f_1, \ldots, f_k\}$ is a set of unary function symbols s.t. for all structures $\mathcal{M} = \langle Dom, \mathcal{S} \rangle$*

$$\mathcal{M} \models \exists R \quad \Phi \iff \mathcal{M} \models \exists f_0 \exists f_1 \ldots \exists f_k \quad \Phi'.$$

Proof As for proposition 2.2 we give the proof only for $\mathcal{S} = \emptyset$. We divide it into two parts. Let k be a positive integer.

- Assume Φ is a first-order sentence of type $\{R\}$. Let us exhibit a first-order sentence Φ' of type $\{R', Z\}$, where Z is a unary predicate symbol, such that for every positive integer n:

there exists $\mathcal{G} = \langle Dom, R \rangle$ of cardinality n which satisfies Φ
and $\mathcal{G}$'s outdegree is bounded by k (may be 0,1,..., k)
iff

there exists $\mathcal{G}' = \langle Dom, R', Z\rangle$ of cardinality n which satisfies Φ'
and each vertex of $\mathcal{G}'$ has an outdegree for R' between 1 and k

Intuitively Z is the subset containing all the elements x of Dom of outdegree zero. We replace each atomic subformula of φ of the form $R(x,y)$ with $R'(x,y) \wedge \neg Z(x)$. Φ' is the conjunction of the resulting formula and of the following

$$\exists\gamma\forall x \quad (Z(x) \rightarrow R'(x,\gamma)).$$

Let $\mathcal{G} \models \Phi$, we build $\mathcal{G}'$ to be a model of Φ' as follows: edges of R' are given by those of R together with edges (x,γ) where x is of outdegree 0 (for R) and γ is some fixed element. Conversely, if $\mathcal{G}' \models \Phi'$, then the structure $\mathcal{G}$ such that "$R(a,b)$ holds iff $R'(a,b) \wedge \neg Z(a)$" is a model of Φ (by construction of φ') and if $\mathcal{G}'$ has an outdegree bounded by k then so has $\mathcal{G}$.

- From now on we transform R' and Z into unary functions. We only have to replace in Φ' each sub-formula of the form $R'(x,y)$ with $f_1(x) = y \vee \ldots \vee f_k(x) = y$ where the f_is' are new unary function symbols and to replace each subformula $Z(x)$ by the formula $f_0(x) = z$ where f_0 is a unary function and z is a new variable. We denote $\Phi''(z)$ the resulting formula.

The idea is to "label" the (at most) k edges $R'(x,y_1), R'(x,y_2), \ldots, R'(x,y_k)$ starting from any x by respective arrows $f_1 : x \mapsto y_1, \ldots, f_k : x \mapsto y_k$. The reader should be easily convinced that the following equivalence holds for $|Dom| \geq 2$:

there exists $\mathcal{G}' = \langle Dom, R', Z\rangle$ which satisfies Φ' and where
each vertex has an outdegree (for R') between 1 and k
iff
there exists $\mathcal{F} = \langle Dom, f_0, f_1, \ldots, f_k\rangle$ (on the same domain)
which satisfies $\exists z \Phi''(z)$

□

We obtain as an easy consequence of proposition 2.4:

Corollary 2.5 *For every signature $\mathcal{S}$:*

$$Deg^+(\mathcal{S}) \subseteq Func_1^\omega(\mathcal{S}).$$

Obviously, corollaries 2.3 and 2.5 imply theorem 2.1.

Concerning first-order or existential second-order definability some corollaries can be derived. Let S be a set of integers and let $Func_d^\omega(d\forall)$ be the class of spectra of first-order formula of signature containing at most d-ary function symbols and d universal f.o. variables. Grandjean has proved (see [Gra85]):

$$S \in NRAM(n^d) \iff S \in Func_d^\omega(d\forall)$$

where $d \geq 1$ and n is the input integer. Then,

$$NRAM(n) = Func_1^{\omega}(1\forall)) \subseteq Deg^{+}(\mathcal{S}) \subseteq BIN.$$

All "natural" sets of integers seem to belong to the very large class $NRAM(n^d)$ (recall n is the input integer). In particular, talking about spectra (i.e. sets of integer), this implies:

Corollary 2.6 *The set of primes and the set of perfect numbers*[1] *are in* BIN.

Notice that this corollary can also be proved using results of Woods [Woo81]. Let P be a k-ary predicate (on integers). We say that P is *rudimentary* if it can be defined by a first-order sentence Φ in a language containing only equality ($x = y$), addition ($x + y = z$) and multiplication ($x \times y = z$) predicates and whose variables are bounded by the variables of P. For example, it is easy to see that the set of primes is a (unary) rudimentary predicate.

In his thesis [Woo81], Woods shows that every rudimentary set of positive integers is the spectrum of a sentence involving only one binary relation symbol (then, of course, corollary 2.6 follows). Let RUD denote the class of rudimentary sets. Our opinion was that the following list of inclusions hold :

$$RUD \subseteq Func_1^{\omega} \subseteq BIN$$

Recently, F.Olive [Oli96] proved the first inclusion.

As a consequence of corollary 2.3 and of a result in [Gra90c] (which says that connectedness and strong connectedness are expressible by sentences with only unary function symbols as extra predicates), we have:

Corollary 2.7 *Connectedness and strong connectedness are expressible by sentences with a single extra binary relation (of outdegree bounded by a given* k*).*

Definability of connectedness by one binary relation can also be found in [Fag93] (and by bijection symbols in [Sch96]). This "contrasts" with results by Fagin in [Fag93], Fagin, Stockmeyer and Vardi in [FSV93], de Rougemont in [dR87] and Schwentick in [Sch94, Sch95] that connectedness is not definable by a monadic second-order sentence even in the presence of an underlying successor relation (or even in the presence of an underlying linear order).

1. a perfect number is a positive integer which is the sum of all its divisors. For example, 6 is a perfect number: $6 = 1 + 2 + 3$.

2.3 d-ary functions vs. one $(d+1)$-ary relation

In this section we prove a generalization of proposition 2.2. More precisely we show that for any positive integer d a single $(d+1)$-ary relation is at least as powerfull as any number of d-ary functions.

In the following, we will consider (d,d)-ary functions that is functions which mapps d-tuples to d-tuples. A d-ary function can easily be seen as a particular case of such functions verifyng:

$$\forall x_1 \ldots \forall x_d \exists y \ f(x_1,\ldots,x_d) = (y,\ldots,y)$$

Proposition 2.8 *Let $\mathcal{S}$ be any signature, d be a positive integer. Let Φ be a prenex first-order formula of type $\mathcal{S} \cup \{f_1,\ldots,f_k\}$ where $\{f_1,\ldots,f_k\}$ is a set of (d,d)-ary function symbols. Then, there exists a f.o. formula Φ' of type $\mathcal{S} \cup \{R\}$ where R is a $(d+1)$-ary relation symbol s.t. for all structures $\mathcal{M} = \langle Dom, \mathcal{S}\rangle$*

$$\mathcal{M} \models \exists f_1 \ldots \exists f_k \ \ \Phi \iff \mathcal{M} \models \exists R \ \ \Phi'.$$

Proof. Proof of this proposition mimics those of prop. 2.2. So, we just sketch how to construct a mapping *red* from functional structures $\langle Dom, f_1,\ldots,f_k\rangle$ to relational ones of the form $\langle Dom, R\rangle$. Formulas are left to the reader.

Let $u_i^j, v_i^j, a^j, b^j, c^j$ $(1 \le i \le k,\ 1 \le i \le d)$ be $(2k+3)d$ distinct elements of Dom. We use it to define $(2k+3)d$ subsets $U_i^j, V_i^j, A^j, B^j, C^j$ subsets of the domain in the following way (e.g. for A^1)

$$\text{for all } x \in Dom \backslash \{u_1^1,\ldots,c^d\},\ x \in A^1 \iff R(x,x,\ldots,x,a^1)$$

As in the proof of proposition 2.2 we suppose that these above-defined subsets are pairwise disjoint.

The cartesian product $U_i^1 \times U_i^2 \times \ldots \times U_i^d$ is denoted by $\overline{U_i}$ (similarly $\overline{V_i}$, $\overline{A}$, $\overline{B}$ and $\overline{C}$ are introduced as notations).

1. Dom is represented in $\overline{A} \times \overline{B}$ by associating injectively by R a pair of d-tuples $(\overline{a_y}, \overline{b_y}) = (a_y^1,\ldots,a_y^d,b_y^1,\ldots,b_y^d)$ of $\overline{A} \times \overline{B}$ to each d-tuples $\overline{y}$ in the following way:

   $$R(\overline{y},a_y^1),\ldots,R(\overline{y},a_y^d),R(\overline{y},b_y^1),\ldots,R(\overline{y},b_y^d)$$

   Here injective means that for two distincts tuples cannot be associated to the same pair.

2. Bijections from each product $\overline{U_1}, \overline{V_1}, \ldots, \overline{A}, \overline{B}$ to $\overline{C}$ are defined. The one-one correspondance between tuples $\overline{a'} = (a'^1, \ldots, a'^d)$ in, say, $\overline{A}$ and tuples $\overline{c'} = (c'^1, \ldots, c'^d)$ of $\overline{C}$ is made by:

$$R(\overline{a'}, c'^1), \ldots, R(\overline{a'}, c'^d)$$

Now, let $\overline{x}, \overline{y}$ be two tuples verifying $f_i(\overline{x}) = \overline{y}$ for a given i. This is encoded as follows in our new structure: we read the representation $(\overline{a_y}, \overline{b_y})$ of $\overline{y}$ in $\overline{A} \times \overline{B}$. Because of the bijections, a unique pair $(\overline{u_{i,y}}, \overline{v_{i,y}})$ in $\overline{U_i} \times \overline{V_i}$ corresponds to $(\overline{a_y}, \overline{b_y})$. Then, we just have to associate $\overline{x}$ with $(\overline{u_{i,y}}, \overline{v_{i,y}})$ by creating:

$$R(\overline{x}, u^1_{i,y}), \ldots, R(\overline{x}, u^d_{i,y}), R(\overline{x}, v^1_{i,y}), \ldots, R(\overline{x}, v^d_{i,y}).$$

The rest of the proof (in particular arguments to show that the construction is "unambiguous") is similar to the proof of prop. 2.2. □.

2.4 Polynomial transformations of spectra

This last section is devoted to the study of the image by polynomials of $\mathbb{Q}[X]$ of certain classes of spectra. In particular, we will give a positive answer to the following question due to M. More [Mor94a, Mor94b]: *let $P(X) \in \mathbb{Q}[X]$ be asymptotically greater than X^2 and let $R_1, R_2, \ldots, R_h$ be binary relation symbols. Is the image by $P(X)$ of the class of spectra of first-order formulas of type $\{R_1, R_2, \ldots, R_h\}$ included in the class of spectra of first-order formulas with only one binary relation symbol (i.e. in BIN)?*

Our aim is to prove the more general following proposition (obviously, with the notations stated in the intoduction $Rel^\omega_2 \subseteq Func^\omega_2$) which improves previous results in [Fag75b, Mor94a, Mor94b]:

Proposition 2.9 *Let $P(X) \in \mathbb{Q}[X]$ of degree $m \geq k$ and with a strictly positive dominating coefficient. Then,*

$$S \in Func^\omega_k \Rightarrow \lceil P(S) \rceil = \{\lceil P(n) \rceil,\ n \in S\} \in Func^\omega_1$$

From this proposition and corollary 2.3, it will follow immediately:

Corollary 2.10 *Let k be a positive integer. Let $P(X) \in \mathbb{Q}[X]$ of degree $m \geq k$ and with a strictly positive dominating coefficient. then,*

$$S \in Func^\omega_k \Rightarrow \lceil P(S) \rceil \in BIN$$

Remark. Malika More's conjecture is obtained (in a stronger form) for $k = 2$.

In order to proceed, we will divide our proof into several easy lemmas.

Lemma 2.11 *If $S \in Func^\omega_k$ for a positive integer k, then $S^k = \{n^k,\ n \in S\} \in Func^\omega_1$.*

Proof The idea is very simple. Each element z of the new domain of size n^k will be represented bijectively by a tuple $(x_1, x_2, \ldots, x_k)$ of elements of a subset X of size n. Suppose we have a k-ary function f. In order to encode $f(x_1, x_2, \ldots, x_k) = y$ ($x_i \in X$ for $i = 1, \ldots, k$), we introduce $k+1$ new unary function symbols $p_1, p_2, \ldots, p_k$ (the projections of the above-mentioned bijection) and f_1 (which intuitively represents f) such that there exists z, s.t.

$$\bigwedge_{i=1}^{k} p_i(z) = x_i \wedge f_1(z) = y \qquad \text{holds.}$$

More precisely, let φ be a first-order formula of type containing only k-ary function symbols: $f^1, f^2, \ldots, f^h$. Let $\mathcal{T}$ be a type consisting only in:

- $k + h$ unary function symbols $p_1, p_2, \ldots, p_k, f_1^1, f_1^2, \ldots, f_1^h$,
- one unary relation symbol X.

We write now two formulas Ψ and φ^{Δ} of type $\mathcal{T}$.

$$\Psi : \forall z \quad \bigwedge_{i=1}^{k} X(p_i(z)) \wedge$$

$$\forall z \forall z' \quad [(\bigwedge_{i=1}^{k} p_i(z) = p_i(z')) \rightarrow z = z'] \wedge$$

$$(\forall x_1 X(x_1))(\forall x_2 X(x_2)) \ldots (\forall x_k X(x_k)) \exists z'' \quad \bigwedge_{i=1}^{k} p_i(z'') = x_i$$

φ^{Δ} is obtained from φ by replacing each $\exists x$ with $(\exists x X(x))$, each $\forall x$ with $(\forall x X(x))$ and each occurence of $f^j(x_1, x_2, \ldots, x_k) = y$ with $\exists z \bigwedge_{i=1}^{k} p_i(z) = x_i \wedge f_1^j(z) = y$.

Then, clearly, $Sp(\varphi)^k = Sp(\Psi \wedge \varphi^{\Delta})$. $\square$

We will now state and prove a claim which will be very useful in the following.

Claim 1 *Let $b \in \mathbb{Z}$. Let X, U, V be three unary predicate symbols and f_U, g_X be two unary function symbols. There exists a first-order formula φ of type $\mathcal{T} = \{X, U, V, f_U, g_X\}$ such that, for all structures $\mathcal{F}_1$:*

$$\mathcal{F}_1 = \langle Dom_1, \mathcal{T}^{\mathcal{F}_1} \rangle \models \varphi \Rightarrow \begin{cases} |V^{\mathcal{F}_1}| = |U^{\mathcal{F}_1}| \times |X^{\mathcal{F}_1}| + b, & \text{if } b \geq 0 \\ |U^{\mathcal{F}_1}| > 0, \ |X^{\mathcal{F}_1}| \geq |b|, & \text{if } b < 0 \end{cases}$$

where, e.g, $U^{\mathcal{F}_1}$ denotes the interpretation of U in $\mathcal{F}_1$.

Proof of the Claim Let f_U, g_X be two unary function symbols.

- First we consider the case $b \geq 0$. φ asserts: *there exist b elements $v_1, v_2, \ldots, v_b$ such that,*

$$(f_U, g_X)\colon V \backslash \{v_1, v_2, \ldots, v_b\} \longrightarrow U \times X$$

is a bijection.

$$\varphi:\ (\exists v_1 V(v_1))\ldots(\exists v_b V(v_b)) \quad \bigwedge_{1\le i<j\le b} v_i \neq v_j \wedge$$
$$(\forall v(V(v) \wedge \bigwedge_{1\le i\le b} v \neq v_j)) \quad U(f_U(v)) \wedge X(g_X(v)) \wedge$$
$$(\forall v'(V(v') \wedge \bigwedge_{1\le i\le b} v' \neq v_j \wedge v' \neq v)) \quad \neg[f_U(v') = f_U(v) \wedge g_X(v') = g_X(v)] \wedge$$
$$(\forall x X(x))(\forall u U(u))(\exists v''(V(v'') \wedge \bigwedge_{i=1}^{b} v'' \neq v_i) \quad f_U(v'') = u \wedge g_X(v'') = x$$

- Now, if $b < 0$, then φ states: *there exist* $|b|$ *pairs* (u_1, x_1), (u_1, x_2), ..., $(u_1, x_{|b|})$ *of* $U \times X$ *such that,*

$$(f_U, g_X)\colon V \longrightarrow (U \times X)\backslash\{(u_1, x_1), (u_1, x_2), \ldots, (u_1, x_{|b|})\}$$

is a bijection

$$\varphi:\ (\exists u_1 U(u_1))(\exists x_1 X(x_1))\ldots(\exists x_{|b|} X(x_{|b|})) \quad \bigwedge_{1\le i<j\le |b|} x_i \neq x_j \wedge$$
$$(\forall v V(v)) \quad U(f_U(v)) \wedge X(g_X(v)) \wedge$$
$$\neg(f_U(v) = u_1 \wedge g_X(v) = x_1) \wedge \ldots \wedge \neg(f_U(v) = u_1 \wedge g_X(v) = x_{|b|}) \wedge$$
$$(\forall v'(V(v') \wedge v' \neq v)) \quad \neg[f_U(v') = f_U(v) \wedge g_X(v') = g_X(v)] \wedge$$
$$(\forall x X(x))(\forall u U(u)) \quad (u = u_1 \wedge \bigvee_{i=1}^{b} x = x_i) \vee (\exists v''\ V(v'') \wedge f_U(v'') = u \wedge g_X(v'') = x) \qquad \square$$

Lemma 2.12 *Let* $P(X) = a_m X^m + a_{m-1} X^{m-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ *with* $m \geq k$ *and* $a_m \geq 2$. *Then,*

$$S \in Func_k^\omega \Rightarrow P(S) \in Func_1^\omega.$$

Proof We denote by φ a first-order sentence of type $\{f^1, f^2, \ldots, f^h\}$ where $f^1, f^2, \ldots, f^h$ are k-ary function symbols. As usual, we will give a sentence φ' of unary type such that:

φ has a model $\mathcal{F}_k = \langle Dom_k, f^1, f^2, \ldots, f^h\rangle$
iff
φ' has a model $\mathcal{F}_1$ of unary type and of domain Dom_1
with $|Dom_1| = P(|Dom_k|)$.

First, we show how to force the cardinality of the new structure to be $P(n)$ where n is the original size of the domain.

$$\begin{aligned} P(X) =& a_m X^m + a_{m-1}X^{m-1} + \cdots + a_1 X + a_0 \qquad a_m \geq 2 \\ =& a_0 + X(a_1 + X(\cdots + X(a_{m-1} + a_m X))\cdots) \end{aligned}$$

We introduce $m+1$ new unary relation symbols $X, U_0, \ldots, U_{m-1}$. According to the *Claim*, we can express the following conditions by a formula using only unary function symbols:

$$\begin{cases} |U_0| = a_m > 1 \\ |U_1| = a_{m-1} + |U_0| \times |X| \\ \vdots \\ |U_{m-1}| = a_1 + |U_{m-2}| \times |X| \\ |Dom_1| = a_0 + |U_{m-1}| \times |X| \end{cases}$$

Let Φ be such a formula. It is easily shown that:

$$1 < |U_0| \leq |U_1| \leq \ldots \leq |U_{m-1}| \leq |Dom_1|,$$

for $|X| \geq max(|a_i|,\ a_i < 0)$

Now, notice that $P(X)$ is asymptotically greater than X^k ($m \geq k$, $a_m \geq 2$). Then, for a sufficiently large n, we can encode each k-ary function on Dom_k by unary functions on a subset V of Dom_1 of size n^k. It is described by the following Ψ and φ^Δ which are almost the same as those of Lemma 2.11. Again, we introduce $k+h$ new unary function symbols $p_1, \ldots, p_k, f_1^1, \ldots, f_1^h$ and one unary relation symbol X.

$$\Psi : \ (\forall v V(v)) \quad \bigwedge_{i=1}^{k} X(p_i(v))$$

$$(\forall v V(v))(\forall v' V(v')) \quad [(\bigwedge_{i=1}^{k} p_i(v) = p_i(v')) \rightarrow v = v'] \wedge$$

$$(\forall x_1 X(x_1))(\forall x_2 X(x_2)) \ldots (\forall x_k X(x_k))(\exists v'' V(v'')) \quad \bigwedge_{i=1}^{k} p_i(v'') = x_i$$

φ^Δ is obtained from φ by replacing each $\exists x$ with $(\exists x X(x))$, each $\forall x$ with $(\forall x X(x))$ and each occurence of $f_k^j(x_1, x_2, \ldots, x_k) = y$ with $(\exists v V(v)) \bigwedge_{i=1}^{k} p_i(v) = x_i \wedge f_1^j(v) = y$.

$\varphi' = \Phi \wedge \Psi \wedge \varphi^\Delta$ is the expected formula.□

Proof of proposition 2.9 Let $P(X) \in \mathbb{Q}[X]$:

$$P(X) = \frac{a_m}{b_m} X^m + \frac{a_{m-1}}{b_{m-1}} X^{m-1} + \cdots + \frac{a_1}{b_1} X + \frac{a_0}{b_0}$$

Where $a_i \in \mathbb{Z}, b_i \in \mathbb{N}$ (for $i = 0, \ldots, m$) and $\frac{a_m}{b_m} > 0$. Let $b = 2lcm(b_0, \ldots, b_m)$, then,

$$bP(X) = \frac{ba_m}{b_m}X^m + \frac{ba_{m-1}}{b_{m-1}}X^{m-1} + \cdots + \frac{ba_1}{b_1}X + \frac{ba_0}{b_0} \in \mathbb{Z}[X]$$

According to Lemma 2.12, if $S \in Func_k^\omega$ then $bP(S) \in Func_1^\omega$ ($m \geq k$ and $\frac{ba_m}{b_m} \geq 2$. Let's denote $A_i = \{\ n :\ bn - i \in bP(S)\}$. The reader should be easily convinced that, for $i = 0, \ldots, b-1$, $bP(S) \in Func_1^\omega$ implies $A_i \in Func_1^\omega$ and because of

$$A_0 \cup A_1 \cup \ldots \cup A_{b-1} = \lceil \frac{1}{b}(bP(S)) \rceil = \lceil P(S) \rceil,$$

we have the expected conclusion:

$$S \in Func_k^\omega \Rightarrow \lceil P(S) \rceil \in Func_1^\omega. \quad \square$$

Remark In the previous lemmas, the use of '$\lceil n \rceil$' is not essential at all. An other kind of approximation like '$\lfloor n \rfloor$' (the last integer before n) may be used too.

Chapitre 3

Unary functions vs. one partial order (and vs. one bipartite graph)

In the previous chapter we have proved that a single binary relation is powerful enough to replace any number of unary function symbols, as second order resources. Our aim here is to strengthen this result by adding semantical restrictions to this binary relation. It turns out that theorem 2.1 still holds if the extra binary relation is taken from the following list of binary predicates:

- Directed relations
  1. a partial order
  2. a directed bipartite relation (see definition below)
- Undirected relations
  1. a symmetric and irreflexive relation
  2. a symmetric and bipartite relation

Moreover in the case when unary functions are bijective a slight modification of the proof of our main result will permit us to show that they can be simulated by a *single* binary relation of bounded degree (i.e. whose indegree and outdegree are bounded by a constant h depending only on the number of bijections).

Definition 3.1 *$G = \langle Dom, R\rangle$ is a directed bipartite graph (Dir–Bip for short) if there are X, Y s.t. X, Y realize a partition of Dom and every edge of G is of the form $R(x, y)$ with $x \in X$ and $y \in Y$ i.e. if R is a partial order of depth 1. Analogously, G is a symmetric bipartite graph (Sym–Bip for short) if its edges are of the form $R(x, y)$ for $x \in X$ and $y \in Y$.*

A binary relation symbol R will be said to be a *Dir–Bip*-symbol (resp. a *Sym–Bip*-symbol) if we impose that all its interpretations are *Dir–Bip* (resp. are *Sym–Bip*).

Notations. In this chapter, $\oplus$ (resp. $\ominus$) will denote the modulo 4 addition (resp. substraction) symbol.

$\overline{U}$ stands for the set of the following $(8k+12)$ unary relation symbols:

$$\begin{array}{l} A_0^0, B_0^0, \ldots, A_t^0, B_t^0, \ldots, A_k^0, B_k^0 \\ A_0^1, B_0^1, \ldots, A_t^1, B_t^1, \ldots, A_k^1, B_k^1 \\ A_0^2, B_0^2, \ldots, A_t^2, B_t^2, \ldots, A_k^2, B_k^2 \\ A_0^3, B_0^3, \ldots, A_t^3, B_t^3, \ldots, A_k^3, B_k^3 \\ H^0, H^1, H^2, H^3 \end{array}$$

The crux for proofs of the results of this chapter is the following proposition:

Proposition 3.2 *Let $\mathcal{S}$ be any signature. Let Φ be a prenex first-order formula of type $\mathcal{S} \cup \{f_1, \ldots, f_k\}$ where $\{f_1, \ldots, f_k\}$ is a set of unary function symbols. Then, there exists a f.o. formula Φ' of type $\mathcal{S} \cup \{R\} \cup \overline{U}$ where R is a Dir–Bip symbol s.t. for all structures $\mathcal{M} = \langle Dom, \mathcal{S} \rangle$*

$$\mathcal{M} \models \exists f_1 \ldots \exists f_k \;\; \Phi \iff \mathcal{M} \models \exists R \; \exists \overline{U} \;\; \Phi'.$$

Note that prop. 3.2 is the wanted result except that we use additional unary relation symbols of $\overline{U}$.

3.1 Proof of proposition 3.2

The proof given here is a little bit more complicated than it should be. Our aim is to anticipate the future improvement of this proposition without the unary predicates of $\overline{U}$. As usual the proof is given only for $\mathcal{S} = \emptyset$

3.1.1 General outline of the proof

We construct three objects:

- a mapping red, which maps every structure $\mathcal{F} = \langle Dom, f_1, f_2, \ldots, f_k \rangle$ to a structure $red(\mathcal{F}) = \langle Dom, R, \overline{U} \rangle$ on the same domain where R is a *Dir–Bip*,
- a first-order formula Ψ over $\{R\} \cup \overline{U}$,
- for every f.o formula Φ over $\{f_1, \ldots, f_k\}$ a f.o formula Φ^* over $\{R\} \cup \overline{U}$ such that:
  1. For all $\mathcal{F}$, $red(\mathcal{F}) \models \Psi$,
  2. If $\mathcal{G} \models \Phi$, for a $\{R\} \cup \overline{U}$-structure $\mathcal{G}$, then there is a structure $\mathcal{F} = \langle Dom, f_1, f_2, \ldots, f_k \rangle$ s.t. $\mathcal{G} = red(\mathcal{F})$
  3. $\mathcal{F} \models \Phi \iff red(\mathcal{F}) \models \Phi^*$

The expected Φ' will be $\Psi \wedge \Phi^*$.

3.1.2 The reduction of the models

Let $\mathcal{F} = \langle Dom, f_1, \ldots, f_k \rangle$ with $|Dom| = n$.
We will construct a structure $\mathcal{G} = \langle Dom, R, \overline{U} \rangle$ which simulates $\mathcal{F}$. The interpretation of each unary relation symbol in $\overline{U}$ is called a *segment*.

Let us recall the contents of $\overline{U}$. The segments of the form H^j are called *head-segments*. We denote by Rem (for *remainder*) the sets of elements of Dom which do not belong to any segments.

According to the superscript of each subset we obtain a partition of Dom into 6 "levels" Dom^i (for $i = 0 \ldots 3$), $Head$ and Rem:

- Dom^i which is the union of $A_0^i, B_0^i, \ldots, A_t^i, B_t^i, \ldots, A_k^i, B_k^i$.
- $Head$ which is the union of H^0, H^1, H^2, H^3.
- Rem.

$R : X \longmapsto Y$ abbreviates the following expression: *the restriction of the binary relation R to $X \times Y$*.

Bijection-edges. The segments will have the same cardinality. To fulfil this condition, we first make bijective the restriction of R between the segments of level i and $H^{i \oplus 1}$ (for $i = 0 \ldots 3$):

For $t = 1, \ldots, k$, $\left\{ \begin{array}{l} R : A_t^0 \longmapsto H^1 \\ R : B_t^0 \longmapsto H^1 \\ R : A_t^2 \longmapsto H^3 \\ R : B_t^2 \longmapsto H^3 \end{array} \right.$ and $\left\{ \begin{array}{l} R : H^0 \longmapsto A_t^3 \\ R : H^0 \longmapsto B_t^3 \\ R : H^2 \longmapsto A_t^1 \\ R : H^2 \longmapsto B_t^1 \end{array} \right.$ are bijective correspondences.

Secondly, we assume that the restriction of R between the segments of $Head$ is bijective i.e.:

$$\left\{ \begin{array}{l} R : H^0 \longmapsto H^1 \\ R : H^2 \longmapsto H^1 \\ R : H^0 \longmapsto H^3 \end{array} \right. \text{ are bijective correspondences.}$$

Finally and for practical reasons, we assume the restriction of R from H^2 to H^3 is a bijective correspondence, defined as follows: $\forall h^2 \in H^2 \; \forall h^3 \in H^3$

$$R(h^2, h^3) \iff \exists h^0 \in H^0 \; \exists h^1 \in H^1 \quad R(h^0, h^1) \wedge R(h^2, h^1) \wedge R(h^0, h^3)$$

All the edges described above are called *bijection-edges* (see fig.1)

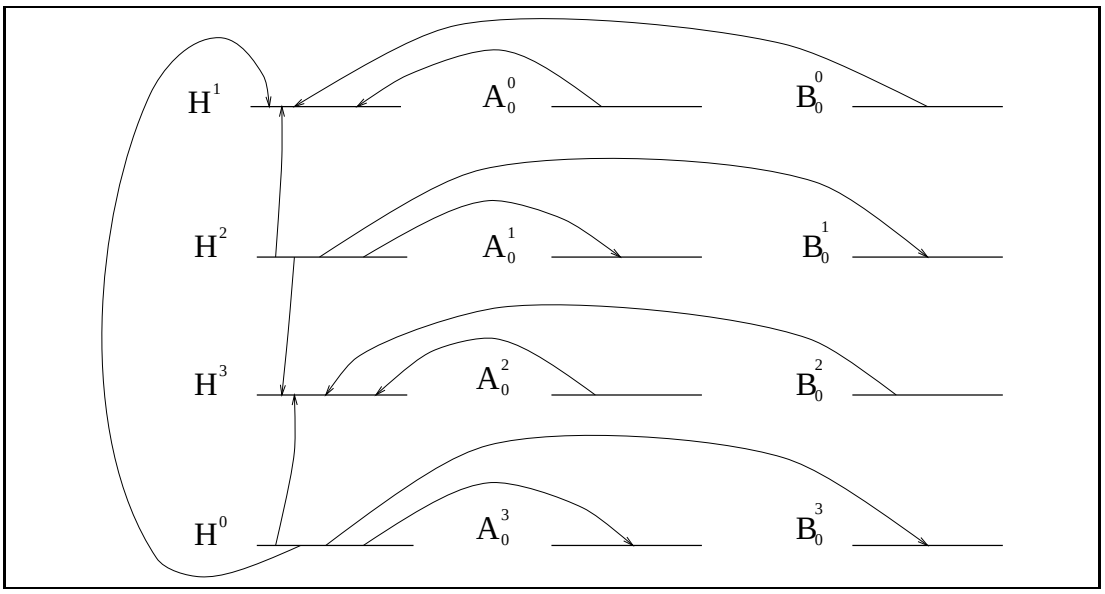

FIG. 3.1 - *some bijection edges*

Two equivalence relations $\sim$ and $\sim_\star$. Using the presence of bijection edges between elements of $Head$, the definition of a (equivalence) relation $\sim$ is given: $\forall i,j \in [0,3], \forall h^i \in H^i, h^j \in H^j$

$$h^i \sim h^j \iff \begin{cases} h^i = h^j \text{ or} \\ R(h^i,h^j) \text{ or} \\ R(h^j,h^i) \text{ or} \\ \exists h^{i\oplus 1} \in H^{i\oplus 1} \begin{cases} R(h^i,h^{i\oplus 1}) \wedge R(h^j,h^{i\oplus 1}) \text{ or} \\ R(h^{i\oplus 1},h^i) \wedge R(h^{i\oplus 1},h^j) \end{cases} \end{cases}$$

Intuitively, two elements h^i, h^j of $Head$ are in the same class for $\sim$ if there exists a "path" (in a generalized sense i.e. without taking care of the orientation of the edges) of bijection-edges containing both h^i and h^j. We remark that there are only 4 elements in each class: one in each H^i (the definition of the restriction of R from H^2 to H^3 is useful here).

Trivially, we extend $\sim$ to pairs as follows:

$$(h_0^i,h_1^i) \sim (h_0^j,h_1^j) \iff h_0^i \sim h_0^j \text{ and } h_1^i \sim h_1^j$$

for any $h_0^i, h_1^i \in H^i$ and $h_0^j, h_1^j \in H^j$.

Relation $\sim_\star$ whose definition follows will concern each element of the $8k+12$ segments (i.e. all the domain except elements of Rem).

For all $i, i' \in [0,3]$. Let $a,b \in A_t^i \times B_t^i; a',b' \in A_t^{i'} \times B_t^{i'}$.

$$(a,b) \sim_\star (a',b') \iff \begin{cases} \exists h_0, h_1 \in H^i \; \exists h'_0, h'_1 \in H^{i'} \quad (h_0,h_1) \sim (h'_0,h'_1) \\ and \begin{cases} R(a,h_0) \wedge R(b,h_1) \wedge R(a',h'_0) \wedge R(b',h'_1) \; or \\ R(a,h_0) \wedge R(b,h_1) \wedge R(h'_0,a') \wedge R(h'_1,b') \; or \\ R(h_0,a) \wedge R(h_1,b) \wedge R(a',h'_0) \wedge R(b',h'_1) \; or \\ R(h_0,a) \wedge R(h_1,b) \wedge R(h'_0,a') \wedge R(h'_1,b') \; or \end{cases} \end{cases}$$

As before, two pairs (a,b) and (a',b') are in the same class for $\sim_\star$ if we can join a to a' and b to b' by two "paths" of bijection-edges. It is also easily seen that each class contains exactly $4(k+1)$ pairs: one for each product $A_t^i \times B_t^i$.

Remark 1 At this step, each edge is of the form $R(x,y)$ where:

$$x \in X = Dom^0 \cup Dom^2 \cup H^0 \cup H^2 \cup Rem$$
$$y \in Y = Dom^1 \cup Dom^3 \cup H^1 \cup H^3$$

i.e. R is well a directed bipartite graph.

Representation edges. In the following, the reason for introducing segments will appear clearly. According to the subscript of the notation of the segments, we define (for each $t \leq k$):

$$Dom_t = (A_t^0 \times B_t^0) \cup (A_t^1 \times B_t^1) \cup (A_t^2 \times B_t^2) \cup (A_t^3 \times B_t^3)$$

Dom_0 is used to represent explicitely the domain Dom. To each element $x \in Dom$ is "associated" injectively a pair $rep(x) = (a,b)$ in Dom_0, by this way:

- If $x \in Dom^0 \cup H^0 \cup Rem$ then $R(x,a)$ and $R(x,b)$ hold for exactly one pair $(a,b) \in A_0^1 \times B_0^1$
- If $x \in Dom^1 \cup H^1$ then $R(a,x)$ and $R(b,x)$ hold for exactly one pair $(a,b) \in A_0^2 \times B_0^2$
- If $x \in Dom^2 \cup H^2$ then $R(x,a)$ and $R(x,b)$ hold for exactly one pair $(a,b) \in A_0^3 \times B_0^3$
- If $x \in Dom^3 \cup H^3$ then $R(a,x)$ and $R(b,x)$ hold for exactly one pair $(a,b) \in A_0^0 \times B_0^0$

The general scheme is the following:

• If $x \in Dom^i \cup H^i$ ($\cup Rem$ when $i = 0$) then we have $R(x,a)$ and $R(x,b)$ if $i = 0,2$ or $R(a,x)$ and $R(b,x)$ if $i = 1,3$ with $(a,b) \in A_0^{i \oplus 1} \times B_0^{i \oplus 1}$

Such edges described above are called *representation-edges*. The representation is injective means (intuitively) that: for two distinct elements x and y of Dom and their respective representative (a_x,b_x) and (a_y,b_y) of Dom_0, $(a_x,b_x) \not\sim_\star (a_y,b_y)$.

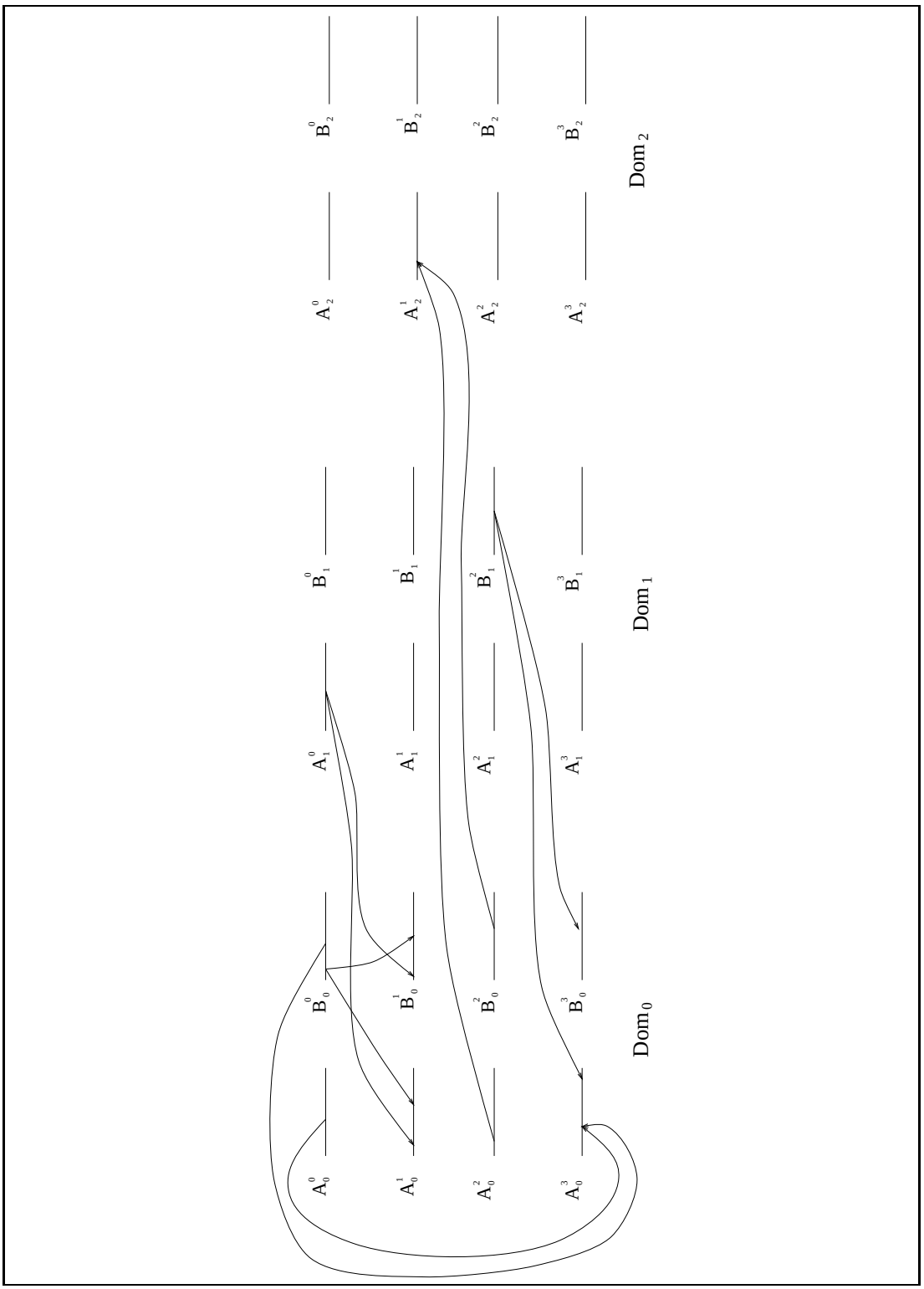

FIG. 3.2 - *some representation edges from Dom_0, Dom_1, Dom_2 to Dom_0 (head-segments are omitted)*

Remark 2 Intuitively each product $A_0^i \times B_0^i$ (for $i = 0, .., 3$) can be seen as a *copy* of the whole domain Dom. Let x be an element and (a_x, b_x) be its representative in some $A_0^i \times B_0^i$. By relation $\sim_\star$ we know that (a_x, b_x) is equivalent to three other pairs of Dom_0. Then these pairs will also be considered implicitely as representatives for x.

The condition of injectivity implies that Dom could be represented in each product $A_t^i \times B_t^i$ and then each subset is of size at least $\lceil\sqrt{n}\rceil$ where $n = |Dom|$.

At this step of the simulation, *Remark 1* is still true. It is also easy to see that there is no possible confusion between representation and bijection edges i.e. no edge is used both as a representation-edge and as a bijection-edge (see subsection 3.1.3 for more details).

Avoided pairs. The purpose of this paragraph is to $(k+1)(8k+12)$ distinct pairs $(\alpha_0[1], \beta_0[1]), (\alpha_0[2], \beta_0[2]) \ldots, (\alpha_k[8k+12], \beta_k[8k+12])$ verifying:

1. $\forall i \in [1..8k+12], \forall t \in [0..k], \quad (\alpha_t[i], \beta_t[i]) \in A_t^0 \times B_t^0$
2. $\forall i < j \in [1..8k+12], \quad (\alpha_0[i], \beta_0[i]) \neq (\alpha_0[j], \beta_0[j])$
3. for all $x \in Dom$, $rep(x) \not\sim_\star (\alpha, \beta)$ with $(\alpha, \beta) \in \{(\alpha_0[1], \beta_0[1]), \ldots, (\alpha_0[8k+12], \beta_0[8k+12])\}$.

Although unnecessary here, this restriction will be useful later for the elimination of unary predicates.

Function edges. Last, we have to encode the functions f_t of $\mathcal{F}$. The method is quite the same as those we employ to represent Dom on Dom_0 (except that now each Dom_t will serve). Suppose we have in $\mathcal{F}$, $f_t(x) = y$ with $x \in Dom^i \cup H^i$ ($\cup Rem$ if $i = 0$), $y \in Dom^j \cup H^j$ ($\cup Rem$ if $j = 0$) for $i, j \in [0, 3]$. First, we read the representation of y, $rep(y) = (a_0^{j\oplus 1}, b_0^{j\oplus 1}) \in A_0^{j\oplus 1} \times B_0^{j\oplus 1}$. Then, we find the only pair $(a_t^{i\oplus 1}, b_t^{i\oplus 1})$ of $A_t^{i\oplus 1} \times B_t^{i\oplus 1}$ such that:

$$(a_0^{j\oplus 1}, b_0^{j\oplus 1}) \sim_\star (a_t^{i\oplus 1}, b_t^{i\oplus 1})$$

Finally, we construct:

$$R(x, a_t^{i\oplus 1}) \wedge R(x, b_t^{i\oplus 1}) \text{ if } i = 0, 2$$
$$R(a_t^{i\oplus 1}, x) \wedge R(b_t^{i\oplus 1}, x) \text{ if } i = 1, 3$$

Above created edges are called *function-edges*. The pair $(a_t^{i\oplus 1}, b_t^{i\oplus 1})$ is called the f_t-*representative* of x. Recalling the definition of the so-called representation edges, they can be seen as function-edges for a very special function: the identity.

Remark 3 Clearly, two elements x_1, x_2 verifying $f_t(x_1) = f_t(x_2) = y$ will have equivalent (for $\sim_\star$) f_t-representatives.

Figure 3.3 below gives some general overview of the encoding of $f_t(x) = y$ in our construction. Figure 3.4 gives a particular example for $x \in A_1^2$ and $y \in A_1^1$.

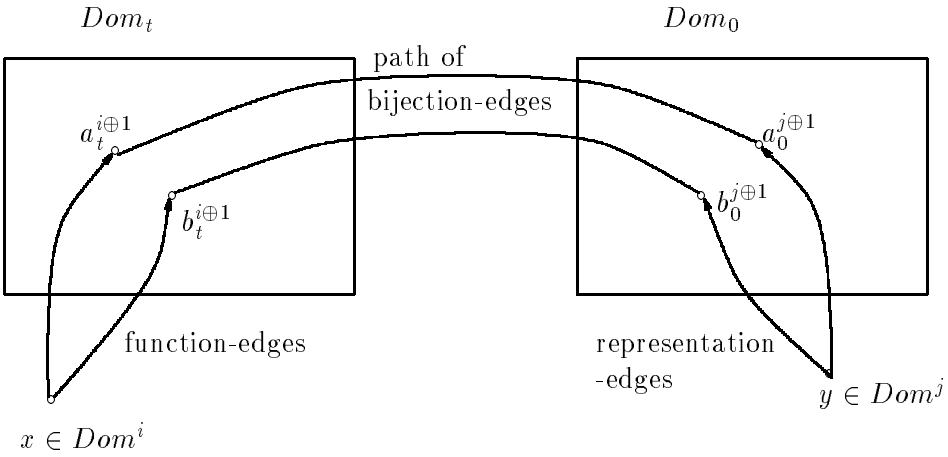

FIG. 3.3 - *encoding* $f_t(x) = y$

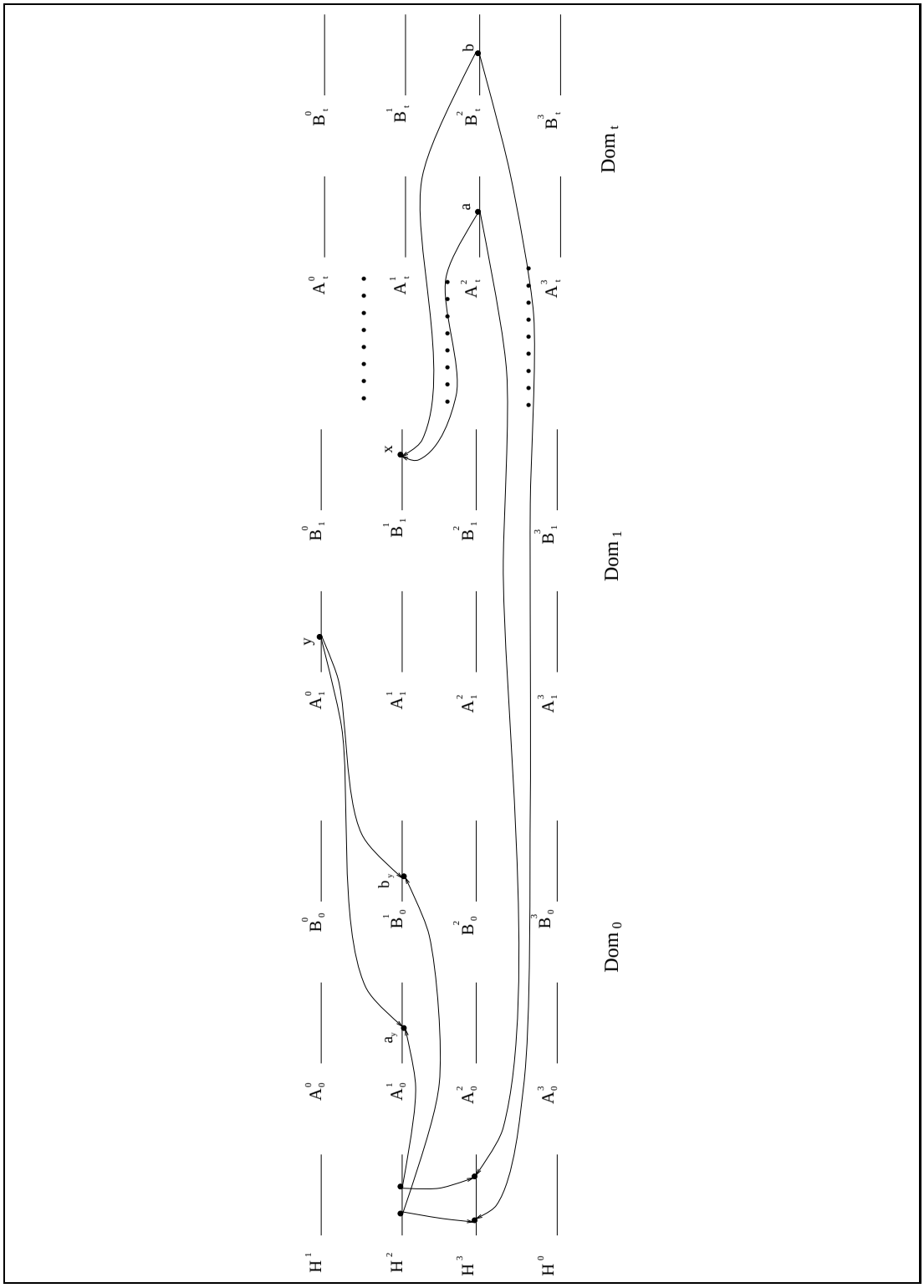

FIG. 3.4 - $f_t(x) = y$ *with* $x \in B_1^1$ *and* $y \in A_1^0$ *(*Dom_2*,... are omitted)*

3.1.3 Unambiguity of the construction

The purpose of this paragraph is to show that the construction we have made is unambiguous i.e taking an arbitrary edge in $red(\mathcal{F})$ it can be viewed only as *bijection-edge, representation-edge* or *function-edge*.

Let x belong to A^i_j for some i, j. Then

- x is represented on $A_0^{i\oplus 1} \times B_0^{i\oplus 1}$ (edges Id in the array below: recall that representation edges can also be viewed as function edges for the function Id).
- For every $t \leq k$, x has its f_t-representative in $A_t^{i\oplus 1} \times B_t^{i\oplus 1}$ (edges f_t below).
- x can be the first coordinate of the f_j-representative of some element in $A_j^{i\ominus 1}$ or $B_j^{i\ominus 1}$ (edges f_j–rep below).
- There is a bijection edge between x and some element in $H^{i\oplus 1}$.

$\downarrow x, y \rightarrow$	$A_0^{i\oplus 1}$	$B_0^{i\oplus 1}$	$A_t^{i\oplus 1}$	$B_t^{i\oplus 1}$	$A_j^{i\ominus 1}$	$B_j^{i\ominus 1}$	$H^{i\oplus 1}$
A^i_j	Id	Id	f_t	f_t	f_j–rep	f_j–rep	bij
B^i_j	Id	Id	f_t	f_t	f_j–rep	f_j–rep	bij

FIG. 3.5 - *Classification of edges*

3.1.4 The reduction of the formulas

Let's define some abbreviations

$Dom^i(x)$: $A^i_0(x) \vee B^i_0(x) \vee \ldots \vee A^i_t(x) \vee B^i_t(x) \vee \ldots \vee A^i_k(x) \vee B^i_k(x)$

$Head(x)$: $H^0(x) \vee H^1(x) \vee H^2(x) \vee H^3(x)$

$Rem(x)$: $\neg Dom^0(x) \wedge \neg Dom^1(x) \wedge \neg Dom^2(x) \wedge \neg Dom^3(x) \wedge \neg Head(x)$

The formula below asserts that all the subsets are pairwise disjoint:

$$PARTITION : \forall x \bigwedge_{X \neq Y \in \overline{U}} \neg(X(x) \wedge Y(x))$$

Bijection edges.

Let $Bijection(X,Y)$, where X and Y are unary relation symbols, abbreviate

$$[(\forall x\ X(x))\ (\exists! y\ Y(y))\ R(x,y)] \wedge [(\forall y\ Y(y))\ (\exists! x\ X(x))\ R(x,y)]$$

$BIJECT-EDGE$ is the conjunction of the following formulas:

$$\bigwedge_{t=1}^{k}\ [\bigwedge_{i=0,2} Bijection(A_t^i, H^{i\oplus 1}) \wedge Bijection(B_t^i, H^{i\oplus 1}) \wedge \bigwedge_{i=1,3} Bijection(H^{i\oplus 1}, A_t^i) \wedge Bijection(H^{i\oplus 1}, B_t^i)]$$

$$Bijection(H^0,H^1) \wedge Bijection(H^2,H^1) \wedge Bijection(H^0,H^3) \wedge$$

$$(\forall h^2 H^2(h^2))(\forall h^3 H^3(h^3))\quad [R(h^2,h^3) \iff (\exists h^1 H^1(h^1))\ (\exists h^0 H^0(h^0))\ R(h^0,h^1) \wedge R(h^2,h^1) \wedge R(h^0,h^3)]$$

From now on, recalling the definition of $\sim$ and $\sim_\star$ we will use directly these symbols in formulas.

Avoided pairs.

For each $t = 0,\ldots,k$, $Avoid_t(x,y)$ abbreviates

$$(x,y) \sim_\star (\alpha_t[1],\beta_t[1]) \vee \ldots \vee (x,y) \sim_\star (\alpha_t[8k+12],\beta_t[8k+12])$$

$AVOID-PAIR$ is the following formula:

$$\exists\alpha_0[1]\exists\beta_0[1]\ldots\exists\alpha_k[8k+12]\exists\beta_k[8k+12]\quad \bigwedge_{t=0}^{k}\bigwedge_{i=1}^{8k+12}(A_t^0,B_t^0)(\alpha_t[i],\beta_t[i]) \wedge \bigwedge_{i<j\in[1..8k+12]}(\alpha_0[i],\beta_0[i])\ \neq (\alpha_0[j],\beta_0[j])$$

Representation edges.

Formulas asserting the existence of representation edges are given here. Let $Rep(x,a,b)$ stand for

$$\bigvee_{i=0,2}((Dom^i(x) \vee H^i) \wedge R(x,a) \wedge R(x,b) \wedge A_0^{i\oplus 1}(a) \wedge B_0^{i\oplus 1}(b)) \vee \bigvee_{i=1,3}((Dom^i(x) \vee H^i) \wedge R(a,x) \wedge R(b,x) \wedge A_0^{i\oplus 1}(a) \wedge B_0^{i\oplus 1}(b)) \vee (Rem(x) \wedge R(x,a) \wedge R(x,b) \wedge A_0^1(a) \wedge B_0^1(b))$$

$REPRES-EDGE$ is the conjunction of the three formulas below.

$$\forall x \exists!(a,b)\quad \neg Avoid_0(a,b) \wedge Rep(x,a,b)$$

$$\forall x \forall x' \forall(a,b)\forall(a',b')\quad [x \neq x' \wedge Rep(x,a,b) \wedge Rep(x',a',b') \rightarrow (a,b) \not\sim_\star (a',b')]$$

The two first formulas express that Rep is an injection from Dom to $Dom_0 \backslash \{(a,b) : Avoid_0(a,b)\}$. The latest one asserts that the representation pairs of two elements are not equivalent by $\sim_\star$.

Function edges.

Intuitively each Dom_t ($t \in [1..k]$) is used to simulate function f_t. So, to each $x \in Dom$ is associated one pair of Dom_t which corresponds to $f_t(x)$. Let $Func_t(x,a,b)$ abbreviate

$$\begin{array}{l} \bigvee_{i=0,2}((Dom^i(x) \vee H^i) \wedge R(x,a) \wedge R(x,b) \wedge A_t^{i\oplus 1}(a) \wedge B_t^{i\oplus 1}(b)) \vee \\ \bigvee_{i=1,3}((Dom^i(x) \vee H^i) \wedge R(a,x) \wedge R(b,x) \wedge A_t^{i\oplus 1}(a) \wedge B_t^{i\oplus 1}(b)) \vee \\ \qquad (Rem(x) \wedge R(x,a) \wedge R(x,b) \wedge A_t^1(a) \wedge B_t^1(b)) \end{array}$$

$FUNC-EDGE$ is the conjunction for each $t \in [1..k]$ of the following:

$\forall x \exists !(a,b) \quad Func_t(x,a,b)$

The formula Ψ.

The desired formula Ψ is the conjunction of $PARTITION$, $BIJECT-EDGE$, $AVOID-PAIR$, $REPRES-EDGE$ and $FUNC-EDGE$.

The formula Φ^*.

Φ^* is obtained from Φ by replacing each term of the form $f_t(x) = y$ with

$$(*_t)(x,y): \quad \exists a'_y \exists b'_y \exists a_y \exists b_y \; Func_t(x,a'_y,b'_y) \wedge Rep(y,a_y,b_y) \wedge (a'_y,b'_y) \sim_\star (a_y,b_y)$$

Cardinality conditions.

All the subsets $D \in \overline{U}$ have the same size m (because of $PARTITION$ and $BIJECT-EDGES$) where m satisfies:

- $m^2 - (8k+12) \geq n$ where $n = |Dom|$ (to represent each $x \in Dom$ injectively in each $A_0^i \times B_0^i$ where $|A_0^i| = |B_0^i| = m$).
- $(8k+12) \times m \leq n$ (the sum of the cardinalities of the subsets must be lower than the size of the domain)

Those inequations are easily satisfiable by, e.g., $m = \lceil \sqrt{n} \rceil$ if $n \geq (8k+13)^2$.

Proof of proposition 3.2.

Let $\mathcal{G} = \langle Dom, R, \overline{U} \rangle$ be a model of Φ' and let $\mathcal{F} = \langle Dom, f_1, \ldots, f_k \rangle$ be the functional structure on the same domain defined for every $t = 1, ..., k$ and each $x, y \in Dom$ by:

$$\mathcal{F} = \langle Dom, f_1, \ldots, f_k \rangle \models f_t(x) = y \iff \mathcal{G} \models (*_t)(x,y).$$

If $\mathcal{G}$ satisfies Ψ then for each element x there exists exactly one y s.t. $(*_t)(x,y)$ holds in $\mathcal{G}$. Each f_t is clearly a well defined function and $\mathcal{F} \models \Phi$.

Conversely, let $\mathcal{F}$ be a model of Φ (with a sufficiently large domain). Its associated *Dir–Bip* graph $red(\mathcal{F})$ satisfies Ψ by construction and satisfies Φ^* also because of the equivalence

$$\mathcal{F} \models f_t(x) = y \iff red(\mathcal{F}) \models (*_t)(x, y). \quad \square$$

3.2 Elimination of unary predicates

The aim of this section is to strengthen proposition 3.2 in the following way (this time, unary predicates are not allowed):

Proposition 3.3 *Let $\mathcal{S}$ be any signature. Let Φ be a prenex first-order formula of type $\mathcal{S} \cup \{f_1, \ldots, f_k\}$ where $\{f_1, \ldots, f_k\}$ is a set of unary function symbols. Then, there exists a f.o. formula Φ_1 of type $\mathcal{S} \cup \{R\}$ where R is a Dir–Bip symbol s.t. for all structures $\mathcal{M} = \langle Dom, \mathcal{S} \rangle$*

$$\mathcal{M} \models \exists f_1 \ldots \exists f_k \quad \Phi \iff \mathcal{M} \models \exists R \quad \Phi_1.$$

Taking as a starting point the proof of proposition 3.2, a proof of this result is presented. Formulas Ψ and Φ^* are re-used.

3.2.1 Proof of proposition 3.3

The main idea here is to define unary predicates by labelling. In other words, a point x is said to belong to a subset A if and only if it is associated by an edge of R (called a *labelling edge*) to a distinguished point a of Dom. The symbol $\overline{u}$ stands for the following list of $8k + 12$ pairwise distincts elements:

$$\begin{array}{c} a_0^0, b_0^0, \ldots, a_t^0, b_t^0, \ldots, a_k^0, b_k^0 \\ a_0^1, b_0^1, \ldots, a_t^1, b_t^1, \ldots, a_k^1, b_k^1 \\ a_0^2, b_0^2, \ldots, a_t^2, b_t^2, \ldots, a_k^2, b_k^2 \\ a_0^3, b_0^3, \ldots, a_t^3, b_t^3, \ldots, a_k^3, b_k^3 \\ h^0, h^1, h^2, h^3. \end{array}$$

Let $red(\mathcal{F})$ be as in prop. 3.2. We will modify it a little bit. Elements of $\overline{u}$ are chosen in Rem. Now, we introduce new edges between elements of a given segment U of $\overline{U}$ and the corresponding point u of $\overline{u}$. More precisely, for all $t \in [1..k]$ We define:

$$\text{for } i = 0, 2, \quad A_t^i(x) \iff R(x, a_t^i),\ B_t^i(x) \iff R(x, b_t^i),\ H^{i\oplus 1}(x) \iff R(x, h^{i\oplus 1})$$

$$\text{for } i = 1, 3, \quad A_t^i(x) \iff R(a_t^i, x),\ B_t^i(x) \iff R(b_t^i, x),\ H^{i\oplus 1}(x) \iff R(h^{i\oplus 1}, x)$$

Then, the segments are dropped. Such a modification is, in a sense, not sufficient. Elements of $\overline{u}$ are also elements of Dom. Consequently they are preimages and they might be images for each function f_t. But, introducing representation edges and function edges for these labelling points could lead to contradictions. Let's consider the case of a_0^0 as an example. As the other elements of the domain, a_0^0 should admit a representative in Dom_0. Because of the existence of labelling edges from A_0^0 to a_0^0, these representatives could only be chosen in $A_0^2 \times B_0^2$ (taking it in Dom_0 but outside $A_0^2 \times B_0^2$ would contradict the fact that R is Dir–Bip). Now consider a_0^2. For similar reasons a representative of a_0^2 would belong to $A_0^0 \times B_0^0$. This means there would exist at least two elements, one in A_0^0 the other one in A_0^2, related to a_0^0 and b_0^2. Then, there would be no way to distinguish labelling edges and representation edges. Similar problems hold for function edges.

In the proof of proposition 3.2 the existence of $(k+1)(8k+12)$ avoided pairs is assumed. This fact will be useful here: to each element of $\overline{u}$ will correspond $k+1$ avoided pairs, one in each Dom_t. Let $g_0, g_1, \ldots, g_k$ be $k+1$ (meta) bijections which establish correspondences between labelling points and avoided pairs: $\forall t \in [0..k], \forall u \in \overline{u},\ g_t(u) \in Dom_t$. The solution consists in considering $g_0(u)$ as the representative of u and each $g_t(u)$ $(t > 0)$ as the f_t-representative of u.

Let $DISTINCT(\overline{u})$ be the formula expressing that points of $\overline{u}$ are pairwise different.

$REPRES - EDGE_1$ is the conjunction of:

$$(\forall x \notin \overline{u})\exists!(a,b) \quad \neg Avoid_0(a,b) \wedge Rep(x,a,b)$$

$$(\forall x \notin \overline{u})(\forall x' \notin \overline{u})\forall(a,b)\forall(a',b') \quad [\neg Avoid_0(a,b) \wedge \neg Avoid_0(a',b') \wedge x \neq x' \wedge Rep(x,a,b) \wedge Rep(x',a',b') \rightarrow (a,b) \not\sim_\star (a',b')$$

Let Ψ_1 be the conjunction of $DISTINCT(\overline{u})$, $PARTITION$, $BIJECT - EDGE$, $AVOID - PAIR$, $REPRES - EDGE_1$ and $FUNC - EDGE$ (Ψ_1 admits elements of $\overline{u}$ as free variables).
$\Phi_1^*(\overline{u})$ is Φ where each term $f_t(x) = y$ is replaced with the following $(*_t)_1(x,y)$:

$$x, y \notin \overline{u} \rightarrow \exists a_x \exists b_x \exists a_y \exists b_y\ Func_t(x,a_x,b_x) \wedge Rep(y,a_y,b_y) \wedge (a_x,b_x) \sim_\star (a_y,b_y)$$
$$x \notin \overline{u} \wedge y \in \overline{u} \rightarrow \exists a_x \exists b_x\ Func_t(x,a_x,b_x) \wedge (a_x,b_x) \sim_\star g_0(y)$$
$$x \in \overline{u} \wedge y \notin \overline{u} \rightarrow \exists a_y \exists b_y\ Rep(y,a_y,b_y) \wedge (a_y,b_y) \sim_\star g_t(x)$$
$$x, y \in \overline{u} \rightarrow g_0(y) \sim_\star g_t(x)$$

The expected Φ_1 is $\exists \overline{u}\ \Phi_1^* \wedge \Psi_1$. $\square$

3.3 Bijections vs. one degree bounded binary relation

In what follows, a new method for elimination of unary predicates is given. This method is introduced in order to obtain an interesting corollary: if in the statement of prop. 3.3 interpretations of unary functions are chosen among the more restricted

class of bijections then the resulting relation R can be taken in the class of directed graphs of bounded degree (both in- and outdegree). More precisely, let $Biject^{\omega}$ (resp. $h-DEG^{\pm}$) be the class of all bijections (resp. of all directed graphs of outdegree and indegree bounded by some constant h).

Proposition 3.4 *Let $\mathcal{S}$ be any signature. Let Φ be a prenex first-order formula of type $\mathcal{S} \cup \{f_1, \ldots, f_k\}$ where $\{f_1, \ldots, f_k\}$ is a set of Biject symbols. Then, there exist some integer h and a f.o. formula Φ_2 of type $\mathcal{S} \cup \{R\}$ where R is a $h-DEG^{\pm}$ symbol s.t. for all structures $\mathcal{M} = \langle Dom, \mathcal{S} \rangle$*

$$\mathcal{M} \models \exists f_1 \ldots \exists f_k \quad \Phi \iff \mathcal{M} \models \exists R \quad \Phi_2.$$

The same technique as in proposition 3.2 is also used here.

3.3.1 Proof of proposition 3.4

The resulting relation R of proposition 3.2 is $Dir{-}Bip$ and has, of course, no cycle at all. The idea is then to define subsets of the domain by creating cycles of some length (for R). More precisely, a point x of Dom will be said to belong to a subset A if and only if x is on a cycle of a given length a. Let $g : \overline{U} \mapsto [1..8k+12]$ be a bijection which associates a number less or equal to $8k+12$ to each symbol of $\overline{U}$. For all $D \in \overline{U}$, $D(x)$ abbreviates

$$\exists d_2 \exists d_3 \ldots \exists d_{g(D)} \bigwedge_{i<j} d_i \neq d_j \wedge R(x, d_2) \wedge R(d_2, d_3) \wedge \ldots \wedge R(d_{g(D)}, x).$$

The rest of the proof is similar to the proof of prop. 3.2. Of course, the notion of avoided pair is of no use here and $REPRES-EDGE$ must be rephrased as the conjunction of:

$$\forall x \exists !(a,b) \quad Rep(x,a,b)$$

$$\forall x \forall x' \forall (a,b) \forall (a',b') \quad [x \neq x' \wedge Rep(x,a,b) \wedge Rep(x',a',b') \rightarrow (a,b) \not\sim_{\star} (a',b')]$$

The formula Φ_2 is the conjunction of $PARTITION, BIJECT{-}EDGE, REPRES{-}EDGE, FUNC-EDGE$ and formula Φ^* of prop. 3.2.

Remark Here $PARTITION$ asserts that if an element is on a cycle of length, say, 3 then it is not on another cycle of length $1, 2, 4, 5, \ldots, 8k+12$.

The size of each $D \in \overline{U}$ (i.e. the number of elements which belong to a cycle of length $g(D)$) is the same. Then, we must add to the cardinality conditions that $|D|$ is a common multiple of the $8k+12$ first numbers. I.e. $m = |D|$ must satisfy:

1. $m^2 \geq n$

2. $(8k+12) \times m \leq n$

3. $m = common - mult(1, 2, 3, \ldots, 8k+12)$.

Edges defining cycles apart, not every element can have both positive indegree and outdegree. Then, from now on, to investigate the degree of R we will consider it as an undirected relation (to avoid taking care of the orientation of the edges).

Let $deg(x)$ denote the degree of an x of Dom. It is easily seen that bijection-edges induce a maximum degree of $2k+4$ (for elements of $Head$).

Every point admits a representative on Dom_0 and f_t-representative on each Dom_t. Then, similarly the cumulative degree is now in the worst case $4k+6 = 2k+4+2(k+1)$.

Bijections have replaced unary functions in the statement of the proposition. This fact has as a consequence that two distinct elements admit as f_t-representatives (for any t) two non equivalent pairs for $\sim_\star$. Then, function-edges induced an injective mapping from Dom to each Dom_t.

It will be shown now that it is possible to represent Dom (or to choose f_t-representatives for its elements) in such a way that any point on a cycle (i.e. in a subset) appears as (first or second) coordinate of a representative (or f_t-representative) a bounded number of times. Let m satisfy, say, $\lfloor \frac{n}{(8k+13)} \rfloor \leq m \leq \lfloor \frac{n}{(8k+12)} \rfloor$ and the cardinality conditions (such a m exists[1]). Let A, B be two segments satisfying $|A| = |B| = m$. An injective mapping (pr_A, pr_B) from Dom to a product of subsets $A \times B$ can be found with the restriction that any point α of A or β of B verifies:

$$\#\{b : \exists x \ (pr_A, pr_B)(x) = (\alpha, b)\} \leq (8k+14)$$

$$\#\{a : \exists x \ (pr_A, pr_B)(x) = (a, \beta)\} \leq (8k+14)$$

Conclusion: the interpretation of R can be chosen among directed graphs of indegree and outdegree bounded by $h = (8k+14) + 4k + 6 + 2 = 12k + 22$ □

3.4 General results

Theorem 3.5 *For any signature $\mathcal{S}$, the class $Func_1^\omega(\mathcal{S})$ is included in each of the following classes:*

1. $Dir\text{–}Bip(\mathcal{S})$
2. $PartOrd(\mathcal{S})$
3. $Sym\text{–}Bip(\mathcal{S})$

1. If n is sufficiently large, there is at least one common multiple of $1, 2, \ldots, 8k+12$ between $\lfloor \frac{n}{(8k+13)} \rfloor$ and $\lfloor \frac{n}{(8k+12)} \rfloor$. For such a m the two first cardinality conditions are also obviously true.

4. $\neg Refl(\mathcal{S})$

Proof.

1. This is an another formulation of proposition 3.3.
2. A *Dir–Bip* is a partial order of depth one.
3. Let us recall the array of section 3.1.3. It is a matter of fact that in the construction of our mapping *red* the signification of a given edge (bijection-edge or ...) depends on its two endpoints (and not only on one of theim). For example, an edge between an element of B_1^1 and an element of A_t^2 (for a given $t \geq 1$) is always a function-edge. Consequently, orientation of the edges does not help with knowing signification of edges. Then, proposition 3.3 still holds in case R is a *Sym–Bip*-symbol (with the same formula Φ_1 and by considering instead of $red(\mathcal{F})$ its symmetric closure $\overline{red}(\mathcal{F})$).
4. As above. a *Sym–Bip* graph is also irreflexive. □

Let $Deg^{\pm}(\mathcal{S}) = \bigcup_{h \geq 0} h\text{–}Deg^{\pm}(\mathcal{S})$.

Theorem 3.6 *For any* $\mathcal{S}$*, the following equality holds:*

$$Biject^{\omega}(\mathcal{S}) = Deg^{\pm}(\mathcal{S})$$

Proof. The left-to-right inclusion is implied by proposition 3.4. The converse part can be easily proved using a general form of Vizing's theorem [2] ([DLS96, Wil94]).

2. Vizing's Theorem says that edges of an undirected graph of degree d can be colored with at most $d+1$ colours (in such a way that no two adjacent edges have the same colour).

Chapitre 4

One binary relation of bounded outdegree and the power of one universal quantifier

In chapter 2 it was proved that each existential second-order formula Ψ with second order quantifiers ranging over unary function symbols is logically equivalent, on finite structures, to a second-order formula Ψ' with a second order part restricted to a single binary relation symbol of bounded outdegree. Unfortunately, the proof of this result does'nt preserve the first-order prefix of Ψ. The main goal of this chapter is to improve the above mentioned result by showing that, for all integers $d \geq 1$, if Ψ has a first-order quantifier prefix of the form $\exists^*\forall^d\exists^*$, then we can find a formula Ψ' as above with a f-o prefix of the same form as that of Ψ. The converse result was already proved in chapter 2. Consequently, an equality of exprimability classes is obtained.

Let $\mathcal{C}$ be a complexity class, $\mathcal{L}$ a logic. If for every set P decidable in $\mathcal{C}$ there exists a formula φ in $\mathcal{L}$ whose finite models are exactly the elements of P then $\mathcal{C}$ is *characterized* by $\mathcal{L}$. Moreover, if for every formula φ of $\mathcal{L}$ the set of models of φ is decidable in $\mathcal{C}$ then the characterization is said to be *exact*. One of the main application of our result is to provide an *exact* characterization of non deterministic linear time, namely of the class $NLIN$ defined by Grandjean. In fact, it will be shown that $NLIN$ can be seen as the class of model sets of formulas of the form

$$\exists R\ \exists\overline{y}\forall x\exists\overline{z}\varphi(R,\mathcal{S})$$

where R is a bounded outdegree binary relation symbol and $\mathcal{S}$ is a functional signature[1]. This is shown in section 4 where a discussion is also initiated concerning "realistic" models of computations for this complexity class.

In section 3, after giving an other corollary of the main result we focus on decidability problems of the prefixed first-order theory of one bounded outdegree relation.

1. $NLIN$ will deal with functions, instead as word, as inputs

In particular, the undecidability of the satisfiability problem of the first-order theory of formulas with prefix $\exists^*\forall\exists^*$ and signature restricted to one binary relation symbol of outdegree bounded by two is proved. This result contrast with the fact that the following problem (i.e. satisfiability problem for Ackermann formulas) is decidable:

Instance A first-order prenex sentence Φ with $Pre(\Phi) \in P(\exists^*\forall\exists^*)$ and with relational signature

Question Is Φ satisfiable (or finitely satisfiable)?

This also underlines the importance of the "outdegree" condition.

In section 1, most useful definitions and notations are given. Section 2 is devoted to the proof of the main result (its easy reciprocal is also stated).

4.1 Definitions and Notations

A *prefix* is a word in the alphabet $\{\forall, \exists\}$. $\forall^n$ (resp. $\exists^n$) is a word consisting of n occurences of $\forall$ (resp. $\exists$), where n is a natural number. Let w be a word in the alphabet $\{\forall, \exists, \forall^*, \exists^*\}$. Following the notations of [Gur76], the set of prefixes $P(w)$ is:

$$P(\forall^n) = \{\forall^i : \ 0 \leq i \leq n\}, \ P(\forall^*) = \{\forall^i : \ i \geq 0\}$$
$$P(\exists^n) = \{\exists^i : \ 0 \leq i \leq n\}, \ P(\exists^*) = \{\exists^i : \ i \geq 0\}$$
$$P(w_1 w_2) = \{u_1 u_2 : \ u_1 \in P(w_1), \ u_2 \in P(w_2)\}.$$

In this paper, we focus on the prefix $P(\exists^*\forall^d\exists^*) = \{\exists^i\forall^j\exists^k : \ i, j, k \geq 0, j \leq d\}$ and especially the case $d = 1$.

- Let Φ be a first-order sentence in prenex form. Its prefix is denoted $Pre(\Phi)$.
- $R\restriction(A \times B)$ where A, B are subsets of the domain is the set of pairs (a, b) in $(A \times B)$ which satisfy $R(a, b)$. $R\restriction A$ is usually written instead of $R\restriction(A \times A)$.
- Let A be a subset of the domain of a given structure. Then, the cardinality of A is denoted $|A|$.
- $\oplus$ is the symbol of addition modulo 2, ω is the set of integers.

Let $P(w)$ be a set of prefixes and h be a positive integer. We denote

$$BIN(w)(\mathcal{S}) \ \ (\text{resp. } h-Deg^+(w)(\mathcal{S}), \ \text{ resp. } Func_1^{\omega}(w)(\mathcal{S}))$$

the class of generalized spectra of formulas of type $\mathcal{S}$ where the only second-order quantified symbol is a single binary relation symbol (resp. is a $h-Deg^+$ binary relation symbol, resp. are unary function symbols) and whose first-order prefix is in $P(w)$. Finally, let $Deg^+(w)(\mathcal{S}) = \bigcup_{h \geq 0} h-Deg^+(w)(\mathcal{S})$.

4.2 Main result

Théorème 4.1 *For all integers $d \geq 1$, for all signatures $\mathcal{S}$:*

$$Func_1^{\omega}(\exists^*\forall^d\exists^*)(\mathcal{S}) = Deg^+(\exists^*\forall^d\exists^*)(\mathcal{S}).$$

The left to right inclusion of theorem 4.1 is implied by the following result.

Proposition 4.1 *Let $\mathcal{S}$ be a signature and d be a positive integer. Let Ψ be a prenex first-order formula of type $\mathcal{S} \cup \{f_1, \ldots, f_k\}$ with a first-order prefix in $P(\exists^*\forall^d\exists^*)$. Then, there exist two f.o. formulas Ψ' and Φ of type $\mathcal{S} \cup \{R\}$ where R is a $(3k+7)$-Deg^+ binary relation symbol and with $Pre(\Psi') \in P(\exists^*\forall^d\exists^*)$ and $Pre(\Phi) \in P(\exists^*\forall\exists^*)$ s.t. for all structures $\mathcal{M} = \langle Dom, \mathcal{S}\rangle$*

$$\mathcal{M} \models \exists f_1 \ldots \exists f_k \quad \Psi \iff \mathcal{M} \models \exists R \quad \Phi \wedge \Psi'.$$

As said before, whatever the signature $\mathcal{S}$ is the difficulty of the proof is unchanged. So, without loss of generality, we can assume that $\mathcal{S} = \emptyset$. Ψ can be seen as a first-order formula of signature $\{f_1, \ldots, f_k\}$.

A weak version of prop. 4.1 in which we make use of additional unary relational predicates is first proved. In this case, the outdegree of the binary relation is bounded by $3k+6$. Let $\overline{U}$ stand for the set of the following (unary relation) symbols.

$$A_0^0, B_0^0, C_0^0 \ldots, A_t^0, B_t^0, C_t^0, \ldots, A_k^0, B_k^0, C_k^0$$
$$A_0^1, B_0^1, C_0^1, \ldots, A_t^1, B_t^1, C_t^1, \ldots, A_k^1, B_k^1, C_k^1, A, B, Order, Rem$$

Proposition 4.2 *Let $\mathcal{S}$ be a signature and d be a positive integer. Let Ψ be a prenex first-order formula of type $\mathcal{S} \cup \{f_1, \ldots, f_k\}$ with a first-order prefix in $P(\exists^*\forall^d\exists^*)$. Then, there exist two f.o. formulas Ψ' and Φ of type $\mathcal{S} \cup \{R\} \cup \overline{U}$ where R is a $(3k+6)$-Deg^+ binary relation symbol and with $Pre(\Psi') \in P(\exists^*\forall^d\exists^*)$ and $Pre(\Phi) \in P(\exists^*\forall\exists^*)$ s.t. for all structures $\mathcal{M} = \langle Dom, \mathcal{S}\rangle$*

$$\mathcal{M} \models \exists f_1 \ldots \exists f_k \quad \Psi \iff \mathcal{M} \models \exists R \exists\, \overline{U} \quad \Phi \wedge \Psi'.$$

4.2.1 General outline of the proof of prop. 4.2

What we have to construct is,

- a mapping, $red : F \mapsto red(F)$, from the class of all $\{f_1, \ldots, f_k\}$-structures to the class of all $\{R\} \cup \overline{U}$-structures where R is a $(3k+6)$-Deg^+ binary relation. F and $red(F)$ will have the same domain.
- for every formula Ψ of signature $\{f_1, \ldots, f_k\}$ and with $Pre(\Psi) \in P(\exists^*\forall^d\exists^*)$, two formulas Φ and Ψ' of signature $\{R\} \cup \overline{U}$ with $Pre(\Phi) \in P(\exists^*\forall\exists^*)$ and $Pre(\Psi') \in P(\exists^*\forall^d\exists^*)$ s.t.:
  1. for all F, $red(F) \models \Phi$.

2. if $F \models \Psi$ then $red(F) \models \Psi'$.
3. Let G be a $\{R\} \cup \overline{U}$-structure, if $G \models \Phi \wedge \Psi'$ then there exists F s.t. $G = red(F)$ and $F \models \Psi$.

4.2.2 An intuitive idea of the reduction of the models

Let $F = \langle Dom, f_1, \ldots, f_k \rangle$ with $|Dom| = n$. We suppose that n is sufficiently large. Subsets

$$A_0^0, B_0^0, C_0^0 \ldots, A_t^0, B_t^0, C_t^0, \ldots, A_k^0, B_k^0, C_k^0$$
$$A_0^1, B_0^1, C_0^1, \ldots, A_t^1, B_t^1, C_t^1, \ldots, A_k^1, B_k^1, C_k^1, A, B, Order, \text{ and } Rem$$

are supposed to be pairwise disjoint and to realize a partition of the domain. The union of the subsets of the first (resp. second) row form a new subset DOM^0 (resp. DOM^1). We proceed as follows to construct $Red(F)$ (the reader is invited to have a look at the figures of this chapter).

1. A one-one correspondence is established, by R, from each A_i^j, B_i^j, C_i^j $(i = 0, 1, \ldots, k,$ $j = 0, 1)$ to B. This implies that all these subsets have the same cardinality (which is intended to be at least in $O(\lceil \sqrt[3]{n} \rceil)$). These edges are called *bijection* edges.

   For all $i = 0, 1, \ldots, k$, Let $DOM_i = (A_i^0 \times B_i^0 \times C_i^0) \cup (A_i^1 \times B_i^1 \times C_i^1)$.

2. R will associate to each $y \in Dom$ a unique representative $(y_0, y_1, y_2) \in DOM_0$ satisfying $R(y, y_0), R(y, y_1)$ and $R(y, y_2)$ s.t.:

   if $y \in DOM^0$ then $(y_0, y_1, y_2) \in A_0^1 \times B_0^1 \times C_0^1$,

   if $y \in DOM^1$ then $(y_0, y_1, y_2) \in A_0^0 \times B_0^0 \times C_0^0$.

   These edges are called *representation* edges. An important condition is that representatives are chosen in such a way that representation and bijection edges induce an injective mapping from the domain to $B \times B \times B$ (see fig.2).

Now, let $x, y \in Dom$ and suppose $f_i(x) = y$. This is what we have to encode. First, we read the representation $(y_0, y_1, y_2) \in DOM_0$ of y. There are exactly two tuples in DOM_i which are related, by bijection edges, to the same tuple of $B \times B \times B$ as (y_0, y_1, y_2). Let $(\alpha_i^0, \beta_i^0, \gamma_i^0) \in A_i^0 \times B_i^0 \times C_i^0$ and $(\alpha_i^1, \beta_i^1, \gamma_i^1) \in A_i^1 \times B_i^1 \times C_i^1$ be these two tuples. Acording to which level (DOM^0 or DOM^1) x belongs, we associate x with exacly one of them. That is,

if $x \in DOM^0$ (resp. DOM^1), we add $R(x, \alpha_i^1), R(x, \beta_i^1)$ and $R(x, \gamma_i^1)$ (resp. $R(x, \alpha_i^0)$, $R(x, \beta_i^0)$ and $R(x, \gamma_i^0)$). (see fig.3)

The separation of the domain into two levels, DOM^0 and DOM^1, could seem unatural. In fact, we are convinced that it makes the proof simpler and easier to understand. It is obvious to see that, at this moment, R is of outdegree bounded by $3k + 4$.

The above-defined construction must be expressed with only *one* first-order universal quantifier. This extremely restrictive condition justify in some sense to complicate a little

bit more the construction. In particular, to express with only one universal quantifier that there exists bijection and representation edges, it appears as convenient to define R as a successor relation on each subset. This is made, together with the definition of bijection edges, in the three first "Steps" of the proof. There will remain two "steps" in this proof, one (step 4) devoted to the definition of representation edges, the other (step 5) to the encoding of the input functions.

4.2.3 The proof

For each $D \in \overline{U}$, two constants 0_D and 1_D are introduced. Instead of "unary relation symbol" the terms "segment" or "subset" will sometimes be used.

Step 1. The first step of the simulation (see $\varphi_1, \ldots, \varphi_{11}$ below) consists, under certains conditions, in defining R as a successor relation on two distinguished subsets A and B of the domain. The technique used is now classical (see [Gra90c]). .

$$\varphi_1 : \forall x \quad \neg(A(x) \wedge B(x)) \wedge \neg(A(x) \wedge Order(x)) \wedge \neg(B(x) \wedge Order(x))$$

$$\varphi_2 : \quad A(0_A) \wedge A(1_A) \wedge B(0_B) \wedge B(1_B) \wedge R(1_A, 0_A) \wedge R(1_B, 0_B) \wedge R(0_A, 0_B) \wedge R(1_A, 1_B) \wedge (0_A \neq 1_A) \wedge (0_B \neq 1_B)$$

φ_3 is the conjunct of the two formulas φ_A, φ_B where

$$\varphi_A : \forall x \qquad (A(x) \rightarrow \exists y \; x \neq y \wedge A(y) \wedge R(x,y)) \wedge (A(x) \rightarrow \exists y \; x \neq y \wedge A(y) \wedge R(y,x))$$

(replace A by B in φ_A to obtain φ_B.). φ_1 states that A, B and $Order$ are pairwise disjoint. φ_2 gives constraints to be satisfied by the constants of A and B, and φ_3 expresses that each element of A (resp. B) is related by R to at least one other element of A (resp. of B).

For practical reasons, a one-one correspondence between A and B is established ($\varphi_4, \varphi_5, \varphi_6$ below):

$$\varphi_4 : \forall x \quad (A(x) \rightarrow \exists y \; B(y) \wedge R(x,y) \wedge R(y,x))$$

$$\varphi_5 : \forall x \quad (B(x) \rightarrow \exists y \; A(y) \wedge R(x,y) \wedge R(y,x))$$

$$\varphi_6 : \forall x \quad (A(x) \rightarrow \exists x' \exists y \exists y' \; A(x') \wedge B(y) \wedge B(y') \wedge x \neq x' \wedge y \neq y' \wedge R(x,x') \wedge R(y,y') \wedge R(x,y) \wedge R(x',y'))$$

We are now ready to state a first claim which will clarify the situation:

Claim 1 *Let $\langle Dom, R, A, B, Order \rangle$ be a model of the conjunction $\bigwedge_{i \leq 6} \varphi_i$ and suppose, for all $a \in A \cup B \cup Order$, $Outdeg(a) = 2$ for R restricted to $(A \cup B \cup Order)$ then:*

- *$R{\restriction}A$ is a permutation of A (idem for B).*
- *$R{\restriction}(A \times B)$ is an isomorphism from structure $(A, R{\restriction}A)$ to structure $(B, R{\restriction}B)$ whose converse is $R{\restriction}(B \times A)$*

Proof. It is a consequence of $\varphi_1, \ldots, \varphi_6$ that for all x in A (resp. in B), there exists x' in A (resp. in B) and y in B (resp. in A) s.t. $x \neq x'$, $R(x,x')$, $R(x,y)$ and $R(y,x)$. Suppose $R \restriction (A \times B)$ is not an injective mapping from A to B. Then, obviously, there is an element $b \in B$ of outdegree at least three which contradicts the hypothesis. So, $R\restriction(A \times B)$ is an injection from A to B. Moreover, φ_5 implies that it is also surjective. The bounded outdegree condition implies that $R\restriction A$ and $R\restriction B$ are permutations of A and B respectively and φ_6 implies that $R\restriction(A \times B)$ is an isomorphism from permutation $R\restriction A$ to $R\restriction B$. □

Definition 4.3 *Let $\langle Dom, R, A, B, Order\rangle$ be as in Claim 1 and let x in A (resp. in B). We denote by Sx (for "successor") the only point x' in A (resp. in B) satisfying $R(x,x')$. The same notation is kept for its natural extension to the lexicographic successor on tuples on A (resp. B).*

From now on, the symbol S is used in the formulas (to improve readability). Our aim is to define $R\restriction A$ and $R\restriction B$ (and incidentally $R\restriction Order$) as permutations with only one cycle (i.e. as a successor relation). To do this, each element of $Order$ will be related to pairs (x, y_1) where $x \in A$, $x \neq 1_A$, $y_1 \in \{Sy, S^2y, \ldots, 1_B\}$, with $y \in B$ s.t. $R(x,y)$ holds. This kind of projection (from $Order$ to $A \times B$) is forced to be injective.

$\varphi_7 :\ Order(0_{Order}) \wedge Order(1_{Order}) \wedge R(0_{Order}, 0_A) \wedge R(0_{Order}, S(0_B)) \wedge \exists\alpha(A(\alpha) \wedge R(1_{Order}, \alpha) \wedge R(\alpha, 1_A) \wedge R(1_{Order}, 1_B)) \wedge R(1_{Order}, 0_{Order})$

$\varphi_8 :\ \forall x \quad [(A(x) \wedge x \neq 1_A) \rightarrow \exists y \exists t\ (B(y) \wedge R(x,y) \wedge R(t,x) \wedge R(t,Sy) \wedge Order(t))]$

$\varphi_9 :\ \forall t \quad [(Order(t) \wedge \neg R(t,1_B)) \rightarrow \exists t' \exists x \exists y\ (A(x) \wedge B(y) \wedge R(t,x) \wedge R(t,y) \wedge Order(t') \wedge R(t',x) \wedge R(t',Sy) \wedge R(t,t'))]$

$\varphi_{10} :\ \forall t \quad [(Order(t) \wedge t \neq 1_{Order} \wedge R(t,1_B)) \rightarrow \exists t' \exists x \exists y\ (Order(t') \wedge A(x) \wedge B(y) \wedge R(t,x) \wedge R(x,y) \wedge R(t',Sx) \wedge R(t',S^2y) \wedge R(t,t'))]$

$\varphi_{11} :\ \forall t \quad [Order(t) \rightarrow \exists x \exists y\ (A(x) \wedge B(y) \wedge R(t,x) \wedge R(t,y) \wedge \neg R(x,y))]$

$\varphi_{12} :\ \forall x \quad \neg Order(x) \rightarrow R(x,x)$

Fig. 4.1 describes how elements of $Order$ are related to pairs of $A \times B$.

Claim 2 *Let $\langle Dom, R, A, B, Order\rangle$ be a model of the conjunction $\bigwedge_{i\leq 12} \varphi_i$ and suppose, for all $a \in A \cup B \cup Order$, $Outdeg(a) = 3$ for R restricted to $(A \cup B \cup Order)$ then:*

- *The conclusions of Claim 1 hold.*
- *$R\restriction A$ (resp. $R\restriction B$) is a permutation of A (resp.B) with only one cycle, the cycle of 0_A and 1_A (resp. of 0_B and 1_B).*

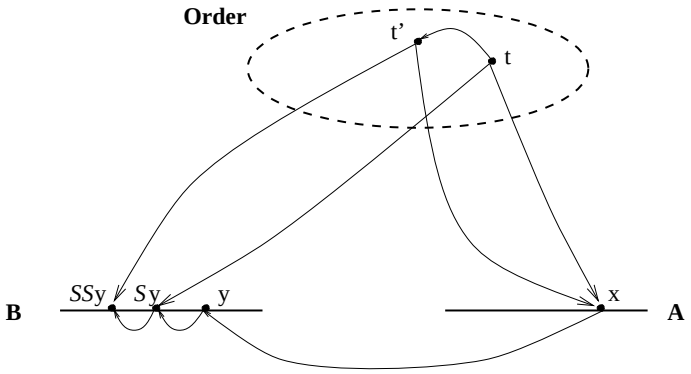

FIG. 4.1 -

– *$R\restriction Order$ is a permutation of $Order$ with only one cycle, the cycle of 0_{Order} and 1_{Order}.*

Proof. φ_{12} implies that R is reflexive for all vertices x (with $x \notin Order$). Then, reflexive edges $R(x,x)$ apart, $R\restriction(A \cup B)$ is of outdegree 2 and the conclusions of Claim 1 still hold. Suppose there is a cycle $\mathcal{C}$ in A different from the cycle of 0_A and 1_A. Let $\mathcal{C}'$ the corresponding cycle in B (recall that $R\restriction(A \times B)$ is an isomorphism from A to B). Let e_1 in $\mathcal{C}$ and $e_2 \in \mathcal{C}'$ s.t. $R(e_1, e_2)$ holds. The point 1_A is not in $\mathcal{C}$ and, of course $1_B \notin \mathcal{C}'$. So, $\varphi_8 \wedge \varphi_9$ implies that, for all i, there is,

$$t \in Order, \text{ such that } R(t, e_1) \wedge R(e_1, e_2) \wedge R(t, S^i e_2).$$

Take $i = card(C)$. Then, we have $R(t, e_1)$ and $R(t, e_2)$ with $t \in Order$. This contradicts φ_{11}. The third assertion is easy to prove (see φ_9, φ_{10}). Remark that φ_{12} is written to ensure that for each element $R\restriction(A \cup B \cup Order)$ is of outdegree 3. □

Step 2. This section is devoted to define $R\restriction D$ for each $D \in \overline{U}$ as a successor relation on D (as it was made for, e.g., A). Let's make a partition of the domain into two "levels" DOM^0, DOM^1 where:

DOM^0 is the union of $A_0^0, B_0^0, C_0^0 \ldots, A_t^0, B_t^0, C_t^0, \ldots, A_k^0, B_k^0, C_k^0$.
DOM^1 is the union of $A_0^1, B_0^1, C_0^1, \ldots, A_t^1, B_t^1, C_t^1, \ldots, A_k^1, B_k^1, C_k^1, A, B, Order, Rem$.

Rem (for *remainder*) will be supposed to be the complement in the domain of the union of the other subsets. We assume also that all the subsets above are pairwise disjoint (by giving a new formula φ_1) and we make bijective the restriction of R between the segments of each level (except *Rem*) and B. All the edges constructed till now are called *bijection edges*:

$$\varphi_1 : \forall x \quad \bigwedge_{D,E\in\overline{U}} \neg(D(x)\wedge E(x)) \wedge \bigvee_{D\in\overline{U}} D(x)$$

$$\varphi_{13}^D : R(0_D, 0_B) \wedge R(1_D, 1_B)$$

$$\varphi_{14}^D : \forall x \quad (D(x) \to \exists y\ B(y)\wedge R(x,y)) \wedge (B(x) \to \exists y\ D(y)\wedge R(y,x)) \wedge (D(x) \to \exists x'\exists y\ D(x')\wedge B(y)\wedge R(x,x')\wedge R(x,y)\wedge R(x',Sy))$$

φ_{13} is the conjunction for all $D \in \overline{U}\backslash Rem$ of φ_{13}^D.
φ_{14} is the conjunction for all $D \in \overline{U}\backslash Rem$ of φ_{14}^D.

The case of Rem is treated separately. Rem will be supposed to contain less elements than $Order$. So, we just state that there is an injection from Rem to $Order$:

$$\varphi_{Rem} : \forall x \quad (Rem(x)\wedge x \to \exists y\ Order(y)\wedge R(x,y))$$

$$\varphi_{15}^{Rem} : \forall x \quad (Rem(x)\wedge x \neq 1_{Rem} \to \exists x'\exists y\ Rem(x')\wedge Order(y)\wedge R(x,x')\wedge R(x,y)\wedge R(x',Sy))$$

We set $\varphi_{15} = \varphi_{Rem}\wedge\varphi_{15}^{Rem}\wedge Rem(0_{Rem})\wedge Rem(1_{Rem})\wedge R(0_{rem},0_{Order})\wedge R(1_{rem},0_{Rem})$.

Claim 3 *Let $\langle Dom, R, \overline{U}\rangle$ be a model of the conjunction $\bigwedge_{i\leq 15}\varphi_i$ and suppose, for all $a \in Dom$, $Outdeg(a) = 3$ for then:*

- *The conclusions of the two previous claims hold*
- *For each $D \in \overline{U}$, $R|D$ is a permutation of D with only one cycle.*

Proof. Easy. In the same style as those of the first two claims. □

Step 3. According to the last cglaim, if the outdegree of every point is equal to three then R restricted to each subset is a permutation with only one cycle. Our aim here is to "define" a successor relation for each of the two levels DOM^0 and DOM^1. Intuitively, we want to obtain the following linear order:

$$A_0^0 < B_0^0 < C_0^0 < \ldots A_t^0 < B_t^0 < C_t^0 < \ldots A_k^0 < B_k^0 < C_k^0.$$
$$A_0^1 < B_0^1 < C_0^1 < \ldots A_t^1 < B_t^1 < C_t^1 < \ldots A_k^1 < B_k^1 < C_k^1 < A < B < Order < Rem.$$

The definition of successor S can now be modified a little bit and extended to the whole domain.

Definition 4.4 *On a model of $\bigwedge_{i\leq 15}\varphi_i$, let $x \in DOM^0$*

- *if $x \neq 1_{A_j^0}, 1_{B_j^0}, 1_{C_j^0}$ for all $j \leq k$, then $Sx = y$ where y is the only point in the same subset as x satisfying $R(x,y)$.*

- *for each* $j \leq k$, $S(1_{A_j^0}) = 0_{B_j^0}, S(1_{B_j^0}) = 0_{C_j^0}$ *and, if* $j \neq k$ $S(1_{C_j^0}) = 0_{A_{j+1}^0}$
- $S1_{C_k^0}$ *is not defined.*

We proceed similarly for level DOM^1. S *is defined on* $Order$ *and on* Rem *as follows.*

- *Let* $t, t' \in Order$, $t' \neq 1_{Order}$ *and* $(a,b),(a',b')$ *on* $A \times B$ *verifying* $R(t,a), R(t,b)$ *and* $R(t',a'), R(t',b')$. *Then,*

$$S(a,b) = (a',b') \iff St = t'$$

- $S(1_{Order}) = 0_{Rem}$
- *Let* $r, r' \in Rem$ $(r \neq 1_{Rem},\ r' \neq 1_{Rem})$ *and* t, t' *their image by* R *in* $Order$. *Then,*

$$St = t' \iff Sr = r'$$

- $S(1_{Rem})$ *is not defined.*

Step 4. We need to introduce new notations. Let $\sim$ be an equivalence relation defined in the following way. For each $a^i \in DOM^i$ and $a^j \in DOM^j$ $(i,j \in \{0,1\})$ we set:

$$a^i \sim a^j \iff \vee \begin{cases} a^i = a^j \\ \exists b\ B(b) \wedge R(a^i,b) \wedge R(a^j,b) \end{cases}$$

Intuitively, two points a^i and a^j are in the same class for $\sim$ if either they are equal or they are related (by bijection edges) to the same $b \in B$. The same notation $\sim$ is kept for its natural extension to tuples.

According to the subscript of the notation of the segments, we give the following definition:

$$DOM_i = (A_i^0 \times B_i^0 \times C_i^0) \cup (A_i^1 \times B_i^1 \times C_i^1)$$

Each DOM_i (for $i \geq 1$) will be involved each time an information concerning f_i will be encoded. DOM_i is, in a sense, carateristic of f_i. DOM_0 is used to "represent" the domain Dom: to each element $x \in Dom$ is "associated" injectively a tuple (a_x, b_x, c_x) in DOM_0 by this way:

- If $x \in DOM^1$ then we have $R(x,a_x)$, $R(x,b_x)$ and $R(x,c_x)$ with $(a_x,b_x,c_x) \in A_0^0 \times B_0^0 \times C_0^0$
- If $x \in DOM^0$ then we have $R(x,a_x)$, $R(x,b_x)$ and $R(x,c_x)$ with $(a_x,b_x,c_x) \in A_0^1 \times B_0^1 \times C_0^1$

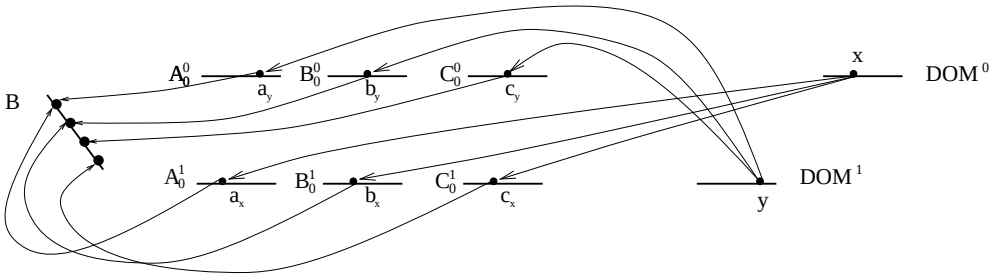

FIG. 4.2 -

Fig. 4.2 describes the representations of some $x \in DOM^0$ and some $y \in DOM^1$. here $a_x \sim a_y$, $b_x \sim b_y$ but $c_x \not\sim c_y$.

Such edges described above are called *representation-edges*. The representation is injective means (intuitively) that: for two distinct elements x and y of Dom and their respective representative (a_x, b_x, c_x) and (a_y, b_y, c_y) of DOM_0, we have $(a_x, b_x, c_x) \not\sim (a_y, b_y, c_y)$. Such a condition of injectivity is difficult to express with only one universal quantifier. Roughly speaking, the method is:

- $0_{A_0^0}$ is represented by $(0_{A_0^1}, 0_{B_0^1}, 0_{C_0^1})$.
- Suppose $x \in DOM^i$ and let (a_x, b_x, c_x) be its representative in $DOM^{i\oplus 1}$, then the representative of Sx will be $S(a_x, b_x, c_x)$. We just have to take care about the relation between the representatives of the last point, $1_{C_k^0}$, of DOM^0 and of the first point, $0_{A_0^1}$, of DOM^1. These two tuples must not be equivalent for $\sim$ (see φ_{18}).

From now on, we adopt the abbreviation $R(x,(a,b,c))$ for $R(x,a) \wedge R(x,b) \wedge R(x,c)$ (and sometimes DOM^i and the relation $\sim$ will appear directly in formulas). The six formulas below describe the above-mentioned method of representation.

φ_{16} : $\forall x[DOM^i(x) \rightarrow \exists a \exists b \exists c\ (A_0^{i\oplus 1}(a) \wedge B_0^{i\oplus 1}(b) \wedge C_0^{i\oplus 1}(c) \wedge R(x,(a,b,c)))]$

φ_{17} : $R(0_{A_0^0}, (0_{A_0^1}, 0_{B_0^1}, 0_{C_0^1}))$

φ_{18} : $\exists a \exists b \exists c \exists a' \exists b' \exists c'\ (A_0^1(a) \wedge B_0^1(b) \wedge C_0^1(c) \wedge A_0^0(a') \wedge B_0^0(b') \wedge C_0^0(c') \wedge R(1_{C_k^0}, (a,b,c)) \wedge ((a,b,c) \sim (a',b',c')) \wedge R(0_{A_0^1}, S(a',b',c'))$

φ_{19} : $\forall x \quad [(DOM^i(x) \wedge \neg R(x, 1_{C_0^{i\oplus 1}})) \rightarrow \exists a \exists b \exists c\ (A_0^{i\oplus 1}(a) \wedge B_0^{i\oplus 1}(b) \wedge C_0^{i\oplus 1}(c) \wedge R(x,(a,b,c)) \wedge R(Sx,(a,b,Sc)))]$

φ_{20} : $\forall x \quad [(DOM^i(x) \wedge \neg R(x, 1_{B_0^{i\oplus 1}}) \wedge R(x, 1_{C_0^{i\oplus 1}})) \rightarrow \exists a \exists b\ (A_0^{i\oplus 1}(a) \wedge B_0^{i\oplus 1}(b) \wedge R(x,(a,b,1_{C_0^{i\oplus 1}})) \wedge R(Sx,(a,Sb,0_{C_0^{i\oplus 1}})))]$

$\varphi_{21}: \forall x \quad [(DOM^i(x) \wedge R(x, 1_{B_0^{i\oplus 1}}) \wedge R(x, 1_{C_0^{i\oplus 1}})) \rightarrow \exists a\ (A_0^{i\oplus 1}(a) \wedge R(x, (a, 1_{B_0^{i\oplus 1}}, 1_{C_0^{i\oplus 1}})) \wedge R(Sx, (Sa, 0_{B_0^{i\oplus 1}}, 0_{C_0^{i\oplus 1}})))]$

Now, every point of the domain admits a unique representative in DOM_0. More precisely:

Claim 4 *Let $\langle Dom, R, \overline{U}\rangle$ be a model of the conjunction $\bigwedge_{i\leq 21}\varphi_i$ and suppose, for all $a \in Dom$, $Outdeg(a) = 6$ then:*

- *The conclusion of the previous claims hold*
- *For each $x \in Dom$ there exists a unique tuple (a_x, b_x, c_x) in DOM_0 representing x, i.e. such that $R(x, (a_x, b_x, c_x))$. Furthermore, let $y \neq x$ and (a_y, b_y, c_y) its representative, then $(a_x, b_x, c_x) \not\sim (a_y, b_y, c_y)$.*

Proof. Easy. A point cannot have two representing tuples because of the outdegree condition. The non equivalence of two representing tuples is true by construction. □

Step 5. Now, we are able to show how to encode the functions f_t. Suppose we have $f_t(x) = y$ with, e.g., $x \in DOM^i$ and $y \in DOM^j$ $(i, j \in \{0, 1\})$. First, we read the representation of y, $(a_y, b_y, c_y) \in A_0^{j\oplus 1} \times B_0^{j\oplus 1} \times C_0^{j\oplus 1}$. Then, following the bijection edges, we find the only tuple $(a_t^{i\oplus 1}, b_t^{i\oplus 1}, c_t^{i\oplus 1})$ of $A_t^{i\oplus 1} \times B_t^{i\oplus 1} \times C_t^{i\oplus 1}$ such that:

$$(a_y, b_y, c_y) \sim (a_t^{i\oplus 1}, b_t^{i\oplus 1}, c_t^{i\oplus 1})$$

Finally, we construct $R(x, a_t^{i\oplus 1}), R(x, b_t^{i\oplus 1})$ and $R(x, c_t^{i\oplus 1})$. These edges are called *function edges*. More precisely, φ_{22} is the conjunction of all $\varphi_{22}^{t,i}$ below for $i = 0, 1$ and $t \in \{1, \ldots, k\}$,

$$\varphi_{22}^{t,i}: \forall x \quad [DOM^i(x) \rightarrow \exists a \exists b \exists c\ (A_t^{i\oplus 1}(a) \wedge B_t^{i\oplus 1}(b) \wedge C_t^{i\oplus 1}(c) \wedge R(x, (a, b, c)))]$$

Ψ' is obtained from Ψ by replacing each subformula of the form $f_t(x) = y$ with the formula $[x, y]_t$ below:

$$\exists a_y \exists b_y \exists c_y \exists a \exists b \exists c \quad \bigwedge_{i,j=0,1} [DOM^i(x) \wedge DOM^j(y) \rightarrow$$

$$[A_0^{j\oplus 1}(a_y) \wedge B_0^{j\oplus 1}(b_y) \wedge C_0^{j\oplus 1}(c_y) \wedge$$
$$A_t^{i\oplus 1}(a) \wedge B_t^{i\oplus 1}(b) \wedge C_t^{i\oplus 1}(c) \wedge$$
$$((a, b, c) \sim (a_y, b_y, c_y)) \wedge$$
$$R(y, (a_y, b_y, c_y)) \wedge R(x, (a, b, c))]$$

We set $\Phi = \bigwedge_{i\leq 22}\varphi_i$.

In fig. 4.3, it is shown how $f_1(x) = y$ with $x \in A_2^0$ and $y \in C_0^1$.

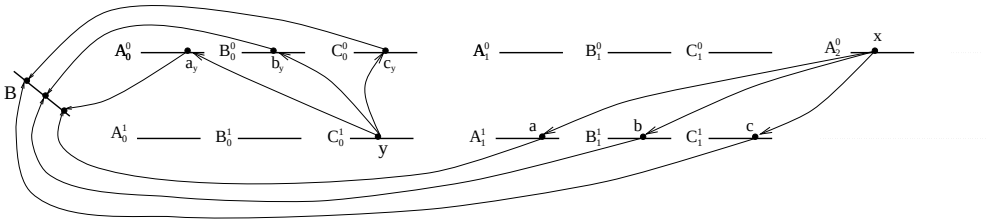

FIG. 4.3 -

Claim 5 *Let $\langle Dom, R, \overline{U}\rangle$ be a model of Φ and suppose, for all $a \in Dom$, $Outdeg(a) = 3k+6$ then:*

- *The conclusions of the previous claims hold.*
- *Let $i = 0,1$, $t = 1,\ldots,k$. For each $x \in DOM^i$ there exists a unique tuple $(a_t^{i\oplus 1}, b_t^{i\oplus 1}, c_t^{i\oplus 1})$ in $A_t^{i\oplus 1} \times B_t^{i\oplus 1} \times C_t^{i\oplus 1}$ related to x i.e. such that $R(x,(a_t^{i\oplus 1}, b_t^{i\oplus 1}, c_t^{i\oplus 1}))$. This time, two different elements x and y of Dom could be related to the same tuple of DOM_t (or to two equivalent tuples for $\sim$).*

Proof. Same arguments as for the previous claims. It is explicitely stated that each element a is related by R to at least $3k+6$ elements (3 bijection edges, 3 representation edges and $3k$ function edges). We know that R is of outdegree bounded by $3k+6$. So, "what is true is what is stated and nothing else".□

We give now the proof of prop 4.2. The left to right side is evident by construction.

Suppose $\langle Dom, R, \overline{U}\rangle \models \Phi \wedge \Psi'$. We define a structure $\langle Dom, f_1, \ldots, f_k\rangle$ by: for all $t = 1,\ldots,k$, for all $\alpha, \beta \in Dom$

$$f_t(\alpha) = \beta \iff \langle Dom, R, \overline{U}, \alpha, \beta\rangle \models [x,y]_t$$

$\langle Dom, R, \overline{U}\rangle \models \Phi$, so each f_t is a well defined function: if for two fixed elements α, β, $[\alpha,\beta]_t$ holds, then there can not be β' s.t. $[\alpha,\beta']_t$ holds. $\langle Dom, f_1, \ldots, f_k\rangle \models \Psi$ follows.□

4.2.4 Proof of prop. 4.1

Let's recall the proof of prop. 4.2. It will be shown here how to avoid the use of unary predicates. The solution consists mainly in labelling the elements of the domain with distinguished points.

Let $\overline{u}$ denote the list of distinct elements below:

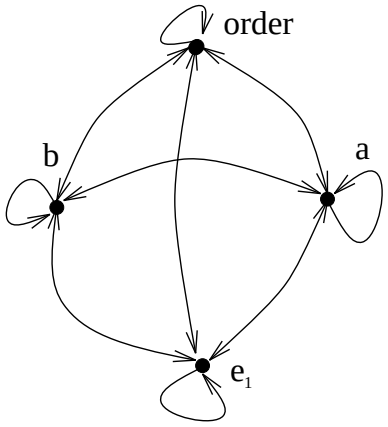

FIG. 4.4 -

$$e_1, a, b, order, e_2, e_3, e_4, rem$$
$$e_0^0, a_0^0, b_0^0, c_0^0 \ldots, e_t^0, a_t^0, b_t^0, c_t^0, \ldots, e_k^0, a_k^0, b_k^0, c_k^0$$
$$e_0^1, a_0^1, b_0^1, c_0^1, \ldots, e_t^1, a_t^1, b_t^1, c_t^1, \ldots, e_k^1, a_k^1, b_k^1, c_k^1$$

Among these points, those whose uppercase version is the name of one of the subsets will be used to define these subsets as follows, e.g.:

$$\forall x (x \notin \overline{u}) \quad A_0^0(x) \iff R(x, a_0^0(x))$$

These edges are called *labelling edges*. Obviously, all points of the domain (except those of $\overline{u}$) are now of outdegree $3k + 7$. As the other elements, points of $\overline{u}$ are consequently preimage for each original function and could be in the set of images for these functions. So, we have to take it in account in the simulation.

First, we have to compensate the missing of bijection and labelling edges starting from any point of $\overline{u}$. In the proof of theorem 4.2 it is stated that R is reflexive (except on $Order$). The set $\overline{u}$ will respect this condition, that is, for all $u \in \overline{u}$, $R(u, u)$ holds.

Now, points of $\overline{u}$ are arranged in four-cliques in the following way:
e_1 with a, b and $order$,
e_2 with e_3, e_4 and rem,
e_i^j with a_i^j, b_i^j and c_i^j for $i = 0, 1; j = 0, 1, \ldots, k$.

These edges are also parts of labelling edges. Fig. 4.4 above represents the four-clique containing $e_1, a, b, order$.

After this step, every $u \in \overline{u}$ is of outdegree 4. The notion of level (of kind DOM^i or DOM_i) should be rephrased. It is agreed that all elements u of $\overline{u}$ in a clique belong to the same level and that each x ($x \notin \overline{u}$) belongs to the same level as its labelling

point. e.g. a_i^j is in DOM^j. The rest of the proof is unchanged. The reader should be easily convinced, by an exhaustive verification, that there cannot be confusion between different kinds of edges (labelling, bijection. representation and function edges).

One remark before concluding: of course, formula $\Phi \wedge \Psi'$ will be the one of prop 4.2 except that a block $\exists e_1 \exists a \exists b \ldots \exists b_k^1 \exists c_k^1$ appears now in front of its first-order quantifier prefix.

The right to left side of theorem 4.1 is a consequence of the proposition below (which was proved in chapter 2).

Proposition 4.5 *Let $\mathcal{S}$ be a signature, d and h be positive integers. Let Ψ be a first-order formula of type $\mathcal{S} \cup \{R\}$ where R is a $h-Deg^+$ binary relation symbol and with $Pre(\Psi) \in P(\exists^* \forall^d \exists^*)$. Then, there exists Ψ' of signature $\mathcal{S} \cup \{f_1, \ldots, f_{h+1}\}$ with a first-order prefix in $P(\exists^* \forall^d \exists^*)$ s.t. for all structure $\mathcal{M} = \langle Dom, \mathcal{S} \rangle$*

$$\mathcal{M} \models \exists R \quad \Psi \iff \mathcal{M} \models \exists f_1 \ldots \exists f_{h+1} \quad \Psi'$$

Remark All the theorems below are still true, not only for $\exists^* \forall^d \exists^*$ as first-order prefix but also for any prefix in $P(w)$ where w is a finite word in $\{\exists^*, \forall\}$ with at least one $\forall$. That is to say, the simulation preserves the generic structure in universal quantifiers.

4.3 Corollaries and related problems

From theorem 4.1, it follows that the hierarchy of properties definable by second-order formulas with only bounded outdegree relation symbols in the second-order part and whose first-order prefix is of the form $\exists^* \forall^d \exists^*$, for a given d, "collapses" at level one. That is to say "<u>one</u> binary relation of bounded outdegree is enough".

Corollary 4.6 *Let $d, k, h_1, \ldots, h_k$ be positive integers. Let Φ be a first-order formula of signature $\mathcal{S} \cup \{R_1, \ldots, R_k\}$ where each R_i is a h_i-Deg^+ binary relation symbol and with $Pre(\Phi) \in P(\exists^* \forall^d \exists^*)$. Then, there exist an integer h and a first-order formula Φ' whose signature is $\mathcal{S} \cup \{R\}$, where R is a $h-Deg^+$ symbol and $Pre(\Phi') \in P(\exists^* \forall^d \exists^*)$ s.t. for all structures $\mathcal{M} = \langle Dom, \mathcal{S} \rangle$*

$$\mathcal{M} \models \exists R_1 \ldots \exists R_k \quad \Phi \iff \mathcal{M} \models \exists R \quad \Phi'.$$

Proof. Easy, it follows from successive applications of Theorem 4.1 and 4.5. the value of h is $6k + \Sigma_{i=1}^{k} 3(h_i + 1)$.

The end of this section is devoted to the study of some question of (un)decidability of first-order theories of one bounded outdegree relation symbol. Let's consider the problem P below:

Instance An integer k and a first-order prenex sentence Φ with $Pre(\Phi) \in P(\exists^* \forall \exists^*)$ and of signature $\{R\}$, for binary R.

Question Is Φ satisfiable (or finitely satisfiable) on a model where the outdegree of R is bounded by k?

It is known from [Gur76] that the class of formulae with only one universal quantifier and of signature containing at least two unary function symbols is undecidable. Then, it can be derived from theorem 4.1 that P is undecidable. The outdegree condition is essential since it was proved (by Shelah) that the following problem is decidable:

Instance A first-order prenex sentence Φ with $Pre(\Phi) \in P(\exists^*\forall\exists^*)$ and of signature consisting in any number of relation symbols of any arities and at most one unary function symbol.

Question Is Φ satisfiable (or finitely satisfiable)?

Suppose now that k is fixed in the problem P and call P_k the resulting problem. An interesting question is to find the minimal k such that P_k is undecidable. It is obvious that P_1 is decidable (the predicate R can then be seen as a unary function). The proposition below shows that the case $k = 2$ is much more difficult:

Proposition 4.7 *Problem P_2 is undecidable.*

Proof The result is obtained by reduction (from the theory of one universal quantifier and two unary functions). Let $\Psi = \forall x\ \psi(x, f_A, f_B)$ be a first-order sentence where f_A, f_B are unary function symbols. It can be supposed that each atomic formula of ψ is of the form $f_A(t) = t'$, $f_B(t) = t'$, $t = t'$ or $t \neq t'$.

Let a, b, c, d be four constant symbols. $A(x)$ (resp. $B(x), C(x), D(x)$) will replace in the following the atomic formula $R(x, a)$ (resp. $R(x, b), R(x, c), R(x, d)$). $Compl(x)$ stands for $\neg(A(x) \vee B(x) \vee C(x) \vee D(x))$. We state that A, B, C, D are pairwise disjoint and a, b, c, d are distinct:

$$\begin{aligned}\phi_0(a,b,c,d):\ \forall x \quad & \neg(A(x) \wedge B(x)) \wedge \neg(A(x) \wedge C(x)) \wedge \ldots \wedge \neg(C(x) \wedge D(x)) \\ & \wedge (a \neq b) \wedge (a \neq c) \wedge \ldots \wedge (c \neq d) \\ & \wedge \neg A(a) \wedge \neg A(b) \ldots \neg D(c) \wedge \neg D(d)\end{aligned}$$

Let's make a comment: an element x satisfies, e.g. $A(x)$, if and only if $R(x, a)$ holds. Then, from now on, for every element x of A, B, C or D we can create at most one edge $R(x, y)$ (with $y \neq a, b, c, d$) starting from x to respect the outdegree condition. We state now that $R|Compl$ is of outdegree at least one:

$$\phi_1(a,b,c,d):\ (\forall x Compl(x))(\exists y Compl(y))\ R(x,y)$$

The relation R is now defined as follows. $R|(E, F)$ is a surjective mapping from E to F with each of the following four respective values for (E, F): $(A \cup B, Compl)$, $(Compl, C \cup D)$, (C, B), (D, A). All these conditions are easily expressible by formulas with only one universal quantifier. Let us denote $\phi_2(a, b, c, d), \ldots, \phi_5(a, b, c, d)$ these formulas. For example, $\phi_4(a, b, c, d)$ is (for (C, B)):

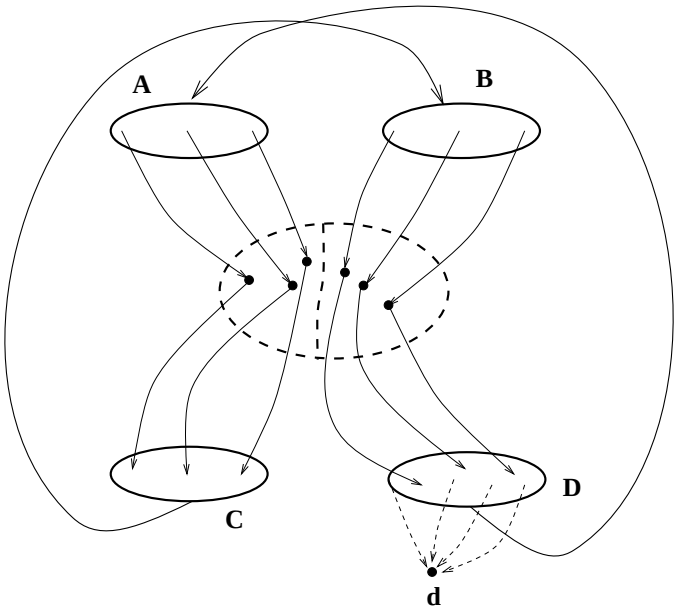

FIG. 4.5 -

$\forall x\ [C(x) \rightarrow \exists y\ B(y) \wedge R(x,y)] \wedge$

$\forall x\ [B(x) \rightarrow \exists y\ C(y) \wedge R(y,x)]$

Next formula $\phi_6(a,b,c,d)$ states that there are "surjective paths" of length two from A to C (and resp. from B to D)." Surjective path" means that each element of C (resp. D) is the extremity of at least one path starting from A (resp. from B). The conjunction of the two formulas below expresses what we have said for, e.g, A and C:

$(\forall x A(x))(\exists y Compl(y))(\exists z C(z))\ [R(x,y) \wedge R(y,z)]$

$(\forall x C(x))(\exists y Compl(y))(\exists z A(z))\ [R(z,y) \wedge R(y,x)]$

The formula Φ_7 below will find its justification later.

$\Phi_7(a,b,c,d)$: $(\forall x A(x))(\exists x_1 Compl(x_1))(\exists x_2 C(x_2))(\exists x_3 B(x_3))(\exists x_4 Compl(x_4))\ (\exists x_5 D(x_5))$
$R(x,x_1) \wedge R(x_1,x_2) \wedge R(x_2,x_3) \wedge R(x_3,x_4) \wedge R(x_4,x_5) \wedge R(x_5,x)$

Fig. 4.5 describes the construction.

Before going further, let us examine what can be derived from the satisfiability of $\bigwedge_{i=0}^{7} \Phi(a,b,c,d)$. It will be shown that where R is defined as a surjective mapping, R is in fact bijective. Suppose E is a subset of the domain and x is a distinguished point, $R(x,E)$ is true if and only if there exists at least one element y in E s.t. $R(x,y)$ hold (and similarly for $R(E,x)$). Let

$$Im(A) = \{y\ :\ y \in Compl \text{ and } \exists x \in A \text{ s.t. } R(x,y)\},$$
$$Im(B) = \{y\ :\ y \in Compl \text{ and } \exists x \in B \text{ s.t. } R(x,y)\}.$$

At this step we don't know if $Im(A) \cap Im(B)$ is empty. The following assertions are successively true (recall that R is of outdegree bounded by 2):

- $R\restriction((A \cup B) \times Compl)$ is a surjective mapping from $(A \cup B)$ to $Compl$ (cause of ϕ_1 and ϕ_2). Similar conclusions hold for $R\restriction(Compl, (C \cup D))$ and $R\restriction((C \cup D), (A \cup B))$. Consequently, $Im(A) \cap Im(B) = \emptyset$.
- Let $x \in Im(A)$ (resp. in $Im(B)$), then $R(x, C)$ is true (resp. false) and $R(x, D)$ is false (resp. true): if not, either x would be of outdegree 3 or ϕ_6 would be contradicted.
- $|A| \geq |Im(A)| \geq |C| \geq |B| \geq |Im(B)| \geq |D| \geq |A|$. Then, the cardinality of each subset is the same.

We are interested in satisfiability in the general case (and not only in finite satisfiability). So, only Φ_7 permits us to conclude that each surjective mapping is in fact bijective.

To complete the proof, we have to show how f_A and f_B are encoded. The idea is very simple: the formula Ψ is relativized to A and f_A (resp. f_B) is encoded by R on $Im(A)$ (resp. on $Im(B)$). From Ψ a new formula $\psi^{\Delta}(a, b, c, d)$ is then obtained by the following substitutions:

$$
\begin{array}{rcl}
\exists x & \longleftrightarrow & (\exists x A(x)) \\
\forall x & \longleftrightarrow & (\forall x A(x)) \\
f_A(a) = b & \longleftrightarrow & (\exists a_1 Compl(a_1))(\exists b_1 Compl(b_1))\ R(a, a_1) \wedge R(b, b_1) \wedge R(a_1, b_1) \\
f_B(a) = b & \longleftrightarrow & (\exists a_1 Compl(a_1))(\exists b_1 Compl(b_1))\ R(a, a_1) \wedge R(b, b_1) \wedge \\
 & & (\exists a_2 C(a_2))(\exists b_2 C(b_2))\ R(a_1, a_2) \wedge R(b_1, b_2) \wedge \\
 & & (\exists a_3 B(a_3))(\exists b_3 B(b_3))\ R(a_2, a_3) \wedge R(b_2, b_3) \wedge \\
 & & (\exists a_4 Compl(a_4))(\exists b_4 Compl(b_4))\ R(a_3, a_4) \wedge R(b_3, b_4) \wedge R(a_4, b_4)
\end{array}
$$

We set $\Psi' = \exists a \exists b \exists c \exists d (\forall x A(x)) \quad \bigwedge_{i=0}^{7} \Phi(a, b, c, d) \wedge \psi^{\Delta}(a, b, c, d)$. The rest of the proof follows easily. $\square$

4.4 A new characterization of nondeterministic linear time

Our aim here is to give a characterization of sets of structures decidable in linear time by the class of formulas we have examined all along this paper, that is, second order formulas with only one universal first-order quantifier and whose second order part is restricted to one binary relation symbol of bounded outdegree. But first of all, we have to extract a good definition of linear time.

It's well known that this notion is particularly hard to formalize. Roughly speaking, a machine is said to run in linear time if it performs $O(n)$ instructions with an input of size n. This intuitive definition raised a first problem which concerns the range of the authorized instructions (successor, addition, multiplication, concatenation, ...) together with the cost of each of them (uniform or logarithmic). A second problem, as crucial as the first one, is the encoding of the input. To keep a model realistic, it is important to avoid padding of the input. This can be illustrated by the following example. A graph $G = \langle V, E \rangle$ can be seen as an input of a machine in (at least) two ways: as the list of its vertices and edges, as its adjacency matrix. With unary notation the first encoding gives an input of size $|V| \times |E|$, the second one $|V|^2$. The significance of linear time is then different in the two cases (for a more detailed discussion of linear time, the reader is invited to consult [Gra94b, Gra94a, Gra90b, Sch78])

The class $NLIN$ defined by Grandjean (see [GO94]) will be our reference here. This class is very robust and powerful (taking into account all the remarks above) and seems to be close of "intuitive" nondeterministic linear time. Models of computation are NRAMs (Nondeterministic Random Access Machine) and a (completely informal) definition with functions as input is:

Definition 4.8 *Let $\mathcal{F}$ be a set of functions.*
$\mathcal{F} \in NLIN$ if there exists an NRAM $\mathcal{R}$ such that

- *$\mathcal{R}$ only uses arithmetic operations $Succ: x \mapsto x+1$ and $Pred: x \mapsto x-1$.*
- *Let $f: m \mapsto m$ be the input. Then, at the beginning of its computation, register R_0 contains m, all the registers $R_1, \ldots, R_m$ respectively contain $w_0, w_1, \ldots, w_{m-1}$ where $w_i = f(i)$ and the other registers R_i $(i > m)$ contain zero..*
- *$\mathcal{R}$ recognizes $\mathcal{F}$ in time $O(m)$.*

Remark - This definition can be generalized to t-tuples of functions $(f_0, f_1, \ldots, f_{t-1})$ (where t is fixed, i.e. does not depend on the input) on the same domain m. This time, at the beginning of the computation R_0 contain m and each register R_{jt+i+1} contains, say, $f_j(i)$.

Notice - $NLIN$'s definition deals with functions as input. An input file is a binary word and any data structure stored in the memory of a computer can be seen as a function: precisely, if max is the maximum integer used in addresses and contents of registers, then the stored input is identified with the function $f: m \mapsto m$ where $m = max + 1$ and where $f(i)$ is equal to the contents of register i.

From now on, it will then be more convenient to consider structures as functional structures. As an example, and following an idea of Courcelle (see [Cou96]) each graph $G = \langle V, E \rangle$ is seen as a structure (identified to G) $G = \langle Dom_V \cup Dom_E, f_1, f_2 \rangle$ where

- $Dom_V = V$

- $Dom_V \cap Dom_E = \emptyset$
- there is a bijective correspondence between E of G and Dom_E which associates a point $e_{x,y}$ to each pair $E(x,y)$.
- f_1, f_2 are unary functions $(Dom_V \cup Dom_E) \mapsto (Dom_V \cup Dom_E)$ defined by:
  $\forall e_{x,y} \in Dom_E \quad f_1(e_{x,y}) = x$ and $f_2(e_{x,y}) = y$
  $\forall x \in Dom_V \quad f_1(x) = x$ and $f_2(x) = x$
  Notice that $\forall x \in Dom_V \cup Dom_E \quad x \in Dom_V \iff f_1(x) = x$

A generalization of this definition to all structures is easy. Rephrasing definition 4.8 a set $\mathcal{P}$ of graphs is in $NLIN$ if and only if there exists an NRAM $\mathcal{R}$ which recognizes the set of structures $G = \langle Dom_V \cup Dom_E, f_1, f_2 \rangle$ of $\mathcal{P}$ in time $O(|Dom_V| + |Dom_E|)$ where the input of $\mathcal{R}$ is any standard encoding of G (e.g $Dom_V = \{0, 1, \ldots, n-1\}$, $Dom_E = \{n, n+1, \ldots, n+e-1\}$ and the initial value of R_0 is $n+e$ and $R_1, R_2, \ldots, R_{n+e}$ respectively contain $f_1(0), f_1(1), \ldots, f_1(n+e-1)$ and $R_{n+e+1}, R_{n+e+2}, \ldots, R_{2n+2e}$ respectively contain $f_2(0), f_2(1), \ldots, f_2(n+e-1)$).

Let $g_1, \ldots, g_p$ be unary function symbols. The theorem below is an easy extension of a theorem in [GO94].

Theorem 4.9 *Let $\mathcal{F}$ be a set of t-tuples of functions. $\mathcal{F}$ is in $NLIN$ if and only if there exists a quantifier-free formula Ψ with one variable x, on signature $\{f_1, \ldots, f_t, g_1, \ldots, g_p, <\}$ such that for each $m > 1$ and each $(f_1, f_2, \ldots, f_t)$ where $f_i : m \mapsto m$ $(1 \leq i \leq t)$:*

$$(f_1, f_2, \ldots, f_t) \in \mathcal{F} \iff \langle m, f_1, \ldots, f_t, < \rangle \models \exists g_1 \ldots \exists g_p \; \forall x \Psi(x, \overline{f}, \overline{g}, <)$$

This result and theorem 4.1 allow us to state a new characterization of $NLIN$:

Theorem 4.10 *Let $\mathcal{F}$ be a set of t-tuples of functions. $\mathcal{F}$ is in $NLIN$ if and only if there exists an integer p and a quantifier-free formula $\Psi(x, y_1, \ldots, y_k, z_1, \ldots, z_h)$, on signature $\{f_1, \ldots, f_t, R, <\}$ where R is a p–Deg^+ binary relation symbol such that for each $m > 1$ and each $(f_1, f_2, \ldots, f_t)$ where $f_i : m \mapsto m$ $(1 \leq i \leq t)$:*

$$(f_1, f_2, \ldots, f_t) \in \mathcal{F} \iff \langle m, f_1, \ldots, f_t, < \rangle \models \exists R \; \exists \overline{y} \forall x \exists \overline{z} \; \Psi(x, \overline{y}, \overline{z}, \overline{f}, R, <)$$

It is proved in [Gra90c] that linear orders are definable by unary functions with only one first-order variable. So,

Corollary 4.11 *If $\mathcal{F}$ is closed under isomorphism then the characterization remains true without the "built-in" linear order $<$.*

Chapitre 5

Hiérarchies

This chapter is divided into two distincts parts

1. Let us recall the main result of chapter 2:

$$Func_1^{\omega}(\mathcal{S}) \subseteq BIN(\mathcal{S}).$$

   In the first part of this chapter, we show that the inclusion is strict if $\mathcal{S}$ contains at least one binary relation symbol E_2. More precisely the following class of graphs $P_2 = \{G_2 = \langle V_2, E_2 \rangle : \ |E_2| \text{ is even } \}$ can be defined with only one binary relation as the only second-order resources but not with any number of unary functions.

2. We establish a new transfer lemma for spectra. Let S be a set of integers and $S^k = \{n^k : \ n \in S\}$. Then, for all k, d, d' s.t. $k \geq 2$, $d \geq d' \geq 1$:

$$S \in Func_{kd'}^{\omega}(\exists^* \forall^{kd} \exists^*) \iff S^k \in Func_{d'}^{\omega}(\exists^* \forall^{d} \exists^*).$$

   Using well known characterizations of non-deterministic polynomial time bounded RAMs, this result permits us to show that there is a strict hierarchy on spectra based both on arities of predicates and on the number of universal quantifiers. i.e. for all $d \geq d' \geq 1$

$$Func_{d'}^{\omega}(d\forall) \subset Func_{d'+1}^{\omega}((d+1)\forall),$$

   and for $d \geq d' + 1 \geq 2$

$$Func_{d'}^{\omega}(d\forall) \subset Rel_{d'+1}^{\omega}((d+1)\forall),$$

Ce chapitre se décompose en deux parties bien distinctes. Dans la première, on donne

des résultats de définissabilité (et de non-définisabilité) dans les logiques qui nous ont intéréssés jusqu'à maintenant, à savoir le second-ordre existentiel dont les quantifications au second-ordre sont restreintes à un nombre quelconque de fonctions unaires d'une part, à une seule relation binaire d'autre part. La seconde partie, présentera un nouveau théorème de transfert, sur les spectres cette fois, et un résultat de hiérarchie en découlant.

5.1 Sur la parité du nombre d'arêtes dans un graphe

Dans le chapitre 2, on a démontré, en quelque sorte, que le pouvoir d'expression d'une seule relation binaire est au moins aussi fort que celui d'un nombre quelconque de fonctions unaires. Ceci se traduisait, avec nos notations, par l'inclusion suivante:

$$Func_1^{\omega}(\mathcal{S}) \subseteq BIN^{\cdot}(\mathcal{S})$$

A partir de là, une question qui se pose naturellement, est de savoir s'il existe des signatures particulieres $\mathcal{S}$ pour lesqueslles l'inclusion est stricte. Si une réponse semble pour l'instant hors d'atteinte dans le cas des spectres (i.e. pour $\mathcal{S} = \emptyset$), il n'en est pas de même, comme nous allons le voir, des que $\mathcal{S}$ contient au moins un symbole de relation binaire.

Dans ce qui suit, et comme d'habitude, les f_i (resp. R_i, E_i) désignent des symboles de fonction (resp. de relation) d'arité i. On va s'intéresser ici aux propriétés sur les graphes.

Soit $P_2 = \{G_2 = \langle V_2, E_2\rangle : |E_2| \text{ est pair }\}$. On montre:

Proposition 5.1

$$P_2 \in BIN(E_2)$$
$$P_2 \notin Func_1^{\omega}(E_2)$$

5.1.1 La parité n'est pas définissable par des fonctions unaires

Dans cette sous-section, les résultats démontrés par Ajtai dans [Ajt83], interviennent de manière essentielle. Soient P_2' et P_4 les deux ensembles suivants:

$$P_2' = \{G_2 = \langle V_2, E_2\rangle : |V_2| \text{ est un carré, } |E_2| \text{ est pair }\},$$
$$P_4 = \{G_4 = \langle V_4, E_4\rangle : |E_4| \text{ est pair }\},$$

on montre :

Proposition 5.2 $P_2 \notin Func_1^{\omega}(E_2)$

Preuve

Fait 1 *Si* $P_2' \in Func_1^{\omega}(E_2)$ *alors* $P_4 \in Func_2^{\omega}(E_4)$

Bien que ce résultat soit intuitivement assez évident, nous allons en donner une preuve détaillée.

Preuve Soit Ψ une formule de la forme

$$\exists f_1^1 \ldots \exists f_1^k \quad \Phi(f_1^1, \ldots, f_1^k, E_2)$$

(où Φ est du premier ordre) définissant P_2'. On supposera que dans φ toutes les formules atomiques sont de la forme: $t_1 = t_2$ ou $f_1^i(t_1) = t_2$ ou encore $E_2(t_1, t_2)$ où t_1 et t_2 sont des termes (pas de composition de fonctions). On va exhiber une formule Ψ' de signature adéquate qui va paraphraser Ψ.

Entre P_2' et P_4, on établit une correspondance biunivoque *code* telle que:

$$G_2 \in P_2' \longmapsto code(G_2) = G_4 \in P_4$$

Informellement, tout sommet $x < n^2$ va être codé par un couple $i, j < n$ tel que $x = ni + j$ et toute arête $E_2(x, y)$ par un quadruplet $E(i, j, i', j')$ avec $x = ni + j$ et $y = ni' + j'$.

De $\Phi = Q_1 x_1 \ldots Q_h x_h \quad \varphi(x_1, \ldots, x_h)$ on obtient une formule

$$\Phi' = Q_1 x_1^1 Q_1 x_1^2 \ldots Q_h x_h^1 Q_h x_h^2 \quad \varphi((x_1^1, x_1^2), \ldots, (x_h^1, x_h^2))$$

en effectuant les substitutions suivantes:

- Au premier ordre, chaque quantification $\forall x$ va être dédoublée dans Φ' en $\forall x_1 \forall x_2$. De même, chaque $\exists x$ devient $\exists x_1 \exists x_2$.
- A chaque symbole de fonction unaire f_1^i de Φ, on associe, dans Φ', deux symboles de fonction binaire f_2^{2i} et f_2^{2i+1}:
  $f_1^i(x) = y$ sera remplacée par $f_2^{2i}(x_1, x_2) = y_1 \wedge f_2^{2i+1}(x_1, x_2) = y_2$.
- A chaque symbole E_2 on asocie E_4 :
  $E_2(x, y)$ est remplacée $E_4(x_1, x_2, y_1, y_2)$
- Toute sous-formule égalitaire $x = y$ est remplacée par $x_1 = y_1 \wedge x_2 = y_2$.

Soit $G_2 \models \Phi$. Par définition, $G_2 \in P_2'$. Il existe donc un entier n tel que $|V_2| = n^2$. Soit V_4 un ensemble de cardinalité n. On établit une correspondance bijective implicite g de V_2 vers $V_4 \times V_4$:

$$g : a \mapsto (a_1, a_2)$$

On définit une structure $G_4 = \langle V_4, E_4 \rangle$ comme suit:

$$(G_2, a, b) \models E_2(x, y) \iff (G_4, g(a), g(b)) \models E_4(x_1, x_2, y_1, y_2)$$

$$(G_2, a, b) \models f_1^i(x) = y \iff (G_4, g(a), g(b)) \models f_2^{2i}(x_1, x_2) = y_1 \wedge f_2^{2i+1}(x_1, x_2) = y_2.$$

De même pour l'égalité. Clairement G_4 est un modèle de Φ'. De plus $|E_2| = |E_4|$. Donc, $G_4 \in P_4$. la réciproque est similaire. □

Fait 2 $Func_2^\omega(E_4) \subseteq Rel_3^\omega(E_4)$

Preuve On simule chaque f_2^i (fonction binaire) par une relation ternaire:

$$f_2^i(x,y) = z \text{ devient } R_3^i(x,y,z).$$

On ajoute une contrainte disant que chaque R_3^i est une fonction binaire:

$$\forall x \forall y \exists ! z \quad R_3^i(x,y,z). \ \square$$

D'après les deux résultats précédents, si $P_2' \in Func_1^\omega(E_2)$ alors $P_4 \in Rel_3^\omega(E_4)$. Or, d'après un résultat d'Ajtai ([Ajt83]), cette dernière relation n'est pas possible. Donc $P_2' \notin Func_1^\omega(E_2)$. On a encore:

Fait 3 $C = \{G_2 = \langle V_2, E_2 \rangle : |V_2| \textit{ est un carré } \} \in Func_1^\omega(E_2)$.

Preuve C peut se définir par:

il existe un sous ensemble U du domaine V_2 et deux fonctions unaires f, g tels que,

$$(f,g) : V_2 \longrightarrow U \times U \textit{ soit une bijéction.}$$

Ce qui s'écrit très facilement.$\square$

La classe $Func_1^\omega(E_2)$ étant de plus close par intersection, on a:

$$P_2 = \{G_2 = \langle V_2, E_2 \rangle : |E_2| \text{ est pair } \} \notin Func_1^\omega(E_2),$$

car sinon on aurait $P_2' = P_2 \cap C \in Func_1^\omega(E_2)$, ce qui conclut la preuve de la proposition. $\square$

5.1.2 La parité est définissable à l'aide d'une seule relation binaire

Dans la suite R et E désignent des symboles de relation binaire. On montre la proposition suivante:

Proposition 5.3 $P_2 \in BIN(E)$. *Plus précisement, il existe une formule existentielle du second ordre $\Psi = \exists R \ \Phi(R,E)$ telle que, pour tout graphe fini $\mathcal{G} = \langle V, E \rangle$:*

$$\mathcal{G} \models \Psi \iff |E| \textit{ est pair}$$

On supposera que $\mathcal{G} = \langle V, E \rangle$ est un graphe orienté. La parité du nombre d'arêtes d'un graphe symétrique est aussi définissable par une formule similaire à celle que nous allons donner (la preuve étant même plus facile).

Preuve Nous allons définir le plus économiquement possible, à l'aide de R, un ordre de parcours des éléments de V (que l'on étendra aux couples de $V \times V$). Puis, en utilisant cet ordre de parcours et en éliminant d'entrée, deux par deux, certains arcs du processus de comptage (arcs verifiants une condition que nous donnerons), nous évaluerons la parité du nombre d'arcs de $\mathcal{G}$.

1. L'ordre de parcours

On partitionne le domaine V en deux sous-ensembles de même cardinalité C_1 et C_2. Si la taille du domaine n'est pas paire, au plus un élément ne sera ni dans C_1, ni dans C_2.

Soient c_1 et c_2 deux éléments distincts du domaine. On pose $C_i(x)$ pour $R(x,c_i) \wedge x \neq c_1 \wedge x \neq c_2$. La formule Φ_0, conjonction des quatre formules qui suivent, résume ce que nous venons de dire:

$\exists c_1 \exists c_2 \forall x \quad \neg C_1(x) \vee \neg C_2(x)$

$\forall x \forall x' \quad x = x' \vee C_1(x) \vee C_1(x') \vee C_2(x) \vee C_2(x') \vee$
$x = c_1 \vee x = c_2 \vee x' = c_1 \vee x' = c_2$

$(\forall x C_1(x))(\exists y C_2(y)) \quad R(x,y) \wedge$
$(\forall x' C_1(x) \wedge x \neq x') \quad \neg R(x',y)$

$(\forall y C_2(y))(\exists x C_1(x)) \quad R(x,y) \wedge$
$(\forall y'\ C_2(y') \wedge y \neq y') \quad \neg R(x,y')$

Les deux dernières formules imposent à R d'être une correspondance bijective de C_1 vers C_2.

On appelle Φ_1 la formule disant que R restreint à C_1 est un ordre total. On obtient alors un ordre sur C_2 induit par celui sur C_1 et par la correspondance bijective de C_1 vers C_2. On peut donc définir un ordre de parcours des sommets du graphe $\mathcal{G}$ comme suit:

$$c_1 < c_2 < C_1 < C_2 (< c).$$

c est l'éventuel élément du domaine qui n'est ni dans C_1 ni dans C_2.
Dans la suite, on posera $x < y$ pour:

$(x = c_1 \wedge y \neq c_1) \vee$
$(x = c_2 \wedge y \neq c_1, c_2) \vee$
$(C_1(x) \wedge C_1(y) \wedge R(x,y)) \vee$
$(C_1(x) \wedge C_2(y)) \vee$
$(C_2(x) \wedge C_2(y) \wedge ((\forall x' C_1(x'))(\forall y' C_1(y')) \quad R(x',x) \wedge R(y',y) \rightarrow R(x',y')) \vee$
$(x = c_1 \vee x = c_2 \vee C_1(x) \vee C_2(x)) \wedge (y \neq c_1 \wedge y \neq c_2 \wedge \neg C_1(y) \wedge \neg C_2(y)).$

On étend facilement cet ordre de parcours sur les sommets de $\mathcal{G}$ à un ordre de parcours sur les couples de sommets de $\mathcal{G}$:

$$(x,y) < (x',y') \iff x < x' \textit{ ou } (x = x' \textit{ et } y < y')$$

2. Le comptage

Le fait qu'il y ait déja des contraintes sur R (ordre total sur C_1, ...) va nous obliger à prendre en compte certains arcs $E(x,y)$ de manière détournée.

De plus, dans le parcours du graphe, on s'abstiendra de compter certains arcs de $\mathcal{G}$, arcs que l'on identifiera au moyen de la formule Δ (à deux variables libres) suivante:

$$\Delta(x,y) = \left\{ \begin{array}{l} (E(x,y) \wedge E(y,x) \wedge x \neq y) \vee \\ (x = y \wedge C_1(x) \wedge (\forall x'(C_2(x') \wedge R(x,x') \rightarrow E(x,x) \wedge E(x',x'))) \vee \\ (x = y \wedge C_2(x) \wedge (\forall x'(C_1(x') \wedge R(x',x) \rightarrow E(x,x) \wedge E(x',x'))). \end{array} \right.$$

En fait, Δ regroupe implicitement deux par deux certains arcs de $\mathcal{G}$ (principalement ceux du type $E(x,y), E(y,x)$ pour tout couple (x,y) donné). Oublier ces arcs dans le processus de comptage ne change évidemment rien à la parité de $|E|$.
Posons $\nabla(x,y) = \neg\Delta(x,y) \wedge E(x,y)$

La (méta)formule Φ_2 d'évaluation de la parité du nombre d'arcs de E va être[1] :

$$\forall x \forall y \quad \Big[\nabla(x,y) \wedge [\forall x' \forall y' \quad ((x',y') < (x,y) \rightarrow \neg\nabla(x',y'))] \longrightarrow R(f(x,y))\Big] \wedge$$

$$\forall x \forall y \forall x' \forall y' \quad \Big[((x,y) < (x',y')) \wedge \nabla(x,y) \wedge \nabla(x',y') \wedge [\forall x'' \forall y'' \quad ((x,y) < (x'',y'') < (x',y') \rightarrow \neg\nabla(x'',y''))] \longrightarrow [R(f(x,y)) \leftrightarrow \neg R(f(x',y'))]\Big] \wedge$$

$$\forall x \forall y \quad \Big[\nabla(x,y) \wedge [\forall x'' \forall y'' \quad ((x,y) < (x'',y'') \rightarrow \neg\nabla(x'',y''))] \longrightarrow \neg R(f(x,y))\Big],$$

où la fonction f à deux arguments et à deux valeurs est définie comme suit:

- $x = c_1, \forall y \quad \left\{ \begin{array}{l} f(x,y) = (x,y) \\ f(y,x) = (x,y) \end{array} \right.$
- $x = c_2, \forall y \neq c_1 \quad \left\{ \begin{array}{l} f(x,y) = (x,y) \\ f(y,x) = (x,y) \end{array} \right.$
- $x \in C_1, y \in C_1 \quad f(x,y) = \left\{ \begin{array}{l} (x_2,y_2)\ si\ x < y \\ (y_2,x_2)\ sinon \end{array} \right.$

  où (x_2,y_2) est le seul couple de $C_2 \times C_2$ vérifiant $R(x,x_2)$ et $R(y,y_2)$.
- $x \in C_1, y \in C_2 \quad \left\{ \begin{array}{l} f(x,y) = (y,x) \\ f(y,x) = (y,x) \end{array} \right.$
- $x \in C_2, y \in C_2 \quad f(x,y) = \left\{ \begin{array}{l} (y,x)\ si\ x_1 < y_1 \\ (x,y)\ sinon \end{array} \right.$

  où (x_1,y_1) est le seul couple de $C_1 \times C_1$ vérifiant $R(x_1,x)$ et $R(y_1,y)$.
- $x = c, \forall y \quad \left\{ \begin{array}{l} f(x,y) = (y,x) \\ f(y,x) = (y,x) \end{array} \right.$

1. la méthode est la suivante : on colorie (par R) le couple image par la fonction f d'un couple (x,y) sur deux vérifiant ∇. Si le nombre d'arêtes est pair alors la couleur (de l'image par f) du premier et du dernier couple doit être la même.

Bien entendu, le symbole f n'est qu'une (méta)notation. Il permet d'éviter une écriture in-extenso fastidieuse de Φ_2.

La définition de f implique:

$$\forall(x,y) \quad f(x,y) = f(y,x) \text{ et}$$
$$\forall(x',y') \neq (x,y),(y,x) \quad f(x',y') \neq f(x,y).$$

Or, on ne prend pas en compte les couples (x,y) vérifiants à la fois $E(x,y)$ et $E(y,x)$ (cf. Δ). Si on appelle $\nabla = \{(x,y) : \nabla(x,y)\}$, on voit donc que f restreinte à ∇ est injective. Ce qui implique qu'au cours du processus de comptage, deux couples distincts n'auront jamais la même image par f.

Le dernier danger éventuel de ce codage pourrait être l'émergence de contradictions du type $R(x,y)$ et $\neg R(x,y)$ dues au double rôle de R: définition d'un ordre de parcours et évaluation de la parité du nombre d'arcs de E. Un examen cas par cas montre qu'il n'en est rien.

La formule Ψ recherchée est donc:

$$\Psi = \exists R \ \Phi_0(R) \wedge \Phi_1(R) \wedge \Phi_2(R,E).$$

5.2 Un lemme de transfert

Dans cette section les formules considérées seront sous forme prénexe. De plus, les quantificateurs universels présents dans le préfixe d'une formule seront regroupés en "blocs", i.e dans la suite toute formule aura un préfixe de la forme:

$$\exists \overline{y} \forall x_1 \forall x_2 \ldots \forall x_d \exists \overline{z}.$$

Notre intention est de présenter un nouveau théorème de transfert sur les spectres prenant en considération aussi bien l'arité des prédicats que les ressources en quantificateurs universels. Soient k, d, d' trois entiers vérifiants $k \geq 2$, $d \geq d' \geq 1$. On va principalement démontrer que si S est spectre d'une formule du premier ordre φ de préfixe contenant un bloc de dk quantificateurs $\forall$ et de signature restreinte à un nombre quelconque de symboles de relations ou fonctions d'arités au plus $d'k$, alors il existe une formule φ^* de préfixe contenant un bloc de d quantificateurs $\forall$ et de signature restreinte cette fois à des symboles d'arités au plus d' dont $S^k = \{n^k : n \in S\}$ est le spectre. Ce résultat se dessinera au fur et à mesure des propositions qui vont suivre.

Le cas $d = 1$ pose quelques problèmes particuliers (qui peuvent d'ailleurs être résolus par un argument de complexité). Toutefois, par souci d'uniformisation, nous allons présenter une preuve générale. Pour ce faire, deux résultats dus à E. Grandjean ([Gra90c]) vont être utiliser.

Soit $\mathcal{S}$ une signature contenant:

- $U, ORDRE_U, U_1, U_2, \ldots, U_{k-2}$ des symboles de relation unaire,
- les quatres listes suivantes de symboles de fonction unaire:
  - f_1, f_2,
  - $S_U, S_{U_1}, S_{U_2}, \ldots, S_{U_{k-2}}$,
  - $\pi_1, \pi_2, \ldots, \pi_{k-1}$,
  - $\pi^1, \pi^2, \ldots, \pi^{k-1}$.

Pour chacun des symboles A de relation unaire (excepté $ORDRE_U$) deux constantes max_A et min_A sont introduites.

Définition 5.4 *On dit que S est une relation successeur sur un ensemble A si et seulement si:*

1. *S est une permutation des éléments de A.*
2. *S n'a qu'un seul cycle.*

Proposition 5.5 (Grandjean) *Il existe une formule du premier ordre*

$$SUCC(S_U)$$

de signature $\mathcal{S}$ et de préfixe $\forall\exists$ telle que, pour toute structure $\mathcal{M} = \langle Dom, \mathcal{S}^{\mathcal{M}}\rangle$:

$$\mathcal{M} \models SUCC(S_U) \;\Rightarrow\; S_U \text{ est une relation successeur sur } U$$

Preuve. Dans le chapitre 4 on a déja démontré un résultat similaire (quoique dans un contexte différent). Ce qui suit est, à peu de chose près, la preuve originale. $SUCC(S_U)$ est la conjonction des six formules suivantes:

$\varphi_1 : \forall x\ [U(x) \rightarrow U(S_U(x))]$

$\varphi_2 : \forall x\ [U(x) \rightarrow \exists y\ (U(y) \wedge S_U(y) = x)]$

$\varphi_3 : U(min_U) \wedge U(max_U) \wedge S_U(max_U) = min_U \wedge max_U \neq min_U$

$\varphi_4 : \forall x\ [(U(x) \wedge x \neq max_U) \rightarrow \exists t\ [(f_1(t), f_2(t)) = (x, S_U(x)) \wedge ORDRE_U(t)]]$

$\varphi_5 : \forall t\ [(ORDRE_U(t) \wedge f_1(t) \neq max_U) \rightarrow \exists t'\ [(f_1(t'), f_2(t')) = (f_1(t), S_U(f_2(t))) \wedge ORDRE_U(t')]]$

$\varphi_6 : \forall t\ [f_1(t) = f_2(t) \rightarrow \neg ORDRE_U(t)]$

De $\varphi_1 \wedge \varphi_2$, on peut déduire que la fonction S_U restreinte à U est une permutation de U. Supposons que S_U a un cycle C distinct de celui comprenant min_U et max_U. $\varphi_4 \wedge \varphi_5$ induisent que pour tout $x \in U$ on a:

$$\exists t \in ORDRE_U\ (f_1(t), f_2(t)) = (x, S_U^i(x))$$

pour tout i tel que $max_U \notin \{x, S_U(x), \ldots, S_U^{i-1}(x)\}$.

Soient $e \in C$, et $i = card(C)$, alors il existe $t \in ORDRE_U$ tel que $(f_1(t), f_2(t)) = (e, S_U^i(e)) = (e, e)$. Ce qui contredit φ_6. $\square$

Remarque. Les constantes min_A et max_A dans la proposition précédente peuvent évidemment être existentiellement définies.

Proposition 5.6 (Grandjean) *Il existe une formule du premier ordre*

$$PROJ((\pi_{k-1}, \pi^{k-1}), U_1, (U, U))$$

de signature $\mathcal{S}$ et de préfixe $\forall\exists$ telle que, pour toute structure $\mathcal{M} = \langle Dom, \mathcal{S}^{\mathcal{M}}\rangle$ satisfaisant $SUCC(S_U)$:

$$\mathcal{M} \models PROJ((\pi_{k-1}, \pi^{k-1}), U_1, (U, U)) \Rightarrow \begin{cases} (\pi_{k-1}, \pi^{k-1}) : U_1 \longmapsto U \times U \text{ est une bijection,} \\ S_{U_1} \text{ est une relation successeur sur } U_1. \\ |U_1| = |U|^2 \end{cases}$$

Preuve. $PROJ((\pi_{k-1}, \pi^{k-1}), U_1, (U,U))$ est la conjonction des six formules suivantes:

$\psi_1 : \forall x\ [U_1(x) \rightarrow U_1(S_{U_1})]$

$\psi_2 : \forall x\ [U_1(x) \rightarrow \exists y\ [U_1(y) \wedge S_{U_1}(y) = x]$

$\psi_3 : U_1(min_{U_1}) \wedge U_1(max_{U_1}) \wedge S_{U_1}(max_{U_1}) = min_{U_1} \wedge max_{U_1} \neq min_{U_1}$

$\psi_4 : \forall x\ [U_1(x) \rightarrow U(\pi_{k-1}(x)) \wedge U(\pi^{k-1}(x))] \wedge [(\pi_{k-1}, \pi^{k-1})(x) = (min_U, min_U) \leftrightarrow x = min_{U_1}]$

$\psi_5 : \forall x \neq max_{U_1}\ [U_1(x) \wedge \pi^{k-1}(x) \neq max_U \rightarrow (\pi_{k-1}, \pi^{k-1})(S_{U_1}(x)) = (\pi_{k-1}(x), S_U(\pi^{k-1}(x)))]$

$\psi_6 : \forall x \neq max_{U_1}\ [U_1(x) \wedge \pi_{k-1}(x) \neq \max_U \wedge \pi^{k-1}(x) = max_U \rightarrow (\pi_{k-1}, \pi^{k-1})(S_{U_1}(x)) = (S_U(\pi_{k-1}(x)), min_U)]$

Soient $\mathcal{M}$ une structure satisfaisant $SUCC(S_U) \wedge PROJ((\pi_{k-1}, \pi^{k-1}), U_1, (U,U))$. S_U est une fonction successeur sur U. De $\psi_1 \wedge \psi_2$ on peut déduire que S_{U_1} est une permutation de U_1. Par un argument similaire à celui de la propositon précédente, on peut conclure que S_{U_1} n'a qu'un seul cycle.

On montre facilement par induction que (π_{k-1}, π^{k-1}) est une bijection de U_1 vers $U \times U$. □

Proposition 5.7 *Il existe une formule du premier ordre*

$$PUISS_k$$

de signature $\mathcal{S}$ et de préfixe $\forall\exists$ telle que pout toute structure $\mathcal{M} = \langle Dom, \mathcal{S}^{\mathcal{M}} \rangle$:

si $\mathcal{M} \models PUISS_k$ alors:

1. $\left\{ \begin{array}{l} (\pi_1, \pi^1) : Dom \longmapsto U \times U_{k-2}, \\ (\pi_2, \pi^2) : U_{k-2} \longmapsto U \times U_{k-3}, \\ \vdots \\ (\pi_i, \pi^i) : U_{k-i} \longmapsto U \times U_{k-i-1}, \\ \vdots \\ (\pi_{k-1}, \pi^{k-1}) : U_1 \longmapsto U \times U, \end{array} \right.$ *sont des bijections,*

2. *pour tout $i \leq k-2$, S_{U_i} est une relation successeur sur U_i,*

3. $|Dom| = |U|^k$

Preuve. $PUISS_k$ est la conjonction de:

$SUCC(S_U)$,

$PROJ((\pi_{k-1}, \pi^{k-1}), U_1, (U, U))$
$PROJ((\pi_{k-2}, \pi^{k-2}), U_2, (U, U_1))$
$\vdots$
$PROJ((\pi_i, \pi^i), U_{k-i}, (U, U_{k-i-1}))$
$\vdots$
$PROJ((\pi_2, \pi^2), U_{k-2}, (U, U_{k-3}))$
$PROJ((\pi_1, \pi^1), Dom, (U, U_{k-2}))$

Si $\mathcal{M}$ est un modèle de $PUISS_k$ alors, en vertu de la proposition précédente, S_{U_1} est une fonction successeur sur U_1 et (π_{k-1}, π^{k-1}) est bien une bijection de U_1 vers $U \times U$. En procédant par induction, on obtient, pas à pas, le résultat désiré. □

Remarque. Sans l'aide des deux premières propositions, il aurait fallu une ressource en quantificateur de l'ordre de $\forall\forall\exists$ [2] (soit un quantificateur $\forall$ de plus) pour écrire une formule équivalente à $PUISS_k$. Le cas d'un seul $\forall$ se résolvant alors, comme il est dit plus haut, par un argument de complexité.

Dans la suite, la fonction π^{k-1} sera parfois désignée par le (nouveau) symbole π_k. Soit $\mathcal{M}$ un modèle de $PUISS_k$. A tout élément a du domaine de $\mathcal{M}$, on peut faire correspondre un unique k-uplet $(a_1, a_2, \ldots, a_k)$ défini comme suit (cf. figure 5.1):

$$a_1 = \pi_1(a), \ldots, a_i = \pi^1\pi^2 \ldots \pi^{i-1}\pi_i(a), \ldots, a_k = \pi^1\pi^2 \ldots \pi^{k-1}\pi_k(a).$$

Soit S un ensemble d'entiers quelconque et $S^k = \{n^k : \ n \in S\}$.

Proposition 5.8 *$\forall k \geq 1$, $\forall d, d'$, $d \geq d' \geq 1$:*

$$S \in Func^{\omega}_{kd'}(\exists^*\forall^{kd}\exists^*) \Rightarrow S^k \in Func^{\omega}_{d'}(\exists^*\forall^{d}\exists^*)$$

Preuve. Soit Φ la formule suivante:

$$\exists\overline{y}\underbrace{\forall x_1 \ldots \forall x_k}_{\text{bloc } 1}\underbrace{\forall x_{k+1} \ldots \forall x_{2k}}_{\text{bloc } 2} \ldots \underbrace{\forall x_{(d-1)k+1} \ldots \forall x_{dk}}_{\text{bloc } d'} \exists\overline{z} \quad \phi(\overline{y}, \overline{x}, \overline{z}, \overline{f_{kd'}})$$

où chaque $f_{kd'}$ est un symbole de fonction d'arité kd'. On va transformer Φ en une nouvelle formule Φ' de préfixe contenant seulement d quantificateurs universels et de signature restreinte à des symboles de fonctions d'arité d. I.e. Φ' va être de la forme:

$$\exists\overline{y}'\forall x_1 \forall x_2 \ldots \forall x_d \exists\overline{z}' \quad \phi'(\overline{y}', \overline{x}, \overline{z}', \overline{f_{d'}}).$$

2. Pour exprimer le fait que chaque application (π_i, π^i) est une bijection de U_{k-i} vers $U \times U_{k-i-1}$

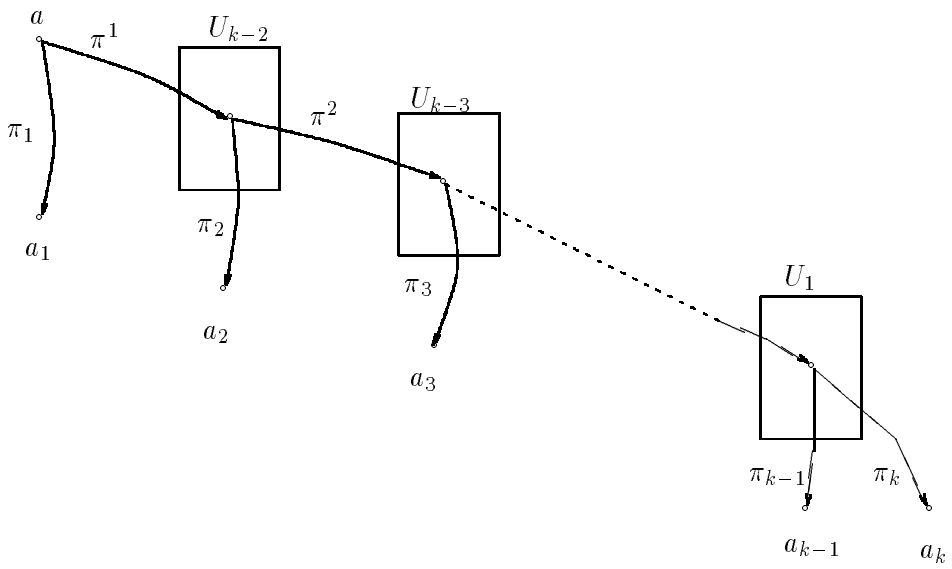

FIG. 5.1 - *représentation de a*

Soit S le spectre de Φ (i.e. l'ensemble formé des cardinalités des modèles de Φ). La formule Φ' obtenue aura pour spectre l'ensemble S^k. Intuitivement chaque variable x_i de Φ' vaudra pour un bloc entier (le i^{eme}) de variables universellement quantifiées de Φ.

Φ' va s'écrire comme la conjonction de $PUISS_k$ (de la prop. 5.7) et d'une formule Φ^Δ obtenue de Φ comme suit:

- toutes les quantifications existentielles sont relativisées à U. I.e. Chaque $\exists y$ devient $\exists y U(y)$. En clair, on va maintenant raisonner dans un univers de taille $|U|^k$.

- pour chaque fonction kd'-aire $f_{kd'}$ on introduit une nouvelle fonction d'-aire $f_{d'}$. Soit $f_{kd'}(t_1, t_2, \ldots, t_{kd'}) = t_{kd'+1}$ une formule atomique de Φ, chaque t_i pouvant être universellement ou existentiellement quantifiées. Cette formule atomique va être remplacée dans Φ' par

$$\exists s_1 \ldots \exists s_{d'} \quad f_{d'}(s_1, \ldots, s_{d'}) = \begin{cases} t_{kd'+1} & \text{si } t_{kd'+1} \text{ est une variable existentielle (de } \Phi) \\ \pi^1\pi^2 \ldots \pi^{h-1}\pi_h(x_j) & \text{si } t_{kd'+1} \text{ est une var. universelle apparaissant en } h^{eme} \text{ position dans le } j^{eme} \text{ bloc univ. de } \Phi \end{cases}$$

avec, pour tout $i = 1, \ldots, d'$, pour tout $l = 1, \ldots, k$,

$$\pi^1\pi^2\ldots\pi^{l-1}\pi_l(s_i) = \begin{cases} t_{(i-1)k+l} & \text{si } t_{(i-1)k+l} \text{ est une variable existentielle} \\ \pi^1\pi^2\ldots\pi^{h-1}\pi_h(x_j) & \text{si } t_{(i-1)k+l} \text{ est une var. universelle apparaissant en } h^{eme} \text{ position dans le } j^{eme} \text{ bloc universel de } \Phi \end{cases}$$

□

Remarque On ne sait pas si la proposition précédente est encore vraie dans le cas où les quantificateurs universels n'apparaissent pas "en bloc" dans le préfixe de la formule (i.e. s'il est possible de diviser le *nombre* de $\forall$ par k moyennant une augmentation (de n à n^k) de la taille du domaine). Ce cas semble loin d'être évident à résoudre.

La réciproque de la proposition que nous venons de démontrer s'établit plus facilement (voir [Fag75b] pour le cas relationnel):

Proposition 5.9 (Fagin) $\forall k \geq 1$, $\forall d, d'$, $d \geq d' \geq 1$:

$$S^k \in Func^{\omega}_{d'}(\exists^*\forall^d\exists^*) \Rightarrow S \in Func^{\omega}_{kd'}(\exists^*\forall^{kd}\exists^*)$$

Preuve. Soit Ψ une formule de spectre S^k:

$$\Phi : \ \exists\overline{y}\forall x_1\forall x_2\ldots\forall x_d\exists\overline{z} \quad \phi(\overline{y},\overline{x},\overline{z},\overline{f_{d'}}).$$

où chaque $f_{d'}$ est un symbole de fonction d'-aire. On obtient de Φ une formule Φ' de spectre S après les transformations suivantes:

- toute variable t existentiellement (resp. universellement) quantifiée, est remplacée par un bloc de k nouvelles variables $t_1, t_2, \ldots, t_k$ existentielles (resp. universelles). Ces k nouvelles variables sont désignées par $\overline{t}$.

- pour chaque symbole de fonction d'-aire f, k nouveaux symboles $f_1, f_2\ldots f_k$, d'arités kd', sont introduits. Une formule atomique quelconque $f(t^1, t^2, \ldots, t^k) = t^{k+1}$ est alors remplacée par:

$$f_1(\overline{t^1},\overline{t^2},\ldots,\overline{t^k}) = t_1^{k+1},\ f_2(\overline{t^1},\overline{t^2},\ldots,\overline{t^k}) = t_2^{k+1},\ \ldots,\ f_k(\overline{t^1},\overline{t^2},\ldots,\overline{t^k}) = t_k^{k+1} \quad \square$$

Les proposition 5.8 et 5.9 impliquent les lemmes de transfert suivants[3]

Lemme 5.10 $\forall k \geq 1$, $\forall d, d'$, $d \geq d' \geq 1$*:*

$$S \in Func^{\omega}_{kd'}(\exists^*\forall^{kd}\exists^*) \iff S^k \in Func^{\omega}_{d'}(\exists^*\forall^{d}\exists^*)$$

Lemme 5.11 $\forall k \geq 1$, $\forall d, d'$, $d \geq 3$, $d \geq d' \geq 1$*:*

$$S \in Rel^{\omega}_{kd'}(\exists^*\forall^{kd}\exists^*) \iff S^k \in Rel^{\omega}_{d'}(\exists^*\forall^{d}\exists^*)$$

5.2.1 Deux théorèmes de hierarchie sur les spectres

A l'aide des théorèmes de transfert précédents, on va montrer l'existence d'une hiérarchie stricte fondée sur le nombre de quantificateurs universels et l'arité des prédicats.

Théorème 5.12 *Pour tout* $d \geq d' \geq 1$, $Func^{\omega}_{d'}(d\forall) \subset Func^{\omega}_{d'+1}((d+1)\forall)$

Preuve. On raisonne par l'absurde. Supposons qu'il existe d, d' (avec $d \geq d' \geq 1$) tels que:

$$Func^{\omega}_{d'}(d\forall) = Func^{\omega}_{d'+1}((d+1)\forall).$$

Alors, d'après le théorème de transfert, on a, pour tout entier k:

$$Func^{\omega}_{kd'}(kd\forall) = Func^{\omega}_{k(d'+1)}(k(d+1)\forall).$$

Soit i un entier positif. Considérons successivement $k = dd' + i$ et $k = dd' + i + 1$. On note:

$A_i = Func^{\omega}_{(dd'+i)d'}((dd'+i)d\forall)$

$B_i = Func^{\omega}_{(dd'+i)(d'+1)}((dd'+i)(d+1)\forall)$

$A_{i+1} = Func^{\omega}_{(dd'+i+1)d'}((dd'+i+1)d\forall)$

$B_{i+1} = Func^{\omega}_{(dd'+i+1)(d'+1)}((dd'+i+1)(d+1)\forall)$

D'après les hypothèses on a: $A_i = B_i$ et $A_{i+1} = B_{i+1}$. Comme $d, d' \geq 1$,

3. Le théorème 5.11 se déduit du théorème 5.10 en remarquant que la formule à trois quantificateurs, $\varphi : \forall x \forall y \forall z\ R(x,y) \wedge R(x,z) \rightarrow y = z$, exprime que R est une fonction

$$(dd'+i)(d+1) \geq (dd'+i+1)d, \quad (dd'+i)(d'+1) \geq (dd'+i+1)d'$$

On obtient alors que $A_{i+1} \subseteq B_i$, et donc $A_i = B_i = A_{i+1} = B_{i+1}$. Par induction, on a pour tout i: $A_1 = A_i = B_i$.

Un des résultats de caractérisation logique des classes de complexité en temps non déterministe polynomial([Gra85]), nous donne:

$$\text{pour tout } d \geq 1, \quad \mathbf{NRAM}(n^d) = Func^{\omega}_{d}((d\forall)).$$

Ceci nous permet de conclure que:

$$\begin{aligned} A_1 = Func^{\omega}_{(dd'+1)d'}((dd'+1)d\forall) &\subseteq NRAM(n^{(dd'+1)d}) \\ &\subset NRAM(n^{(dd'+1)d+1}) \quad ([\text{Coo73}]) \\ &\subseteq Func^{\omega}_{(dd'+(d^2+1))d'}((dd'+(d^2+1))d\forall) = A_{d^2+1} \end{aligned}$$

Ce qui nous amène à une contradiction. □

Par une preuve quasiment identique à celle du théorème précèdent, on établit :

Théorème 5.13 *Pour tous* $d \geq 2$, $d' \geq 1$, $Func^{\omega}_{d'}(d\forall) \subset Rel^{\omega}_{d'+1}((d+1)\forall)$

Chapitre 6

Jeux et structures en quantificateurs

The property of being a graph of outdegree bounded by a given constant k (i.e. of being a $k-Deg^+$ graph) appeared many times along this thesis. This small chapter focuses on the minimal quantifier prefix of a first-order definition of this class of graphs. If it is easily seen that prefixes of the form $\forall\exists^k\forall$ or $\forall^{k+2}$ are sufficients, it will be shown that for all words $w \in \{\forall,\exists\}^{k+1}$, this class can not be defined by any first-order formula whose quantifier prefix is of the form $\exists^* w \exists^*$.

Au chapitre 4, il a été démontré, entre autres, que toute formule Σ_1^1 dont le second-ordre est restreint à un nombre quelconque de fonction unaires est logiquement équivalente, sur les structures finies, à une formule Σ_1^1 avec un seul symbole de relation binaire (de degré extérieur borné) au second-ordre et qui de plus a le même nombre de quantificateurs universels au premier ordre. Avec nos notations, cela se traduisait par :

$$Func_1^\omega(\exists^*\forall^d\exists^*)(\mathcal{S}) = Deg^+(\exists^*\forall^d\exists^*)(\mathcal{S}).$$

(La réciproque, vraie elle aussi, étant beaucoup plus facile à montrer). Comme les résultats d'indécidabilité qui suivaient l'ont montré, la condition portant sur le degré extérieur joue un rôle crucial lorsque le nombre de $\forall$ dans w est un. L'objet de ce petit chapitre est d'étudier quelles sont les structures en quantificateurs requises pour définir, au premier-ordre, la propriété sur les graphes C_k: "être de degré extérieur borné par k" (pour un entier k fixé).
Soient les deux formules ci-dessous:

$$\forall x \exists y_1 \ldots \exists y_k \forall z \;\; [R(x,z) \rightarrow \bigvee_{i=1}^{k} z = y_i]$$

$$\forall x \forall y_1 \ldots \forall y_k \forall y_{k+1} \quad R(x,y_1) \wedge \ldots \wedge R(x,y_k) \wedge R(x,y_{k+1}) \rightarrow \bigvee_{i<j} y_i = y_j$$

Il est assez facile de voir que ces formules ont toutes deux pour ensemble de modèles l'ensemble des graphes $\langle Dom, R\rangle$ de degré exterieur majoré par k. Le préfixe de la première est de la forme $\forall\exists^k\forall$, celui de la seconde de la forme $\forall^{k+2}$. Ces deux définitions de C_k sont, en un sens, optimales. En effet, on va montrer qu'il ne peut exister de formule du premier ordre définissant C_k dont la structure en quantificateur soit du type $\exists^* w \exists^*$ pour tout mot w sur $\{\forall, \exists\}$ de longueur $k+1$. En particulier, et c'est à comparer aux préfixes des formules plus haut, ni $\forall\exists^{k-1}\forall$ ni $\exists^*\forall^{k+1}\exists^*$ ne suffisent.

Dans les preuves de ces résultats on utilise principalement les jeux de Fraïssé-Ehrenfeucht.

6.1 Les jeux de Fraïssé-Ehrenfeucht

Soient $\mathcal{A}$ et $\mathcal{B}$ deux structures de même signature relationnelle (on supposera dans toute la suite que $\mathcal{A}$ et $\mathcal{B}$ sont des graphes). Le jeu à k coups entre deux joueurs **I** et **II** se déroule ainsi:

- au coup i $(i = 1, \ldots, k)$, le joueur **I** choisit un élément dans une des deux structures $\mathcal{A}$ ou $\mathcal{B}$. Le joueur **II** choisit alors un élément dans l'autre structure. Soient a_i l'élément choisi dans $\mathcal{A}$, b_i l'élément choisi dans $\mathcal{B}$. On appelle g la correspondance bijective dont le graphe contient exactement les couples (a_i, b_i).

- **II** gagne si et seulement si g induit un isomorphisme entre les restrictions de $\mathcal{A}$ et $\mathcal{B}$ aux éléments choisis, i.e. ssi

$$\mathcal{A}{\downarrow}\{a_1, \ldots, a_k\} \cong \mathcal{B}{\downarrow}\{b_1, \ldots, b_k\}$$

Une variante intéressante de ce jeu consiste à ne plus laisser au joueur **I** le soin de choisir la structure dans laquelle il sélectionne un élément. Plus précisement, soit $w = w_1 \ldots w_k$ un mot fini sur l'alphabet $\{\forall, \exists\}$. On définit un w-jeu à k coups entre deux joueurs **I** et **II** sur $\mathcal{A}$ et $\mathcal{B}$, en apportant les modifications suivantes aux règles du jeu classique:

- au coup i $(i = 1, \ldots, k)$, si $w_i = \exists$ (resp. $w_i = \forall$) le joueur **I** choisit un élément dans la structure $\mathcal{A}$ (resp. $\mathcal{B}$). Le joueur **II** répond en séléctionnant un élément dans l'autre structure.

Le vainqueur est désigné de la même manière. Le nombre de coups k qui est la longueur du préfixe w, ne sera plus précisé dans la suite. Le théorème suivant, essentiellement du à Fraïssé, souligne l'intérêt d'un tel jeu pour les questions de définissabilité dans les logiques préfixées.

Théorème 6.1 *Soient $\mathcal{A}$ et $\mathcal{B}$ deux Σ-structures et w un préfixe de longueur k. Si le joueur* **II** *a une stratégie gagnante dans le w-jeu entre $\mathcal{A}$ et $\mathcal{B}$ alors pour toute formule du premier ordre φ t.q. $Pre(\varphi) = w$ on a :*

$$\mathcal{A} \models \varphi \Rightarrow \mathcal{B} \models \varphi$$

On obtient comme corollaire :

Corollaire 6.2 *Soit C un ensemble de graphes. Soient $\mathcal{A} \in C$ et $\mathcal{B} \notin C$ telles que le joueur* **II** *a une stratégie gagnante dans le w-jeu entre $\mathcal{A}$ et $\mathcal{B}$. Alors, C n'est définissable par aucune formule du premier ordre de préfixe w (i.e. C n'est pas définissable dans* $\mathbf{FO}(w)$*).*

6.2 Une application des w-jeux

La preuve du résultat évoqué plus haut se divise en plusieurs parties pour des raisons de lisibilité. Tout d'abord, les structures, ou en tout cas les parties significatives de celles-ci, sur lesquelles les jeux se dérouleront doivent être définies.

Soit $\mathcal{A}^k = \langle Dom, R \rangle$ le graphe orienté construit de la manière suivante. Le domaine Dom, de taille $2(k+1)$, se partage en deux sous-ensembles de même cardinalité $k+1$: les *feuilles*[1] , $\{f_1, \ldots, f_{k+1}\}$ et les *racines*, $\{r_1, \ldots, r_{k+1}\}$. Les seuls arcs de $\mathcal{A}^k$ sont construits comme suit: pour tout k-uplet de feuilles distinctes $f_{i_1}, \ldots, f_{i_k}$, il existe une et une seule racine r_i telle que :

$$R(r_i, f_{i_1}), \ldots, R(r_i, f_{i_k}) \text{ soient vrai.}$$

Réciproquement, chacune des $k+1$ racines est reliée, de cette manière, à un k-uplet de feuilles différent et est, par conséquent, de degré extérieur k. Un autre fait évident par construction est que pour chaque racine r_i, il existe une unique feuille f_i vérifiant $\neg R(r_i, f_i)$. Les figures ci-dessous représentent $\mathcal{A}^3$ et $\mathcal{A}^4$.

1. cette terminologie n'a rien à voir avec celle utilisée habituellement en théorie des arbres

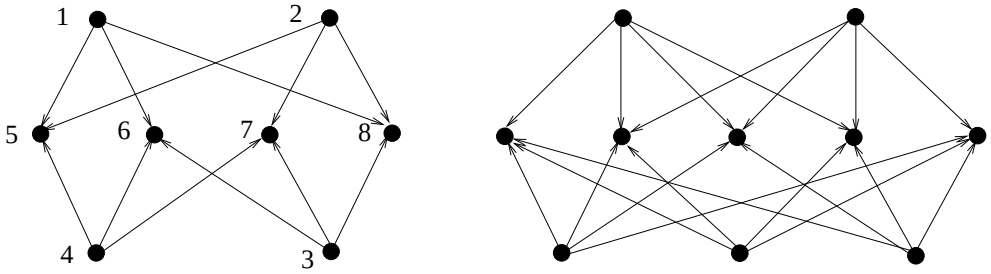

fig : $\mathcal{A}^3$ et $\mathcal{A}^4$. Dans $\mathcal{A}^3$, les sommets numérotés 1,2,3 et 4 représentent les racines.

Un premier lemme, très facile, peut tout de suite être énoncé:

Lemme 6.3 *1. Pour toute feuille f_i (resp. racine r_i), il existe une racine r_i (resp. une feuille f_i) telle que :*

$$\mathcal{A}^k \cong \mathcal{A}^{k+1} \backslash \{r_i, f_i\}$$

2. Soit $h \leq k+1$. Soient $r_{i_1}, \ldots, r_{i_h}$, h racines (resp. feuilles) distinctes, il existe $k+1-h$ feuilles (resp. racines) différentes $f_{j_1}, \ldots, f_{j_{k+1-h}}$ vérifiants :

$$\forall f_j \in \{f_{j_1}, \ldots, f_{j_{k+1-h}}\} \quad R(r_{i_1}, f_j), \ldots, R(r_{i_h}, f_j)$$

Preuve 1. Soit f_i une feuille quelconque, l'unique r_i qui convienne est celle vérifiant $\neg R(r_i, f_i)$. De même pour la réciproque. 2. Chaque racine est reliée à k feuilles (parmi $k+1$). k feuilles distinctes n'ont qu'une seule racine mère. Donc, h racines distinctes ont $k+1-h$ feuilles "en commun". □

Proposition 6.4 II *a une stratégie gagnante dans le jeu classique à $k+1$ coups entre $\mathcal{A}^k$ et $\mathcal{A}^{k+1}$.*

Preuve On commence par une remarque élémentaire sur la stratégie à suivre par **II** . En réponse à chaque coup de **I** , celui-ci devra sélectionner un élément de même type; à savoir une feuille si **I** en a lui-même choisi une, ou une racine, dans le cas contraire. La preuve se fait par récurrence. Au premier coup, quoique **I** joue (et où qu'il le fasse), **II** choisit un point au hasard. Il a juste à respecter la condition qui vient d'être évoquée. Supposons qu'au coup h ($h \leq k$), on ait :

$$\mathcal{A}^k \downarrow \{a_1, \ldots, a_h\} \cong \mathcal{A}^{k+1} \downarrow \{b_1, \ldots, b_h\}.$$

On appelle g la correspondance bijective qui envoie, pour tout i, a_i sur b_i (et g^{-1} sa réciproque). Au coup $h+1$, il y a quatre possibilités de jeu pour **I**: deux pour la structure (dans $\mathcal{A}^k$ ou $\mathcal{A}^{k+1}$?), deux pour le type d'élément (racine ou feuille?).

Si **I** joue f une feuille de $\mathcal{A}^{k+1}$. **II** regarde alors quelle est la structure induite, dans $\mathcal{A}_i^{k+1}$, par f et l'ensemble des racines déja sélectionnées $\{r_{i_1}, \ldots, r_{i_\alpha}\}$ $(\alpha \leq h)$. Deux cas se présentent à nouveau: soit f est reliée à chacune de ces racines et dans ce cas **II** choisit une feuille f' de $\mathcal{A}^k$ reliée à $g^{-1}(r_{i_1})$, ..., $g^{-1}(r_{i_\alpha})$ (comme $h+1 \leq k+1$, il y a toujours au moins une possibilité d'effectuer un tel coup d'après le lemme 6.3); soit il existe r dans $\{r_{i_1}, \ldots, r_{i_\alpha}\}$ qui n'est pas reliée à f, et **II** choisit alors l'unique feuille de $\mathcal{A}^k$ vérifiant $\neg R(g^{-1}(r), f')$.

Le cas où **I** joue une racine r de $\mathcal{A}^{k+1}$ se traite pareillement. Enfin, si **I** décide de jouer son $h+1^{eme}$ coup dans $\mathcal{A}^k$, la stratégie de **II** est identique à l'exception près qu'un plus grand nombre de possibilités s'offre à lui ($\mathcal{A}^{k+1}$ est en quelque sorte un enrichissement de $\mathcal{A}^k$). □

Soient α, β deux entiers. Soient $\mathcal{A}$ et $\mathcal{B}$ les deux structures suivantes :

$$\mathcal{A} = \bigoplus^{\alpha+\beta+2} \mathcal{A}^k \qquad \mathcal{B} = \bigoplus^{\alpha+\beta+1} \mathcal{A}^k \oplus \mathcal{A}^{k+1}$$

$\mathcal{A}$ est la somme directe de $\alpha+\beta+2$ copies de $\mathcal{A}^k$. $\mathcal{B}$ est presque la même structure : $\mathcal{A}^{k+1}$ ayant été substitué à une copie de $\mathcal{A}^k$.

Proposition 6.5 *Pour tous α, β entiers, pour tout mot w dans $\{\forall, \exists\}$ de longueur $k+1$, le joueur* **II** *a une stratégie gagnante dans le $\exists^\alpha w \exists^\beta$-jeu entre $\mathcal{A}$ et $\mathcal{B}$.*

Preuve De par les règles du $\exists^\alpha w \exists^\beta$-jeu **I** est obligé de jouer ses α premiers coups dans $\mathcal{A}$. **II** peut lui répondre aisément de façon à maintenir à chaque coup l'isomorphisme entre les deux structures induites par les éléments sélectionnés. A l'issue de ces coups "existentiels", au plus α copies de $\mathcal{A}^k$ auront vu au moins un de leurs éléments choisis. A partir du coup $\alpha+1$, **I** a la possibilité, et ce pour $|w|$ coups, de jouer dans la structure $\mathcal{B}$. Deux cas sont possibles: soit **I** ignore totalement la sous-structure $\mathcal{A}^{k+1}$ et la stratégie de **II** est triviale; soit **I** joue tout ou partie de ces coups dans $\mathcal{A}^{k+1}$. Il existe une copie, notée $\mathcal{A}_0^k$, de $\mathcal{A}^k$ dans $\mathcal{A}$ qui n'ayant pas eu d'élément sélectionné va servir à **II** pour répondre aux coups de **I** joués dans $\mathcal{A}^{k+1}$. En vertu de la proposition précédente, au bout des $|w|$ étapes supplémentaires, on a :

$$\mathcal{A}{\downarrow}\{a_1, \ldots, a_{\alpha+|w|}\} \cong \mathcal{B}{\downarrow}\{b_1, \ldots, b_{\alpha+|w|}\}.$$

Il reste à montrer maintenant qu'un retour à une série de coups existentiels (quel que soit ce nombre) ne change rien à l'indiscernabilité de $\mathcal{A}$ et $\mathcal{B}$. On utilise pour cela le lemme 6.3. **I** n'a pu jouer qu'au plus $|w|$ coups dans $\mathcal{B}$ or, il y a $|w|+1$ paires (r_i, f_i) satisfaisant l'énoncé du lemme. Soit donc (r, f) une (peut-être la seule) paire telle que ni r, ni f n'ont été sélectionnées. Pour prétendre gagner **I** ne peut plus jouer que dans $\mathcal{A}_0^k$. La stratégie finale de **II** consiste alors à respecter l'isomorphisme entre $\mathcal{A}_0^k$ et $\mathcal{A}^{k+1} \backslash \{r, f\}$ en ne jouant ni r ni f. □

Remarque Soit K_k le graphe complet à k sommets. Le résultat précédent est toujours vrai pour :

$$\mathcal{A} = \bigoplus^{\alpha+\beta+2} K_k \qquad \mathcal{B} = \bigoplus^{\alpha+\beta+1} K_k \oplus K_{k+1}.$$

Corollaire 6.6 *Quel que soit* $w \in \{\forall, \exists\}^{k+1}$, C_k *n'est pas définissable dans* $\mathbf{FO}(\exists^\alpha w \exists^\beta)$.

Soit R_k l'ensemble des graphes k-réguliers (i.e. dont tous les sommets sont de degré extérieur k). Alors :

Corollaire 6.7 *Quel que soit* $w \in \{\forall, \exists\}^{k+1}$, R_k *n'est pas définissable dans* $\mathbf{FO}(\exists^\alpha w \exists^\beta)$.

La preuve est immédiate en considérant les structures $\overline{\mathcal{A}}$ et $\overline{\mathcal{B}}$ obtenues de $\mathcal{A}$ et $\mathcal{B}$, en rajoutant l'arc $R(b,a)$ pour tous a, b vérifiant $R(a,b)$ (les deux nouvelles structures sont les clôtures par symétrie de $\mathcal{A}$ et $\mathcal{B}$).

Conclusion

Lorsque l'on se donne une formule du second ordre

$$\exists R_1 \ldots \exists R_k \ \varphi$$

(où les R_i sont des prédicats d'arité au plus 2), on peut, comme nous l'avons d'ailleurs fait ici, faire porter des conditions sémantiques sur les R_i (par exemple restreindre leurs interprétations à la classe des fonctions unaires, des ordres partiels ...). C'est la démarche suivie aussi dans [DLS96]. En combinant les résultats de ce papier avec certains de la présente thèse, on dégage une hiérarchie, sur 4 niveaux, particulièrement significative.

La figure 6.1 détaille ce que nous venons de dire. Le pouvoir d'expression décroit du haut vers le bas; les classes dans un même cadre ont le même pouvoir d'expression [2].

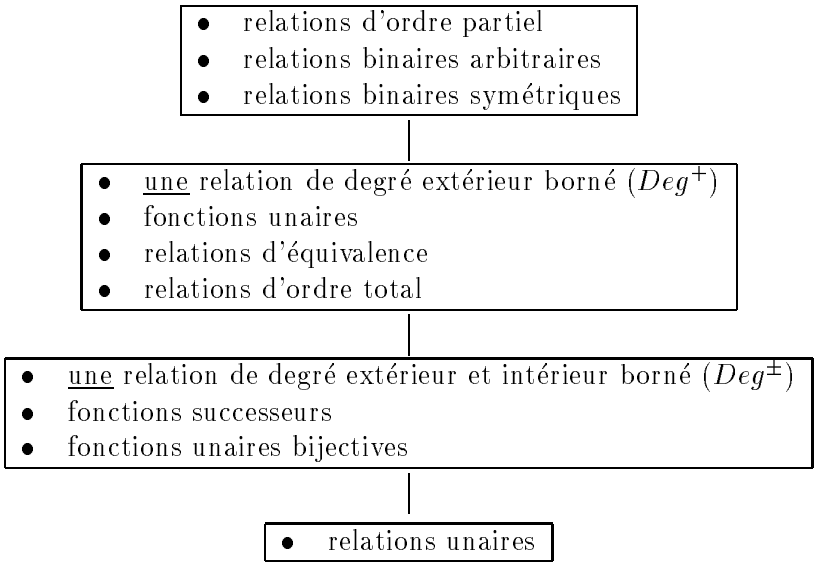

FIG. 6.1 -

2. lorsque l'on ne spécifie pas le nombre de relations, cela signifie que celui-ci est quelconque

On peut affiner les résultats de la figure 6.1 par les remarques suivantes :

- Comme on l'a vu, on peut "simuler" un nombre quelconque de fonctions unaires par une relation symétrique, un ordre partiel ou une relation bipartie.
- On a prouvé que dans la "correspondance" entre fonctions unaires et (une) relation de degré extérieur borné le nombre de quantificateurs universels au premier ordre pouvait être préservé. Nous conjecturons que la même chose est possible au niveau inférieur (i.e. entre fonctions unaires bijectives et une relation de degré extérieur et intérieur borné). Un tel résultat pourrait avoir des conséquences intéressantes sur l'éventuelle indécidabilité des problèmes suivants [3] :

  Instance une formule φ de préfixe de la forme $\exists^*\forall\exists^*$ et de signature $\{R\}$ (R : relation binaire)

  Question(s) φ est elle satisfaisable dans un modèle $\langle Dom, R\rangle$ où R est de degré (extérieur + intérieur) borné par 3 (resp. où R est symétrique de degré 3)?
- L'inclusion entre chacune des classes de la figure 6.1 est stricte lorsque l'on se restreint à des problèmes de graphes. On a montré dans cette thèse que l'ensemble des graphes ayant un nombre pair d'arêtes est définissable à l'aide d'une seule relation binaire mais pas avec un nombre quelconque de fonctions unaires. De même, T. Schwentick a montré (dans [Sch96]) que l'ensemble des graphes ayant un nombre d'arêtes égal à leur nombre de sommets sépare la deuxième classe de la troisième (les fonctions unaires bijectives) [4]. Enfin, mais c'est plus du "folklore", l'ensemble des graphes ayant un nombre pair de sommets fait la séparation entre les deux classes les plus basses.

Il est à noter que lorsque le domaine des structures que l'on considère est ordonné (i.e. s'il y a un ordre total préconstruit), les deux classes intermédiaires coïncident. Cette remarque entretien l'espoir de donner une nouvelle caractérisation (exacte) de $NLIN$ en terme de formules de Σ^1_1 dont le second ordre serait réduit à un nombre quelconque de bijections et avec un seul quantificateur universel au premier ordre.

Contrairement à ce que l'on pourrait penser, le statut des deux inclusions

$$Deg^{\pm}(\mathcal{S}) \subset Deg^{+}(\mathcal{S}) \subset BIN(\mathcal{S})$$

n'est pas connu pour toute signature $\mathcal{S}$. Lorsque celle-ci contient au plus des symboles de fonctions unaires (et, en particulier si $\mathcal{S}$ est vide), le problème reste ouvert.

Enfin, on ne peut résister pour conclure à poser la question suivante : existe t'il un problème naturel (disons dans $PSPACE$) sur les graphes qui ne soit pas définissable

3. à condition toutefois de prouver l'indécidabilité du problème de satisfaisabilité des formules du premier ordre avec un seul $\forall$ et de signature restreinte à deux bijections; ce qui semble résulter plus ou moins directement d'un travail de Gurevich [Gur76]

4. on notera que ces deux résultats utilisent de manière essentielle les travaux d'Ajtai ([Ajt83])

par une formule de la forme $\exists R_1 \ldots \exists R_k \ \varphi$ où les R_i sont des relations binaires (non restreintes)? une réponse positive permettrait de donner une première borne inférieure de complexité en temps linéaire non-déterministe pour un tel problème et semble, pour l'instant, hors d'atteinte ...

Bibliographie

[Ajt83] M. Ajtai. $\sum_1^1$-formulae on finite structures. *Ann. of Pure Appl. Logic*, 24:pp.1–48, 1983.

[Ajt89] M. Ajtai. First-order definability on finite structures. *Ann. of Pure Appl. Logic*, 45(3):pp.211–226, 1989.

[Ajt93] M. Ajtai. Geometric properties of sets defined by constant depth circuits. In *Combinatorics, Paul Erdös is Eighty*, volume 1 of *Bolyai Society Mathematical Studies*, pages pp.19–31. Keszthely (Hungary), 1993.

[Ass55] G. Asser. Das Repräsentantenproblem im Prädikatenkalkül der ersten Stufe mit Identität. *Z. Math. Logik Grundlagen Math.*, 1:pp.252–263, 1955.

[Ben62] J.H. Bennett. *On Spectra*. PhD thesis, Princeton University, 1962.

[CH90] K.J. Compton and C.W. Henson. A uniform method for proving lower bounds on the computational complexity of logical theories. *Annals of pure and applied logic*, 48:pp.1–79, 1990.

[Coo73] S.A Cook. A hierarchy for nondeterministic time complexity. *J. Comput. Systems Sci.*, vol.7:pp.343–353, 1973.

[Cos93] S. Cosmadakis. Logical reducibility and monadic NP. In *Proc. 34th IEEE Symp. on foundations of Computer Science*, pages pp 52–61, 1993.

[Cou96] B. Courcelle. The expression of graph properties and graph transformations in monadic second-order logic. In G. Rozenberg, editor, *Handbook of graph grammars, vol 1: Foundations*. World Scientific Publisher, 1996.

[Cre93] N. Creignou. *Temps linéaire et problèmes NP-Complets*. PhD thesis, Université de Caen, 1993.

[DLS96] A. Durand, C. Lautemann, and T. Schwentick. Subclasses of Binary-NP. Technical Report 96-2, les cahiers du GREYC, 1996.

[dR87] M. de Rougemont. Second-order and inductive definability on finite structures. *Z. Math. Logik und Grundlagen der Math.*, vol.33:pp.47–63, 1987.

[DR94] A. Durand and S. Ranaivoson. First-order spectra with one binary predicate. *In Proc. 1994 of the Annual Conference of the EACSL*, pages pp.177–189, 1994.

[DR96a] A. Durand and S. Ranaivoson. First-order spectra with one binary predicate. *Theoretical Computer Science, to appear*, 1996.

[DR96b] A. Durand and S. Ranaivoson. Unary functions vs. one partial order. In preparation, 1996.

[Dur96] A. Durand. Binary-NP, linear time and the power of one first-order universal quantifier. Technical Report 96-1, les Cahiers du GREYC, 1996.

[EF95] H.-D. Ebbinghaus and J. Flum. *Finite Model theory*. Springer Verlag, 1995.

[EFT89] H.D. Ebbinghaus, J. Flum, and W. Thomas. *Mathematical Logic*. Springer Verlag, 1989.

[Ehr61] A. Ehrenfeucht. An application of games to the completeness problem for formalized theory. *Fund. Math.*, (49):pp 129–141, 1961.

[Fag74] R. Fagin. Generalized first-order spectra and polynomial-time recognizable sets. *Complexity of computations*, vol.7:pp.43–73, 1974.

[Fag75a] R. Fagin. Monadic generalized spectra. *Z. Math. Logik. Grundlag. Math.*, 21:pp.89–96, 1975.

[Fag75b] R. Fagin. A spectrum hierarchy. *Z. Math. Logik Grundlag. Math.*, (21):pp.123–134, 1975.

[Fag93] R. Fagin. Finite-model theory - a personal perspective. *Theoretical Computer Science*, (116):pp.3–31, 1993.

[Fag96] R. Fagin. Easier ways to win logical games. In *Proc. of the DIMACS workshop on finite models and descriptive complexity*. American Mathematical Society, 1996.

[Fra54] R. Fraïssé. Sur quelques classifications des systèmes de relation. *Publi. Sci. Univ. Alger Sér. A.*, (1):pp. 35–182, 1954.

[FSV93] R. Fagin, L. Stockmeyer, and M. Y. Vardi. On monadic NP vs monadic co-NP. *Information and Computation*, 120(1):78–92, july 1993.

[GJ79] M.R. Garey and D.S. Johnson. *Computers and Intractability*. W.H. Freeman and Company, New York, 1979.

[GL80] P. Gács and L. Lovász. Some remarks on generalized spectra. *Z. Math. Logik. Grundlag. Math.*, pages pp.547–553, 1980.

[GO94] E. Grandjean and F. Olive. Monadic logical definability of NP-complete problems. *In Proc. 1994 of the Annual Conference of the EACSL*, pages pp.190–204, 1994. extended version submitted.

[Gra84] E. Grandjean. The spectra of first-order sentences and computational complexity. *SIAM J. Comput.*, vol.13:pp.356–373, 1984.

[Gra85] E. Grandjean. Universal quantifiers and time complexity of random access machine. *Math. Systems Theory*, vol.18:pp.171–187, 1985.

[Gra90a] E. Graedel. On solvable cases of Hilbert's 'Entscheidungsproblem'. Universität Basel, Habilitationsschrift, 1990.

[Gra90b] E. Graedel. On the notion of linear time computability. *International J. of Foundations of Computer Science*, (1):pp.295–307, 1990.

[Gra90c] E. Grandjean. First-order spectra with one variable. *J. Comput. Systems Sci.*, vol.40(2):pp.136–153, 1990.

[Gra92] E. Graedel. Capturing complexity classes by fragments of second-order logic. *Theoretical Computer Science*, 101(1):pp.35–57, 1992. Special issue on logic and applications to computer science. Guest editor: E. Grandjean.

[Gra94a] E. Grandjean. Invariance properties of RAMs and linear time. *Comput. Complexity*, vol.4:pp.62–106, 1994.

[Gra94b] E. Grandjean. Linear time algorithms and NP-complete problems. *SIAM J. Comput.*, vol.23(3):pp.573–597, 1994.

[Gra96] E. Grandjean. Sorting, linear time and the satisfiability problem. *to appear in special issue of Annals of Math. and Artificial Intelligence*, 1996.

[Gri89] S. Grigorieff. Décidabilité et complexité des théories logiques. In B. Courcelle, editor, *Logique et Informatique : une introduction*. INRIA, Collection Didactique, 1989.

[Gur76] Y. Gurevich. The decision problem for standard classes. *J. Symb. Logic*, 41(2):pp.460–464, 1976.

[Gur84] Y. Gurevich. Toward logic tailored for computational complexity. In *Computation and Proof Theory*, volume 1104 of *Lecture Notes in Math.*, pages 175–216. Springer-Verlag, M.M. Richter and al. edition, 1984.

[Gur86] Y. Gurevich. Logic and the challenge of computer science. In E. Boerger, editor, *Current trends in theoretical computer science*, pages 1–55. Computer Science, Rockville, MD, 1986.

[HP93] P. Hájek and P. Pudlák. *Metamathematics of First-Order Arithmetics.* Springer-Verlag, 1993.

[HU79] J.E. Hopcroft and J.D. Ullman. *Introduction to Automata theory, Languages and Computation.* Addison Wesley, 1979.

[Imm89] N. Immerman. Descriptive and computational complexity. In J. Hartmanis, editor, *Proceedings of symposia in applied mathematics*, volume vol.38, pages pp.75–91, 1989.

[JS74] N.D Jones and A.L Selman. Turing machines and the spectra of first-order formulas with equality. *J. Symb. Logic*, vol.39:pp.139–150, 1974.

[LdR93] R. Lassaigne and M. de Rougemont. *Logique et fondements de l'informatique.* Hermès, Paris, 1993.

[LdR96] R. Lassaigne and M. de Rougemont. *Logique et complexité.* Hermès, Paris, 1996.

[Loe] B. Loescher. One unary function says less than two in existential second order logic. Preprint, 1996.

[LST94] C. Lautemann, T. Schwentick, and D. Thérien. Logics for context-free languages. In *Proc. 1994 of the annual conference of the EACSL*, 1994.

[Lyn82] J.F. Lynch. Complexity classes and theories of finite models. *Math. Systems Theory*, vol.15:pp.127–144, 1982.

[Lyn92] J.F. Lynch. The quantifier structure of sentences that characterize nondeterministic time complexity. *Computational Complexity*, pages pp. 40–66, 1992.

[Mor94a] M. More. *Définissabilité dans les graphes finis et en arithmétique bornée.* PhD thesis, Université d'Auvergne - Clermont 1, 1994.

[Mor94b] M. More. Investigation of binary spectra by explicit polynomial transformations of graphs. *Theoretical Computer Science*, vol.124(2):221–272, 1994.

[Oli96] F. Olive. *Caractérisation logique des problèmes NP: robustesse et normalisation.* PhD thesis, Université de Caen, 1996.

[Pap94] C.H. Papadimitriou. *Computational Complexity.* Addison Wesley, 1994.

[Pud75] P. Pudlák. The observational predicate calculus and complexity of computations. *Comment. Math. Univ. Carolin.*, vol.16, 1975.

[Rab] M.O. Rabin. A simple method for undecidability proofs and some applications. In North Holland, editor, *Proc. 1964 of the Internat. Congr. of Logic, Methodology and Philosophy of Science*, pages pp.58–68.

[Ran90] S. Ranaivoson. *Bornes inférieures non triviales pour des problèmes naturels en théorie des graphes et des automates.* PhD thesis, Université de Caen, 1990.

[Ran91] S. Ranaivoson. Nontrivial lower bounds for some NP-complete problems on directed graphs. In *CSL 90*, volume 533 of *Lecture notes in comput. science*, pages pp.318–339, 1991.

[Ric89] D. Richard. Equivalence of some questions in mathematical logic with some conjectures in number theory. In *Number theory and applications.* R. mollin edition, 1989.

[Sch] T. Schwentick. On winning Ehrenfeucht games and monadic NP. To appear in *Ann. of Pure and Appl. Logic.*

[Sch78] C.P Schnorr. Satisfiability is quasilinear complete in NQL. *J. ACM*, 25:pp.136–145, 1978.

[Sch94] T. Schwentick. Graph connectivity and monadic NP. In *Proc. 35th IEEE Symp. on Foundations of Computer Science*, pages pp. 614–622, 1994.

[Sch95] T. Schwentick. Graph connectivity, monadic NP and built-in relations of moderate degree. In *Proc. 22nd International Colloq. on Automata, Languages and Programming*, pages pp. 405–416, 1995.

[Sch96] T. Schwentick. Bijections vs. unary functions. In *Proc. of the 13th annual symposium on theoretical aspects of computer science*, 1996.

[Ste90] J. Stern. *Fondements Mathématiques de l'Informatique.* McGraw Hill, 1990.

[Wil94] R. Willard. Hereditary undecidability of some theories of finite structures. *Journal of Symb. Logic*, 59(4):pp. 1254–1262, December 1994.

[Woo81] A.R. Woods. *Some problems in logic and number theory and their connections.* PhD thesis, University of Manchester, 1981.

La définissabilité logique sur les structures finies s'est beaucoup developpée ces dernières années principalement en raison des nombreuses connexions qui existent entre ce domaine et la théorie de la complexité algorithmique. Dans cette optique, cette thèse s'intéresse à l'étude du pouvoir d'expression de fragments particulièrement significatifs de la logique existentielle du second ordre.

On montre tout d'abord que, dans cette logique, toute formule dont la quantification au second ordre porte sur un nombre quelconque de fonctions unaires est logiquement équivalente, sur les structures finies, à une formule où une seule relation binaire est quantifiée.

On raffine ensuite ce résultat de plusieurs manières. Celui-ci reste vrai si la relation binaire est restreinte à une relation symétrique, un ordre partiel ou même une relation bipartie. De plus, on montre que l'on peut conserver le nombre de quantificateurs universels dans le préfixe du premier ordre. Ce dernier résultat nous permet de donner une nouvelle caractérisation logique de $NLIN$ (temps linéaire non-déterministe).

En utilisant un théorème d'Ajtai, on donne ensuite un résultat de séparation en montrant que la parité du nombre d'arêtes d'un graphe n'est pas définissable avec des fonctions unaires au second ordre mais qu'elle l'est avec une seule relation binaire.

Enfin, on présente un nouveau théorème de hiérarchie sur les spectres prenant en compte à la fois l'arité des prédicats et le nombre de quantificateurs universels.

Pré-rapporteurs
Erich Grädel, Professeur à l'université de Aachen (Allemagne)
Clemens Lautemann, Professeur à l'université de Mainz (Allemagne)
Michel de Rougemont, Professeur à l'université de Paris II

Jury
Patrick Dehornoy, Professeur à l'université de Caen
Patrice Enjalbert, Professeur à l'université de Caen
Etienne Grandjean, Directeur, Professeur à l'université de Caen
Stéphane Grumbach, Chargé de recherches à l'INRIA, Rocquencourt
Michel de Rougemont, Professeur à l'université de Paris II
Jacques Stern, Professeur à l'École Normale Supérieure, Paris
Friedrich Wehrung, Chargé de recherches au CNRS, université de Caen