Complexity of model checking parameterised by the model.

Relativisation of quantifiers matters a lot

Florent Madelaine

Université de Caen, GREYC

Beyond NP
Paris, 10/05/2017.

$$\text{Structure} \models \text{a sentence}$$

Fixed Finite Structure $\models$ an input sentence

Research program

Understand the complexity of the problem for a given logic, parameterised by the model.
Notation for the decision problem : logic(model) as in $\mathscr{L}(\Gamma)$

Fixed Finite Structure $\models$ an input sentence

Research program

Understand the complexity of the problem for a given logic, parameterised by the model.
Notation for the decision problem : logic(model) as in $\mathscr{L}(\Gamma)$

Examples

- Logic = primitive positive FO ($\{\exists, \wedge\}$-FO)

$\rightsquigarrow$ (non uniform) Constraint Satisfaction Problem

- Logic = positive Horn ($\{\exists, \forall, \wedge\}$-FO)

$\rightsquigarrow$ (non uniform) Quantified Constraint Satisfaction Problem

- More generally any syntactic fragment of FO specified by the presence or absence of symbols from $\{\exists, \forall, \wedge, \vee, =, \neq\}$

This talk

Beyond NP, relativisation of quantifiers is the only known explanation that takes the complexity down to some complexity class in NP.

Examples

- Logic = primitive positive FO ($\{\exists, \wedge\}$-FO)

$\rightsquigarrow$ (non uniform) Constraint Satisfaction Problem

- Logic = positive Horn ($\{\exists, \forall, \wedge\}$-FO)

$\rightsquigarrow$ (non uniform) Quantified Constraint Satisfaction Problem

- More generally any syntactic fragment of FO specified by the presence or absence of symbols from $\{\exists, \forall, \wedge, \vee, =, \neq\}$

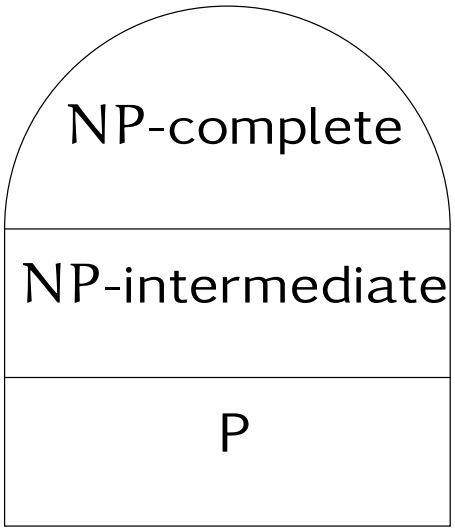
This talk

Beyond NP, relativisation of quantifiers is the only known explanation that takes the complexity down to some complexity class in NP.

Resisting to go beyond NP for now

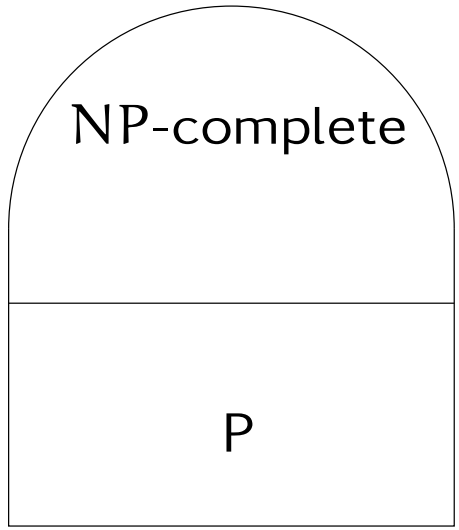
Constraint Satisfaction Problem and dichotomy

Real World [1]



Ladner's theorem ['75]

CSP world



Feder et Vardi Conjecture['93]

1. *provisio* $P \neq NP$

CSP and the dichotomy phenomenon

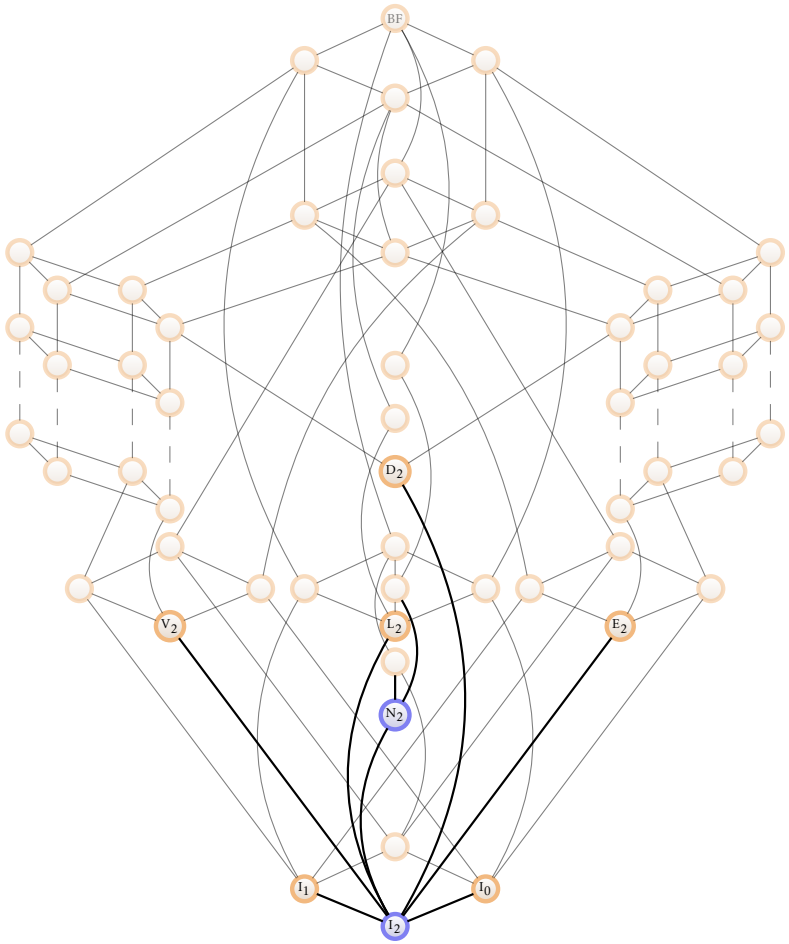
1. Generalized Sat (CSP of Domain size 2) [Schaefer '78]
2. H-coloring (model is an undirected graph) [Hell and Nešetřil '90]
3. Domain size 3 [Bulatov '02]

   ... a lot of work more and more algebraic ...
4. 3 proposed proofs for the general case in 2017 available on ArXiv [Rafiey, Feder, Kinne] [Bulatov] and [Zhuk]

key concept $\mathrm{Pol}(\Gamma)$

The polymorphisms of Γ, a generalisation of homomorphism to arbitrary arity.

Post lattice and dichotomy for Sat



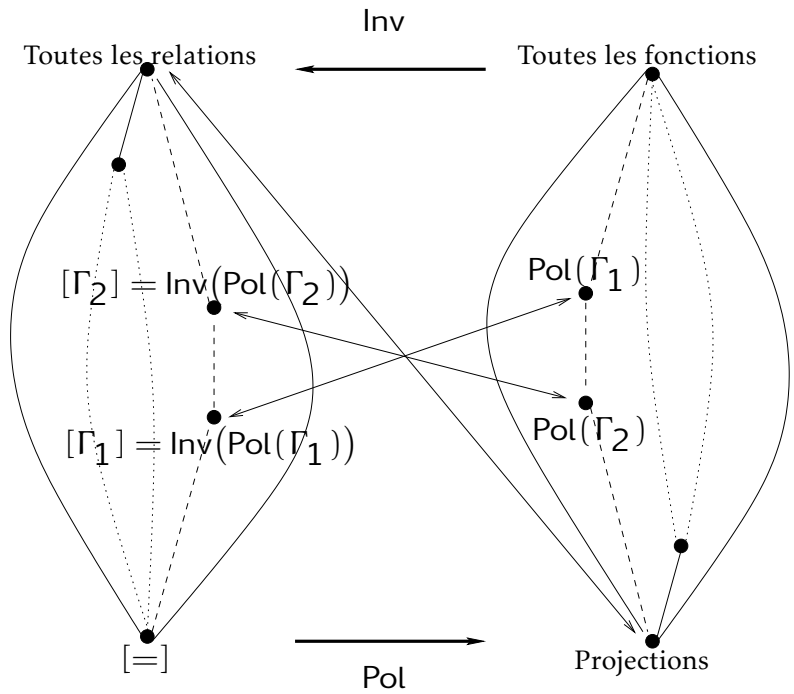
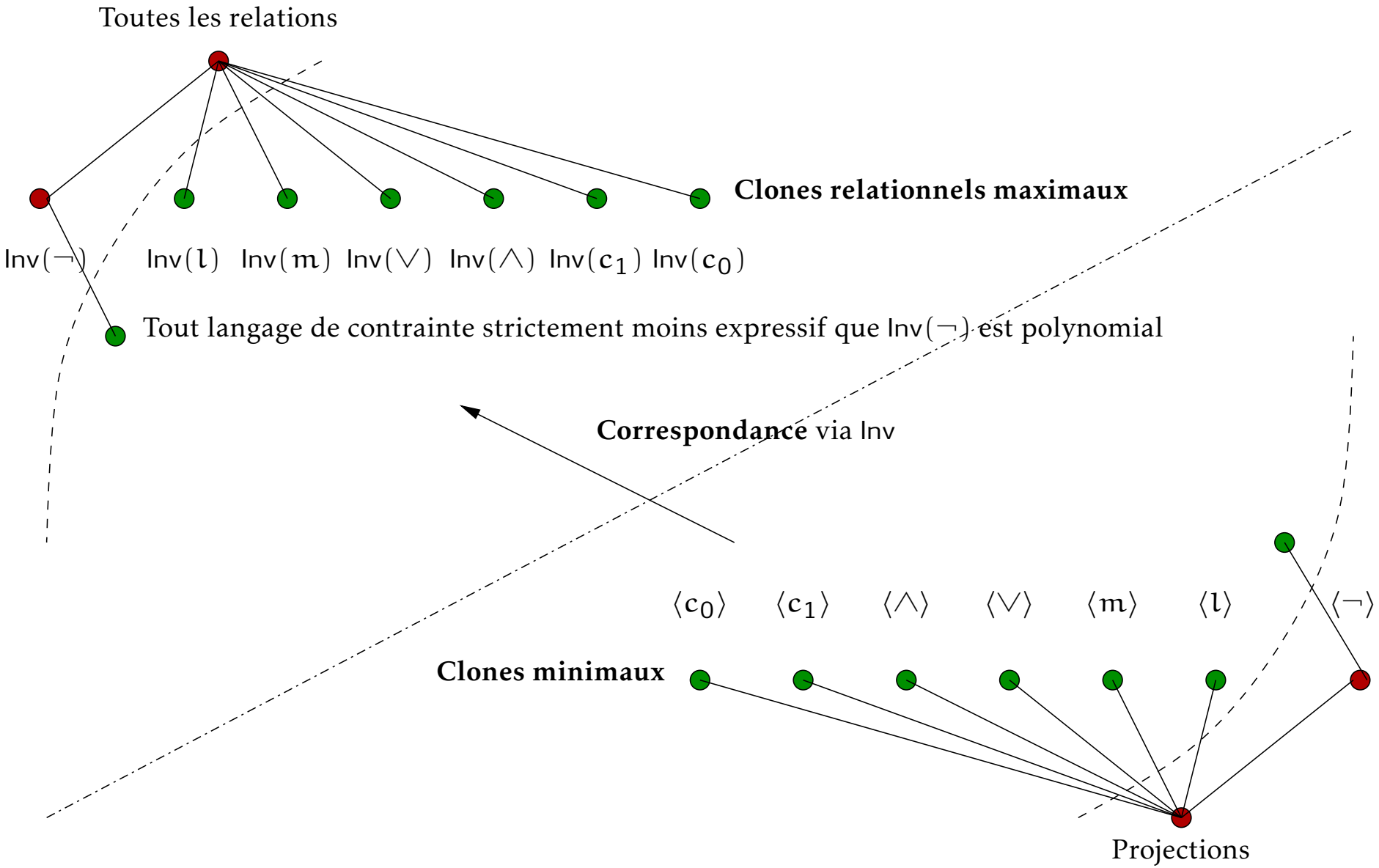


Illustration de la preuve du théorème de Schaeffer



Schaefer's theorem and Post lattice

Theorem (Post, 1941)

Pour tout langage de contrainte Γ *sur* $D = \{0,1\}$*, on est dans l'un des cas suivants*

- *Les constantes 0 ou 1 sont dans* $\mathrm{Pol}(\Gamma)$ — $\textsc{Sat}(\Gamma)$ *est trivial*
- $\wedge \in \mathrm{Pol}(\Gamma)$ — $\textsc{Sat}(\Gamma) \subseteq$ ***Horn-Sat***
- $\vee \in \mathrm{Pol}(\Gamma)$ — $\textsc{Sat}(\Gamma) \subseteq$ ***dual Horn-Sat***
- $\mathfrak{m} \in \mathrm{Pol}(\Gamma)$ — $\textsc{Sat}(\Gamma) \subseteq$ ***2-Sat***
- $\mathfrak{l}$ *est dans* $\mathrm{Pol}(\Gamma)$ — $\textsc{Sat}(\Gamma) \subseteq$ ***équations linéaires***
- $\mathrm{Pol}(\Gamma) \subseteq \mathrm{Pol}\langle R_{NAE} \rangle$. — ***NAE-Sat*** $\subseteq \textsc{Sat}(\Gamma)$

Corollary (Schaefer, 1978)

Pour tout langage de contrainte Γ *sur* $D = \{0,1\}$, $\textsc{Sat}(\Gamma)$ *est soit polynomial soit NP-complet.*

Beyond NP

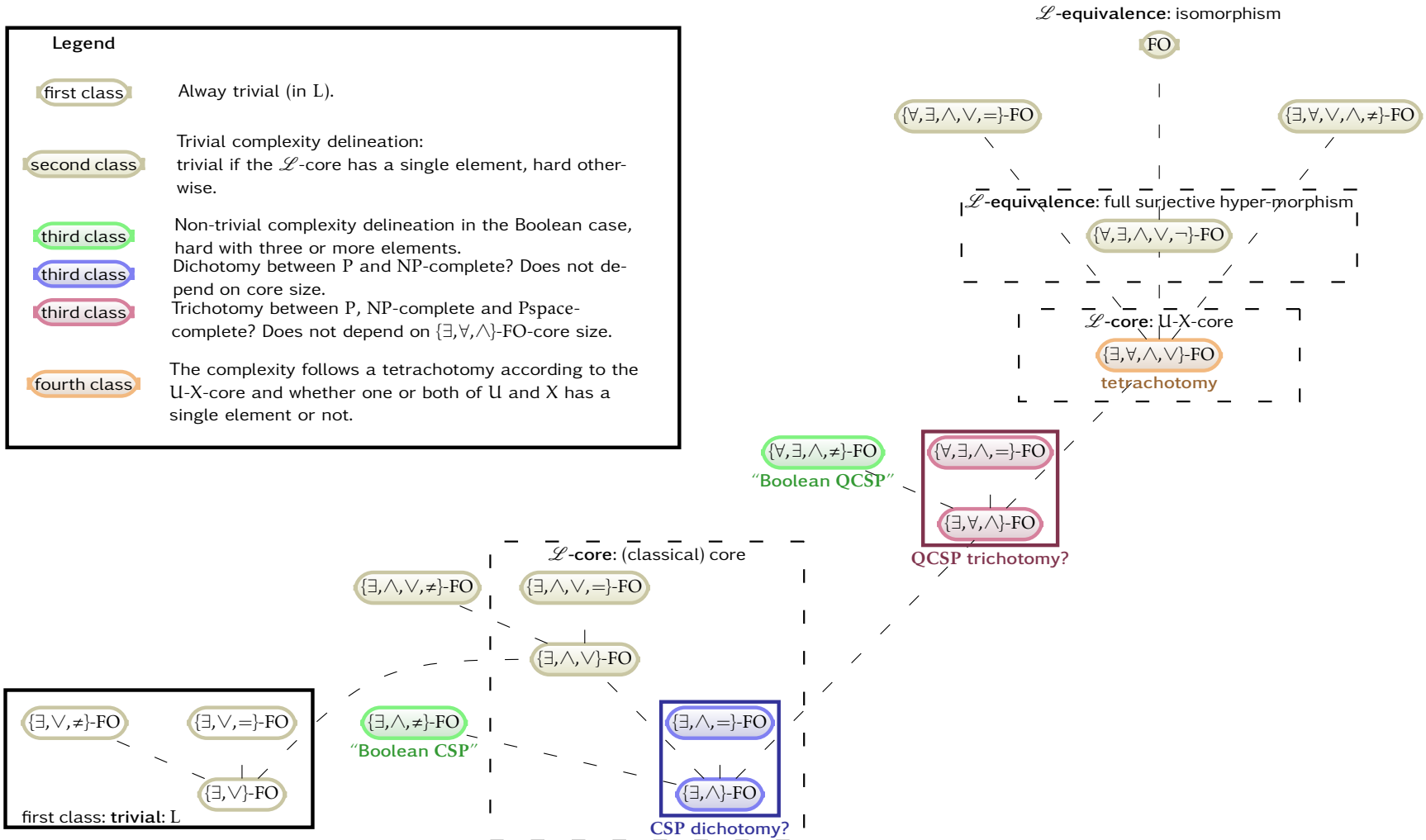
We now turn our attention to model checking for fragments of FO defined by the presence or absence of symbols from $\{\exists, \forall, \wedge, \vee, =, \neq\}$.

This is joint work with Barnaby D. Martin from Durham.

There are two ingredients :

- find the correct Galois connection
- find the correct notion of a core

Model checking for such fragments of FO : QCSP and perhaps CSP the only open cases.



Polychotomies of the model checking problem

Fragment	Dual	Classification?
$\{\exists, \vee\}$ $\{\exists, \vee, =\}$	$\{\forall, \wedge\}$ $\{\forall, \wedge, \neq\}$	Trivial (in L).
$\{\exists, \wedge, \vee\}$ $\{\exists, \wedge, \vee, =\}$	$\{\forall, \wedge, \vee\}$ $\{\forall, \wedge, \vee, \neq\}$	Trivial (in L) if the core of $\mathfrak{D}$ has one element and NP-complete otherwise.
$\{\exists, \wedge, \vee, \neq\}$	$\{\forall, \wedge, \vee, =\}$	Trivial (in L) if $\lvert \mathrm{D} \rvert = 1$ and NP-complete otherwise.
$\{\exists, \wedge\}$ $\{\exists, \wedge, =\}$	$\{\forall, \vee\}$ $\{\forall, \vee, \neq\}$	**CSP dichotomy** phenomenon: P or NP-complete.
$\{\exists, \wedge, \neq\}$	$\{\forall, \vee, =\}$	Trivial if $\lvert \mathrm{D} \rvert = 1$; in P if $\lvert \mathrm{D} \rvert = 2$ and $\mathfrak{D}$ is affine or bijunctive; and, NP-complete otherwise.
$\{\exists, \forall, \wedge\}$ $\{\exists, \forall, \wedge, =\}$	$\{\exists, \forall, \vee\}$ $\{\exists, \forall, \vee, \neq\}$	A **QCSP trichotomy** is observed: P, NP-complete, or Pspace-complete.
$\{\exists, \forall, \wedge, \neq\}$	$\{\exists, \forall, \vee, =\}$	Trivial if $\lvert \mathrm{D} \rvert = 1$; in P if $\lvert \mathrm{D} \rvert = 2$ and $\mathfrak{D}$ is affine or bijunctive; and, Pspace-complete otherwise.
$\{\forall, \exists, \wedge, \vee\}$		**Positive equality free tetrachotomy**: P, NP-complete, co-NP-complete or Pspace-complete
$\{\neg, \exists, \forall, \wedge, \vee\}$		Trivial when $\mathfrak{D}$ contains only trivial relations (empty or all tuples, and Pspace-complete otherwise.
$\{\forall, \exists, \wedge, \vee, =\}$ $\{\forall, \exists, \wedge, \vee, \neq\}$ $\{\neg, \exists, \forall, \wedge, \vee, =\}$		Trivial when $\lvert \mathrm{D} \rvert = 1$, Pspace-complete otherwise.

Galois Connections

The algebraic method has been used to great effect in the study of both the CSP and the QCSP. The relevant connections are:

- $\langle \mathbb{A} \rangle_{\{\exists,\wedge,=\}\text{-FO}} = \mathsf{Inv\text{-}Pol}(\mathbb{A})$.
- $\langle \mathbb{A} \rangle_{\{\exists,\forall,\wedge,=\}\text{-FO}} = \mathsf{Inv\text{-}sPol}(\mathbb{A})$.

Many other connections exist, for example

- $\langle \mathbb{A} \rangle_{\{\exists,\wedge,\vee,=\}\text{-FO}} = \mathsf{Inv\text{-}End}(\mathbb{A})$.
- $\langle \mathbb{A} \rangle_{\{\exists,\forall,\wedge,\vee,=\}\text{-FO}} = \langle \mathbb{A} \rangle_{\{\neg,\exists,\forall,\wedge,\vee,=\}\text{-FO}} = \mathsf{Inv\text{-}Aut}(\mathbb{A})$.

Ferdinand Börner's tips for Galois Connections

relation closed under	preserved by "operation"
absence of $\exists$	partial
presence of $\forall$	surjective
presence of $\bigvee$	unary
presence of $=$	functions
absence of $=$	hyperfunctions
presence of $\neq$	injective
presence of atomic $\neg$	full

Which Galois Connection for $\{\exists, \forall, \wedge, \vee\}$-FO?

relation closed under	preserved by "operation"
absence of $\exists$	partial
presence of $\forall$	"surjective"
presence of $\vee$	unary
presence of $=$	functions
absence of $=$	hyperfunctions
presence of $\neq$	injective
presence of atomic $\neg$	full

Lower bounds

Quantifier Elimination by relativisation to a constant

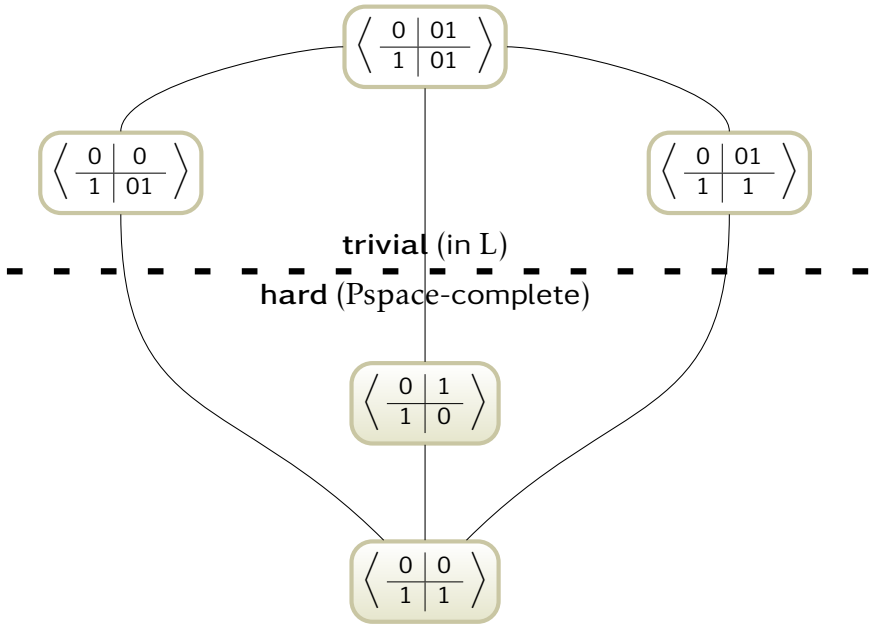
presence of a she	complexity drops to	"algorithm"
with $f(u) = D$	NP	evaluate all $\forall$ to u
with $f^{-1}(x) = D$	co-NP	evaluate all $\exists$ to x
both	L	simultaneously do both

Lower bounds

Quantifier Elimination by relativisation to a constant

presence of a she	complexity drops to	"algorithm"
A-shop	NP	evaluate all $\forall$ to $\mathfrak{u}$
E-shop	co-NP	evaluate all $\exists$ to $\mathfrak{x}$
both	L	simultaneously do both

Treillis des monoides et complexité pour $\{\exists, \forall, \wedge, \vee\}$-FO



Analogue Schaeffer

Analogue Bulatov.
Tétrachotomie entre L, NP-complet, coNP-complet et Pspace-complet.

Pour un domaine de taille 3, on calcule à la main (une partie adaptée) du treillis des monoides
Pour un domaine de taille 4, on calcule par ordinateur ce treillis.

Tetrachotomy for all finite domains

Theorem

Let $\mathcal{B}$ be any finite structure.

I. *If* $\mathrm{shE}(\mathcal{B})$ *contains both an* A*-shop and an* E*-shop, then* $\{\exists,\forall,\wedge,\vee\}$-$\mathrm{FO}(\mathcal{B})$ *is in* L.

II. *If* $\mathrm{shE}(\mathcal{B})$ *contains an* A*-shop but no* E*-shop, then* $\{\exists,\forall,\wedge,\vee\}$-$\mathrm{FO}(\mathcal{B})$ *is* NP*-complete*.

III. *If* $\mathrm{shE}(\mathcal{B})$ *contains an* E*-shop but no* A*-shop, then* $\{\exists,\forall,\wedge,\vee\}$-$\mathrm{FO}(\mathcal{B})$ *is* co-NP*-complete*.

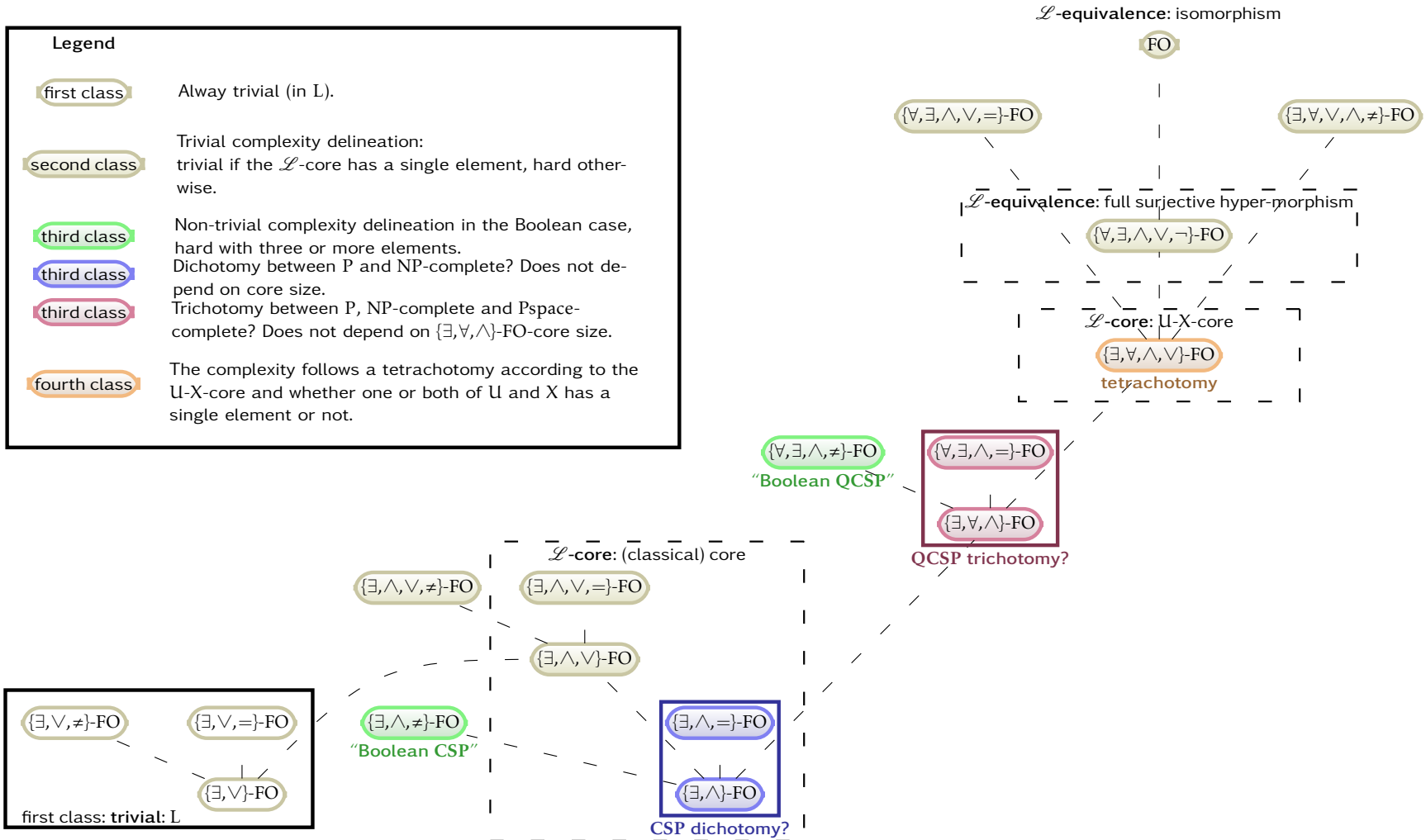
IV. *If* $\mathrm{shE}(\mathcal{B})$ *contains neither an* A*-shop nor an* E*-shop, then* $\{\exists,\forall,\wedge,\vee\}$-$\mathrm{FO}(\mathcal{B})$ *is in* Pspace*-complete.*

proved for domain size 2,3,4 using the lattice.
need to move away from the lattice for general case.

Sketch of the proof.

- The lower bounds were already proved, the main technical hurdle is to show Pspace-hardness (case IV)
- A new notion, the U-X-shop
- The presence of a U-X-shop characterises the possibility of relativising of quantifiers
- We impose minimality conditions on the set U and X
  $\Rightarrow$ U-X-core
- We may assume w.l.o.g. that the domain of the structure $\mathcal{B}$ is $U \cup X$ (the U-X-core is the $\{\exists, \forall, \wedge, \vee\}$-FO-core)
- We derive a normal form of the monoid associated with the structure $\mathcal{B}$.
- If we establish hardness for a larger monoid then it is OK
  More operation $\Longrightarrow$ less relations (complexity is $\leqslant$).
- We use relatively simple proof techniques for these larger monoids (the reduction are essentially present in the classification of the 4 element case).

Model checking for such fragments of FO : QCSP and perhaps CSP the only open cases.



The FürstenProblem : QCSP

Model checking problem for ($\{\exists, \forall, \wedge\}$-FO)

3 complexity observed in nature : Pspace-complete, NP-complete and in P.

Drop from Beyond NP to NP explained by a generalisation of relativisation, best explained as the fact that a general family of Skolem function can be interpolated from a family of partial Skolem functions.

Collapsibility

Introduced by Hubie Chen

Idea : $\forall$ plays all universal variables on a constant but for a fixed number of variables. A general winning strategy can be derived.

Un exemple : Horn

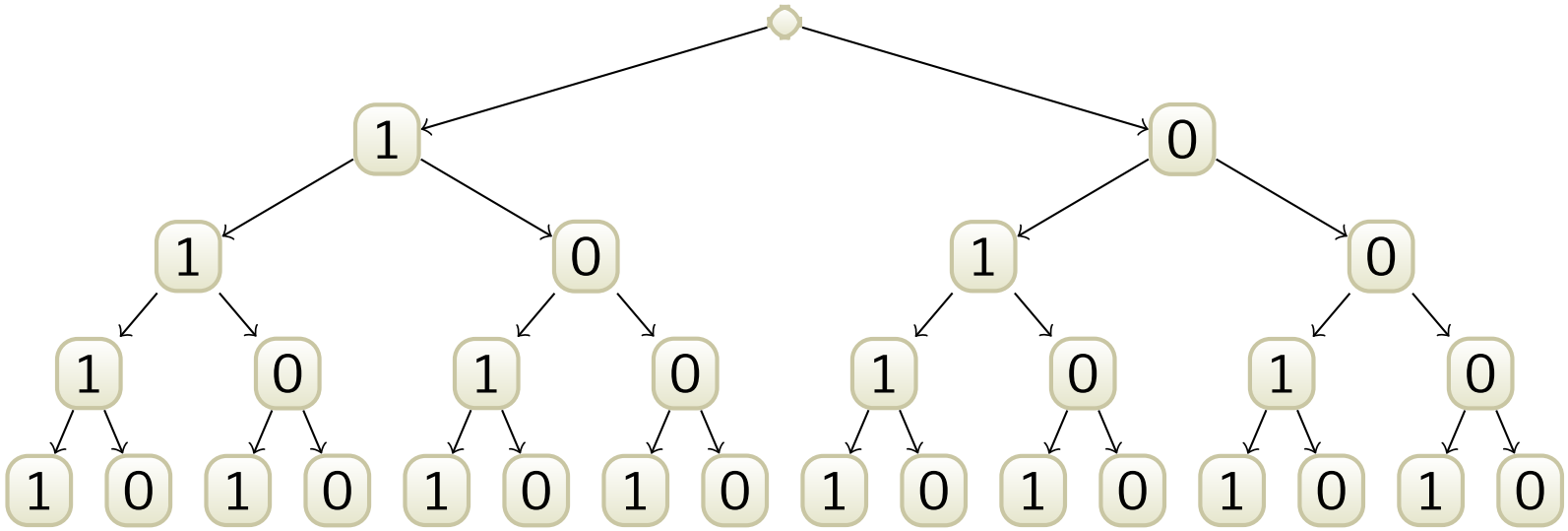
Pour un langage de contrainte de type Horn, on a cette propriété.

Pourquoi?

À cause de la préservation par $\wedge$.

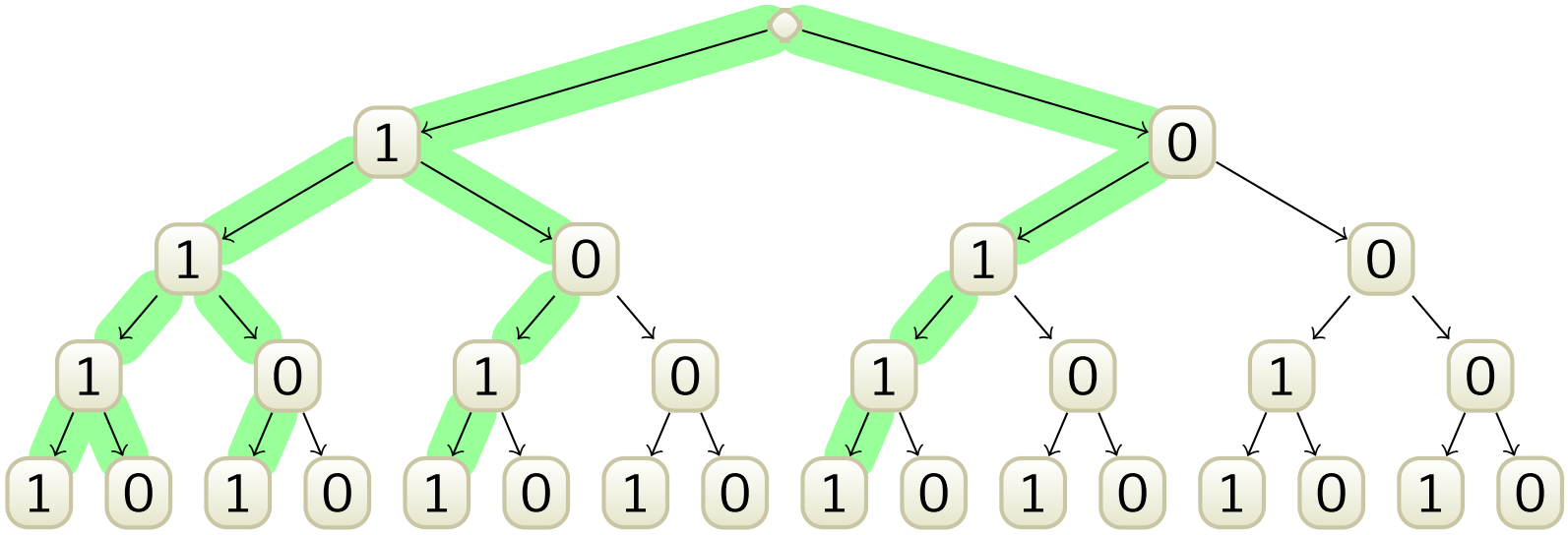
Construire la réponse à partir d'une petite partie des cas

Exemple pour 4 variables universelles.



Construire la réponse à partir d'une petite partie des cas

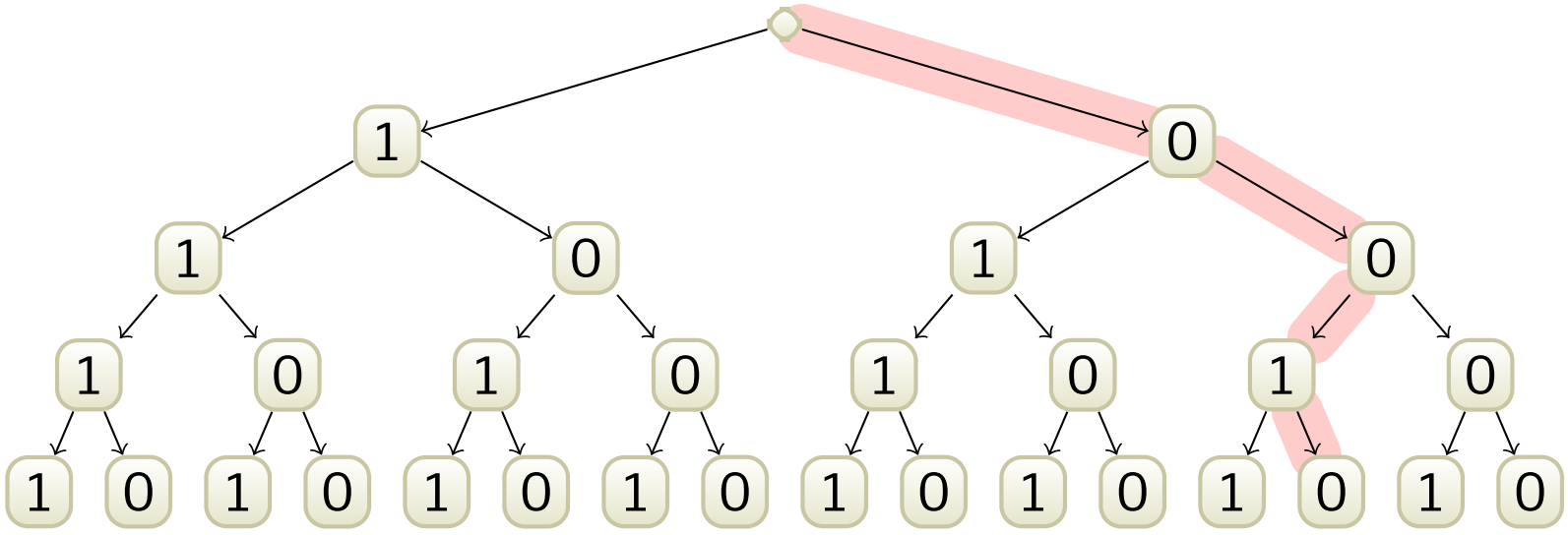
Exemple pour 4 variables universelles.



Il suffit de garder au plus une variable universelle à 0. Si un cas est NON alors NON

Construire la réponse à partir d'une petite partie des cas

Exemple pour 4 variables universelles.

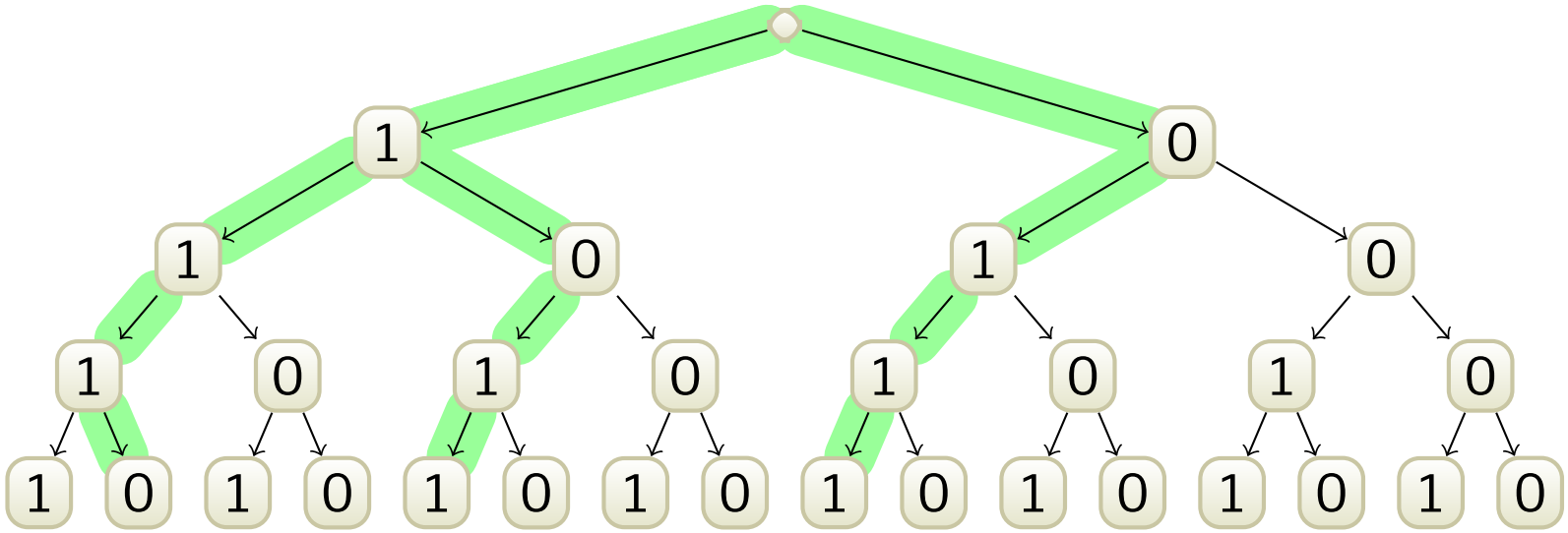


Il suffit de garder au plus une variable universelle à 0. Si un cas est NON alors NON

Sinon pour n'importe quel autre cas, on peut reconstruire une solution à partir des cas précédents (préservation par $\wedge$)

Construire la réponse à partir d'une petite partie des cas

Exemple pour 4 variables universelles.

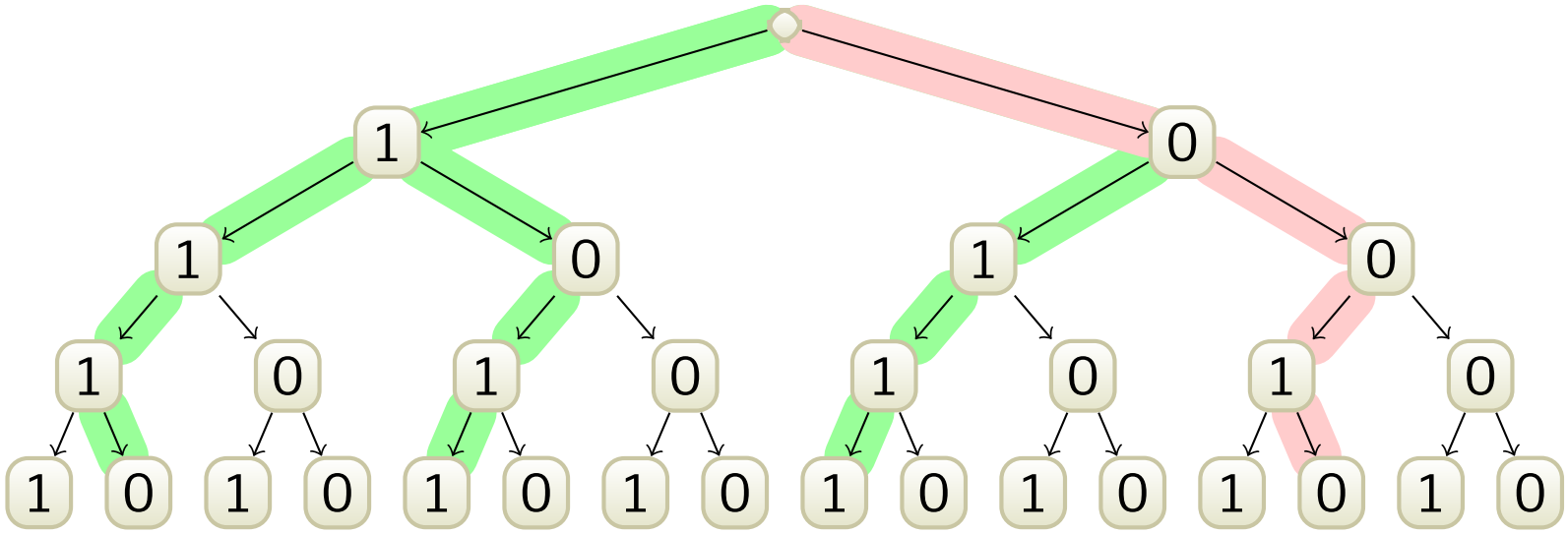


Il suffit de garder au plus une variable universelle à 0. Si un cas est NON alors NON

Sinon pour n'importe quel autre cas, on peut reconstruire une solution à partir des cas précédents (préservation par $\wedge$)

Construire la réponse à partir d'une petite partie des cas

Exemple pour 4 variables universelles.



Il suffit de garder au plus une variable universelle à 0. Si un cas est NON alors NON

Sinon pour n'importe quel autre cas, on peut reconstruire une solution à partir des cas précédents (préservation par $\wedge$)

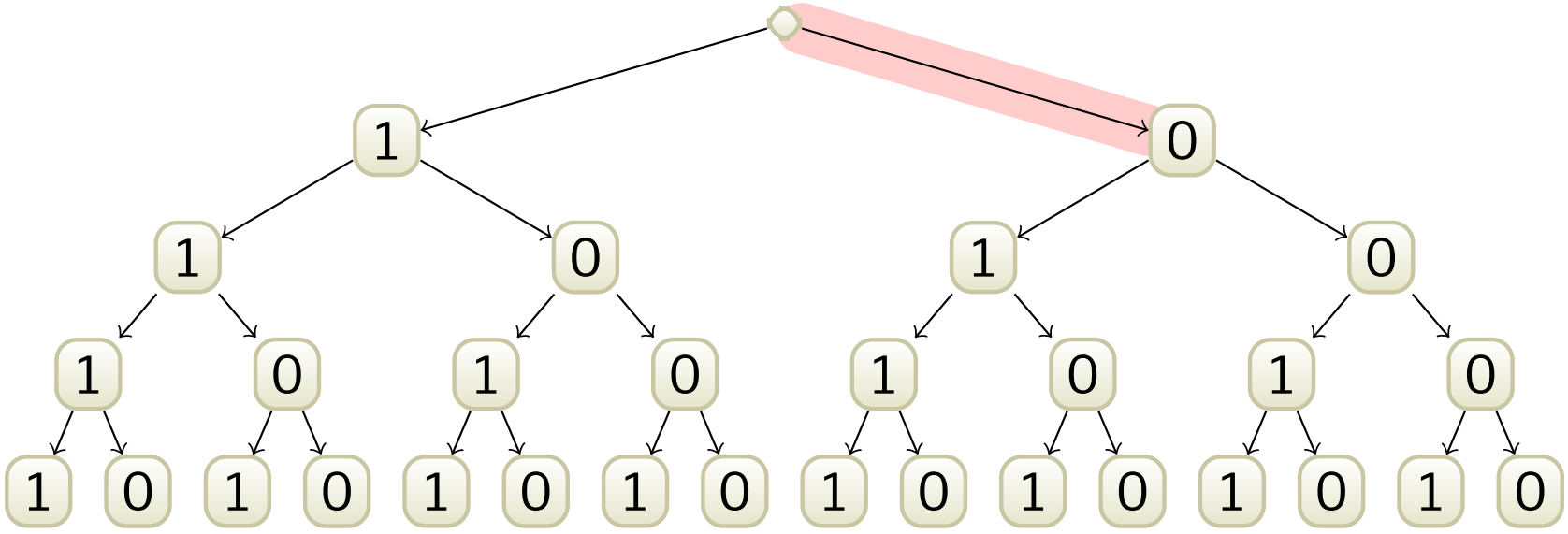
Et en général?

- Pour des formules avec plus d'alternances de quantificateurs mais en nombre borné (par exemple $\forall^\star\exists^\star\forall^\star\exists^\star$), on peut faire une réduction un peu plus compliqué
- Mais dans le cas général ça ne marche pas (puisque par exemple, l'approche ci-dessus nous fait payer m^{2p} cas pour 4 alternances).

Mais : pour la *collapsibility* on montre que cela fonctionne même dans le cas non borné.
En particulier, c'est le cas pour Horn avec $\wedge$.

Retour sur l'exemple Horn

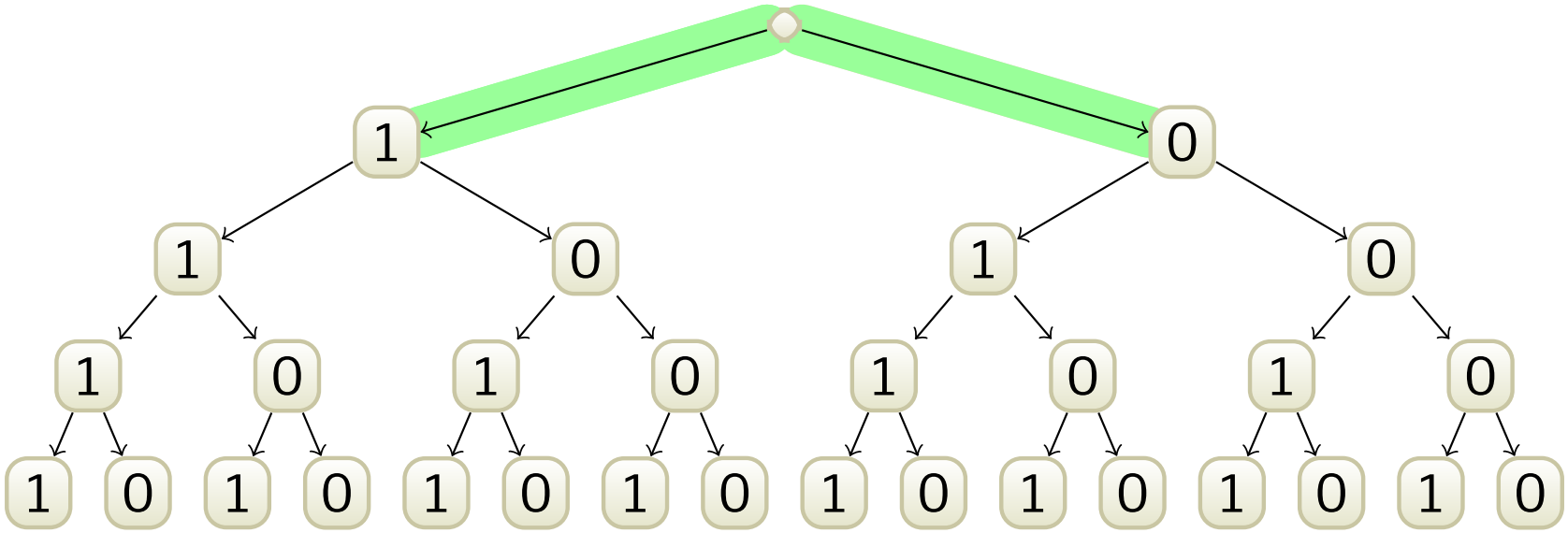
Exemple pour 4 variables universelles.



Si nombre d'alternance est non borné, on procède sur le même principe mais de manière incrémentale.

Retour sur l'exemple Horn

Exemple pour 4 variables universelles.

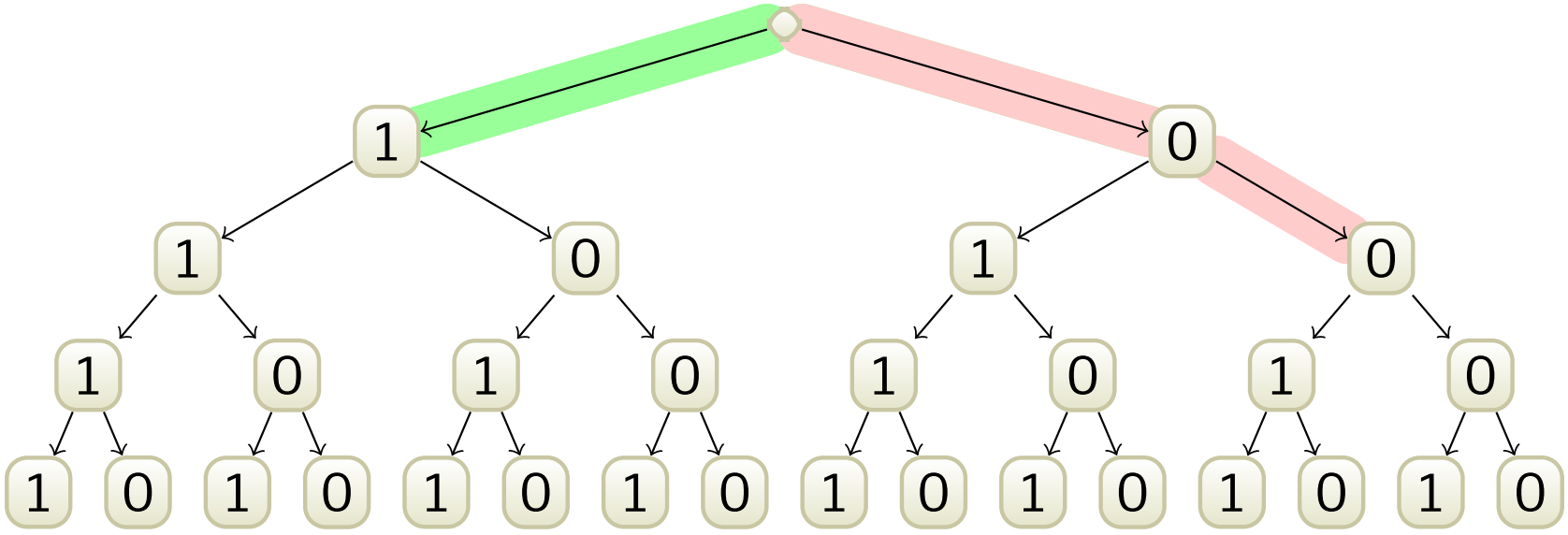


Si nombre d'alternance est non borné, on procède sur le même principe mais de manière incrémentale.

Donc : si il y a des quantificateurs existentiels entre les quantificateurs universels, on peut donner la réponse avant de connaître la valeur des variables universelles qui suivent.

Retour sur l'exemple Horn

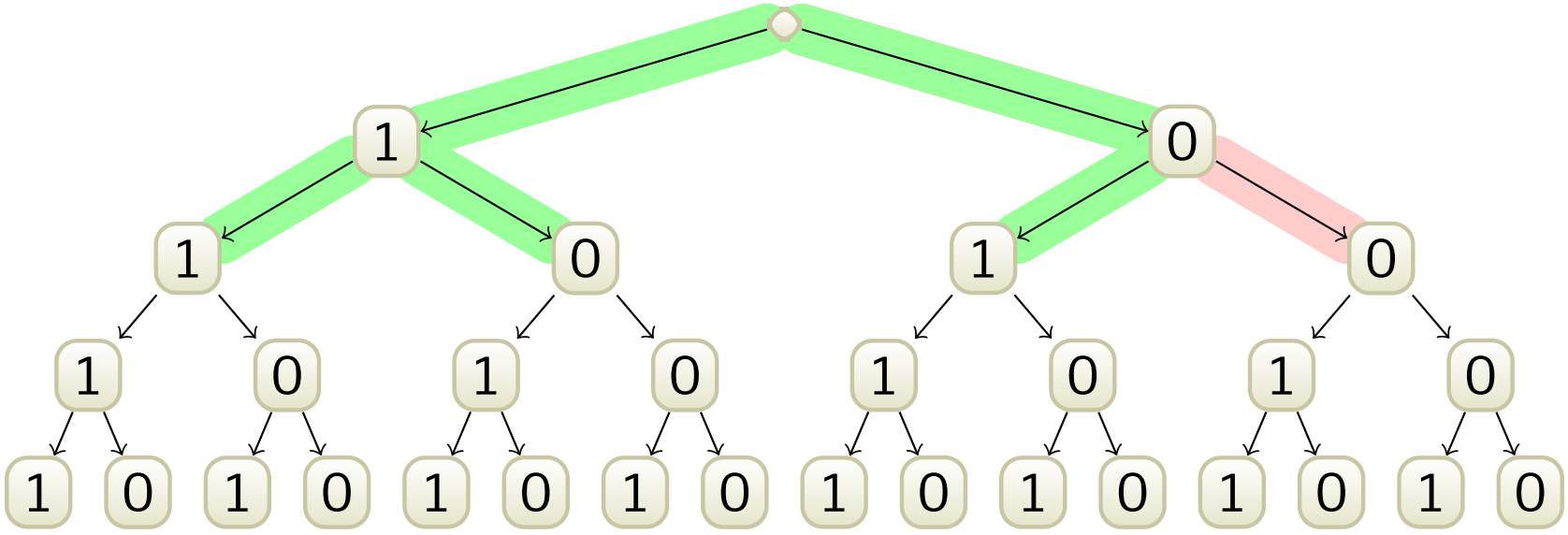
Exemple pour 4 variables universelles.



Si nombre d'alternance est non borné, on procède sur le même principe mais de manière incrémentale.

Retour sur l'exemple Horn

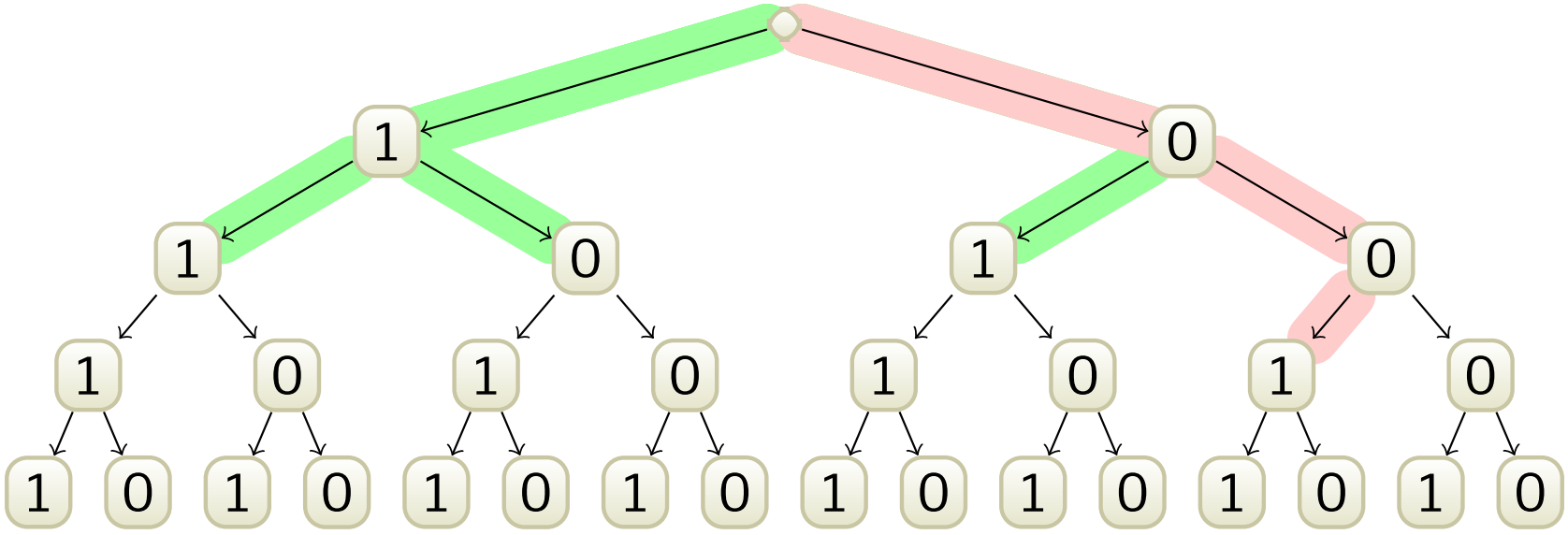
Exemple pour 4 variables universelles.



Si nombre d'alternance est non borné, on procède sur le même principe mais de manière incrémentale.

Retour sur l'exemple Horn

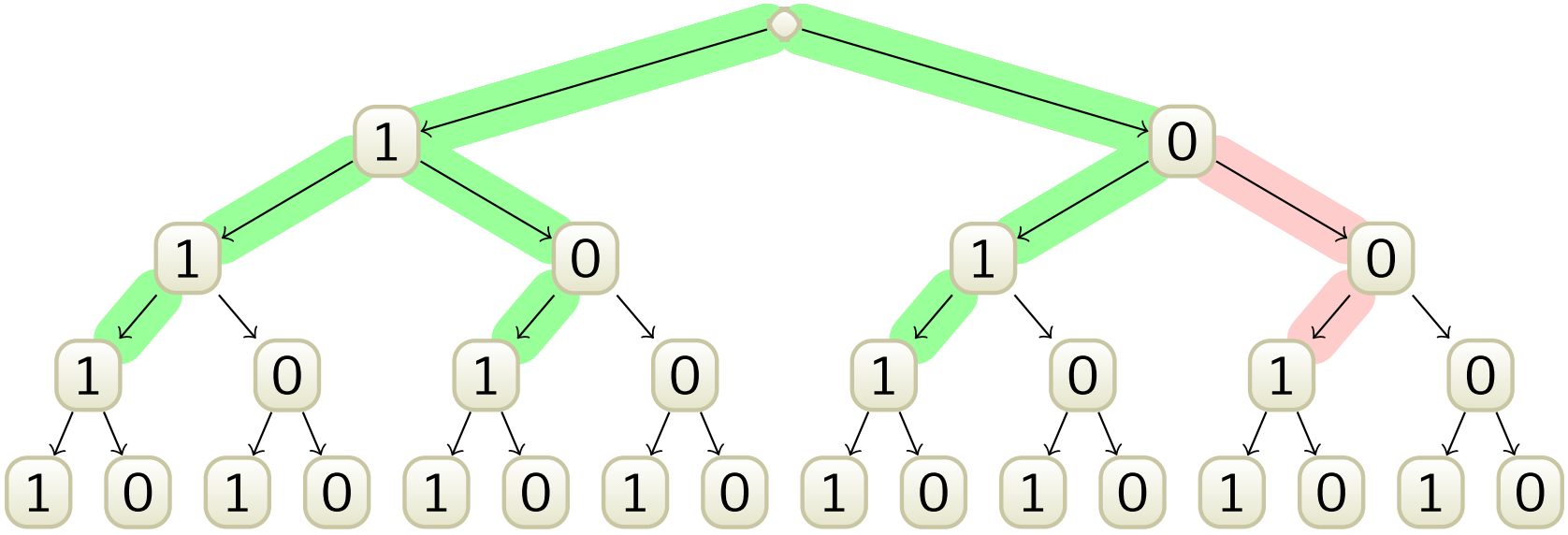
Exemple pour 4 variables universelles.



Si nombre d'alternance est non borné, on procède sur le même principe mais de manière incrémentale.

Retour sur l'exemple Horn

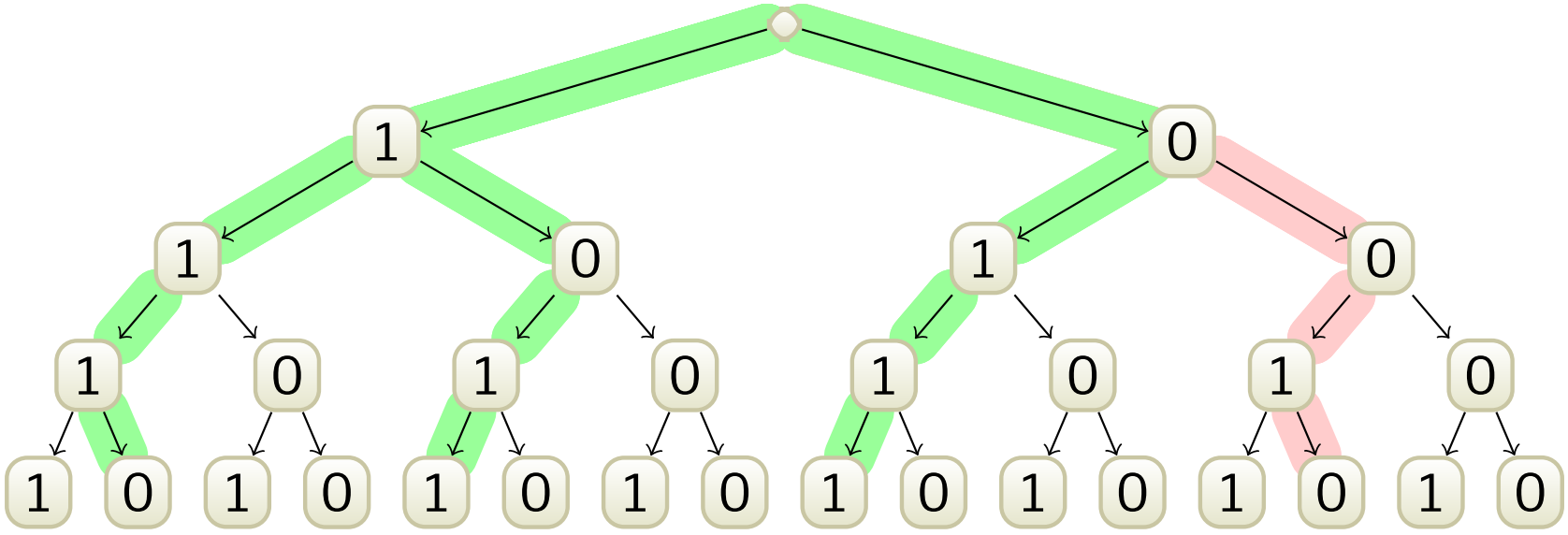
Exemple pour 4 variables universelles.



Si nombre d'alternance est non borné, on procède sur le même principe mais de manière incrémentale.

Retour sur l'exemple Horn

Exemple pour 4 variables universelles.



Si nombre d'alternance est non borné, on procède sur le même principe mais de manière incrémentale.

Exo

Montrez qu'on peut procéder de manière similaire pour le cas bijonctif (prendre $\mathfrak{p} = 2$ et une valeur quelconque pour $\mathfrak{c}$).
On rappelle que le cas bijonctif est caractérisé par $\mathfrak{m}$, la fonction ternaire de majorité (argument le + fréquent).

Exo explique algo pour Q2SAT

Volume 8, number 3 INFORMATION PROCESSING LETTERS March 1979

A LINEAR-TIME ALGORITHM FOR TESTING THE TRUTH OF CERTAIN QUANTIFIED BOOLEAN FORMULAS *

Bengt ASPVALL, Michael F. PLASS and Robert Endre TARJAN
Computer Science Department, Stanford University, Stanford, CA 94305, U.S.A.

Received 22 August 1978, revised version received 16 October 1978

Quantified Boolean formula, strongly connected components, 2-CNF, 2-satisfiability

Exo explique algo pour Q2SAT

$Q_1x_1\ Q_2x_2 \cdots Q_nx_n\ C$ such that C is in conjunctive normal form with at most two literals per clause. We can assume without loss of generality that there are no clauses with only one literal since the clause u is equivalent to the clause $u \vee u$. We construct a directed graph $G(F)$ with $2n$ vertices and $2|C|$ edges (counting multiple edges) as follows:

1(i) For each variable x_i, we add two vertices named x_i and $\bar{x}_i$ to $G(F)$. We identify $\bar{x}_i$ with x_i, and we call x_i and $\bar{x}_i$ *complements* of each other.

1(ii) For each clause $(u \vee v)$ of C, we add edges $\bar{u} \to v$ and $\bar{v} \to u$ to $G(F)$.

The graph $G(F)$ has the following *duality property*: $G(F)$ is isomorphic to the graph obtained from $G(F)$ by reversing the directions of all the edges and complementing the names of all the vertices. See Fig. 1.

Our algorithm relies upon identifying the strong components of $G(F)$. A graph is *strongly connected* if there is a path from any vertex to any other. The

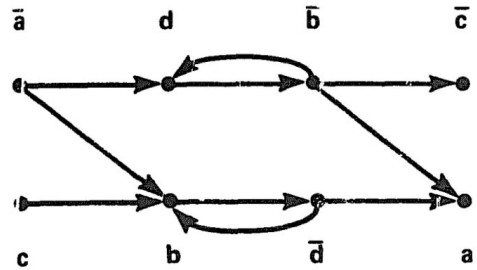


Fig. 1. Graph constructed for the set of clauses $C = \{a \vee b, b \vee \bar{c}, \bar{b} \vee \bar{d}, b \vee d, d \vee a\}$.

Exo explique algo pour Q2SAT

Theorem 2. *The formula F is true if and only if none of the following three conditions holds:*

3(i) *An existential vertex u is in the same strong component as its complement $\bar{u}$.*

3(ii) *A universal vertex u_i is in the same strong component as an existential vertex u_j such that $j < i$ (i.e., x_j is not quantified within the scope of Q_i).*

3(iii) *There is a path from a universal vertex u to another universal vertex v. (This condition includes the case that $v = \bar{u}$.)*

The FürstenProblem : QCSP

- PGP vs EGP gap and PGP implies Π_2-switchability [Zhuk ′15]
- Π_2-switchability is the same as switchability [Carvalho, Madelaine, Martin ′15]
- Corollary : PGP implies drop in complexity from Pspace-complete in general to within NP.

Open

Does EGP implies Pspace-completeness?

A few pointers

To start

- Hubie Chen: Logic Column 17: A Rendezvous of Logic, Complexity, and Algebra. CoRR abs/cs/0611018 (2006).

Surveys

- Hubie Chen: Meditations on Quantified Constraint Satisfaction. Logic and Program Semantics 2012: 35-49.
- Barnaby Martin: Quantified Constraints in Twenty Seventeen. The Constraint Satisfaction Problem 2017: 327-346

Biblio specific to « relativisation »

- Florent R. Madelaine, Barnaby Martin: On the complexity of the model checking problem .CoRR abs/1210.6893 (2012).
- Catarina Carvalho, Florent R. Madelaine, Barnaby Martin: From Complexity to Algebra and Back: Digraph Classes, Collapsibility, and the PGP. LICS 2015: 462-474
- Catarina Carvalho, Barnaby Martin, Dmitriy Zhuk: The complexity of quantified constraints. CoRR abs/1701.04086 (2017).