Chapitre 9 : Logique propositionnelle

(Sémantique et mise sous forme normale)

slides disponibles sur `http://cahier-de-prepa/mp2i-fermat`

Plan

Interprétation - définition

On considère encore $\mathcal{Q}$ un ensemble non vide de variables.
On note encore $\mathbb{B}$ l'algèbre de Boole.

Définition

*Un **environnement propositionnel** est une fonction de $\mathcal{Q}$ dans $\mathbb{B}$.*

Définition

*Soit $\rho \in \mathbb{B}^{\mathcal{Q}}$ un environnement propositionnel. On définit l'**interprétation selon** ρ des formules de la logique propositionnelle sur $\mathcal{Q}$ comme étant la fonction $[\bullet]^\rho$ ci-contre.*

$$
\left(\begin{array}{rcl}
\mathbb{F}_p(\mathcal{Q}) & \to & \mathbb{B} \\
\top & \mapsto & V \\
\bot & \mapsto & F \\
q \in \mathcal{Q} & \mapsto & \rho(q) \\
\neg A & \mapsto & \overline{[A]^\rho} \\
A \vee B & \mapsto & [A]^\rho + [B]^\rho \\
A \wedge B & \mapsto & [A]^\rho \cdot [B]^\rho \\
A \to B & \mapsto & \overline{[A]^\rho} \cdot [B]^\rho \\
A \leftrightarrow B & \mapsto & ([A]^\rho \cdot [B]^\rho) \\
 & & +(\overline{[A]^\rho} \cdot \overline{[B]^\rho})
\end{array}\right)
$$

Vocabulaire

Définition

Soit $A \in \mathbb{F}_p(\mathcal{Q})$.

*Pour $\rho \in \mathbb{B}^{\mathcal{Q}}$, si $[A]^\rho = V$, on dit que ρ **satisfait** A.*
*On dit que A est **satisfiable** s'il existe $\rho \in \mathbb{B}^{\mathcal{Q}}$ tel que $[A]^\rho = V$.*
*On dit que A est **une tautologie** (ou valide) si $\forall \rho \in \mathbb{B}^{\mathcal{Q}}$, $[A]^\rho = V$.*
*On dit que A est **une antilogie** (ou insatisfiable) si $\forall \rho \in \mathbb{B}^{\mathcal{Q}}$, $[A]^\rho = F$.*

Attention : antilogie n'est pas la négation de tautologie, mais celle de formule satisfiable.

Fonction booléenne associée à une formule - définition

informel Changement de point de vue : $[A]^\rho$ dépend de A et de ρ.
Pour la dépendance en A on a, pour $\rho \in \mathbb{B}^{\mathcal{Q}}$ fixé, la fonction $[\bullet]^\rho = A \mapsto [A]^\rho$.
Pour celle en ρ on veut, pour $A \in \mathbb{F}_p(\mathcal{Q})$ fixée, la fonction $\rho \mapsto [A]^\rho$.

Définition

Soit $A \in \mathbb{F}_p(\mathcal{Q})$.
*On appelle **fonction booléenne associée** à la formule A la fonction*

$$[\![\bullet]\!]^A = \begin{pmatrix} \mathbb{B}^{\mathcal{Q}} & \to & \mathbb{B} \\ \rho & \mapsto & [A]^\rho \end{pmatrix}$$

Remarque : Toute fonction booléenne d'arité $n \in \mathbb{N}^*$ est la fonction booléenne associée d'une formule propositionnelle sur un ensemble de variables propositionnelles de cardinal n.
(voir section mise sous forme normale)

Équivalence logique - définition

Définition

On définit la relation binaire $\equiv$ sur $\mathbb{F}_p(\mathcal{Q})$ par

$$\begin{aligned} \forall (A,B) \in \mathbb{F}_p(\mathcal{Q})^2,\ A \equiv B \text{ ssi } & [\![\bullet]\!]^A = [\![\bullet]\!]^B \\ \text{ssi } & \forall \rho \in \mathbb{B}^{\mathcal{Q}},\ [\![\rho]\!]^A = [\![\rho]\!]^B \\ \text{ssi } & \forall \rho \in \mathbb{B}^{\mathcal{Q}},\ [A]^\rho = [B]^\rho \end{aligned}$$

Autrement dit, $\left\{\rho \in \mathbb{B}^{\mathcal{Q}} \middle| [A]^\rho = V\right\} = \left\{\rho \in \mathbb{B}^{\mathcal{Q}} \middle| [B]^\rho = V\right\}$.

Propriété

La relation $\equiv$ est une relation d'équivalence sur $\mathbb{F}_p(\mathcal{Q})$.

Définition

Soit $(A,B) \in \mathbb{F}_p(\mathcal{Q})^2$.
*On dit que A et B sont **logiquement équivalentes** si $A \equiv B$.*

Équivalence logique - exemples

Pour $(A,B) \in \mathbb{F}_p(\mathcal{Q})^2$ on a $A \vee B \equiv B \vee A$.

En effet, $\forall \rho \in \mathbb{B}^{\mathcal{Q}}$, $[A \vee B]^\rho = [A]^\rho + [B]^\rho$ par déf de l'interprétation
$= [B]^\rho + [A]^\rho$ par commutativité de $+$
$= [B \vee A]^\rho$ par déf de l'interprétation

Exercice : Soit $(A,B) \in \mathbb{F}_p(\mathcal{Q})^2$. Montrer que

- $A \wedge B \equiv B \wedge A$
- $A \to B \equiv (\neg A) \vee B$
- $A \to B \equiv (\neg B) \to (\neg A)$
- $A \leftrightarrow B \equiv (A \to B) \wedge (B \to A)$
- $A \vee \neg A \equiv \top$
- $\neg(A \wedge B) \equiv \neg A \vee \neg B$
- $\neg(A \vee B) \equiv \neg A \wedge \neg B$

Conséquence logique - définition

Définition

Soit $(A,B) \in \mathbb{F}_p(\mathcal{Q})^2$.
*On dit que B est **conséquence logique** de A, noté $A \vDash B$ ssi tout environnement propositionnel satisfaisant A satisfait aussi B.*
c'est-à-dire en terme d'ensemble d'environnements ? Autrement dit, $\left\{\rho \in \mathbb{B}^{\mathcal{Q}} \middle| [A]^\rho = V\right\} \subseteq \left\{\rho \in \mathbb{B}^{\mathcal{Q}} \middle| [B]^\rho = V\right\}$.

Propriété

La relation binaire $\vDash$ est réflexive et transitive.

Propriété

Soit $(A,B) \in \mathbb{F}_p(\mathcal{Q})^2$. $A \equiv B$ ssi $A \vDash B$ et $B \vDash A$.

preuve à faire (+ remarque csq sémantique vs déduction)

Conséquence logique - exemples

Définition

Soit $X \subseteq \mathbb{F}_p(\mathcal{Q})$. Soit $B \in \mathbb{F}_p(\mathcal{Q})$.
On note $X \vDash B$ ssi tout environnement propositionnel satisfaisant ***toutes*** *les formules de X satisfait aussi B.*
Autrement dit, $\left\{\rho \in \mathbb{B}^{\mathcal{Q}} \middle| \forall A \in X,\ [A]^\rho = V\right\} \subseteq \left\{\rho \in \mathbb{B}^{\mathcal{Q}} \middle| [B]^\rho = V\right\}$.

différence avec "B est conséquence de la conjonction des formules de X" ? $\hookrightarrow$ *X peut être de cardinal infini.*

Exercice : Soit $(A, B) \in \mathbb{F}_p(\mathcal{Q})^2$. Montrer que
- $\rightarrow$ $\{(A \to B), A\} \vDash B$
- $\rightarrow$ $\{(A \to B), \neg B\} \vDash \neg A$

Reformulation des définitions avec $\equiv$

Propriété

Soit $A \in \mathbb{F}_p(\mathcal{Q})$.
- $\rightarrow$ *A est une tautologie ssi $A \equiv \top$*
- $\rightarrow$ *A est une antilogie ssi $A \equiv \bot$*
- $\rightarrow$ *A est une tautologie ssi $\neg A$ est une antilogie*

Propriété

Soit $(A, B) \in \mathbb{F}_p(\mathcal{Q})^2$.
- $\rightarrow$ *$A \equiv B$ ssi $A \leftrightarrow B \equiv \top$ (i.e. $A \leftrightarrow B$ est une tautologie)*
- $\rightarrow$ *$A \vDash B$ ssi $A \to B \equiv \top$ (i.e. $A \to B$ est une tautologie)*

preuves à faire en exercice

Espace quotient

L'espace des formules logiques quotienté par équivalence $\mathbb{F}_p(\mathcal{Q})/\equiv$ est en bijection avec $\mathcal{F}(\mathbb{B}^{\mathcal{Q}}, \mathbb{B})$. En effet une classe d'équivalence selon $\equiv$ est caractérisée par la fonction booléenne à laquelle sont associées tous ses éléments. Cela justifie que $[\![\bullet]\!]^A$ soit parfois appelée la **représentation** de A.

$\hookrightarrow$ Quel est représentant d'une classe préfère-t-on ?
$\hookrightarrow$ Peut-on choisir une formule canonique pour représenter une classe de formules équivalentes ?

Plan

Sur un exemple

Comment mettre sous FND la formule $A = (a \vee b) \to (c \wedge a)$

a	b	c	$(a \vee b)$	$(c \wedge a)$	A	
V	V	V	V	V	V	$\to (a \wedge b \wedge c)$
V	V	F	V	F	F	
V	F	V	V	V	V	$\to (a \wedge \neg b \wedge c)$
V	F	F	V	F	F	
F	V	V	V	F	F	
F	V	F	V	F	F	
F	F	V	F	F	V	$\to (\neg a \wedge \neg b \wedge c)$
F	F	F	F	F	V	$\to (\neg a \wedge \neg b \wedge \neg c)$

$$(a \wedge b \wedge c) \vee (a \wedge \neg b \wedge c) \vee (\neg a \wedge \neg b \wedge c) \vee (\neg a \wedge \neg b \wedge \neg c)$$

$$(a \wedge b \wedge c) \vee \underbrace{(a \wedge \neg b \wedge c) \vee (\neg a \wedge \neg b \wedge c)}_{(\neg b \wedge c)} \vee (\neg a \wedge \neg b \wedge \neg c)$$

Table de vérité d'une formule

On étend ici la définition de table de vérité aux formules, pour une numérotation des variables fixée : $\mathcal{Q} = \{q_1, q_2, \dots q_n\}$ où $n = \text{Card}(\mathcal{Q})$.

Une table de vérité d'une formule $A \in \mathbb{F}_p(\mathcal{Q})$ est en fait une table de vérité de la fonction associée $[\![\bullet]\!]^A$:

- $\to \{(T_{i,j})_{j \in [1..n]} \mid i \in [1..2^n]\} = \mathbb{B}^{\mathcal{Q}}$
- $\to$ pour tout $i \in [1..2^n]$, $T_{i,n+1}$ vaut $[\![\rho^i]\!]^A$ où $\rho^i \in \mathbb{B}^{\mathcal{Q}}$ est défini par $\forall j \in [1..n]$, $\rho^i(q_j) = T_{i,j}$.

En calculant une FND à partir de T on calcule bien quelque chose qui ne dépend pas exactement de A mais de sa classe...

Calculer une FND à partir d'une table de vérité - 1/3

Soit $A \in \mathbb{F}_p(\mathcal{Q})$ où $\mathcal{Q} = \{q_1, q_2, \dots q_n\}$.
Soit T une table de vérité de A suivant cette numérotation de $\mathcal{Q}$.

Pour tout $i \in [1..2^n]$ et $j \in [1..n]$, on note $\ell_{i,j}$ comme étant

- $\to$ le littéral q_j si $T_{i,j} = V$
- $\to$ le littéral $\neg q_j$ si $T_{i,j} = F$

Lemme

$\forall i \in [1..2^n]$, $\forall j \in [1..n]$, $[\ell_{i,j}]^{\rho^i} = V$

Preuve: Soit $i \in [1..2^n]$. Soit $j \in [1..n]$.

Si $T_{i,j} = V$, alors $\ell_{i,j} = q_j$, donc $[\ell_{i,j}]^{\rho^i} = \rho^i(q_j)$ par définition de l'interprétation d'une variable. Or par définition de ρ^i, $\rho^i(q_j) = T_{i,j}$, donc $[\ell_{i,j}]^{\rho^i} = V$.

Si $T_{i,j} = F$, alors $\ell_{i,j} = \neg q_j$ donc $[\ell_{i,j}]^{\rho^i} = \overline{\rho^i(q_j)}$ par définition de l'interprétation d'une négation. Or par définition de ρ^i, $\rho^i(q_j) = T_{i,j} = F$, donc $[\ell_{i,j}]^{\rho^i} = \overline{F} = V$.

Calculer une FND à partir d'une table de vérité - 2/3

Ensuite on pose, pour tout $i \in [1..2^n]$, $L^i = \bigwedge_{j=1}^{n} \ell_{i,j}$.

Lemme

- $\forall i \in [1..2^n]$, $[L^i]^{\rho^i} = V$
- $\forall (i,k) \in [1..2^n]^2$, $i \neq k$, $[L^i]^{\rho^k} = F$

Preuve : Soit $i \in [1..2^n]$. Par définition de l'interprétation d'une conjonction, $[L^i]^{\rho^i} = \prod_{j=1}^{n} [\ell_{i,j}]^{\rho^i} = \prod_{j=1}^{n} V$ d'après le lemme précédent, d'où $[L^i]^{\rho^i} = V$.
Soit $k \in [1..2^n]$ tel que $k \neq i$.Puisque les lignes de T restreintes à leurs n premières colonnes sont deux à deux distinctes, il existe $j_0 \in [1..n]$ tel que $T_{i,j_0} \neq T_{k,j_0}$.
$\hookrightarrow$Si $T_{i,j_0} = V$, alors $\ell_{i,j_0} = q_{j_0}$ et $T_{k,j_0} = F$. Par déf. de l'interprétation d'une variable $[\ell_{i,j_0}]^{\rho^k} = \rho^k(q_{j_0})$, or par déf. de ρ^k on a $\rho^k(q_{j_0}) = T_{k,j_0} = F$, donc $[\ell_{i,j_0}]^{\rho^k} = F$.
$\hookrightarrow$Si au contraire $T_{i,j_0} = F$, alors $\ell_{i,j_0} = \neg q_{j_0}$ et $T_{k,j_0} = V$. Par déf. de l'interprétation de la négation d'une variable $[\ell_{i,j_0}]^{\rho^k} = \overline{\rho^k(q_{j_0})}$ or par déf. de ρ^k on a $\rho^k(q_{j_0}) = T_{k,j_0} = V$, donc $[\ell_{i,j_0}]^{\rho^k} = \overline{V} = F$.

Dans les deux cas le terme d'indice j_0 de la somme qu'est l'interprétation de L^i vaut F, et F étant absorbant pour $\times$, on en déduit que $[L^i]^{\rho^k} = F$.

Calculer une FND à partir d'une table de vérité - 3/3

Finalement on pose $D = \bigvee_{\substack{i\in[1..2^n] \\ T_{i,n+1}=V}} L^i$

Propriété

$D \equiv A$.

Preuve : Soit $\rho \in \mathbb{B}^{\mathcal{Q}}$. On note $I = \{i \in [1..2^n] \mid T_{i,n+1} = V\}$ ainsi $D = \bigvee_{i\in I} L^i$.

De plus par déf. de l'interprétation d'une disjonction $[D]^\rho = \sum_{i\in I} [L^i]^\rho$.

Puisque les lignes de T restreintes à leurs n premières colonnes couvrent $\mathbb{B}^{\mathcal{Q}}$, il existe $i_0 \in [1..2^n]$ tel que $\rho = \rho^{i_0}$.

↪ Si $[A]^\rho = V$, on a $V = [\![\rho]\!]^A = [\![\rho^{i_0}]\!]^A = T_{i_0,n+1}$, donc $i_0 \in I$. Ainsi le terme $[L^{i_0}]^\rho$ apparaît dans la somme qu'est $[D]^\rho$, or par le lemme préc., $[L^{i_0}]^\rho = [L^{i_0}]^{\rho^{i_0}} = V$,et V étant absorbant pour la somme, on en déduit que $[D]^\rho = V$, soit $[D]^\rho = [A]^\rho$.

↪ Si au contraire $[A]^\rho = F$, alors $T_{i_0,n+1} = F$ donc $i_0 \notin I$. Autrement dit $\forall i \in I$, $i \neq i_0$ donc d'après le lemme précédent $[L^i]^{\rho^{i_0}} = F$ soit $[L^i]^\rho = F$. Une somme de F étant F, on en déduit que $[D]^\rho = F$, soit $[D]^\rho = [A]^\rho$.

Sur le même exemple

Comment mettre sous FNC la formule $A = (a \vee b) \to (c \wedge a)$

a	b	c	$(a \vee b)$	$(c \wedge a)$	A	
V	V	V	V	V	V	
V	V	F	V	F	F	$\to (\neg a \vee \neg b \vee c)$
V	F	V	V	V	V	
V	F	F	V	F	F	$\to (\neg a \vee b \vee c)$
F	V	V	V	F	F	$\to (a \vee \neg b \vee \neg c)$
F	V	F	V	F	F	$\to (a \vee \neg b \vee c)$
F	F	V	F	F	V	
F	F	F	F	F	V	

$$(\neg a \vee \neg b \vee c) \wedge (\neg a \vee b \vee c) \wedge (a \vee \neg b \vee \neg c) \wedge (a \vee \neg b \vee c)$$

Calculer une FNC à partir d'une table de vérité

Soit $A \in \mathbb{F}_p(\mathcal{Q})$ où $\mathcal{Q} = \{q_1, q_2, \dots q_n\}$.
Soit T une table de vérité de A suivant cette numérotation de $\mathcal{Q}$.

Pour tout $i \in [1..2^n]$ et $j \in [1..n]$, on note $r_{i,j}$ comme étant
→ le littéral $\neg q_j$ si $T_{i,j} = V$
→ le littéral q_j si $T_{i,j} = F$

Ensuite on pose, pour tout $i \in [1..2^n]$, $R^i = \bigvee_{j=1}^{n} r_{i,j}$.

Finalement on pose $C = \bigwedge_{\substack{i\in[1..2^n] \\ T_{i,n+1}=F}} R^i$

Propriété

→ $\forall i \in [1..2^n]$, $\forall j \in [1..n]$, $[r_{i,j}]^{\rho^i} = F$
→ $\forall i \in [1..2^n]$, $[R^i]^{\rho^i} = F$ *et* $\forall k \in [1..2^n]$, $k \neq i$, $[R^i]^{\rho^k} = V$
→ $C \equiv A$

Bilan sur FNC/FND

- certaines formules sont à la fois sous FNC et FND
exemple : $a \vee b \vee c$

- il y a **existence** de la FNC/FND équivalente à une formule
(on vient de le montrer).

- il n'y a **pas unicité** de de la FNC équivalente à une formule
ex : $(a \vee \neg b) \wedge (c \vee d) \equiv (c \vee d) \wedge (a \vee \neg b)$ du à la commutativité
$(a \vee \neg b \vee b) \wedge (c \vee d) \equiv a \wedge (c \vee d)$ du à la simplfication

- Attention **la taille peut exploser** en passant d'une forme à l'autre
ex : $A = \bigvee_{i=1}^{n} (a_i \wedge b_i)$ est une conj. de n termes, écrite avec $2n$ littéraux,
mais une FND équivalente est une disjonction de 2^n termes étant chacun le produit de n littéraux (pour chaque $i \in [1..n]$, a_i ou b_i apparaît)
$A \equiv (a_1 \vee a_2 \vee a_3 \dots a_n) \wedge (b_1 \vee a_2 \vee a_3 \dots a_n) \wedge (a_1 \vee b_2 \vee a_3 \dots a_n) \dots \wedge (a_1 \vee b_2 \vee a_3 \dots \vee a_{n-1} \vee b_n) \dots \wedge (b_1 \vee b_2 \vee b_3 \dots \vee b_{n-1} \vee b_n)$

Exercices

Quelques simplifications utiles :

- $A \wedge \neg A \equiv \bot$
- $A \wedge \top \equiv A$
- $A \wedge \bot \equiv \bot$
- $A \wedge (\neg A \vee B) \equiv A \wedge B$
- $(A \vee B) \wedge (\neg A \vee B) \equiv B$
- $A \vee \neg A \equiv \top$
- $A \vee \top \equiv \top$
- $A \vee \bot \equiv A$
- $A \vee (\neg A \wedge B) \equiv A \vee B$
- $(A \wedge B) \vee (\neg A \wedge B) \equiv B$

Mettre sous FNC et FND les formules suivantes :

- $U : (x \wedge y) \vee (z \wedge \neg z \wedge q) \vee (\neg x \wedge z)$
- $W : (x \wedge q) \rightarrow ((y \vee \neg z) \wedge q)$
- $X : (x \wedge y) \leftrightarrow (\neg x \wedge z)$

Plan

Le problème

Dans cette section on s'intéresse à la satisfiabilité des formules (sur un ensemble de variables fini, *i.e.* $\text{Card}(\mathcal{Q}) \in \mathbb{N}$.)

Pourquoi ? Une formule propositionnelle peut modéliser un problème concret dont une solution serait donnée par un environnement satisfaisant la formule.

exemple du sudoku : la valeur de vérité d'une variable $p_{i,j,k}$ indique si la case i,j contient la valeur k, l'environnement complet décrit une solution, et s'il satisfait la formule, alors c'est une solution valide.

Mais on s'intéresse déjà au problème de décision (plus simple) de savoir si une formule est satisfiable, sans demander par quel environnement.

SAT || entrée : $A \in \mathbb{F}_p(\mathcal{Q})$
sortie : oui si A est satisfiable, non sinon

Remarque : puisque la satisfiabilité d'une formule ne dépend que de sa classe, on peut résoudre le problème sur une formule ayant une forme particulière, mais attention au coût de transformation.

Variantes du problème SAT

SAT || entrée : $A \in \mathbb{F}_p(\mathcal{Q})$
sortie : oui si A est satisfiable, non sinon

FND-SAT || entrée : $A \in \mathbb{F}_p(\mathcal{Q})$ sous FND
sortie : oui si A est satisfiable, non sinon

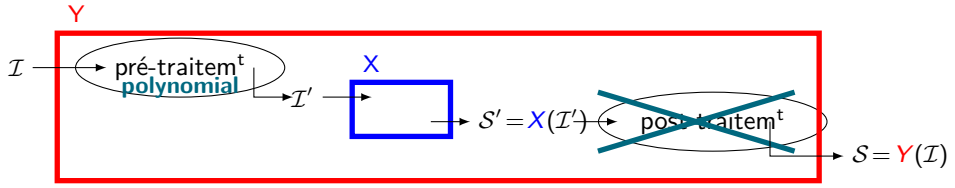
FNC-SAT || entrée : $A \in \mathbb{F}_p(\mathcal{Q})$ sous FNC
sortie : oui si A est satisfiable, non sinon

3-SAT || entrée : $A \in \mathbb{F}_p(\mathcal{Q})$ sous FNC ac des clauses de 3 littéraux seulem^t
sortie : oui si A est satisfiable, non sinon

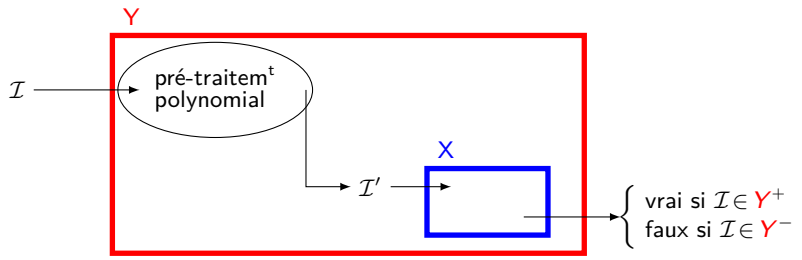
2-SAT || entrée : $A \in \mathbb{F}_p(\mathcal{Q})$ sous FNC ac des clauses de 2 littéraux seulem^t
sortie : oui si A est satisfiable, non sinon

Quels liens entre ces variantes ?

Rappel : réduction **polynomiale** entre problèmes



Réduction **polynomiale** entre problèmes de décision



Définition

Soient X et Y deux problèmes de décisions.
On note X^+ (resp. X^-) les instances positives (resp. négatives) de X, i.e. celles pour lesquelles la sol. est vrai (resp. faux). On définit de m̂ Y^+ et Y^-.

On dit que Y ***se réduit*** *à X* ***en temps polynomial*** *s'il existe une une transformation φ, calculable en temps polynomial, qui transforme toute instance de Y en une instance de X de sorte que*

$$\forall \mathcal{I},\ \varphi(\mathcal{I}) \in X^+ \Leftrightarrow \mathcal{I} \in Y^+$$

Réductions entre les variantes de SAT - 1/2

- **SAT** est plus dur que **FND-SAT** et **FNC-SAT**
  - ↪ **FNC-SAT** se réduit à **SAT** (pour $\varphi = id$)
  - ↪ **FND-SAT** se réduit à **SAT** (pour $\varphi = id$)
- **FNC-SAT** est plus dur que **2-SAT** et **3-SAT**
  - ↪ **2-SAT** se réduit à **FNC-SAT** (pour $\varphi = id$)
  - ↪ **3-SAT** se réduit à **FNC-SAT** (pour $\varphi = id$)
- **FNC-SAT** se réduit à **3-SAT**
  - ↪ on transforme chaque clause de taille < 3 en clause de taille 3

$$a \equiv (a \vee a \vee a) \qquad (a \vee b) \equiv (a \vee a \vee b)$$

  - ↪ on transforme chaque clause de taille > 3 en conjonction de clauses de taille 3 en ajoutant des nouvelles variables

$$(a \vee b \vee c \vee d) \rightsquigarrow (a \vee b \vee z) \wedge (\neg z \vee c \vee d)$$

$$(a \vee b \vee c \vee d \vee e) \rightsquigarrow (a \vee b \vee z_1) \wedge (\neg z_1 \vee c \vee z_2) \wedge (\neg z_2 \vee d \vee e)$$

  - ↪ transformations en temps poly. qui préservent la satisfiablilité

Exercice - pour la réduction de **FNC-SAT** à **3-SAT**

Soit $C = \ell_1 \vee \ell_2 \vee \ell_3 \vee \ldots \ell_k$ une clause de $\mathbb{F}_p(\mathcal{Q})$ de taille $k > 3$.
Soit z une nouvelle variable (*i.e.* $z \notin \mathcal{Q}$).
On pose alors $C_1 = (\ell_1 \vee \ell_2 \vee z)$ et $C_2 = (\neg z \vee \ell_3 \vee \ldots \ell_k)$.

Montrer les deux propositions suivantes :

→ $\forall \rho \in \mathbb{B}^{\mathcal{Q}},\ [C]^\rho = V \Rightarrow \left(\exists \tilde{\rho} \in \mathbb{B}^{\mathcal{Q} \cup \{z\}},\ \tilde{\rho}|_{\mathcal{Q}} = \rho \text{ et } [C_1 \wedge C_2]^{\tilde{\rho}} = V\right)$

→ $\forall \tilde{\rho} \in \mathbb{B}^{\mathcal{Q} \cup \{z\}},\ [C_1 \wedge C_2]^{\tilde{\rho}} = V \Rightarrow [C]^{\tilde{\rho}} = V$

La même stratégie permet-elle de réduire **FNC-SAT** *à* **2-SAT** *?*

Réductions entre les variantes de SAT - 2/2

- **FNC-SAT** ne se réduit pas à **2-SAT**
  - ↪ on verra que **2-SAT** se résout en temps poly. (cf chap. graphes),
  - ↪ vous verrez que **3-SAT** est NP-complet (th. de Cook, 2eme année)
  - ↪ à moins que P=NP, ces deux problèmes ne sont pas équivalents
- **FNC-SAT** ne se réduit pas à **FND-SAT**
  - ↪ la transfo. d'une forme à l'autre se fait en temps exponentiel et peut aussi augmenter la taille de l'entrée de manière exponentielle
  - ↪ on verra que **FND-SAT** se résout en temps polynomial (juste après),
  - ↪ à moins que P=NP, ces deux problèmes ne sont pas équivalents

À retenir : importance de la forme sous laquelle sont données les entrées d'un problème !

Modéliser une FND

FND = disjonction de conjonctions de littéraux.
D'un point de vue sémantique (*i.e.* dans $\mathbb{F}_p(\mathcal{Q})/\equiv$),

- → l'ordre des littéraux au sein d'une conjonction est-il important ? et leur multiplicité ? **non**, une conjonction est satisfaite par un env. prop. ssi il satisfait l'ensemble de ses termes.
- → quel objet mathématique est adapté pour modéliser les conjonctions de littéraux ? un **ensemble de littéraux** ou un **couple d'ensembles de variables** : d'une part celles apparaissant dans les littéraux positifs, d'autre part celles apparaissant dans les littéraux négatifs
- → l'ordre des conjonctions au sein de la disjonction est-il important ? et leur multiplicité ? **non**, une disjonction est satisfaite par un env. prop. ssi il satisfait l'un de ses termes.
- → quel objet mathématique est adapté pour modéliser une FND ?
  un ensemble de conjonction
- → quelle structure de données est adaptée pour modéliser une FND ?
  une liste de liste de littéraux convient

FND-SAT (FNC-SAT)

On suppose que $\mathcal{Q}=\{q_1, q_2, \dots q_N\}$.

FND-SAT
entrée : $\left((\ell_{i,j})_{i\in[1..n_j]}\right)_{j\in[1..n]}$ une famille de littéraux de $\mathcal{Q}$
sortie : oui si $A = \bigvee_{j=1}^{n} \bigwedge_{i=1}^{n_j} \ell_{i,j}$ est satisfiable,
non sinon

FNC-SAT
entrée : $\left((\ell_{i,j})_{i\in[1..n_j]}\right)_{j\in[1..n]}$ une famille de littéraux de $\mathcal{Q}$
sortie : oui si $A = \bigwedge_{j=1}^{n} \bigvee_{i=1}^{n_j} \ell_{i,j}$ est satisfiable,
non sinon

FND-SAT - exemple 1/2

la formule initiale :
$(a \wedge b \wedge \neg c) \vee (\neg b \wedge \neg c) \vee (a \wedge c)$
sous forme d'ensemble d'ensembles de littéraux :
$\{\{a, b, \neg c\}, \{\neg b, \neg c\}, \{a, c\}\}$
sous forme d'ensemble de couples :
$\{(\{a, b\}, \{c\}), (\emptyset, \{b, c\},), (\{a, c\}, \emptyset)\}$

la formule initiale :
$(a \wedge b \wedge \neg c) \vee (a \wedge c \wedge a) \vee (\neg b \wedge \neg c)$
sous forme d'ensemble d'ensembles de littéraux :
$\{\{a, b, \neg c\}, \{\neg b, \neg c\}, \{a, c\}\}$
sous forme d'ensemble de couples :
$\{(\{a, b\}, \{c\}), (\emptyset, \{b, c\},), (\{a, c\}, \emptyset)\}$

FND-SAT - exemple 2/2

la formule initiale :
$(a \wedge b \wedge \neg a) \vee (a \wedge c \wedge \neg a) \vee (\neg b \wedge \neg c)$
sous forme d'ensemble d'ensembles de littéraux :
$\{\{a, b, \neg a\}, \{a, \neg a, \neg c\}, \{\neg b, \neg c\}\}$
sous forme d'ensemble de couples :
$\{(\{a, b\}, \{a\}), (\{a\}, \{a, c\}), (\emptyset, \{b, c\},), \}$

Cette formule est-elle satisfiable ? Justifier.
Par quelle procédure décider ?

Algorithme pour FND-SAT

Algorithme FND-SAT sur $\mathcal{Q}=\{q_1, q_2, \dots q_N\}$

entrée : $\left((\ell_{i,j})_{i\in[1..n_j]}\right)_{j\in[1..n]}$ une famille de littéraux de $\mathcal{Q}$

sortie : vrai si $A = \bigvee_{j=1}^{n} \bigwedge_{i=1}^{n_j} \ell_{i,j}$, faux sinon

Pour j allant de 1 à n :
  Créer T un tableau indicé par $[1..N]$ initialisé à -1
  Essayer :
    Pour i allant de 1 à n_j :
      Si $\ell_{i,j} = q_k$
      alors si $T[k] = -1$, alors $T[k] \leftarrow 1$
        sinon si $T[k] = 0$ alors déclencher "conj. non sat."
      Si $\ell_{i,j} = \neg q_k$
      alors si $T[k] = -1$, alors $T[k] \leftarrow 0$
        sinon si $T[k] = 1$ alors déclencher l'exception "conj. non sat."
    Retourner **vrai**
  Rattraper "conj. non sat."
Retourner **faux**

Modélisation - exemple du solitaire 1/3

État initial du jeu : Sur chaque case d'un damier carré de $m \times m$ cases, il y a une pierre bleue (b), ou bien une pierre rouge (r) ou rien.

But du jeu : enlever des pierres de manière à ce que :

→ sur chaque colonne toutes les pierres sont de la même couleur

→ sur chaque ligne il y a au moins une pierre

Exercice :

1. Formaliser le problème de décision consistant à savoir si une partie peut être gagnée.
2. Réduire ce problème à **3-SAT**
3. Réduire **3-SAT** à ce problème (bonus)

À retenir : puissance d'encodage de **3-SAT**

Modélisation - exemple du solitaire 2/3

1. **JEU** entrée : $m \in \mathbb{N}^*$ la taille du damier
   $B \subseteq [1..m]^2$ l'ensemble des cases init. bleues.
   $R \subseteq [1..m]^2 \setminus B$ l'ensemble des cases init. rouges.
   sortie : oui s'il existe $B' \subseteq B$ et $R' \subseteq R$ tel que :
   → $\forall j \in [1..m]$, $B' \cap [1..n]\times\{j\} = \emptyset$ ou $R' \cap [1..m]\times\{j\} = \emptyset$
   → $\forall i \in [1..m]$, $(R' \cup B') \cap \{i\}\times[1..m] \neq \emptyset$

2. Soit (m, B, R) une instance de **JEU**.
On cherche à construire, en temps polynomial, une FNC A telle que $A \in$ **3-SAT**$^+$ ssi $(m, B, R) \in$ **JEU**$^+$, c'est-à-dire telle que A est satisfiable ssi il existe $B' \subseteq B$ et $R' \subseteq R$ tel que ...

Pour chaque $(i,j) \in [1..m]^2$, on introduit 2 variables :
- $b'_{i,j}$ modélisant $(i,j) \in B'$
- $r'_{i,j}$ modélisant $(i,j) \in R'$

Modélisation - exemple du solitaire 3/3

On A doit modéliser les 4 contraintes ci-dessous :

→ $B' \subseteq B$

→ $R' \subseteq R$

→ $\forall j \in [1..m]$, $B' \cap [1..n]\times\{j\} = \emptyset$ ou $R' \cap [1..m]\times\{j\} = \emptyset$

→ $\forall i \in [1..m]$, $(R' \cup B') \cap \{i\}\times[1..m] \neq \emptyset$

On pose alors A la conjonction des 4 formules ci-dessous :

→ $\bigwedge_{(i,j)\in[1..m]\setminus B} \neg b_{i,j}$

→ $\bigwedge_{(i,j)\in\in[1..m]\setminus R} \neg r_{i,j}$

→ $\bigwedge_{j\in[1..m]} \bigwedge_{(i,i')\in[1..m]^2} \neg b_{i,j} \vee \neg r_{i',j}$

→ $\bigwedge_{i\in[1..m]} \bigvee_{j\in[1..m]} r_{i,j} \vee b_{i,j}$