

Logique propositionnelle

Dans ce chapitre, on étudie les outils mathématiques permettant de modéliser les expressions booléennes sans entrer dans le détail des sous-expressions non booléennes.

Rappel : On peut représenter les expressions booléennes à l'aide d'arbres de syntaxe.

Exemple : Considérons un jeu de Sudoku en 4×4 .

On note $(M_{i,j})_{\substack{i \in [1..4] \\ j \in [1..4]}}$ les cases du tableau.

Alors, si on note $\mathcal{P}_{i,j,k}$ la propriété “ $M_{i,j} = k$ ”, on a : $\bigwedge_{k=1}^4 \bigwedge_{i=1}^4 \left(\bigvee_{j=1}^4 \mathcal{P}_{i,j,k} \right)$.

Cette formule traduit la règle “pour tout $k \in [1..4]$, il existe sur chaque ligne i une colonne j telle que la case (i, j) contient k ”.

Remarque : Les quantificateurs sur des ensembles finis se traduisent donc par des conjonctions et des disjonctions finies. La logique avec des quantificateurs s'appelle la logique du 1^{er} ordre.

Remarque : On fera bien la distinction entre ce qui relève de la syntaxe des formules, *c-à-d* comment elles sont écrites, et ce qui relève de leur sémantique, *c-à-d* les valeurs qu'on leur donne.

1 Syntaxe de la logique propositionnelle

Pour toute cete partie, on fixe \mathcal{Q} un ensemble non vide de symboles appelés variables propositionnelles.

1.1 Définition inductive des formules

1.1.1 Avec des règles de construction

Définition :

L'ensemble des formules de la logique propositionnelle, noté $\mathbb{F}_p(\mathcal{Q})$, est construit par induction à partir des règles de construction suivantes :

- $\mathcal{Var}|_{\mathcal{Q}}^0$
- $\top|_{\{\}}^0$ (vrai)
- $\perp|_{\{\}}^0$ (faux)
- $\neg|_{\{\}}^1$ (négation)
- $\wedge|_{\{\}}^2$ (conjonction)
- $\vee|_{\{\}}^2$ (disjonction)
- $\rightarrow|_{\{\}}^2$ (implication)
- $\leftrightarrow|_{\{\}}^2$ (équivalence – mais attention, ce n'est pas une relation d'équivalence !)

Remarque : Ce système n'est pas minimal, autrement dit on pourrait avoir un ensemble de formules comprenant moins de règles. Par exemple, on peut écrire $\neg((\neg A) \wedge (\neg B))$ pour désigner $A \vee B$.

Afin d'alléger les écritures, on note désormais :

$$\begin{aligned}
& \top \text{ pour } (\top, _) \\
& \perp \text{ pour } (\perp, _) \\
& \mathcal{V}ar(q) \text{ pour } (\mathcal{V}ar, q) \\
& \neg A \text{ pour } (\neg, _, A) \\
& A \wedge B \text{ pour } (\wedge, _, A, B) \\
& A \vee B \text{ pour } (\vee, _, A, B) \\
& A \rightarrow B \text{ pour } (\rightarrow, _, A, B) \\
& A \leftrightarrow B \text{ pour } (\leftrightarrow, _, A, B)
\end{aligned}$$

1.1.2 En français

1.2 Représentation sous forme d'arbres

Une formule de $\mathbb{F}_p(\mathcal{Q})$ peut être représentée par un arbre binaire non vide dont les feuilles sont étiquetées par $\mathcal{Q} \cup \{\top, \perp\}$ et dont les nœuds d'arité 1 et 2 sont respectivement étiquetés par $\{\neg\}$ et $\{\vee, \wedge, \rightarrow, \leftrightarrow\}$.

Exemple : Pour $\mathcal{Q} = \{x, y, z\}$, on a :

Remarque : Dans cette représentation, une sous-formule correspond alors à un sous-arbre.

Définition :

La hauteur (resp. taille) d'une formule est la hauteur (resp. taille) de l'arbre qui le représente. Formellement, on définit la hauteur (resp. taille) des formules de $\mathbb{F}_p(\mathcal{Q})$ par induction comme suit :

$$h = \left(\begin{array}{l} \mathbb{F}_p(\mathcal{Q}) \rightarrow \mathbb{N} \\ \left. \begin{array}{l} \top \\ \perp \\ q \in \mathcal{Q} \end{array} \right\} \mapsto 0 \\ \neg A \mapsto 1 + h(A) \\ A \alpha B \mapsto 1 + \max(h(A), h(B)) \end{array} \right) \quad s = \left(\begin{array}{l} \mathbb{F}_p(\mathcal{Q}) \rightarrow \mathbb{N} \\ \left. \begin{array}{l} \top \\ \perp \\ q \in \mathcal{Q} \end{array} \right\} \mapsto 1 \\ \neg A \mapsto 1 + s(A) \\ A \alpha B \mapsto 1 + s(A) + s(B) \end{array} \right)$$

où à chaque fois on a $\alpha \in \{\vee, \wedge, \rightarrow, \leftrightarrow\}$.

Exercice : Donner de même la définition de fonctions donnant les nombres et les ensembles de feuilles et de variables.

1.3 Conjonction et disjonction

Soit $(A_i)_{i \in [1..n]} \in \mathbb{F}_p(\mathcal{Q})^n$ avec $n \in \mathbb{N}^*$.

- On notera $\bigwedge_{i=1}^n A_i$ pour désigner $((A_1 \wedge A_2) \wedge A_3 \dots) \wedge A_n$. Formellement,

$$\begin{aligned} & \cdot \bigwedge_{i=1}^1 A_i = A_1 \\ & \cdot \text{pour } n \geq 2, \bigwedge_{i=1}^n A_i = \left(\bigwedge_{i=1}^{n-1} A_i \right) \wedge A_n \end{aligned}$$

De même, on notera $\bigvee_{i=1}^n A_i$ pour désigner $((A_1 \vee A_2) \vee A_3 \dots) \vee A_n$.

- Plus généralement, si $I \neq \emptyset$ est un ensemble ordonné et si $(A_i)_{i \in I} \in \mathbb{F}_p(\mathcal{Q})^I$, on s'autorisera à écrire $\bigwedge_{i \in I} A_i$ et $\bigvee_{i \in I} A_i$. Enfin, si $I = \emptyset$, $\bigwedge_{i \in I} A_i$ désigne \top et $\bigvee_{i \in I} A_i$ désigne \perp .

1.4 Formes normales

Définition :

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

A est un littéral s'il existe $q \in \mathcal{Q}$ tel que $A = q$ ou $A = \neg q$.

A est une clause (disjonctive) si c'est une disjonction de littéraux.

Pour $n \in \mathbb{N}^*$, A est une n -clause si c'est une disjonction d'exactly n littéraux.

A est sous forme normale conjonctive (FNC) si c'est une conjonction de clauses disjonctives.

A est sous forme normale disjonctive (FND) si c'est une disjonction de conjonctions de littéraux.

Exemples : $((x \vee y) \vee \neg z) \vee \neg x \vee x$ est une 5-clause.

$(a \vee b) \wedge (a \vee b \vee c)$ est une formule sous FNC.

Remarque : Si $q \in \mathcal{Q}$, q et $\neg q$ sont des clauses (ce sont des 1-clauses).

2 Algèbre booléenne

2.1 Définition

Définition :

Notons \mathbb{B} l'ensemble $\{\mathbf{V}, \mathbf{F}\}$. On munit \mathbb{B} des opérations suivantes :

$$+ = \begin{pmatrix} \mathbb{B} \times \mathbb{B} \rightarrow \mathbb{B} \\ (\mathbf{F}, \mathbf{F}) \mapsto \mathbf{F} \\ (\mathbf{F}, \mathbf{V}) \mapsto \mathbf{V} \\ (\mathbf{V}, \mathbf{F}) \mapsto \mathbf{V} \\ (\mathbf{V}, \mathbf{V}) \mapsto \mathbf{V} \end{pmatrix} \quad \times = \begin{pmatrix} \mathbb{B} \times \mathbb{B} \rightarrow \mathbb{B} \\ (\mathbf{F}, \mathbf{F}) \mapsto \mathbf{F} \\ (\mathbf{F}, \mathbf{V}) \mapsto \mathbf{F} \\ (\mathbf{V}, \mathbf{F}) \mapsto \mathbf{F} \\ (\mathbf{V}, \mathbf{V}) \mapsto \mathbf{V} \end{pmatrix} \quad \overline{\cdot} = \begin{pmatrix} \mathbb{B} \rightarrow \mathbb{B} \\ \mathbf{V} \mapsto \mathbf{F} \\ \mathbf{F} \mapsto \mathbf{V} \end{pmatrix}$$

\mathbb{B} muni de ces opérations, c'est-à-dire $(\mathbb{B}, +, \times, \overline{\cdot})$, est appelée l'algèbre de Boole.

Remarque : $\bar{\cdot}$ ne correspond pas au passage à l'opposé (inversion pour $+$), ni au passage à l'inverse (inversion pour \times).

Propriétés :

- i.* $+$ et \times sont associatives et commutatives.
- ii.* $\bar{\cdot}$ est involutive.
- iii.* $+$ admet F comme élément neutre et \times admet V comme neutre.
- iv.* V est absorbant pour $+$ et F est absorbant pour \times .

◆ **Preuve :**

i. On montre l'associativité en étudiant tous les cas possibles, que l'on présente dans un tableau appelé table de vérité (*cf.* définition de table de vérité plus loin). Soit donc $(a, b, c) \in \mathbb{B}^3$. On a :

Propriétés :

- i.* $+$ est distributive par rapport à \times , c'est-à-dire

$$\forall (a, b, c) \in \mathbb{B}^3, \begin{cases} (a \times b) + c = (a + c) \times (b + c) \\ c + (a \times b) = (c + a) \times (c + b) \end{cases}$$
- ii.* \times est distributive par rapport à $+$, c'est-à-dire

$$\forall (a, b, c) \in \mathbb{B}^3, \begin{cases} (a + b) \times c = (a \times c) + (b \times c) \\ c \times (a + b) = (c \times a) + (c \times b) \end{cases}$$

◆ **Preuve :**

2.2 Fonctions booléennes

Pour $n \in \mathbb{N}^*$, on appelle fonction booléenne d'arité n une fonction de \mathbb{B}^n dans \mathbb{B} .

Remarque : $\text{Card}(\mathbb{B}^n) = 2^n$ et $\text{Card}(\mathbb{B}^{\mathbb{B}^n}) = \text{Card}(\mathcal{F}(\mathbb{B}^n, \mathbb{B})) = 2^{2^n}$.

Définition :

Soit $n \in \mathbb{N}^*$ et $f \in \mathcal{F}(\mathbb{B}^n, \mathbb{B})$.

On appelle table de vérité de f un tableau T ayant 2^n lignes (indicées de 1 à 2^n) et $n + 1$ colonnes (indicées de 1 à $n + 1$), à valeurs dans \mathbb{B} et tel que :

$$\begin{aligned} \cdot \quad & \left\{ (T_{i,j})_{j \in [1..n]} \mid i \in [1..2^n] \right\} = \mathbb{B}^n \\ \cdot \quad & \forall i \in [1..2^n], f((T_{i,j})_{j \in [1..n]}) = T_{i,n+1} \end{aligned}$$

Autrement dit, les lignes de T couvrent l'ensemble des n -uplets de \mathbb{B}^n et pour chaque ligne, la dernière colonne donne l'image par f du n -uplet constitué des premières cases de cette ligne.

Remarque : Il est recommandé d'énumérer les 2^n n -uplets de manière logique (en comptant en binaire) afin de les lister exhaustivement et sans doublons plus facilement.

Remarque : On s'autorisera à rassembler les tables de vérité de plusieurs fonctions booléennes de même arité dans un même tableau en factorisant les premières colonnes.

3 Sémantique de la logique propositionnelle

Dans cette partie, on fixe à nouveau \mathcal{Q} un ensemble non vide de symboles et on note \mathbb{B} l'algèbre de Boole.

3.1 Interprétation

On appelle environnement propositionnel une fonction de \mathcal{Q} dans \mathbb{B} . On l'appelle également valeurs de vérité, ou encore assignation des variables.

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} par :

$$[\cdot]^\rho = \left(\begin{array}{l} \mathbb{F}_p(\mathcal{Q}) \rightarrow \mathbb{B} \\ \top \mapsto \mathbf{V} \\ \perp \mapsto \mathbf{F} \\ q \in \mathcal{Q} \mapsto \rho(q) \\ \neg A \mapsto [A]^\rho \\ A \vee B \mapsto [A]^\rho + [B]^\rho \\ A \wedge B \mapsto [A]^\rho \times [B]^\rho \\ A \rightarrow B \mapsto \overline{[A]^\rho} + [B]^\rho = [\neg A \vee B]^\rho \\ A \leftrightarrow B \mapsto ([A]^\rho \times [B]^\rho) + (\overline{[A]^\rho} \times \overline{[B]^\rho}) \end{array} \right)$$

Définitions :

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

- Si $\rho \in \mathbb{B}^{\mathcal{Q}}$ est telle que $[A]^\rho = \mathbb{V}$, alors on dit que ρ satisfait A .
- On dit que A est satisfiable s'il existe $\rho \in \mathbb{B}^{\mathcal{Q}}$ tel que ρ satisfait A .
- On dit que A est valide ou bien que A est une tautologie ssi $\forall \rho \in \mathbb{B}^{\mathcal{Q}}, \rho$ satisfait A .
- On dit que A est insatisfiable ou que c'est une antilogie ssi $\forall \rho \in \mathbb{B}^{\mathcal{Q}}, \rho$ ne satisfait pas A .

Exemples : \top et $(x \vee \neg x)$ sont des tautologies. \perp et $(x \wedge \neg x)$ sont quant à elles des antilogies.

Remarque : Il est à noter qu'antilogie n'est pas la négation de tautologie.

3.2 Fonction booléenne associée à une formule

On change maintenant de point de vue : en effet, $[A]^\rho$ dépend de A mais aussi de ρ .

Dans la section précédente, on a vu que la dépendance en A pour $\rho \in \mathbb{B}^{\mathcal{Q}}$ fixé était donnée par la fonction $[\cdot]^\rho = A \mapsto [A]^\rho$. De même, pour la dépendance en ρ à $A \in \mathbb{F}_p(\mathcal{Q})$ fixé, on aura la fonction $\llbracket \cdot \rrbracket^A = \rho \mapsto [A]^\rho$ définie ci-après.

Définition :

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

$$\llbracket \cdot \rrbracket^A = \left(\begin{array}{c} \mathbb{B}^{\mathcal{Q}} \rightarrow \mathbb{B} \\ \rho \mapsto [A]^\rho \end{array} \right)$$

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 (cf. section "mise sous forme normale").

Définition :

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

$$\begin{aligned} \forall (A, B) \in \mathbb{F}_p(\mathcal{Q})^2, A \equiv B &\iff \llbracket \cdot \rrbracket^A = \llbracket \cdot \rrbracket^B \\ &\iff \forall \rho \in \mathbb{B}^{\mathcal{Q}}, \llbracket \rho \rrbracket^A = \llbracket \rho \rrbracket^B \\ &\iff \forall \rho \in \mathbb{B}^{\mathcal{Q}}, [A]^\rho = [B]^\rho \end{aligned}$$

On dit alors que A et B sont logiquement équivalentes, et on parlera d'équivalence logique, si $A \equiv B$.

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

Exemple : 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 définition de l'interprétation
= $[B]^\rho + [A]^\rho$ par commutativité de $+$
= $[B \vee A]^\rho$ en réutilisant la définition de l'interprétation

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

- a)** $A \wedge B \equiv B \wedge A$
- b)** $A \rightarrow B \equiv (\neg A) \vee B$
- c)** $A \rightarrow B \equiv (\neg B) \rightarrow (\neg A)$
- d)** $A \leftrightarrow B \equiv (A \rightarrow B) \wedge (B \rightarrow A)$
- e)** $A \vee \neg A \equiv \top$
- f)** $(A \rightarrow B) \wedge A \equiv A \wedge B$.

◆ **Correction :**

- a)** $\forall \rho \in \mathbb{B}^{\mathcal{Q}}, [A \wedge B]^{\rho} = [A]^{\rho} \times [B]^{\rho} = [B]^{\rho} \times [A]^{\rho} = [B \wedge A]^{\rho}$ d'où $A \wedge B \equiv B \wedge A$.
- b)** $\forall \rho \in \mathbb{B}^{\mathcal{Q}}, [A \rightarrow B]^{\rho} = \overline{[A]^{\rho}} + [B]^{\rho} = \overline{[\neg A]^{\rho}} + [B]^{\rho} = [\neg A \vee B]^{\rho}$, d'où $A \rightarrow B \equiv \neg A \vee B$.
- d)** $\forall \rho \in \mathbb{B}^{\mathcal{Q}}, [A \leftrightarrow B]^{\rho} = ([A]^{\rho} \times [B]^{\rho}) + (\overline{[A]^{\rho}} \times \overline{[B]^{\rho}})$ par définition

$$= ([A]^{\rho} + \overline{[A]^{\rho}}) \times ([A]^{\rho} + \overline{[B]^{\rho}}) \times ([B]^{\rho} + \overline{[A]^{\rho}}) \times ([B]^{\rho} + \overline{[B]^{\rho}})$$

$$= ([A]^{\rho} + \overline{[B]^{\rho}}) \times ([B]^{\rho} + \overline{[A]^{\rho}})$$
 car $\forall X \in \mathbb{B}, X + \overline{X} = V$

$$= [B \rightarrow A]^{\rho} \times [A \rightarrow B]^{\rho}$$
 par commutativité de $+$ puis par définition

$$= [A \rightarrow B]^{\rho} \times [B \rightarrow A]^{\rho}$$
 par commutativité de \times

$$= [(A \rightarrow B) \wedge (B \rightarrow A)]^{\rho}.$$

D'où $A \leftrightarrow B \equiv (A \rightarrow B) \wedge (B \rightarrow A)$.

3.3 Conséquence logique

Définition :

Soit $(A, B) \in \mathbb{F}_p(\mathcal{Q})^2$. On dit que B est conséquence logique de A , ce que l'on note $A \models B$, ssi tout environnement propositionnel satisfaisant A satisfait aussi B , autrement dit

$$\{\rho \in \mathbb{B}^{\mathcal{Q}} \mid [A]^{\rho} = V\} \subseteq \{\rho \in \mathbb{B}^{\mathcal{Q}} \mid [B]^{\rho} = V\}$$

Remarque : L'équivalence logique correspond au cas d'égalité de l'inclusion précédente.

Propriété : La relation binaire \models est réflexive et transitive.

Exercice : Prouver cette propriété.

Définition :

Soit $X \subseteq \mathbb{F}_p(\mathcal{Q})$ et $B \in \mathbb{F}_p(\mathcal{Q})$. On note $X \models B$ ssi tout environnement propositionnel satisfaisant toutes les formules de X satisfait aussi B , autrement dit

$$\{\rho \in \mathbb{B}^{\mathcal{Q}} \mid \forall A \in X, [A]^{\rho} = V\} \subseteq \{\rho \in \mathbb{B}^{\mathcal{Q}} \mid [B]^{\rho} = V\}$$

Remarque : Il faut distinguer ceci de " B est conséquence logique de la conjonction des formules de X " (*i.e.* $(\bigwedge_{A \in X} A) \models B$), puisque X peut être de cardinal infini. La définition précédente caractérise donc en fait une propriété plus forte que celle-ci, qui coïncide avec elle si X est fini.

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

- a)** $\{(A \rightarrow B), A\} \models B$
- b)** $\{(A \rightarrow B), \neg B\} \models \neg A$.

3.4 Reformulations avec des équivalences

Propriétés :

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

Propriété :

- | |
|--|
| Soit $(A, B) \in \mathbb{F}_p(\mathcal{Q})^2$. Alors :
• $A \equiv B$ ssi $A \leftrightarrow B \equiv \top$ (<i>i.e.</i> $A \leftrightarrow B$ est une tautologie).
• $A \models B$ ssi $A \rightarrow B \equiv \top$ (<i>i.e.</i> $A \rightarrow B$ est une tautologie). |
|--|

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 associés tous ses éléments.

Cela justifie que $\llbracket \cdot \rrbracket^A$ soit parfois appelée la représentation de A .

On peut alors être amené à se demander quel représentant l'on préférera pour une classe donnée, et s'il est envisageable de choisir une forme canonique pour représenter une classe de formules équivalentes.

4 Mise sous forme normale

4.1 Mise sous FND à partir d'une table de vérité

4.1.1 Sur un exemple

On cherche à mettre sous FND la formule $A = (a \vee b) \rightarrow (c \wedge a)$, dont voici la table de vérité :

On en déduit, en prenant la disjonction des clauses conjonctives formées par les lignes du tableau "satisfaisant" A (c -à- d telles que la dernière case contienne \vee) :

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

ce que l'on peut encore simplifier en $(a \wedge b \wedge c) \vee (\neg b \wedge c) \vee (\neg a \wedge \neg b \wedge \neg c)$.

4.1.2 Table de vérité d'une formule

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

Définition :

Une table de vérité d'une formule $A \in \mathbb{F}_p(\mathcal{Q})$ est une table de vérité T de la fonction booléenne associée $\llbracket \cdot \rrbracket^A$, de sorte qu'on a :

$$\begin{aligned} & \cdot \left\{ (T_{i,j})_{j \in [1..n]} \mid i \in [1..2^n] \right\} = \mathbb{B}^{\mathcal{Q}} \\ & \cdot \forall i \in [1..2^n], T_{i,n+1} = \llbracket \rho^i \rrbracket^A \end{aligned}$$

où pour tout $i \in [1..2^n]$, ρ^i est défini par $\forall j \in [1..n], \rho^i(q_j) = T_{i,j}$.

Remarque : En calculant une FND à partir du tableau T , on calcule donc bien quelque chose qui ne dépend pas exactement de A mais de sa classe...

4.1.3 Calculer une FND 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} et $(\rho^i)_{i \in [1..2^n]}$ la famille des environnements propositionnels définis comme précédemment selon T .

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

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

◆ Preuve :

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

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

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

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

Lemme :

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

◆ **Preuve :**

i. Soit $i \in [1..2^n]$. Par définition de l'interprétation d'une conjonction,

$$[L^i]^{\rho^i} = \prod_{j=1}^n [\ell_{i,j}]^{\rho^i} = \prod_{j=1}^n \mathbf{V} = \mathbf{V}$$

d'après le lemme précédent appliqué aux couples $((i, j))_{j \in [1..n]}$. D'où $[L^i]^{\rho^i} = \mathbf{V}$.

ii. Soit $k \in [1..2^n]$ tel que $k \neq i$. Puisque les lignes de T restreintes à leur n premières colonnes sont deux à deux distinctes (il y en a 2^n et elles couvrent $\mathbb{B}^{\mathcal{Q}}$ qui est de cardinal 2^n), il existe $j_0 \in [1..n]$ tel que $T_{i,j_0} \neq T_{k,j_0}$.

→ Si $T_{i,j_0} = \mathbf{V}$, alors $\ell_{i,j_0} = q_{j_0}$ et $T_{k,j_0} = \mathbf{F}$. Par définition de l'interprétation d'une variable, $[\ell_{i,j_0}]^{\rho^k} = \rho^k(q_{j_0})$, or par définition de ρ^k , $\rho^k(q_{j_0}) = T_{k,j_0} = \mathbf{F}$ donc $[\ell_{i,j_0}]^{\rho^k} = \mathbf{F}$.

→ Si $T_{i,j_0} = \mathbf{F}$, alors $\ell_{i,j_0} = \neg q_{j_0}$ et $T_{k,j_0} = \mathbf{V}$. Par définition de l'interprétation de la négation d'une variable, $[\ell_{i,j_0}]^{\rho^k} = \overline{\rho^k(q_{j_0})}$ qui vaut, par définition de ρ^k , $\rho^k(q_{j_0}) = \overline{T_{k,j_0}} = \overline{\mathbf{V}} = \mathbf{F}$.

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

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

Propriété : On a $D \equiv A$.

◆ **Preuve :**

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

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

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 $[A]^\rho = \mathbf{V}$, on a $\mathbf{V} = \llbracket \rho \rrbracket^A = \llbracket \rho^{i_0} \rrbracket^A = T_{i_0,n+1}$ donc $i_0 \in I$.

Ainsi, le terme $[L^{i_0}]^\rho$ apparaît dans la somme qu'est $[D]^\rho$, or par le lemme précédent, $[L^{i_0}]^\rho = [L^{i_0}]^{\rho^{i_0}} = \mathbf{V}$ et \mathbf{V} étant absorbant pour $+$, on en déduit que $[D]^\rho = \mathbf{V}$, soit $[D]^\rho = [A]^\rho$.

→ Si au contraire $[A]^\rho = \mathbf{F}$, alors $T_{i_0,n+1} = \mathbf{F}$ donc $i_0 \notin I$.

Autrement dit, $\forall i \in I, i \neq i_0$ ce qui donne d'après le lemme précédent $[L^i]^\rho = [L^i]^{\rho^i} = \mathbf{F}$. Une somme de \mathbf{F} valant \mathbf{F} , on en déduit que $[D]^\rho = \mathbf{F}$, soit $[D]^\rho = [A]^\rho$.

4.2 Mise sous FNC à partir d'une table de vérité

4.2.1 Sur le même exemple

On veut mettre sous FNC la formule vue au début de la section précédente, $A = (a \vee b) \rightarrow (c \wedge a)$. Pour cela, reprenons sa table de vérité :

En prenant cette fois-ci la conjonction des négations respectives des clauses conjonctives formées par les lignes satisfaisant $\neg A$ (c -à- d telles que la dernière case contienne F), puis en distribuant la négation sur chaque clause, on obtient :

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

4.2.2 Calculer une FNC à partir d'une table de vérité

Soit $A \in \mathbb{F}_p(\mathcal{Q})$ où $\mathcal{Q} = \{q_1, q_2, \dots, q_n\}$ et T une table de vérité de A suivant cette numérotation de \mathcal{Q} ; on définit comme précédemment la famille d'environnements $(\rho^i)_{i \in [1..2^n]}$ à partir de T .

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

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

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

Propriétés :

- On a alors les propriétés suivantes :
 - $\forall i \in [1..2^n], \forall j \in [1..n], [r_{i,j}]^{\rho^i} = \mathbf{F}$
 - $\forall i \in [1..2^n], [R^i]^{\rho^i} = \mathbf{F}$ et $\forall k \in [1..2^n], k \neq i, [R^i]^{\rho^k} = \mathbf{V}$
 - $C \equiv A$.

◆ **Preuve :** En procédant sur le même principe que pour la mise sous FND.

* Bilan sur la FNC/FND

- Certaines formules sont à la fois sous FNC et FND.
- Il y a existence de la FNC/FND équivalente à une formule (on vient de le montrer !). Par contre, il n'y a pas unicité de la FNC, ni de la FND équivalente à une formule.
- Il peut y avoir une explosion de la taille (*cf.* exemple ci-dessous).

Exemple : $\bigwedge_{i=1}^n (a_i^1 \vee a_i^2) = \bigvee_{(j_1, j_2, \dots, j_n) \in \{1,2\}^n} \bigwedge_{k=1}^n a_k^{j_k}$.

Dans cet exemple, transformer une FNC à une FND nous a fait passer d'une conjonction de n 2-clauses disjonctives à une disjonction de 2^n n -clauses conjonctives.

Exercice : Voici quelques simplifications utiles ; démontrer chaque équivalence logique.

Exercice : Mettre sous FNC et FND les formules suivantes.

- a) $U = (x \wedge y) \vee (z \wedge \neg z \wedge q) \vee (\neg x \wedge z)$
- b) $V = (x \wedge q) \rightarrow ((y \vee z) \wedge q)$
- c) $W = (x \wedge y) \leftrightarrow (\neg x \wedge z)$.

5 Le problème SAT

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

En effet, une formule propositionnelle peut modéliser un problème concret dont une solution serait donnée par un environnement satisfaisant la formule.

Exemple : Pour le 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. C'est le problème **SAT**, que l'on formalise dans la section suivante.

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.

5.1 Définitions

On donne ci-dessous la formalisation du problème SAT ainsi que quelques unes de ses variantes :

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

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

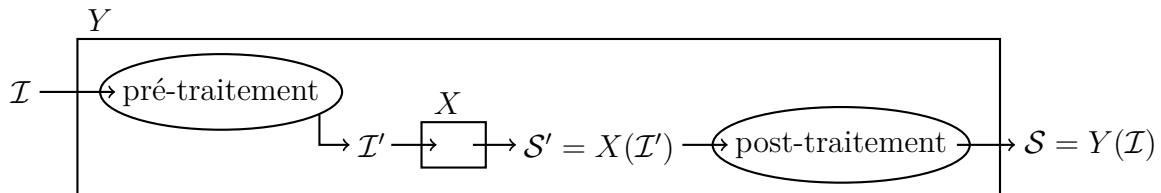
FNC-SAT || entrée : $A \in \mathbb{F}_p(Q)$ sous FNC
 || sortie : oui si A est satisfiable, non sinon

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

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

5.2 Réductions

Rappel (réduction entre problèmes) :



Définition (réduction polynomiale entre problèmes de décision) :

Soient X et Y deux problèmes de décision. On note X^+ (resp. X^-) les instances positives (resp négatives) de X , *i.e.* celles pour lesquelles la solution est “vrai” (resp. “faux”). On définit de même Y^+ et Y^- .

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

$$\forall \mathcal{I}, \varphi(\mathcal{I}) \in X^+ \iff \mathcal{I} \in Y^+ \text{ et } \varphi(\mathcal{I}) \in X^- \iff \mathcal{I} \in Y^-$$

Compte tenu de ces définitions, on a les réductions suivantes :

- SAT est plus dur que FND-SAT et FNC-SAT, en effet :
 - 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, en effet :
 - 2-SAT se réduit à FNC-SAT pour $\varphi = Id$
 - 3-SAT se réduit à FNC-SAT pour $\varphi = Id$
- Inversement, FNC-SAT se réduit à 3-SAT. En effet, on peut transformer toute clause de taille ≤ 2 d’une FNC en clause de taille 3 suivant le modèle des exemples suivants :

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

De même, on transforme chaque clause de taille > 3 en conjonction de clauses de taille 3 en ajoutant successivement des nouvelles variables comme suit :

$$(a \vee b \vee c \vee d) \text{ devient } (a \vee b \vee z) \wedge (\neg z \vee c \vee d) \\ (a \vee b \vee c \vee d \vee e) \text{ devient } (a \vee b \vee z_1) \wedge (\neg z_1 \vee c \vee z_2) \wedge (\neg z_2 \vee d \vee e)$$

On justifie ce processus dans la propriété suivante.

Propriété :

Soit $C = \ell_1 \vee \ell_2 \vee \ell_3 \vee \dots \vee \ell_k$ une clause de $\mathbb{F}_p(\mathcal{Q})$ de taille $k \geq 3$.

Soit z une nouvelle variable (*i.e.* $z \notin \mathcal{Q}$). On pose :

- $C_1 = (\ell_1 \vee \ell_2 \vee z)$
- $C_2 = (\neg z \vee \ell_3 \vee \dots \vee \ell_k)$.

Alors, on a les 2 propositions suivantes :

- i. $\forall \rho \in \mathbb{B}^{\mathcal{Q}}, ([C]^\rho = \mathbf{V} \implies (\exists \tilde{\rho} \in \mathbb{B}^{\mathcal{Q} \cup \{z\}}, \tilde{\rho}|_{\mathcal{Q}} \text{ et } [C_1 \wedge C_2]^{\tilde{\rho}} = \mathbf{V}))$
- ii. $\forall \tilde{\rho} \in \mathbb{B}^{\mathcal{Q} \cup \{z\}}, ([C_1 \wedge C_2]^{\tilde{\rho}} = \mathbf{V} \implies [C]^{\tilde{\rho}} = \mathbf{V})$

◆ **Preuve :**

i. Soit $\rho \in \mathbb{B}^{\mathcal{Q}}$ tel que $[C]^\rho = \mathbf{V}$.

Alors, comme $C = \bigvee_{i=1}^k \ell_i$, i.e. $[C]^\rho = \sum_{i=1}^k [\ell_i]^\rho$, il existe $i_0 \in [1..k]$ tel que $[\ell_{i_0}]^\rho = \mathbf{V}$.

→ Si $[\ell_1]^\rho = \mathbf{V}$ ou $[\ell_2]^\rho = \mathbf{V}$, on pose : $\tilde{\rho} = \begin{pmatrix} \mathcal{Q} \cup \{z\} \rightarrow \mathbb{B} \\ q \in \mathcal{Q} \mapsto \rho(q) \\ z \mapsto \mathbf{F} \end{pmatrix}$.

On a bien $\tilde{\rho}|_{\mathcal{Q}} = \rho$ par cette définition. De plus,

$$[C_1 \wedge C_2]^{\tilde{\rho}} = [C_1]^{\tilde{\rho}} \times [C_2]^{\tilde{\rho}} = \underbrace{[\ell_1 \vee \ell_2 \vee z]^{\tilde{\rho}}}_{=\mathbf{V} \text{ par hypothèse}} \times \left[\bigvee_{i=3}^k \ell_i \vee \neg z \right]^{\tilde{\rho}} = \mathbf{V} \times \underbrace{\left(\sum_{i=3}^k [\ell_i]^{\tilde{\rho}} + [\neg z]^{\tilde{\rho}} \right)}_{=\mathbf{V} \text{ car } [\neg z]^{\tilde{\rho}} = [\overline{z}]^{\tilde{\rho}} = \mathbf{V}} = \mathbf{V} \times \mathbf{V} = \mathbf{V}$$

→ Si $[\ell_1]^\rho = \mathbf{F}$ et $[\ell_2]^\rho = \mathbf{F}$, alors on a $i_0 \geq 3$. On pose donc : $\tilde{\rho} = \begin{pmatrix} \mathcal{Q} \cup \{z\} \rightarrow \mathbb{B} \\ q \in \mathcal{Q} \mapsto \rho(q) \\ z \mapsto \mathbf{V} \end{pmatrix}$.

On a toujours $\tilde{\rho}|_{\mathcal{Q}} = \rho$, et :

$$[C_1 \wedge C_2]^{\tilde{\rho}} = [C_1]^{\tilde{\rho}} \times [C_2]^{\tilde{\rho}} = \underbrace{[\ell_1 \vee \ell_2 \vee \ell_3]^{\tilde{\rho}}}_{=\mathbf{V} \text{ par définition de } \tilde{\rho}} \times \left[\bigvee_{i=3}^k \ell_i \vee \neg z \right]^{\tilde{\rho}} = \mathbf{V} \times \underbrace{\left(\sum_{\substack{i=3 \\ i \neq i_0}}^k [\ell_i]^{\tilde{\rho}} + [\ell_{i_0}]^{\tilde{\rho}} + [\neg z]^{\tilde{\rho}} \right)}_{=\mathbf{V} \text{ car } [\ell_{i_0}]^{\tilde{\rho}} = \mathbf{V} \text{ puisque } i_0 \in [3..k]} = \mathbf{V}$$

Remarque : On a bien des transformations en temps polynomial qui préservent la satisfiabilité. Par contre, elles ne conservent pas nécessairement les classes d'équivalence pour \equiv (c'est entre autres le cas les deux derniers exemples donnés plus haut : considérer l'environnement envoyant toutes les variables sur \mathbf{F}).

Remarque : La même stratégie ne permet pas de réduire FNC-SAT à 2-SAT. En fait, FNC-SAT ne se réduit pas à 2-SAT. En effet, on verra dans l'année de Spé que :

- 2-SAT se résout en temps polynomial (cf. chapitre "Graphes")
- 3-SAT est NP-complet (cf. théorème de Cook en 2^e année)
- FNC-SAT est NP-complet (*idem*)

Donc, à moins que $P = NP$, ces deux problèmes ne sont pas équivalents.

Remarque : FNC-SAT ne se réduit pas à FND-SAT pour deux raisons :

- la transformation d'une forme à l'autre se fait en temps exponentiel (vu dans un exemple plus haut) et peut aussi augmenter la taille de l'entrée de manière exponentielle
- on verra dans la suite que FND-SAT se résout en temps polynomial

Encore une fois, à moins que $P = NP$, ces deux problèmes ne sont pas équivalents.

5.3 Modéliser des FND ou FNC au regard de la satisfiabilité

5.3.1 Modéliser une FND

Rappelons qu'une FND est une disjonction de conjonctions. Ainsi, d'un point de vue sémantique, on peut dire que :

- L'ordre des littéraux au sein des conjonctions n'est pas important, et leur multiplicité non plus, puisqu'une conjonction est satisfaite par un environnement propositionnel ssi ce dernier satisfait l'ensemble de ses termes.
→ L'objet mathématique adapté pour modéliser les conjonctions de littéraux un ensemble de littéraux ou bien un couple d'ensembles de variables : d'une part, celles apparaissant dans les littéraux positifs, d'autre part, celles apparaissant dans les littéraux négatifs.
- De même, l'ordre et la multiplicité des conjonctions au sein de la disjonction ne sont pas importantes non plus, comme une disjonction est satisfaite par un environnement propositionnel ssi il satisfait l'un de ses termes.
→ L'objet mathématique adapté pour modéliser une FND est donc un ensemble de conjonctions.
- Pour ce qui est de la structure de données adaptée pour la modélisation d'une FND, une liste de listes de littéraux convient.

Exemples :

a) 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 : $\{(\{a, b\}, \{c\}), (\emptyset, \{b, c\}), (\{a, c\}, \emptyset)\}$.

5.4 FND-SAT : un problème facile

Voici un algorithme possible pour la résolution de FND-SAT sur $\mathcal{Q} = \{q_1, q_2, \dots, q_N\}$.

<u>FND-SAT</u>	<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;"><u>entrée</u> :</div> <div> $\left((\ell_{i,j})_{i \in [1..n_j]} \right)_{j \in [1..n]}$ </div> <div>une famille de familles de littéraux de \mathcal{Q}</div> </div> <div style="display: flex; align-items: center; margin-top: 10px;"> <div style="margin-right: 10px;"><u>sortie</u> :</div> <div> $\bigvee_{j=1}^n \bigwedge_{i=1}^{n_j} \ell_{i,j}$ </div> <div>est satisfiable, faux sinon</div> </div>
----------------	---

5.5 Puissance d'encodage du **SAT**

5.5.1 Modélisation – exemple du solitaire

5.6 Algorithme de Quine

5.6.1 Substitutions

Définition :

Soit $\sigma \in \mathcal{F}(\mathcal{Q}, \mathbb{F}_p(\mathcal{Q}))$. On appelle support de σ , noté $\text{supp}(\sigma)$, l'ensemble des variables que σ n'envoie pas sur la formule réduite à elle-même :

$$\text{supp}(\sigma) = \{q \in \mathcal{Q} \mid \sigma(q) \neq \text{Var}(q)\}$$

Définition :

Soit $\sigma \in \mathcal{F}(\mathcal{Q}, \mathbb{F}_p(\mathcal{Q}))$. On dit que σ est une substitution si $\text{Card}(\text{supp}(\sigma)) \in \mathbb{N}$.

Dans ce cas, si $\text{supp}(\sigma) = \{q_1, q_2, \dots, q_n\}$, on note

$$\sigma = [q_1 \mapsto \sigma(q_1), q_2 \mapsto \sigma(q_2), \dots, q_n \mapsto \sigma(q_n)]$$

Exemple : Pour $\sigma = \left(\begin{array}{l} \{x, y\} \rightarrow \mathbb{F}_p(\{x, y\}) \\ x \mapsto x \\ y \mapsto \neg x \end{array} \right)$, $\text{supp}(\sigma) = \{y\}$ et on a $\sigma = [y \mapsto \neg x]$.

Définition :

Soit $\sigma \in \mathcal{F}(\mathcal{Q}, \mathbb{F}_p(\mathcal{Q}))$ une substitution. On appelle application de la substitution σ la fonction suivante :

$$\cdot [\sigma] = \left(\begin{array}{l} \mathbb{F}_p(\mathcal{Q}) \rightarrow \mathbb{F}_p(\mathcal{Q}) \\ \top \mapsto \top \\ \perp \mapsto \perp \\ q \mapsto \sigma(q) \\ \neg A \mapsto \neg(A[\sigma]) \\ A \alpha B \mapsto A[\sigma] \alpha B[\sigma] \end{array} \right)$$

où α désigne toujours un symbole quelconque de $\{\vee, \wedge, \rightarrow, \leftrightarrow\}$.

Exercice : Trois personnes a , b et c veulent passer au tableau, selon les règles suivantes :

- Si a passe, alors b ne passe pas.
- Si b passe, alors a et c passent.
- Si c passe, alors a ou b ne passe pas.

1) Modéliser ces affirmations avec des variables de la logique.

2) Peut-on affirmer que a passe forcément ? que b ne passe pas ?

Définition :

Soit σ_1 et σ_2 deux substitutions. On note $\sigma_1 \cdot \sigma_2$ et on appelle composée de σ_1 et σ_2 la fonction suivante :

$$\sigma_1 \cdot \sigma_2 = \left(\begin{array}{l} \mathcal{Q} \rightarrow \mathbb{F}_p(\mathcal{Q}) \\ q \mapsto \sigma_2(q)[\sigma_1] \end{array} \right)$$

Propriété :

La composée de substitutions est associative, c'est-à-dire

$$\forall (\sigma_1, \sigma_2, \sigma_3) \in \mathcal{F}(\mathcal{Q}, \mathbb{F}_p(\mathcal{Q}))^3 \text{ tel que } \forall i \in [1..3], \text{Card}(\text{supp}(\sigma_i)) \in \mathbb{N} \\ (\sigma_1 \cdot \sigma_2) \cdot \sigma_3 = \sigma_1 \cdot (\sigma_2 \cdot \sigma_3)$$

Propriété :

La composée de deux substitutins est encore une substitution (*i.e.* \cdot est interne). De plus :

$$\cdot \forall \sigma_1, \sigma_2 \text{ des substitutions, } \text{supp}(\sigma_1 \cdot \sigma_2) \subseteq \text{supp}(\sigma_1) \cup \text{supp}(\sigma_2)$$

$$\cdot id, \text{ définie par } id = \left(\begin{array}{l} \mathcal{Q} \rightarrow \mathbb{F}_p(\mathcal{Q}) \\ q \mapsto \mathcal{V}ar(q) \end{array} \right), \text{ est le neutre pour la loi } \cdot \text{ (en effet, } \cdot[id] = Id_{\mathbb{F}_p(\mathcal{Q})})$$

Remarque : Toutes les substitutions ne sont pas symétrisables par \cdot .

5.6.2 Règles de simplification

Voici des règles de simplification pouvant s'appliquer à n'importe quelle formule $A \in \mathbb{F}_p(\mathcal{Q})$:

$$\begin{array}{ll} \neg \top \equiv \perp & A \rightarrow \perp \equiv \neg A \\ \neg \perp \equiv \top & A \rightarrow \top \equiv \top \\ A \wedge \top \equiv \top \wedge A \equiv A & \perp \rightarrow A \equiv \top \\ A \wedge \perp \equiv \perp \wedge A \equiv \perp & \top \rightarrow A \equiv A \\ A \vee \top \equiv \top \vee A \equiv \top & A \leftrightarrow \top \equiv \top \leftrightarrow A \equiv A \\ A \vee \perp \equiv \perp \vee A \equiv A & A \leftrightarrow \perp \equiv \perp \leftrightarrow A \equiv \neg A \\ \neg \neg A \equiv A & A \rightarrow A \equiv \top \end{array}$$

Propriété :

Soit $(A, A', B, B') \in \mathbb{F}_p(\mathcal{Q})^4$. Si $A \equiv A'$ et $B \equiv B'$, alors :

$$\begin{array}{l} \cdot A \alpha B \equiv A' \alpha B' \text{ pour } \alpha \in \{\wedge, \vee, \rightarrow, \leftrightarrow\} \\ \cdot \neg A \equiv \neg A' \end{array}$$

Exercice : Vérifier la satisfiabilité des formules suivantes :

$$a) A = ((a \rightarrow b) \wedge (b \rightarrow c)) \rightarrow (a \rightarrow c)$$

$$b) B = ((s \rightarrow (b \vee t)) \wedge ((b \vee a) \rightarrow (r \wedge m)) \wedge \neg r) \rightarrow (s \rightarrow t).$$