Analyse

Arnaud Durand et Pierre Gervais

September 30, 2016

Contents

Part I
Calcul propositionnel

1 Syntaxe

Le *calcul propositionnel* est un langage *inductivement* et *librement engendré* par un ensemble de règles.
C'est à dire qu'une formule ne peut pas être obtenu de deux façons différentes.

Définition 1. Soit $\mathcal{P}$ un ensemble de constantes propositionnelles, on définit $\mathcal{F}_{\mathcal{P}}$ le calcul propositionnel sur $\mathcal{P}$ obtenu par les règles suivantes :

- si $p \in \mathcal{P}$, alors $p \in \mathcal{F}_{\mathcal{P}}$
- $\perp \in \mathcal{F}_{\mathcal{P}}$
- si $F \in \mathcal{F}_{\mathcal{P}}$, alors $(\neg F) \in \mathcal{F}_{\mathcal{P}}$
- si $F, G \in \mathcal{F}_{\mathcal{P}}$ alors $(F \vee G), (F \wedge G), (F \to G) \in \mathcal{F}_{\mathcal{P}}$

Notation 1. S'il n'y a pas d'ambiguïté, on notera $\mathcal{F}_{\mathcal{P}} = \mathcal{F}$

Définition 2. Une définition alternative de $\mathcal{F}$ est $\mathcal{F} = \bigcup\limits_{n \geqslant 0} \mathcal{F}_n$ où

- $\mathcal{F}_0 = \mathcal{P}$
- $\mathcal{F}_{n+1} = \mathcal{F}_n \cup \{(\neg F) \mid F \in \mathcal{F}_n)\} \cup \{(F \star G) \mid F, G \in \mathcal{F}_n,\ \star \in \{\wedge, \vee, \to\}\}$, avec $n \geqslant 0$

On définit la *hauteur* d'une formule F par le plus petit n tel que $F \in \mathcal{F}_n$.

Remarque 1. Ce langage est fortement parenthésé et toute formule peut être représentée par un arbre de décomposition.

Propriété 1. *Propriété de lecture unique*
Pour tout $F \in \mathcal{F}$, un seul de ces cas est vrai :

1. *$F \in \mathcal{P}$*
2. *Il existe un unique $G \in \mathcal{F}$ tel que $F = (\neg G)$*
3. *Il existe d'uniques $G, H \in \mathcal{F}$ et $\star \in \{\vee, \wedge, \to\}$ tels que $F = G \star H$*

C'est-à-dire que toute formule ne peut se décomposer que d'une seule façon.

1.1 Raisonnements

On démontrera généralement les propriétés s'appliquant à $\mathcal{F}$ par induction : pour démontrer une proposition A s'appliquant à $\mathcal{F}$, on la démontre sur $\mathcal{P}$ et pour tout $(F \star G)$ et $(\neg F)$ où on suppose que $F, G \in \mathcal{F}$ vérifient A et $\star \in \{\wedge, \vee, \to\}$.

1.2 Définition alternative de $\mathcal{F}_{\mathcal{P}}$

Soit $\Sigma = \mathcal{P} \cup \{(,), \neg, \wedge, \vee, \to, \perp\}$, Σ^* est l'ensemble des mots sur Σ.
Exemple 1.

- $F = (\wedge \neg x_1)((\in \Sigma^*$
- $F = (\neg x_1) \in \Sigma^*$

Définition 3. $\mathcal{F}$ est le plus petit sous-ensemble de Σ^* contenant $\mathcal{P} \cup \{\perp\}$ et **clos** par les opérations

1. $(F, G) \longmapsto (F \vee G)$

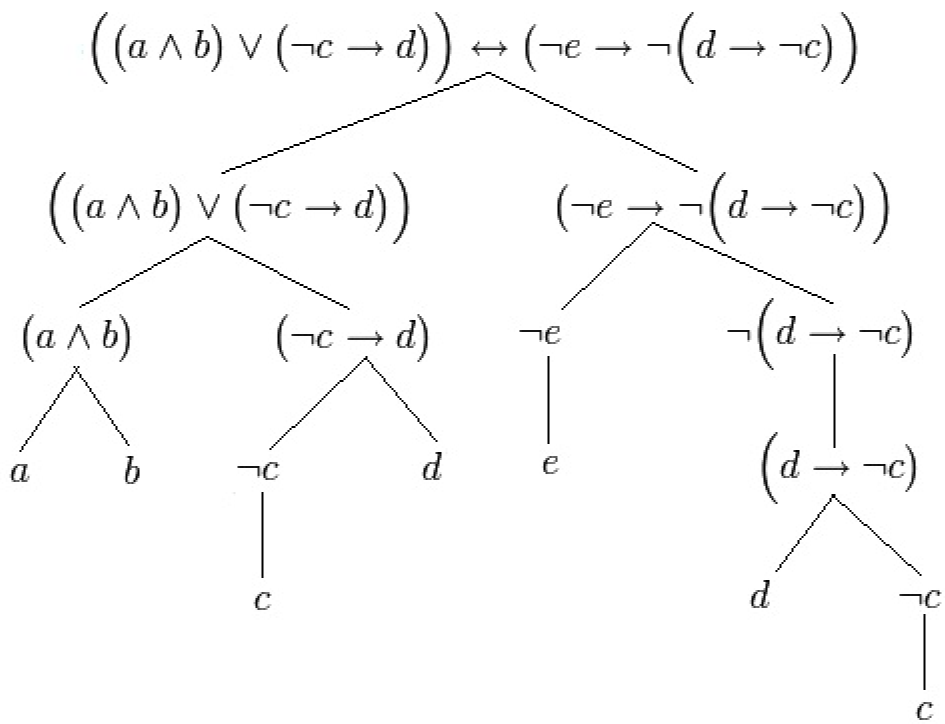

Figure 1: Arbre de décomposition

2. $(F, G) \longmapsto (F \wedge G)$
3. $(F, G) \longmapsto (F \to G)$

Remarque 2. On peut montrer que les deux définitions correspondent. $\mathcal{F}$ satisfait la propriété de lecture unique (voir TD).

1.2.1 Sous-formule, hauteur, arbre de décomposition

Définition 4. Soit $F \in \mathcal{F}$, on définit $\mathcal{S}(F)$ l'ensemble des *sous-formules de* F telles que

- si $F \in \mathcal{P}$, $\mathcal{S}(F) = \{F\}$
- si $F = (\neg G)$ alors $\mathcal{S}(F) = \{F\} \cup \mathcal{S}(G)$
- si $F = (G \star H)$ où $\star \in \{\wedge, \vee, \to\}$, alors $\mathcal{S}(F) = \{F\} \cup \mathcal{S}(G) \cup \mathcal{S}(H)$

TODO : vérifier dernier point

Définition 5. Soit $F \in \mathcal{F}$ on définit la *hauteur* $h(F)$ de F par

- $h(F) = 0$, si $F \in \mathcal{P}$
- si $= (\neg G)$, alors $h(F) = 1 + h(G)$
- si $F = (G \star H)$, alors $h(F) = 1 + \max\{h(G), h(H)\}$

Définition 6. Soit $F \in \mathcal{F}$, l'*arbre de décomposition de F* $arb(F)$ est un graphe étiqueté défini par

1. si $F \in \mathcal{P}$, $arb(F)$ est réduit à un sommet étiqueté par F.
2. si $F = (\neg G)$, alors $arb(F) = \neg - arb(G)$
3. si $F = (G \star H)$, alors $arb(F) = G - \star - H$

Notation 2. Soit F une formule, $var(F)$ est l'ensemble des variables de F, $occ(F)$ est le multi-ensemble des variables de F et $arb(F)$ est le graphe

- dont les sommets sont V
- et muni d'une fonction d'étiquetage $\lambda : V \longrightarrow \{\neg, \bot, \vee, \wedge, \rightarrow\} \cup var(F)$.

Remarque 3. Toutes les définitions sont univoques par la propriété de lecture unique.

Remarque 4. On définit la hauteur d'une formule par la hauteur de son arbre de décomposition, c'est-à-dire la distance maximum entre les feuilles et la racine.

Notation 3.

- $\top$ comme abréviation pour $(\bot \rightarrow \bot)$
- $(p \longleftrightarrow q)$ pour $(p \leftarrow q) \wedge (p \rightarrow q)$
- $\bigwedge_{i=1}^{n} A_i = (((A_1 \wedge A_2) \wedge A_3) ... \wedge A_n)$

2 Sémantique

On s'intéresse à des propositions dont la valeur de vérité est soit vrai soit faux. On a besoin d'une **interprétation** (en terme de vrai ou faux) de ces constantes propositionnelles.

Définition 7. Une *valuation* est une fonction $v : \mathcal{P} \longrightarrow \{0, 1\}$. Étant donné une valuation v, on définit l'*interprétation* $\overline{v} : \mathcal{F} \longrightarrow \{0, 1\}$ comme ceci

- si $F = p \in \mathcal{P}$ alors $\overline{v} = v(p)$
- si $F = (\neg G) \in \mathcal{P}$ alors $\overline{v}(F) = 1$ si et seulement si $\overline{v}(G) = 0$
- $\overline{v}(\bot) = 0$
- $\overline{v}(F \wedge G) = 1$ si et seulement si $\overline{v}(F) = \overline{v}(G) = 1$

On peut décrire l'interprétation d'une formule par sa *table de vérité* :

F	G	$\neg G$	$F \wedge G$	$F \to G$
0	0	1	0	1
0	1	1	0	1

On définit formellement la *table de vérité* par une fonction $v \; : \; \{0,1\}^{\mathcal{P}} \longrightarrow \{0,1\}$

Définition 8.

- $F \in \mathcal{F}$ est dit *satisfaisable* s'il existe une valuation v de $\mathcal{P}$ tel que $\overline{v}(F) = 1$
- F est dit *valide* si pour toute valuation v de $\mathcal{P}$, $\overline{v}(F) = 1$, on dit aussi que F est une *tautologie*.
- F et G sont dites *équivalentes*, notées $F \equiv G$, si pour toute valuation v, $\overline{v}(F) = \overline{v}(G)$

Exercice 1. Vérifier que $F \equiv G$ si et seulement si $F \leftrightarrow G$ est valide.

Proposition 1. *Pour tout $F \in \mathcal{F}$, F est satisfaisable si et seulement si $(\neg F)$ n'est pas valide.*

3 Exemples de formalisation

3.1 Contraites de compatibilité/exclusion

Problème : On possède n produits chimiques à ranger dans $k \leqslant n$ conteneurs. Certains produits ne peuvent pas être stockés ensemble dans un conteneur.

La contrainte est donnée sous la forme d'un ensemble $\mathcal{L} \subseteq [n]$ tel que $I = \{i_1, ..., i_k\} \subseteq \mathcal{L}$ si et seulement si les produits $i_1, .., i_k$ ne peuvent pas être stockés ensemble.

Enjeu : Écrire une formule propositionnelle F telle que F est satisfaisable si le problème a une solution.

Les variables propositionnelles $\mathcal{P} = p(i,j), \; i \leqslant n, \; j \leqslant k$ sont interprétées par "le produit chimique i est dans le camion j".

On exprime deux propositions :

- Chaque produit se trouve dans un unique conteneur : $F = \underbrace{\left(\bigwedge_{i\leqslant n}\left(\bigvee_{j\leqslant k} p(i,j)\right)\right)}_{\substack{\text{Chaque produit } i \text{ est stocké} \\ \text{dans au moins un camion } j}} \wedge \underbrace{\left(\bigwedge_{i\leqslant n}\left(\bigwedge_{\substack{j,j'\leqslant k \\ j\neq j'}} (\neg\,(p(i,j) \wedge p(i,j')))\right)\right)}_{\substack{\text{Pour chaque produit } i \\ \text{et chaque paire de camions } j\neq j' \\ \text{il est faux que } i \text{ est à la fois dans } j \text{ et } j'}}$

- On respecte les incompatibilités : $G = \underbrace{\bigwedge_{I\subseteq\mathcal{L}}\left(\bigwedge_{j\leqslant k} \neg\left(\bigwedge_{i\in I} p(i,j)\right)\right)}_{\substack{\text{Pour chaque ensemble } I \text{ de produits} \\ \text{ne pouvant pas être stockés ensemble} \\ \text{et pour chaque camion } j, \\ \text{aucun produit de } I \text{ n'est présent dans le camion}}}$

4 Équivalence logique usuelles

Proposition 2. *Substitution*
Soient $H_1, ..., H_n \in \mathcal{F}$.

- *Si F est une tautologie, la formule $F' = F[H_1/p_1, ..., H_n/p_n]$ est une tautologie, où F' est la formule dans laquelle on remplace chaque p_i par H_i.*
- *Si $F \equiv G$ alors $F[H_1/p_1, ..., H_n/p_n] \equiv G[H_1/p_1, ..., H_n/p_n]$*

Exemple 2. Soient $F = (p_1 \longrightarrow p_1)$ et $H = ((q_1 \wedge \neg q_3) \vee q_3)$
Si F est une tautologie, alors $(((q_1 \wedge \neg q_3) \vee q_3) \longrightarrow ((q_1 \wedge \neg q_3) \vee q_3))$ est une tautologie.

Remarque 5. La réciproque est fausse.

Lemme 1. *Soit $\mathcal{P} = \{p_1, ..., p_n\}$, $F \in \mathcal{F}$ et $H_1, ..., H_n \in \mathcal{F}$.*
Soit v une valuation de $\mathcal{P}$ avec $\forall i,\ v(H_i) = \delta_i$.
Alors la valuation v' définie par $v'(p_i) = \delta_i$ vérifie $\overline{v}(F[H_1/p_1, ..., H_n/p_n]) = \overline{v'}(F)$
On note $v \models F \iff \overline{v}(F) = 1$, c'est à dire si et seulement si v satisfait F.

Preuve 1. Démontrons le lemme par induction structurelle sur F.
On notera $F[H_1/p_1, ..., H_n/p_n] := F[\overline{H}/\overline{p}]$

- Si $F = \bot$, alors $v(\bot) = v'(\bot) = 0$.
- Si $F = p_1 \in \mathcal{P}$, alors $F' = F[H_1/p_1] = H_1$ <u>et</u> $v'(p_1) = \delta_1 = v(H_1)$.
- Si $F = \neg G$, par hypothèse d'induction $v(G[\overline{H}/\overline{p}]) = v'(G)$.
  $v(F[\overline{H}/\overline{p}]) = 1$
  $v(G[\overline{H}/\overline{p}]) = 1 - v'(G) = v'(F)$
- Si $F = G_1 \wedge G_2$, par hypothèse d'induction

$$\begin{cases} v(G_1[\overline{H}/\overline{p}]) = v'(G_1) \\ v(G_2[\overline{H}/\overline{p}]) = v'(G_2) \end{cases}$$

  or $v(F[\overline{H}/\overline{p}]) = v(G_1[\overline{H}/\overline{p}]) \cdot v(G_2[\overline{H}/\overline{p}]) = v'(G_1) \cdot v'(G_2) = v'(F)$
- etc.

$\square$

Preuve 2. Preuve de la proposition Comme $F \equiv G$ si et seulement si $(F \longleftrightarrow G)$ est une tautologie.
On prouve seulement seulement la première partie de la proposition.
Supposons F ue tautologie, soit v une valuation de $\mathcal{P}$, par le lemme précédent il existe v' telle que $v(F[\overline{H}/\overline{p}]) = v'(F)$ comme F est une tautologie, $v'(F) = 1$ et $v(F[\overline{H}/\overline{p}])$ est une tautologie.

$\square$

Par la suite, pour toutes formules propositionnelles A, B et C, les équivalences suivantes se montreront en substituant des variables aux formules.

Propriété 2.

- *Négation :* $\neg\neg A \equiv A$
- *Lois de Morgan :* $\neg(A \wedge B) \equiv \neg A \vee \neg B$, $\neg(A \vee B) \equiv \neg A \wedge \neg B$, $\neg(A \longrightarrow B) \equiv A \wedge \neg B$
- *Associativité :* $(A \wedge (B \wedge C)) \equiv ((A \wedge B) \wedge C)$ *et* $(A \vee (B \vee C)) \equiv ((A \vee B) \vee C)$
- *Expression des connecteurs :* $\bot \equiv (A \wedge \neg A)$ *et* $\top \equiv (A \vee \neg A)$
- *Distributivité :* $(A \vee (B \wedge C)) = ((A \vee B) \wedge (A \vee C)$
- *Idempotence :* $A \vee A \equiv A \wedge A \equiv A$
- *Absorption :* $(A \wedge \bot)\bot$ *et* $(A \vee \top) \equiv \top$
- *Neutre* $(A \wedge \top) \equiv A$ *et* $(A \vee \bot) \equiv A$

5 Formules normales

Ici $\mathcal{P} = \{x_1, ..., x_n\}$

Définition 9.

- Un *littéral* est une variable ou une négation de variable.
- Une *clause* est une formule C de la forme $C = \bigvee\limits_{i \in A} x_i \vee \bigvee\limits_{i \in B} \neg x_i$ où $A, B \subseteq \{1, ..., n\}$.
- La longueur d'une clause C notée $|C|$ est son nombre de variables : $|C| = |A| + |B|$.
- Si $|C| = 1$, C est une *clause unitaire* (ou *disjonction élémentaire*).

Part II
Compléments

6 Calcul propositionnel

6.1 Théorème de lecture unique

Définition 10. Soient $w_0, w_1 = a_1...a_n \in \mathcal{M}$, on dit que w_0 est un segment initial de w_1, noté $w_0 \subseteq w_1$ si $w_0 = a_1...a_i$ avec $1 \leqslant i \leqslant n$, et w_0 est un segment propre, noté $w_0 \subsetneq w_1$ si $i < n$.

Lemme 2. *Soit* $F \in \mathcal{F}$ *et* $G \subsetneq F$, *alors* $M \notin \mathcal{F}$
Autrement dit, aucune formule n'est le préfixe d'une autre.

Proposition 3. *On note* $o[F]$ *le nombre de parenthèses ouvrantes d'une formule* F *et* $f[F]$ *pour ses parenthèses fermées.*

1. $\forall F \in \mathcal{F},\ o[F] = f[F]$

2. $\forall F \in \mathcal{F}, \forall M \in \Sigma^*,\ M \subsetneq F \Longrightarrow \begin{cases} o[M] > f[M],\ \textit{et donc } M \notin \mathcal{F} & (a) \\ \textbf{\textit{x-ou}}\ M = \neg ... \neg \notin \mathcal{F} & (b) \\ \textbf{\textit{x-ou}}\ M = \varepsilon \notin \mathcal{F} & (c) \end{cases}$

Preuve 3. Soient $F \in \mathcal{F}$ et $M \subsetneq F$, montrons le second point.

- Si $F = \neg G = \neg g_1 ... g_n$
  - cas (c) : $M = \varepsilon$
  - cas (b) : $M = \neg$
  - $M = \neg g_1 ... g_i \subsetneq G,\ i < n$
    alors soit $o[M] = o[g_1 ... g_i] > f[g_1 ... g_i] = f[M]$, ce qui rentre dans le cas (a)
    soit $g_1 ... g_i = \underbrace{\neg ... \neg}_{i \text{ fois}}$, alors $M = \underbrace{\neg ... \neg}_{i+1 \text{ fois}}$: on est encore dans le cas (b).
- Si $F = (G \circ H) = (g_1 ... g_m \circ h_1 ... h_n)$ et $M \subsetneq F$, soit $M = \varepsilon$ (cas (c)), soit $M \neq \varepsilon$ avec
  - $M = ($ alors $o[M] = 1 > f[M] = 0$
  - $M = (g_1 ... g_i,\ 1 \leqslant i \leqslant m$, donc $o[M] = o[g_1 ... g_i] + 1 > f[M] = f[g_1 ... g_i]$
  - $M = (G \circ$ donc $o[M] = 1 + o[G] > f[M] = f[G]$
  - $M = (G \circ h_1 ... h_i,\ 1 \leqslant i \leqslant n$, alors $o[M] = 1 + o[G] + o[h_1 ... h_i]$
    $o[M] = 1 + f[G] + o[h_1 ... h_i] > f[G] + f[h_1 ... h_i] = f[(G \circ h_1 ... h_i] = f[M]$
- Si $F \in \mathcal{P},\ M = \varepsilon$, c'est le cas (c).

□

Preuve 4. Soit $F \in \mathcal{F}$

- Si $F \in \mathcal{P}$ pour tout $q \in \mathcal{P} \backslash \{F\}$, $q \neq F$.
  $\forall G \in \mathcal{F},\ F \neq \neg G$ car $|\neg G| \geqslant 2 > 1 = |F|$
  $\forall G, H \in \mathcal{F},\ \forall \star \in \{\wedge, \vee, \longrightarrow\},\ (G \star H) \neq F$ car $|F| = 1 < 5 \leqslant |(G \star H)|$
- Si $F = \neg G$ avec $G \in \mathcal{F}$, pour tout $q \in \mathcal{F}$ on a $q \neq F$.
  $\forall H \neq G$ on a $\neg H \neq F$
  $\neg G \neq (H \star K)$ pour toute formules H et G et tout opérateur $\star$.
- Si $F = (G_1 \star G_2)$, supposons $F = (H_1 \circ H_2)$ que l'on réécrit

$$a_1 ... a_k \star b_1 ... b_l = c_1 ... c_m \circ d_1 ... d_n$$

  Montrons $G_1 = H_1$, ce qui impliquera $\star = \circ$ et $G_2 = H_2$.
  On est face à l'un des deux cas :

$$(*)\ \underbrace{a_1 a_2 a_3 ... a_k}_{G_1 \in \mathcal{F}} \subseteq \underbrace{c_1 c_2 c_3 ... c_m}_{H_1 \in \mathcal{F}}$$

$$(**)\ c_1c_2c_3...c_m \subseteq a_1a_2a_3...a_n$$

les deux cas sont symétriques, on suppose $(*)$ et par l'absurde que $G_1 \neq H_1$, c'est à dire $G_1 \subsetneq H_1$, ce qui implique d'après le lemme $G_1 \notin \mathcal{F}$.

On a également $\forall F \in \mathcal{F},\ \neg G \neq (G_1 \star G_2)$ et $\forall p \in \mathcal{P},\ p \neq (G_1 \star G_2)$.

$\square$