La logique propositionnelle

Richard Lassaigne

Institut de Mathématiques de Jussieu
Equipe de Logique mathématique
CNRS-Université Paris Diderot

La logique propositionnelle, ou **calcul propositionnel**, est un cadre mathématique élémentaire qui constitue un noyau minimal commun à tous les systèmes logiques utilisés actuellement. D'un point de vue méthodologique, il joue le rôle d'une construction simplifiée qui peut être généralisée à des systèmes beaucoup plus expressifs. Son objet d'étude est la construction inductive des énoncés d'un langage et leur interprétation **sémantique** . Dans la première section, l'ensemble des énoncés, ou **formules**, est défini par **induction**. La deuxième section est dédiée à l'interprétation des formules en termes de valeurs de vérité (vrai, faux). Les notions de **formules équivalentes** et de **conséquence logique** rendent compte des principales propriétés de la logique propositionnelle. Les **formes normales** et le **problème SAT**, c'est-à-dire celui de décider la satisfaction d'une formule propositionnelle sous forme normale conjonctive, sont présentés dans la dernière section.

1 Le langage propositionnel

L'objet de ce paragraphe est de définir l'ensemble des formules du calcul propositionnel et de montrer comment ce genre de définition, qui est présent dans toutes les branches de la logique mathématique, peut être utilisé pour étudier les propriétés des formules du langage considéré.

1.1 Construction des formules

Le langage propositionnel est caractérisé par un ensemble de symboles, appelé **alphabet**, noté $\mathcal{A}$ et constitué par :

- un ensemble $\mathcal{P} = \{p, q, r, ...\}$, fini ou dénombrable, de symboles, appelés **variables propositionnelles**,
- l'ensemble des **connecteurs** (ou symboles logiques) comportant les symboles $\neg$ (**non**), $\wedge$ (**et**), $\vee$ (**ou**), $\rightarrow$ (**implique**), $\leftrightarrow$ (**équivalent à**),
- les parenthèses (et).

Le connecteur $\neg$ est dit **unaire** et les autres binaires. Un **mot**, ou une **expression**, est une suite finie de symboles de $\mathcal{A}$. La **longueur** d'un mot est le nombre de symboles qui le composent. L'ensemble des mots construits à l'aide de l'alphabet $\mathcal{A}$ est noté $\mathcal{A}^*$.
La **concaténation** est la loi de composition définie sur $\mathcal{A}^*$ qui associe à deux mots u, v le mot obtenu en juxtaposant la suite des symboles de u et celle de v : le nouveau mot ainsi obtenu est noté uv.
Un mot u est un segment initial d'un mot v s'il existe un mot w tel que $v = uw$. La relation définie sur $\mathcal{A}^*$ par "u est un segment initial de v" est une relation d'ordre (exercice).

Exemple 1
- *Les suites de symboles* $\neg p$, $(\neg p \wedge (q \vee r))$ *et* $(p \wedge \vee qr)$ *sont des mots de* $\mathcal{A}^*$.
- *Le mot* $(\neg p$ *est un segment initial de* $(\neg p \wedge (q \vee r))$.

Parmi toutes les expressions de $\mathcal{A}^*$, seules certaines sont intéressantes d'un point de vue logique : il s'agit de celles que l'on appelle des **formules**. Dans l'exemple précédent, seules les deux premières expressions sont des formules, à la différence de la dernière.

Définition 1 *L'ensemble des formules du calcul propositionnel construit sur* $\mathcal{P}$ *est le plus petit ensemble* $\mathcal{F}$ *tel que :*
- *toute variable propositionnelle est dans* $\mathcal{F}$,
- *si* $F \in \mathcal{F}$, *alors* $\neg F \in \mathcal{F}$,
- *si* $F, G \in \mathcal{F}$, *alors* $(F \wedge G) \in \mathcal{F}$, $(F \vee G) \in \mathcal{F}$, $(F \rightarrow G) \in \mathcal{F}$ *et* $(F \leftrightarrow G) \in \mathcal{F}$.

L'ensemble $\mathcal{F}$ est bien défini. En effet, il existe des ensembles satisfaisant ces conditions : par exemple, l'ensemble $\mathcal{A}^*$ de tous les mots. Parmi tous ces ensembles, Il en existe un plus petit : c'est leur intersection. Cette intersection n'est pas vide, car elle contient l'ensemble $\mathcal{P}$ des variables propositionnelles.
L'ensemble des formules peut être caractérisé d'une autre manière à l'aide du **principe de récurrence** . Soit P une propriété portant sur les entiers. Si P vérifie :
- P est vraie pour 0 (respectivement pour l'entier n_0),
- si P est vraie pour n, alors elle est vraie pour $n + 1$,

alors la propriété P est vraie pour tout entier (respectivement tout entier $n \geq n_0$).

Définition 2 *Les ensembles* $\mathcal{F}_n$ *sont définis par récurrence sur* n *:*
- $\mathcal{F}_0 = \mathcal{P}$,

- $\mathcal{F}_{n+1} = \mathcal{F}_n \cup \{\neg F : F \in \mathcal{F}_n\} \cup \{(F \alpha G) : F, G \in \mathcal{F}_n \textit{ et } \alpha \textit{ est } \wedge, \vee, \rightarrow \textit{ ou } \leftrightarrow\}$

Il est facile de voir que la suite des ensembles $\mathcal{F}_n$ est croissante (exercice).

Proposition 1 *L'ensemble $\mathcal{F}$ des formules du calcul propositionnel est égal à $\bigcup_{n \in N} \mathcal{F}_n$.*

Preuve : L'ensemble $\bigcup_{n \in N} \mathcal{F}_n$ satisfait les conditions de la définition de $\mathcal{F}$:
- toute variable propositionnelle est dans $\mathcal{F}_0$;
- si $F \in \mathcal{F}_n$, alors $\neg F \in \mathcal{F}_{n+1}$;
- si $F, G \in \bigcup_{n \in N} \mathcal{F}_n$, alors il existe n, m tels que $F \in \mathcal{F}_n$ et $G \in \mathcal{F}_m$; si $p = sup(n, m)$, $F, G \in \mathcal{F}_p$ et les formules $(F \wedge G)$, $(F \vee G)$, $(F \rightarrow G)$ et $(F \leftrightarrow G)$ sont dans $\mathcal{F}_{p+1}$;

L'ensemble $\bigcup_{n \in N} \mathcal{F}_n$ contient donc $\mathcal{F}$ qui est le plus petit ensemble satisfaisant ces conditions. Pour obtenir l'inclusion en sens inverse, il suffit de montrer que : pour tout entier n, $\mathcal{F}_n \subset \mathcal{F}$. Cette propriété se démontre par récurrence sur n :
- $\mathcal{F}_0 = \mathcal{P} \subset \mathcal{F}$;
- on suppose que $\mathcal{F}_n \subset \mathcal{F}$ (hypothèse de récurrence) ; d'après la définition de $\mathcal{F}_{n+1}$ et le fait que l'ensemble $\mathcal{F}$ soit clos par application des connecteurs, $\mathcal{F}_{n+1} \subset \mathcal{F}$.

Définition 3 *La* **complexité** *d'une formule F est le plus petit entier n tel que $F \in \mathcal{F}_n$.*

Exemple 2 *La formule $F = (\neg p \wedge ((q \vee r) \rightarrow s))$ est de complexité 3.*
- *p, q, r, s sont de complexité 0,*
- *$\neg p, (q \vee r)$ sont de complexité 1,*
- *$((q \vee r) \rightarrow s)$ est de complexité 2.*

1.2 Démonstration par induction sur les formules

Dans la suite, de nombreux résultats auront la forme : soit P une propriété portant sur les formules ; alors toute formule du calcul propositionnel possède la propriété P, ou encore l'ensemble des formules qui possèdent la propriété P est égal à $\mathcal{F}$. Pour démontrer ces résultats, on utilisera non pas un raisonnement par récurrence sur la complexité des formules, mais directement un raisonnement dit par **induction** sur les formules. Cette forme de démonstration est justifiée par la proposition suivante.

Proposition 2 *Soit P une propriété, portant sur les formules, qui satisfait les conditions suivantes :*
- *toute variable propositionnelle possède la propriété P,*
- *si G est une formule qui possède la propriété P, alors la formule $\neg G$ la possède aussi,*
- *si G, H sont des formules qui possèdent la propriété P, alors les formules $(G \wedge H)$, $(G \vee H)$, $(G \rightarrow H)$, $(G \leftrightarrow H)$ la possèdent aussi.*

Alors toute formule du calcul propositionnel possède la propriété P.

Preuve : Soit $\mathcal{E}$ l'ensemble des formules de $\mathcal{F}$ qui possèdent la propriété P. Il suffit de montrer que $\mathcal{F} \subset \mathcal{E}$ pour en déduire l'égalité. D'après les hypothèses satisfaites par la propriété P, l'ensemble $\mathcal{E}$ contient les variables propositionnelles et est stable par application des connecteurs. Il contient donc $\mathcal{F}$ qui est le plus petit ensemble vérifiant ces conditions.

Proposition 3 *Toute formule possède exactement le même nombre de parenthèses ouvrantes et fermantes.*

La preuve de la proposition précédente est un exemple simple de démonstration par induction sur l'ensemble des formules et est laissée en exercice.

1.3 Décomposition d'une formule

La proposition suivante fournit une réponse à la question suivante : étant donné une formule, existe-t-il différentes manières de la décomposer en formules plus simples ?

Proposition 4 *Soit F une formule. Alors F est de l'une et une seule des formes suivantes :*
(1) une variable propositionnelle,
(2) $\neg G$ où G est une formule,
(3) $(G \wedge H)$ où G et H sont des formules,
(4) $(G \vee H)$ où G et H sont des formules,
(5) $(G \rightarrow H)$ où G et H sont des formules,
(6) $(G \leftrightarrow H)$ où G et H sont des formules,
De plus, dans chacun des cas (2), (3), (4), (5) et (6), les formules G et H sont uniquement déterminées.

Définition 4 *Une* **sous-formule** *d'une formule F est une formule apparaissant dans la décomposition de F.*

On définit maintenant la notion d'arbre qui sera utilisée pour la représentation de la décomposition d'une formule.

Définition 5 *Un* **arbre** *est un ensemble T muni d'une fonction $h : T \longrightarrow \mathbb{N}$ et d'une relation binaire $P \subseteq T^2$ satisfaisant les conditions suivantes :*

- *il exite un unique élément r de T, appelé la* **racine**, *tel que $h(x) = 0$;*
- *pour tout élément y de T, sauf la racine, il existe un unique élément x tel que $(x, y) \in P$;*
- *pour tout $x \in T$, s'il existe $y \in T$ tel que $(x, y) \in P$, alors $h(y) = h(x) + 1$.*

Les éléments de l'arbre T sont appelés les *noeuds*. Pour tout $x \in T$, $h(x)$ est le *niveau* de x. Si $(x, y) \in P$, x est dit le *prédécesseur* ou le *père* de y et y un *successeur* ou un *fils* de x.

La décomposition des formules justifie la méthode suivante qui permet de :

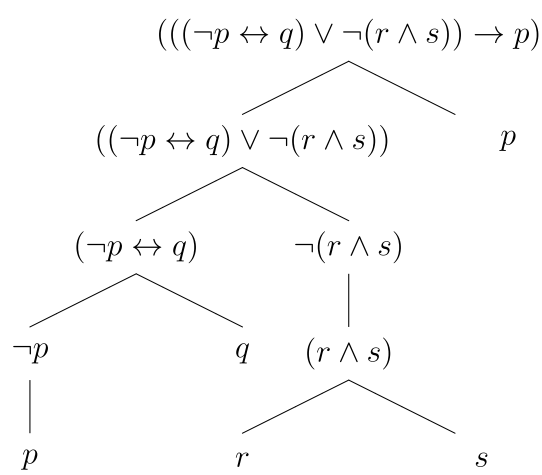
- décider si une expression donnée est une formule,
- dans le cas d'une réponse positive, de construire l'**arbre de décomposition** de cette formule F, c'est-à-dire un arbre dont les noeuds sont étiquetés par les sous-formules qui apparaissent dans la décomposition de la formule donnée. Si F est une variable propositionnelle (cas 1), le noeud correspondant est une feuille. Dans le cas 2, le noeud correspondant a un successeur étiqueté par la formule G. Dans les autres cas, le noeud correspondant a deux successeurs étiquetés par les formules G et H.

Exemple 3 *L'expression suivante est-elle une formule ?*

$$F = (((\neg p \leftrightarrow q) \vee \neg(r \wedge s)) \rightarrow p)$$

- *F est de la forme $(F_1 \rightarrow F_2)$ où $F_2 = p$ est une variable propositionnelle,*
- *F_1 est de la forme $(F_3 \vee F_4)$,*
- *F_3 est de la forme $(F_5 \leftrightarrow F_6)$ où $F_5 = \neg F_7$, $F_6 = q$ et $F_7 = p$ sont des variables propositionnelles,*
- *F_4 est de la forme $\neg F_8$ et F_8 est de la forme $(F_9 \wedge F_{10})$, où $F_9 = r$ et $F_{10} = s$ sont des variables propositionnelles.*

L'expression F est bien une formule. De plus, son arbre de décomposition montre comment elle est construite à partir des variables propositionnelles en utilisant les connecteurs et fournit, au passage, toutes les formules entrant dans cette construction. L'expression F est la racine de l'arbre.



Exemple 4 *Les formules* $(\neg p \leftrightarrow q)$, $(r \wedge s)$ *et* p *sont des sous-formules de l'exemple précédent.*

On remarque que si T est l'arbre de décomposition d'une formule F, alors la complexité de la formule F est égale à $sup\{h(x) \ : \ x \in T\}$.

2 Sémantique

La sémantique est définie à partir de l'interprétation des formules en termes de valeurs de vérité (vrai, faux) : une **valuation**, distribution de valeurs de vérité, sur l'ensemble des variables propositionnelles permet de déterminer la valeur correspondante d'une formule. Dans la suite, 0 représente la valeur **faux**, 1 la valeur **vrai** et ssi est une abréviation pour **si et seulement si**.

Définition 6 *Une valuation* v *est une fonction de l'ensemble des variables propositionnelles* $\mathcal{P}$ *dans* $\{0, 1\}$.

Proposition 5 *Soit* v *une valuation. Alors il existe un prolongement unique* $\overline{v}$ *de* v *à* $\mathcal{F}$ *qui satisfait les conditions suivantes :*

- *pour tout* $p \in \mathcal{P}$, $\overline{v}(p) = v(p)$,
- *si* $F = \neg G$, *alors* $\overline{v}(F) = 1$ *ssi* $\overline{v}(G) = 0$,
- *si* $F = (G \wedge H)$, *alors* $\overline{v}(F) = 1$ *ssi* $\overline{v}(G) = \overline{v}(H) = 1$,
- *si* $F = (G \vee H)$, *alors* $\overline{v}(F) = 0$ *ssi* $\overline{v}(G) = \overline{v}(H) = 0$,
- *si* $F = (G \rightarrow H)$, *alors* $\overline{v}(F) = 0$ *ssi* $\overline{v}(G) = 1$ *et* $\overline{v}(H) = 0$,
- *si* $F = (G \leftrightarrow H)$, *alors* $\overline{v}(F) = 1$ *ssi* $\overline{v}(G) = \overline{v}(H)$.

Preuve : La distribution $\overline{v}$ est définie par induction sur les formules.

- C'est évident pour les variables propositionnelles.
- Si F est de la forme $\neg G$ et $\overline{v}(G)$ est déjà définie (hypothèse d'induction), on pose $\overline{v}(F) = 1$ si $\overline{v}(G) = 0$ et 0 sinon.
- Si F est de la forme $(G \wedge H)$ et $\overline{v}(G)$, $\overline{v}(H)$ sont déjà définis (hypothèse d'induction), on pose $\overline{v}(F) = 1$ si $\overline{v}(G) = \overline{v}(H) = 1$ et 0 sinon.

La démonstration dans les autres cas est analogue : la donnée des valeurs de $\overline{v}(G)$ et de $\overline{v}(H)$ permet de définir celle de $\overline{v}(F)$ en satisfaisant la condition 4), 5) ou 6) suivant le cas. Cette valeur est bien définie de manière unique d'après le théorème de décomposition. L'unicité du prolongement de v est laissée en exercice : si l'on suppose qu'il existe deux prolongements, il est facile de montrer par induction sur les formules, qu'ils sont égaux.

Exemple 5 *La valeur de la formule* $((p \to q) \land (q \lor r))$ *pour la valuation* v *définie par :* $v(p) = v(q) = 0$ *et* $v(r) = 1$ *est* 1.

Un moyen de se représenter les conditions énoncés dans la proposition précédente est de construire un tableau donnant les valeurs de $v(F)$ en fonction des différentes valeurs possibles de v sur les sous-formules immédiates de F. Il est facile de construire ainsi les **tables de vérité** des connecteurs binaires $\land, \lor, \to$:

G	1	1	0	0
H	1	0	1	0
$(G \land H)$	1	0	0	0
$(G \lor H)$	1	1	1	0
$(G \to H)$	1	0	1	1
$(G \leftrightarrow H)$	1	0	0	1

Dorénavant, dès qu'une valuation v est donnée sur $\mathcal{P}$, on considèrera qu'elle est également définie sur l'ensemble $\mathcal{F}$ de toutes les formules et on notera v son prolongement.

2.1 Tautologies. Formules équivalentes

L'interprétation des formules permet de les classer : deux formules possédant toujours la même interprétation seront regroupées dans la même classe. Une classe particulièrement intéressante est constituée par celles qui prennent toujours la valeur vrai.

Définition 7

- *Une formule* F *est* **satisfaite** *par une valuation* v *si* $v(F) = 1$.
- *Une* **tautologie** *est une formule qui est satisfaite par toute valuation.*
- *Deux formules* F, G *sont dites* **équivalentes** *si pour toute valuation* v, $v(F) = v(G)$.

Exemple 6 *Les formules suivantes sont des exemples de tautologies :*

$$(p \to p)$$

$$(p \to (q \to p))$$

$$((p \to (q \to r)) \to ((p \to q) \to (p \to r)))$$

$$(((\neg p \to q) \to ((\neg p \to \neg q) \to p))$$

Les couples de formules suivantes sont des exemples de formules équivalentes :

$$\neg\neg p \text{ et } p$$

$$(p \to q) \ et\ (\neg p \vee q)$$

$$(p \leftrightarrow q) \ et\ ((p \to q) \wedge (q \to p))$$

$$(p \wedge (q \vee r)) \ et\ ((p \wedge q) \vee (p \wedge r))$$

On remarque que deux formules F, G sont équivalentes ssi la formule $(F \leftrightarrow G)$ est une tautologie. La relation binaire $\equiv$ définie sur l'ensemble des formules par : $F \equiv G$ ssi F, G sont équivalentes, est une relation d'équivalence (exercice).

2.2 Conséquence logique

Du point de vue sémantique, l'une des questions fondamentales est de savoir si une formule est conséquence d'un ensemble de formules donné.

Définition 8 *Soient Σ un ensemble de formules et F une formule.*

- *La formule F est dite conséquence de Σ si toute valuation, qui satisfait toutes les formules de Σ à la fois, satisfait aussi la formule F.*
- *Un ensemble de formules Σ est dit satisfaisable s'il existe une valuation qui satisfait toutes les formules de Σ.*

Exemple 7

- *La formule q est conséquence de l'ensemble $\{p, (p \to q)\}$.*
- *L'ensemble de formules $\{p, (p \to q), \neg q\}$ n'est pas satisfaisable.*

Proposition 6 *Une formule F est conséquence de l'ensemble de formules Σ si et seulement si l'ensemble $\Sigma \cup \{\neg F\}$ n'est pas satisfaisable.*

Preuve : Si toute valuation qui satisfait Σ satisfait aussi F, alors il n'existe pas de valuation qui satisfait à la fois Σ et $\neg F$. La réciproque se montre facilement par contraposition : s'il existe une valuation qui satisfait Σ et qui ne satisfait pas F, cette valuation satisfait Σ et $\neg F$.

2.3 Valeur d'une formule et substitution

La valeur d'une formule, par exemple $((p \to q) \wedge (q \vee r))$, peut être déterminée pour une valuation v donnée. Mais comment peut-on calculer la valeur de vérité d'une formule complexe à partir des valeurs de formules plus simples ? Le résultat mentionné dans ce paragraphe répond à cette question : il suffit de composer les valeurs de vérité comme dans le cas des variables propositionnelles.

Définition 9 *Une occurrence de la variable p dans une formule F est la donnée de cette variable et d'une place où elle apparaît dans F.*

Soit G une formule. La formule obtenue par **substitution** de G à p dans F, notée $F(G/p)$ est la formule obtenue en remplaçant toutes les occurrences de p dans F par la formule G.

Exemple 8 *La substitution de la formule $(q \to r)$ à la variable q dans la formule $((p \to q) \wedge (q \vee r))$ donne :*

$$((p \to (q \to r)) \wedge ((q \to r) \vee r))$$

Proposition 7 *Pour obtenir la valeur de la formule $F(G/p)$ pour la valuation v, il suffit de calculer en remplaçant $v(p)$ par $v(G)$, en laissant inchangées les valeurs de v sur les autres variables propositionnelles de F*

Exemple 9

- *Quelles que soient les formules F, G, H, les formules suivantes sont des tautologies :*

$$(F \to F)$$
$$(F \to (G \to F))$$
$$((F \to (G \to H)) \to ((F \to G) \to (F \to H)))$$

- *Quelles que soient les formules F, G, H, les formules suivantes sont équivalentes :*

$$\neg\neg F \equiv F$$

$$(F \to G) \equiv (\neg F \vee G)$$
$$(F \leftrightarrow G) \equiv ((F \to G) \wedge (G \to F))$$

- *Si $F \equiv F'$ et $G \equiv G'$, alors les formules suivantes sont équivalentes :*

$$\neg F \equiv \neg F'$$

$$(F \wedge G) \equiv (F' \wedge G')$$
$$(F \vee G) \equiv (F' \vee G')$$
$$(F \to G) \equiv (F' \to G')$$
$$(F \leftrightarrow G) \equiv (F' \leftrightarrow G')$$

Les équivalences de formules suivantes expriment les principales propriétés des connecteurs :

- *commutativité* :

$$(F \wedge G) \equiv (G \wedge F)$$
$$(F \vee G) \equiv (G \vee F)$$

- *associativité* :

$$(F \wedge (G \wedge H)) \equiv ((F \wedge G) \wedge H)$$
$$(F \vee (G \vee H)) \equiv ((F \vee G) \vee H)$$

- *idempotence* :

$$(F \wedge F) \equiv F$$
$$(F \vee F) \equiv F$$

- *règles de de Morgan* :

$$\neg(F \wedge G) \equiv (\neg F \vee \neg G)$$
$$\neg(F \vee G) \equiv (\neg F \wedge \neg G)$$

- *distributivité* :

$$(F \wedge (G \vee H)) \equiv ((F \wedge G) \vee (F \wedge H))$$
$$(F \vee (G \wedge H)) \equiv ((F \vee G) \wedge (F \vee H))$$

- *absorption* :

$$(F \wedge (F \vee G)) \equiv F$$
$$(F \vee (F \wedge G) \equiv F$$

On rappelle que la notation $F \equiv G$ exprime seulement une relation entre deux formules, mais ne désigne pas une formule du calcul propositionnel ! L'étude des propriétés énoncées dans les exemples qui précèdent suffisent pour la construction des formes normales équivalentes à une formule donnée, question abordée dans la dernière section.

2.4 Système complet de connecteurs

La proposition suivante présente un groupe de connecteurs qui suffisent pour obtenir le pouvoir d'expression de la logique propositionnelle.

Proposition 8 *Toute formule du calcul propositionnel est équivalente à une formule construite avec les seuls connecteurs* $\neg, \wedge$.

La démonstration se fait par induction sur les formules et est laissée en exercice.

Définition 10 *Un ensemble de connecteurs qui possède la propriété énoncée dans la proposition précédente pour* $\{\neg, \wedge\}$ *est appelé un* **système complet.**

A titre d'exercice, il est facile de déduire du résultat précédent que les systèmes de connecteurs $\{\neg, \vee\}$ et $\{\neg, \rightarrow\}$ sont complets.

3 Formes normales

Les formes normales sont des formules particulières, dans lesquelles il est possible de transformer n'importe qu'elle formule, à équivalence près.

3.1 Formes normales disjonctive et conjonctive

Définition 11 *Une* **forme normale disjonctive** *est :*

- *soit une disjonction* $(F_1 \vee F_2 \vee ... \vee F_k)$*, où chaque formule* F_i $(\ i = 1, 2, ..., k\ )$ *est de la forme* $(G_1 \wedge G_2 \wedge ... \wedge G_l)$*, chaque* G_j $(\ j = 1, 2, ..., l\ )$ *étant une variable propositionnelle ou une variable propositionnelle précédée d'une négation.*
- *soit réduite à l'une des formules* F_i*.*

Exemple 10 *Les formules suivantes sont des formes normales disjonctives.*

$$((p \wedge q) \vee (\neg p \wedge \neg q))$$

$$((p \wedge q \wedge \neg r) \vee (\neg p \wedge q))$$

$$(p \wedge \neg q)$$

Définition 12 *Une* **forme normale conjonctive** *est :*

- *soit une conjonction* $(F_1 \wedge F_2 \wedge ... \wedge F_k)$*, où chaque formule* F_i $(\ i = 1, 2, ..., k\ )$ *est de la forme* $(G_1 \vee G_2 \vee ... \vee G_l)$*, chaque* G_j $(\ j = 1, 2, ..., l\ )$ *étant une variable propositionnelle ou une variable propositionnelle précédée d'une négation.*
- *soit réduite à l'une des formules* F_i*.*

Exemple 11 *Les formules suivantes sont des formes normales conjonctives.*

$$((\neg p \vee q) \wedge (p \vee \neg q))$$

$$((p \vee \neg q \vee r) \wedge (\neg p \vee r) \wedge (\neg r \vee \neg s))$$

$$(\neg p \vee q)$$

3.2 Fonction associée à une formule

L'ensemble $\mathcal{P}$ est maintenant supposé fini : $\mathcal{P} = \{p_1, p_2, ..., p_n\}$. Il existe alors 2^n valuations deux à deux distinctes. Chaque formule $F(p_1, p_2, ..., p_n)$ définit une fonction f_F de l'ensemble des valuations $\{0, 1\}^{\mathcal{P}}$ dans $\{0, 1\}$: celle qui, à chaque valuation v, associe la valeur $v(F)$. La propriété suivante est évidente.

Proposition 9 *Deux formules F, G sont équivalentes ssi les deux fonctions associées sont égales.*

Corollaire 1 *Il existe au plus 2^{2^n} formules, deux à deux non équivalentes, du calcul propositionnel construit sur n variables.*

Preuve : Soit $\mathcal{F}/\equiv$ le quotient de l'ensemble des formules par la relation d'équivalence $\equiv$. La fonction de $\mathcal{F}/\equiv$ dans l'ensemble des foncions de $\{0,1\}^{\mathcal{P}}$ dans $\{0,1\}$ qui, à la classe d'équivalence de F, associe la fonction f_F est une injection.

Le théorème suivant exprime que le pouvoir d'expression de la logique propositionnelle est celui de l'ensemble des fonctions booléennes.

Théorème 1 *Toute fonction f de $\{0,1\}^{\mathcal{P}}$ dans $\{0,1\}$ peut être représentée par une formule $F(p_1, p_2, ..., p_n)$, c'est-à-dire il existe une formule $F(p_1, p_2, ..., p_n)$ telle que, pour toute valuation v, $f(v) = v(F)$.*

La démonstration se fait par récurrence sur le nombre n de variables propositionnelles.

Corollaire 2 *Toute formule est équivalente à une forme normale disjonctive et à une forme normale conjonctive.*

Pour obtenir ces formes normales équivalentes à une formule donnée, on peut utiliser une méthode de transformation par équivalences successives.

3.3 Méthode de transformation

En pratique, la méthode consiste à transformer la formule par équivalences successives à l'aide des règles suivantes appliquées dans cet ordre :

- élimination des connecteurs $\rightarrow$ et $\leftrightarrow$ à l'aide des équivalences :

$$(F \rightarrow G) \equiv (\neg F \vee G)$$

$$(F \leftrightarrow G) \equiv ((\neg F \vee G) \wedge (F \vee \neg G))$$

- entrée des négations le plus à l'intérieur possible :

$$\neg(F \wedge G) \equiv (\neg F \vee \neg G)$$

$$\neg(F \vee G) \equiv (\neg F \wedge \neg G)$$

- utilisation des distributivités de $\wedge$ et $\vee$ l'un par rapport à l'autre :

$$(F \wedge (G \vee H)) \equiv ((F \wedge G) \vee (F \wedge H))$$

$$(F \vee (G \wedge H)) \equiv ((F \vee G) \wedge (F \vee H))$$

Exemple 12 *Mettre la formule* $\neg(p \leftrightarrow (q \rightarrow r))$ *sous formes normales disjonctive et conjonctive. La formule est transformée par équivalences successives :*

$$\neg((p \rightarrow (q \rightarrow r)) \wedge ((q \rightarrow r) \rightarrow p))$$

$$\neg((\neg p \vee (\neg q \vee r)) \wedge (\neg(\neg q \vee r) \vee p))$$
$$(\neg(\neg p \vee (\neg q \vee r)) \vee \neg(\neg(\neg q \vee r) \vee p))$$
$$((p \wedge \neg(\neg q \vee r)) \vee ((\neg q \vee r) \wedge \neg p))$$
$$((p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q) \vee (\neg p \wedge r))$$

qui est une forme normale disjonctive ;

$$(((p \wedge q \wedge \neg r) \vee (\neg q \vee r)) \wedge ((p \wedge q \wedge \neg r) \vee \neg p))$$

$$((p \vee \neg q \vee r) \wedge (\neg p \vee q) \wedge (\neg p \vee \neg r))$$

qui est une forme normale conjonctive.

3.4 Le problème SAT

Problème SAT : Etant donné une formule du langage propositionnel à n variables sous forme normale conjonctive, déterminer s'il existe une valuation la satisfaisant.

Ce problème est représentatif des problèmes de la classe de complexité **NP**, pour lesquels on ne connaît pas d'algorithme efficace, c'est-à-dire en **temps polynomial**. Un tel algorithme pour le problème SAT permettrait de donner une réponse positive au problème **P=NP ?**, central en théorie de la complexité depuis les années 70. L'algorithme évident pour le problème SAT, qui consiste à examiner toutes les valuations possibles, est en **temps exponentiel**. Depuis plus de quarante ans, il existe une recherche très active dans le domaine des **SAT-solveurs**, qui ont donné lieu à de nombreuses méthodes de résolution de ce problème.

4 Exercices

Exercice 1. Reconnaître et décomposer une formule.
On considère un ensemble de variables propositionnelles $\mathcal{P} = \{p, q, r, s, \ldots\}$. Déterminer si les expressions suivantes sont des formules du calcul propositionnel construit sur $\mathcal{P}$ et donner (éventuellement) leur arbre de décomposition ainsi que leur complexité :

$$(\neg p \vee (q \wedge r) \to s)) \qquad (((\neg p \leftrightarrow q) \vee \neg(r \vee s)) \to (p \wedge \neg r))$$

Exercice 2. Valeurs de vérité des formules.
Déterminer les valuations sur $\mathcal{P} = \{p, q, r, s\}$ pour lesquelles chacune des formules suivantes prend la valeur 0 :

$$(\neg p \vee ((q \wedge r) \to s))$$

$$(((\neg p \leftrightarrow q) \vee \neg(r \vee s)) \to (p \wedge \neg r))$$

Exercice 3.
Montrer que les formules suivantes sont des tautologies :

$$((p \to (q \to r)) \leftrightarrow ((p \wedge q) \to r))$$

$$((q \to r) \to ((p \to q) \to (p \to r)))$$

$$(((p \to q) \to p) \to p)$$

Exercice 4.
Montrer que les formules suivantes sont équivalentes :

$$(p \leftrightarrow q) \text{ et } ((p \wedge q) \vee (\neg p \wedge \neg q))$$

$$\neg(p \leftrightarrow q) \text{ et } ((p \wedge \neg q) \vee (\neg p \wedge q))$$

$$(p \leftrightarrow (q \leftrightarrow r)) \text{ et } ((p \leftrightarrow q) \leftrightarrow r)$$

$$(p \to (q \wedge r)) \text{ et } ((p \to q) \wedge (p \to r))$$

$$(p \to (q \vee r)) \text{ et } ((p \to q) \vee (p \to r))$$

$$((p \wedge q) \to r) \text{ et } ((p \to r) \vee (q \to r))$$

$$((p \vee q) \to r) \text{ et } ((p \to r) \wedge (q \to r))$$

Exercice 5.
Construire l'arbre de décomposition de la formule et en déduire sa complexité :

$$((p \vee (q \to r)) \wedge \neg(q \leftrightarrow ((r \to s) \vee (\neg r \to t))))$$

Exercice 6.
Montrer que les deux formules suivantes sont équivalentes :

$$(p \leftrightarrow \neg(q \leftrightarrow r)) \text{ et } (\neg(p \leftrightarrow q) \leftrightarrow r)$$

Exercice 7.
La formule $F : \neg(p \to r)$ est-elle conséquence de l'ensemble de formules Σ ?

$$\Sigma = \{(p \to (q \leftrightarrow r))\ ,\ \neg(p \to q)\}$$

Exercice 8.
Déterminer les valuations sur $\{p, q, r, s\}$ satisfaisant la formule H :

$$((p \leftrightarrow (q \leftrightarrow r)) \wedge (q \leftrightarrow (r \leftrightarrow s)))$$

Exercice 9.
Déterminer une forme normale disjonctive et une forme normale conjonctive équivalentes à la formule G :

$$\neg((p \leftrightarrow q) \wedge (r \to s))$$