Résolution Propositionnelle

Système de déduction

Benjamin Wack

Université Grenoble Alpes

Janvier 2025

Au dernier cours

- Équivalences remarquables
- Substitutions et remplacements
- Formes normales

Jean, Pierre et Marie par simplification

$$(p \Rightarrow \neg j) \wedge (\neg p \Rightarrow j) \wedge (j \Rightarrow m) \Rightarrow m \vee p$$

$$\neg((p \Rightarrow \neg j) \wedge (\neg p \Rightarrow j) \wedge (j \Rightarrow m)) \vee m \vee p$$

$$\neg(p \Rightarrow \neg j) \vee \neg(\neg p \Rightarrow j) \vee \neg(j \Rightarrow m) \vee m \vee p$$

$$(p \wedge \neg\neg j) \vee (\neg p \wedge \neg j) \vee (j \wedge \neg m) \vee m \vee p$$

avec $x \vee (x \wedge y) \equiv x$

$$(\neg p \wedge \neg j) \vee (j \wedge \neg m) \vee m \vee p$$

avec $x \vee (\neg x \wedge y) \equiv x \vee y$

$$\neg j \vee j \vee m \vee p = 1$$

Forme normale conjonctive

Définition 1.4.11

Une formule est en forme normale conjonctive (FNC) si et seulement si elle est une conjonction (produit) de clauses.

Appliquer la distributivité (!) de la disjonction sur la conjonction :

- $A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$

L'intérêt des FNC est de mettre en évidence les contre-modèles.

Exemple 1.4.12

$(x \vee y) \wedge (\neg x \vee \neg y \vee z)$ est une FNC, qui a deux contre-modèles

- $x = 0, y = 0$
- $x = 1, y = 1, z = 0.$

Utilisée en modélisation (SAT-solvers)

Exemples 1.4.8 et 1.4.13

Mise en FND de :

$$(a \vee b) \wedge (c \vee d \vee e) \equiv$$

$$\boxed{(a \wedge c) \vee (a \wedge d) \vee (a \wedge e) \vee (b \wedge c) \vee (b \wedge d) \vee (b \wedge e).}$$

Mise en FNC de :

$$(a \wedge b) \vee (c \wedge d \wedge e) \equiv$$

$$\boxed{(a \vee c) \wedge (a \vee d) \wedge (a \vee e) \wedge (b \vee c) \wedge (b \vee d) \wedge (b \vee e).}$$

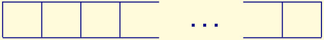
BDDC (*Binary Decision Diagram based Calculator*)

BDDC est un outil pour la manipulation de formules propositionnelles développé par Pascal Raymond et disponible à l'adresse suivante :

http://www-verimag.imag.fr/~raymond/home/tools/bddc/

Exemple de modélisation SAT

Problème



- Chaque case peut contenir un jeton ou pas.
- Deux jetons ne doivent jamais être voisins.

Entrées du problème : la longueur n de la grille

Modélisation booléenne

- À chaque case on associe une variable booléenne (vraie si la case contient un jeton)
- Pour le format Dimacs, on numérote les cases de 1 à n

Comment modéliser « Au moins 2 cases doivent contenir un jeton » ?

Plan

Algèbre de Boole

Fonctions booléennes

Introduction aux systèmes de déduction

Résolution et preuves par résolution

Conclusion

Définition 1.5.1

Une algèbre de Boole est un ensemble :

- d'au moins deux éléments (0 et 1)
- avec trois opérations : complément ($\overline{x}$), somme ($+$) et produit (.)
- telles que :

1. la somme est associative, commutative, élément neutre 0
2. le produit est associatif, commutatif, élément neutre 1
3. le produit est distributif sur la somme
4. la somme est distributive sur le produit
5. les lois du complément :
    - $x + \overline{x} = 1$,
    - $x.\overline{x} = 0$.

La logique propositionnelle est une algèbre de Boole

Les axiomes correspondent à des équivalences remarquables connues (qu'on peut démontrer par tables de vérités).

Autre exemple :

Algèbre de Boole	$\mathcal{P}(X)$
1	X
0	$\emptyset$
$\overline{p}$	$X - p$
$p + q$	$p \cup q$
$p.q$	$p \cap q$

Exemple 1.4.10 avec les notations de l'algèbre de Boole

Soit $A = (a \Rightarrow b) \wedge c \vee (a \wedge d)$.

Déterminer si A est valide.

$$
\begin{array}{lcl}
A & \equiv & (\overline{a}+b).c+a.d \\
\neg A & \equiv & \overline{(\overline{a}+b).c}\ .\ \overline{a.d} \\
 & \equiv & (\overline{\overline{a}+b}+\overline{c})\ .\ (\overline{a}+\overline{d}) \\
 & \equiv & (a.\overline{b}+\overline{c})\ .\ (\overline{a}+\overline{d}) \\
 & \equiv & a.\overline{b}.\overline{a}+a.\overline{b}.\overline{d}+\overline{c}.\overline{a}+\overline{c}.\overline{d} \\
 & \equiv & a.\overline{b}.\overline{d}+\overline{c}.\overline{a}+\overline{c}.\overline{d}
\end{array}
$$

Propriétés d'une algèbre de Boole

Propriété 1.5.3

- Pour tout x, il y a un et un seul y tel que $x + y = 1$ et $xy = 0$, autrement dit le complément est unique.
- 1. $\overline{1} = 0$
  2. $\overline{0} = 1$
  3. $\overline{\overline{x}} = x$
  4. $x.x = x$
  5. $x + x = x$
  6. $1 + x = 1$
  7. $0.x = 0$
  8. Lois de De Morgan :
     - $\overline{xy} = \bar{x} + \bar{y}$
     - $\overline{x + y} = \bar{x}.\bar{y}$

Moralité : certaines équivalences sont fondamentales pour que la logique booléenne fonctionne, les autres peuvent être déduites.

Exemples de preuves en algèbre de Boole

1. $\overline{1} = 0$.
   Comme $x.\overline{x} = 0$, on a $1.\overline{1} = 0$.
   Puisque 1 est neutre, $\overline{1} = 0$.
2. $\overline{0} = 1$.
   Idem : $x + \overline{x} = 1$ donc $0 + \overline{0} = 1$ donc $\overline{0} = 1$.
3. $\overline{\overline{x}} = x$.
   Par commutativité, $\overline{x} + x = 1$ et $\overline{x}.x = 0$
   Par unicité de la négation de $\bar{x}$, on a $\overline{\overline{x}} = x$.

Définition 1.6.1 : Fonction booléenne

Une fonction booléenne est une fonction dont les arguments et le résultat sont dans le domaine $\mathbb{B} = \{0, 1\}$.

Exemple 1.6.2

- $f : \mathbb{B} \rightarrow \mathbb{B} : f(x) = \neg x$
- mais pas $f : \mathbb{N} \rightarrow \mathbb{B} : f(x) = x \bmod 2$

Grâce aux tables de vérité, on peut associer chaque formule booléenne à une fonction booléenne.
La réciproque est-elle vraie ?

Fonctions booléennes et somme de monômes

Théorème 1.6.3

On pose $x^0 = \bar{x}$ et $x^1 = x$.

Pour une fonction booléenne f à n arguments on pose :

$$A = \sum_{f(a_1,\ldots,a_n)=1} x_1^{a_1} \ldots x_n^{a_n}.$$

A est la somme des monômes $x_1^{a_1} \ldots x_n^{a_n}$ tels que $f(a_1, \ldots, a_n) = 1$.

Pour toute assignation v telle que $v(x_1) = a_1, \ldots, v(x_n) = a_n$,
on a $f(a_1, \ldots, a_n) = [A]_v$.

Exemple 1.6.4

La fonction *maj* à 3 arguments vaut 1 lorsqu'au moins 2 de ses arguments valent 1.

Définir la somme de monômes équivalente (théorème 1.6.3)

x_1	x_2	x_3	$maj(x_1, x_2, x_3)$	
0	0	0	0	
0	0	1	0	
0	1	0	0	
0	1	1	1	$\overline{x_1} x_2 x_3$
1	0	0	0	
1	0	1	1	$x_1 \overline{x_2} x_3$
1	1	0	1	$x_1 x_2 \overline{x_3}$
1	1	1	1	$x_1 x_2 x_3$

$$\boxed{maj(x_1, x_2, x_3) = \overline{x_1} x_2 x_3 + x_1 \overline{x_2} x_3 + x_1 x_2 \overline{x_3} + x_1 x_2 x_3}$$

Vérifions le théorème 1.6.3 sur l'exemple 1.6.4

x_1	x_2	x_3	$maj(x_1, x_2, x_3)$	$\overline{x_1}\,x_2\,x_3$	$x_1\,\overline{x_2}\,x_3$	$x_1\,x_2\,\overline{x_3}$	$x_1\,x_2\,x_3$	$\overline{x_1}\,x_2\,x_3 + x_1\,\overline{x_2}\,x_3 + x_1\,x_2\,\overline{x_3} + x_1\,x_2\,x_3$
0	0	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0
0	1	1	1	1	0	0	0	1
1	0	0	0	0	0	0	0	0
1	0	1	1	0	1	0	0	1
1	1	0	1	0	0	1	0	1
1	1	1	1	0	0	0	1	1

$$\boxed{maj(x_1, x_2, x_3) = \overline{x_1}\,x_2\,x_3 + x_1\,\overline{x_2}\,x_3 + x_1\,x_2\,\overline{x_3} + x_1\,x_2\,x_3}$$

Fonctions booléennes et produit de clauses

Théorème 1.6.5

Pour une fonction booléenne f à n arguments on pose :

$$A = \prod_{f(a_1,\ldots,a_n)=0} x_1^{\overline{a_1}} + \ldots + x_n^{\overline{a_n}}.$$

A est le produit des clauses $x_1^{\overline{a_1}} + \ldots + x_n^{\overline{a_n}}$ telles que $f(a_1, \ldots, a_n) = 0$.

Pour toute assignation v telle que $v(x_1) = a_1, \ldots, v(x_n) = a_n$,
on a $f(a_1, \ldots, a_n) = [A]_v$.

Exemple 1.6.6

La fonction *maj* à 3 arguments vaut 1 lorsqu'au moins 2 de ses arguments valent 1.

Définir le produit de clauses équivalent (théorème 1.6.5)

x_1	x_2	x_3	$maj(x_1, x_2, x_3)$	
0	0	0	0	$x_1 + x_2 + x_3$
0	0	1	0	$x_1 + x_2 + \overline{x_3}$
0	1	0	0	$x_1 + \overline{x_2} + x_3$
0	1	1	1	
1	0	0	0	$\overline{x_1} + x_2 + x_3$
1	0	1	1	
1	1	0	1	
1	1	1	1	

$$\boxed{maj(x_1, x_2, x_3) = (x_1 + x_2 + x_3)(x_1 + x_2 + \overline{x_3})(x_1 + \overline{x_2} + x_3)(\overline{x_1} + x_2 + x_3)}$$

Vérifions le théorème 1.6.5 sur l'exemple 1.6.6

x_1	x_2	x_3	$maj(x_1, x_2, x_3)$	$x_1 + x_2 + x_3$	$x_1 + x_2 + \overline{x_3}$	$x_1 + \overline{x_2} + x_3$	$\overline{x_1} + x_2 + x_3$	$(x_1 + x_2 + x_3)$ $(x_1 + x_2 + \overline{x_3})$ $(x_1 + \overline{x_2} + x_3)$ $(\overline{x_1} + x_2 + x_3)$
0	0	0	0	0	1	1	1	0
0	0	1	0	1	0	1	1	0
0	1	0	0	1	1	0	1	0
0	1	1	1	1	1	1	1	1
1	0	0	0	1	1	1	0	0
1	0	1	1	1	1	1	1	1
1	1	0	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1

$$\boxed{maj(x_1, x_2, x_3) = (x_1 + x_2 + x_3)(x_1 + x_2 + \overline{x_3})(x_1 + \overline{x_2} + x_3)(\overline{x_1} + x_2 + x_3)}$$

Plan du Semestre

- Logique propositionnelle *
- Résolution propositionnelle
- Déduction naturelle propositionnelle

PARTIEL

- Logique du premier ordre
- Base de la démonstration automatique (« résolution au premier ordre »)
- Déduction naturelle au premier ordre

EXAMEN

Méthodes de déduction

- Une formule est-elle valide ?
- Un raisonnement est-il correct ?

Deux méthodes :

Les tables de vérités et les transformations

Problèmes

- Si le nombre de variables augmente, ces méthodes sont très longues
- On ne fait que vérifier la cohérence de la conclusion avec les hypothèses mais on ne comprend pas le raisonnement

Exemple

Par une table de vérité, pour vérifier
$a \Rightarrow b, b \Rightarrow c, c \Rightarrow d, d \Rightarrow e, e \Rightarrow f, f \Rightarrow g, g \Rightarrow h, h \Rightarrow i, i \Rightarrow j \models a \Rightarrow j$
il faut tester $2^{10} = 1024$ lignes.

Or, par déduction, ce raisonnement est correct :

1. On sait que $a \Rightarrow b,\ b \Rightarrow c \models a \Rightarrow c$.
2. On peut réutiliser cet argument 8 fois.
3. Il ne nous reste qu'à montrer que $a \Rightarrow j \models a \Rightarrow j$.
4. Or par définition, la formule $a \Rightarrow j$ est une conséquence d'elle-même.

- Formalisation d'un système de déduction

David Hilbert (1862-1943)

- Fondateur de l'école **formaliste** : les mathématiques peuvent et doivent être formalisées pour être démontrées indiscutablement.
- Programme de Hilbert (1920) :
  « *Wir müssen wissen. Wir werden wissen.* »
  en réponse à « *Ignoramus et ignorabimus* »
  - choisir un ensemble fini d'axiomes suffisant pour exprimer toutes les mathématiques
  - démontrer la cohérence de cet ensemble
  - élaborer un algorithme qui décide si une proposition est démontrable (*Entscheidungsproblem*)

- Système *à la Hilbert* : des axiomes comme $\vdash p \Rightarrow (q \Rightarrow p)$
  et quelques règles de déduction comme $\dfrac{\vdash p \Rightarrow q \qquad \vdash p}{\vdash q}$
- Démonstrations complètes mais fastidieuses à écrire et à relire

Aujourd'hui : résolution propositionnelle

- 1 seule règle : la résolution

$$a+\overline{b}, b+c \models a+c$$

  pour des formules mises en FNC (conjonction de clauses)
- Notion formelle de preuve par résolution
- Quelques propriétés de la résolution

Définitions

Définition 2.1.1

Dans une clause, l'ordre des littéraux et les éventuels doublons ne jouent aucun rôle.
Ainsi on dira que :

- Un littéral est élément d'une clause.
- Une clause A est incluse dans une clause B (ou sous-clause) si tous les littéraux de A sont dans B.
- Deux clauses sont égales si elles ont les mêmes littéraux.

Exemple 2.1.2

- Les clauses $p+\overline{q}$, $\overline{q}+p$, et $p+\overline{q}+p$ sont égales
- p est un littéral de $\overline{q}+p+r+p$
- $p+\overline{q}+p$ est une sous-clause de $\overline{q}+p+r$
- $(\overline{q}+p+r+p) - p = \overline{q}+r$
- $(p+p+p) - p = \perp$
- Ajouter le littéral r à la clause p donne la clause $p+r$
- Ajouter le littéral p à la clause $\perp$ donne la clause p

Littéral complémentaire

Définition 2.1.4

Nous notons L^c le littéral complémentaire d'un littéral L :

Si L est une variable, L^c est sa négation.

Si L est la négation d'une variable, L^c est la même sans négation.

Exemple 2.1.5

$x^c = \overline{x}$ et $\overline{x}^c = x$.

Résolvant

Définition 2.1.6

Soient A et B deux clauses.

La clause C est un résolvant de A et B ssi il existe un littéral L tel que

$$A = A' + L, \qquad B = B' + L^c, \qquad C = A' + B'$$

"C est un résolvant de A et B" est représenté par :

$$\frac{A \qquad B}{C}$$

C est engendrée par A et B.
A et B sont les parents de la clause C.

Exemples de résolution

Exemple 2.1.7

Donnez les résolvants de :

- $p+q+r$ et $p+\bar{q}+r$

$$\frac{p+q+r \qquad p+\bar{q}+r}{p+r}$$

- $p+\bar{q}$ et $\bar{p}+q+r$

$$\frac{p+\bar{q} \qquad \bar{p}+q+r}{\bar{p}+p+r} \qquad \frac{p+\bar{q} \qquad \bar{p}+q+r}{\bar{q}+q+r}$$

- p et $\bar{p}$

$$\frac{p \qquad \bar{p}}{\perp}$$

Propriété

Propriété 2.1.8

Si l'un des parents d'un résolvant est valide, le résolvant est valide ou contient l'autre parent.

Preuve.

Cette preuve est demandée dans l'exercice 39. $\square$

Exemple

$$\frac{p+\bar{p}+q \qquad \bar{q}+r}{p+\bar{p}+r} \qquad\qquad \frac{p+\bar{p}+q \qquad \bar{p}+r}{\bar{p}+q+r}$$

Notion de preuve

Définition 2.1.11

Soient Γ un ensemble de clauses et C une clause.

Une preuve de C à partir de Γ est une liste de clauses où :

- toute clause est un élément de Γ
- ou est un résolvant de deux clauses la précédant
- la dernière clause est C.

La clause C est déduite de Γ, notée $\Gamma \vdash C$, s'il y a une preuve de C à partir de Γ.

La taille d'une preuve est le nombre de lignes qu'elle contient.

Exemple de preuve

Exemple 2.1.12

Soit Γ l'ensemble de clauses $\overline{p}+q, p+\overline{q}, \overline{p}+\overline{q}, p+q$.

Nous montrons que $\Gamma \vdash \perp$:

1	$p+q$	Hyp
2	$p+\bar{q}$	Hyp
3	p	Res 1, 2
4	$\bar{p}+q$	Hyp
5	q	Res 3, 4
6	$\bar{p}+\bar{q}$	Hyp
7	$\bar{p}$	Res 5, 6
8	$\perp$	Res 3, 7

Preuve en arbre

Exemple 2.1.12

Soit Γ l'ensemble de clauses $\bar{p}+q, p+\bar{q}, \bar{p}+\bar{q}, p+q$.

Nous montrons que $\Gamma \vdash \bot$:

$$\dfrac{\dfrac{\dfrac{\dfrac{p+q \qquad p+\bar{q}}{p} \qquad \bar{p}+q}{q} \qquad \bar{p}+\bar{q}}{\bar{p}} \qquad \dfrac{p+q \qquad p+\bar{q}}{p}}{\bot}$$

Monotonie et Composition

Propriété 2.1.14

1. Monotonie : Si $\Gamma \vdash A$ et si $\Gamma \subseteq \Delta$ alors $\Delta \vdash A$
2. Composition : Si $\Gamma \vdash A$ et $\Gamma \vdash B$ et si C est un résolvant de A et B alors $\Gamma \vdash C$.

Preuve.

Exercice 38 $\square$

Aujourd'hui

- Utilisation de formes normales conjonctives (FNCs) pour modéliser un problème
- Notations de l'algèbre de Boole
- Toute fonction booléenne peut être représentée par une formule (en forme normale)

- Un système de déduction est composé d'un ensemble de **règles formelles de déduction** (par exemple : la résolution)
- Une preuve est une suite d'applications de ces règles à partir d'**hypothèses**

La prochaine fois

- Cohérence et Complétude du système
- Davis et Putnam
- (Stratégie complète)

À préparer

Hypothèses :

- (H1) : Si Pierre est grand, alors Jean n'est pas le fils de Pierre
- (H2) : Si Pierre n'est pas grand, alors Jean est le fils de Pierre
- (H3) : Si Jean est le fils de Pierre alors Marie est la soeur de Jean

Conclusion (C) : Marie est la soeur de Jean ou Pierre est grand.

Transformer en clauses les hypothèses et $\neg C$.

Que peut-on (doit-on) **démontrer** par résolution ?