Calculabilité, logique et complexité

Chapitre 5

Logique

Acquis d'apprentissage (1)

A l'issue de ce chapitre, les étudiants seront capables de

- Distinguer et décrire les composants d'une logique
- Comprendre les différentes formes d'une formule propositionnelle ; distinguer les formules propositionnelles syntaxiquement correctes
- Comprendre, expliquer et illustrer ce qu'est une interprétation et un modèle d'une formule propositionnelle
- Expliquer comment obtenir la valeur de vérité d'une formule propositionnelle pour une interprétation donnée ; appliquer sur de nouvelles situations
- Expliquer comment déterminer si une interprétation est un modèle d'une formule propositionnelle pour une interprétation donnée ; appliquer sur de nouvelles situations
- Comprendre et expliquer le concept d'équivalence de formules propositionnelles ; démontrer si deux formules propositionnelles données sont équivalentes
- Expliquer et illustrer l'ensemble SAT des formules propositionnelles satisfaisables
- Comprendre et expliquer pourquoi l'ensemble SAT est récursif

Acquis d’apprentissage (2)

A l’issue de ce chapitre, les étudiants seront capables de

- Comprendre et expliquer le concept de tautologie de formules propositionnelles ; démontrer si une formule propositionnelles donnée est une tautologie
- Comprendre et expliquer le concept de conséquences logiques
- Expliquer et démontrer le lien entre satisfiabilité et conséquence logique
- Modéliser au moyen de la logique propositionnelle un problème non élémentaire
- Expliquer et spécifier ce qu’est un solveur SAT ; décrire, expliquer et appliquer un algorithme élémentaire de solveur SAT
- Comprendre, expliquer et illustrer ce qu’est une formule propositionnelle sous forme normale conjonctive (CNF) ; transformer une formule propositionnelle donnée en une formule CNF équivalente
- Comprendre, expliquer et illustrer ce qu’est une règle d’inférence
- Comprendre, expliquer et illustrer la règle de résolution ; justifier l’exactitude de cette règle
- Comprendre, expliquer et illustrer le principe de résolution ; décrire le principe de fonctionnement et expliquer la signification du résultat ; appliquer le principe de résolution sur un exemple donné

Chapitre 5 : Logique

1. Logique des propositions
2. Sémantique
3. Satisfiabilité (SAT) et conséquence logique
4. Modélisation
5. Raisonnement
    - Model checking
    - Résolution

Chapitre 5 : Logique

1. **Logique des propositions**
2. Sémantique
3. Satisfiabilité (SAT) et conséquence logique
4. Modélisation
5. Raisonnement
    - Model checking
    - Résolution

Logique

- Représentation de connaissances
- Raisonnement automatisé sur la représentation des connaissances
- Il existe de multiples formes de logique
  - Logique des propositions
  - Logique des prédicats
  - Logique modale
  - Logique temporelle
  - Logique floue
  - …

Composants d'une logique

- **Syntaxe** : détermine la forme des formules acceptées dans la logique
- **Sémantique** : définit le sens des formules de la logique
- **Raisonnement** : propose des méthodes permettant de manipuler les formules afin d'obtenir des informations pertinentes

Logique des propositions

- Logique « la plus simple » et la plus ancienne
- Basée sur le concept de **proposition**, c'est-à-dire une affirmation qui peut être vraie ou fausse
  - Le soleil brille
  - Le cours de calculabulité se donne le jeudi après-midi
  - Le sommet V_2 du graphe a la couleur rouge
  - La tâche T_3 doit être effectuée avant la tâche T_7

Logique des propositions

- Chaque proposition est représentée par un symbole, appelé variable propositionnelle (A, B, …)
- Une formule permet de relier plusieurs propositions avec des connecteurs logiques tels que la négation, le ET ou le OU

Syntaxe : symboles

- Constantes : True et False
- Variables propositionelles, représentées par des chaines de caractères
- Connecteurs logiques : $\neg$ (négation), $\wedge$ (conjonction), $\vee$ (disjunction), $\Rightarrow$ (implication) et $\Leftrightarrow$ (équivalence)
- Parenthèses

Syntaxe : formules propositionnelles

- Une constante logique ainsi qu'une variable propositionnelle sont des formules propositionelles
- Si p et q sont des formules propositionnelles alors$(\neg p)$, $(p \wedge q)$, $(p \vee q)$, $(p \Rightarrow q)$ et $(p \Leftrightarrow q)$ sont des formules propositionelles

Syntaxe : Conventions

- Les parenthèses externes sont supprimées
- Précédences des operators permet de supprimer des parentheses. L'ordre des précedences est $\neg$, $\wedge$, $\vee$, $\Rightarrow$ et $\Leftrightarrow$, où $\neg$ a la précedence la plus haute et $\Leftrightarrow$ la plus basse
- Les règles de l'associativité définissent l'ordre de deux connecteurs identiques successifs.
  Par convention, $\wedge$ et $\vee$ sont associatifs à gauche tandis que $\Rightarrow$ et $\Leftrightarrow$ sont associatifs à droite

Exemples

$A \wedge B$	$(A \wedge B)$
$\neg A \wedge B$	$((\neg A) \wedge B)$
$A \wedge \neg B$	$(A \wedge (\neg B))$
$A \wedge B \vee C$	$((A \wedge B) \vee C)$
$A \Rightarrow B \vee C$	$(A \Rightarrow (B \vee C))$
$(A \Rightarrow B) \vee C$	$((A \Rightarrow B) \vee C)$
$A \vee B \vee C$	$((A \vee B) \vee C)$
$A \Rightarrow B \Rightarrow C$	$(A \Rightarrow (B \Rightarrow C))$

Chapitre 5 : Logique

1. Logique des propositions
2. **Sémantique**
3. Satisfiabilité (SAT) et conséquence logique
4. Modélisation
5. Raisonnement
   - Model checking
   - Résolution

Sémantique

- La sémantique d'une formule vise à déterminer le sens de cette formule
- Le sens d'une formule dépend d'un contexte où certaines propositions sont considérées comme vraies et d'autres comme fausses

Interprétation

- Une interprétation définit un contexte possible pour une formule propositionnelle
- Une **interprétation** d'une formule est une assignation d'une valeur de vérité (*true* ou *false*) à chacune des variables propositionnelles de la formule
- Si une formule a *n* variables différentes, il y a donc 2^n intreprétations possibles

Valeur de vérité d'une formule pour une interprétation (1)

Etant donné une interprétation *I*, la valeur de vérité d'une formule est dérivée selon les règles suivantes

- La valeur de vérité des constantes True et False sont respectivement *true* et *false*
- La valeur de vérité d'une variable propositionelle A est la valeur de cette variable dans l'interprétation *I*

Valeur de vérité d'une formule pour une interprétation (2)

- La valeur de verité d'une formule propositionelle de la forme $(\neg p)$, $(p \wedge q)$, $(p \vee q)$, $(p \Rightarrow q)$ or $(p \Leftrightarrow q)$ dépend de la valeur de vérité des formules p et q dans I, selon la table suivante

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$
true	*true*	*false*	*true*	*true*	*true*	*true*
true	*false*	*false*	*false*	*true*	*false*	*false*
false	*true*	*true*	*false*	*true*	*true*	*false*
false	*false*	*true*	*false*	*false*	*true*	*true*

Exemple

- Soit l'interprétation avec l'assignation
  (A=*true*, B=*false*, C=*false*)
- Valeur de vérité de la formule
  $(A \vee B) \wedge (B \Rightarrow \neg C)$
  dans cette interpretation ?
- $(\mathit{true} \vee \mathit{false}) \wedge (\mathit{false} \Rightarrow \neg \mathit{false})$ qui se réduit à
  $\mathit{true} \wedge (\mathit{false} \Rightarrow \mathit{true})$ qui se réduit à
  $\mathit{true} \wedge \mathit{true}$ qui se réduit à
  true

Modèles

- Une interprétation dans laquelle une formule est vraie est un **modèle** de cette formule
- Le sens d'une formule propositionnelle, c'est-à-dire sa sématique, est défini par les différents modèles de cette formule

Formules équivalentes

- Deux formules (avec les mêmes variables propositionelles) sont **équivalentes** si elles ont les mêmes modèles
- Une (sous-)formule peut toujours être remplacée par une (sous-)formule équivalente sans changer sa sémantique

Exemples de formules équivalentes

$\neg(\neg p)$	est équivalent à	p	(double négation)
$p \wedge q$	est équivalent à	$q \wedge p$	(commutativité de $\wedge$)
$p \vee q$	est équivalent à	$q \vee p$	(commutativité de $\vee$)
$p \Leftrightarrow q$	est équivalent à	$(p \Rightarrow q) \wedge (p \Rightarrow q)$	($\Leftrightarrow$ élimination)
$p \Rightarrow q$	est équivalent à	$\neg p \vee q$	($\Rightarrow$ élimination)
$p \Rightarrow q$	est équivalent à	$\neg q \Rightarrow \neg p$	(contraposition)
$\neg(p \vee q)$	est équivalent à	$\neg p \wedge \neg q$	(de Morgan)
$\neg(p \wedge q)$	est équivalent à	$\neg p \vee \neg q$	(de Morgan)
$p \vee (q \wedge r)$	est équivalent à	$(p \vee q) \wedge (p \vee r)$	(distributivité)
$p \wedge (q \vee r)$	est équivalent à	$(p \wedge q) \vee (p \wedge r)$	(distributivité)

Chapitre 5 : Logique

1. Logique des propositions
2. Sémantique
3. **Satisfiabilité (SAT) et conséquence logique**
4. Modélisation
5. Raisonnement
    - Model checking
    - Résolution

Que peut-on déduire d'une formule logique ?

Problème de satisfiabilité

- La formule F a-t-elle un modèle ?
- Ce modèle est une « solution » de la formule F

Conséquence logique

- Etant donné une formule F, quelles sont les formules qui sont des conséquences de F ?
- Quelles sont les formules qui sont vraies lorsque F est vraie

Satisfiabilité

- Une formule propositionelle est **satisfaisable** si elle possède au moins un modèle
- Si la formule ne possède aucun modèle elle est **non statisfaisable**
  La formule est aussi appelé une *contradiction*
- SAT : ensemble des formules propositionelles satisfaisables

Satisfiabilité

- Etant donné une interprétation et une formule propositionnelle, sa valeur de vérité peut être déterminée par un algorithme
- Pour une formule avec *n* variables propositionnelles, il existe 2^n interprétations possibles
- L'ensemble SAT est donc récursif

Exemple

$(A \vee B) \wedge (A \vee \neg B) \wedge (\neg A \vee B) \wedge (\neg A \vee \neg B \vee \neg C) \wedge (\neg A \vee C)$

- non satisfaisable
- Pour chacune de ses 8 interprétations possibles, cette formule s'évalue à *false*

Tautologies

- Une formule est une **tautologie** lorsqu'elle est vraie dans toutes les interprétations
- $A \vee \neg A$ est une tautologie

Propriété

- p est une tautologie ssi $\neg p$ est non satisfaisable

Conséquence logique

- Une formule q est une **conséquence logique** d'une formule p si la formule $p \Rightarrow q$ est une tautologie
- Autres definitions équivalentes
  - Tous les modèles de p sont aussi des modèles de q
  - La formule q est vraie dans tous les modèles de p

Notation

- $p \vDash q$

Conséquence logique

Propriété

- $p \models q$ ssi $(p \wedge \neg q)$ est non satisfaisable

Preuve

- $p \models q$ ssi $p \Rightarrow q$ est une tautologie
- ssi $p \Rightarrow q$ est vrai dans toutes les interprétations
- ssi $\neg (p \Rightarrow q)$ est faux dans toutes les interprétations
- ssi $\neg (p \Rightarrow q)$ est non satisfaisable
- ssi $\neg (\neg p \vee q)$ est non satisfaisable
- ssi $(\neg \neg p \wedge \neg q)$ est non satisfaisable
- ssi $(p \wedge \neg q)$ est non satisfaisable

Conséquence logique

Attention

- Si q n'est pas une conséquence logique de p, on n'a pas nécessairement que $\neg q$ est une conséquence logique de p
- Il est donc possible d'avoir $p \not\models q$ et $p \not\models \neg q$, c'est-à-dire aucune des formules $(p \Rightarrow q)$ et $(p \Rightarrow \neg q)$ n'est une tautologie

Exemple

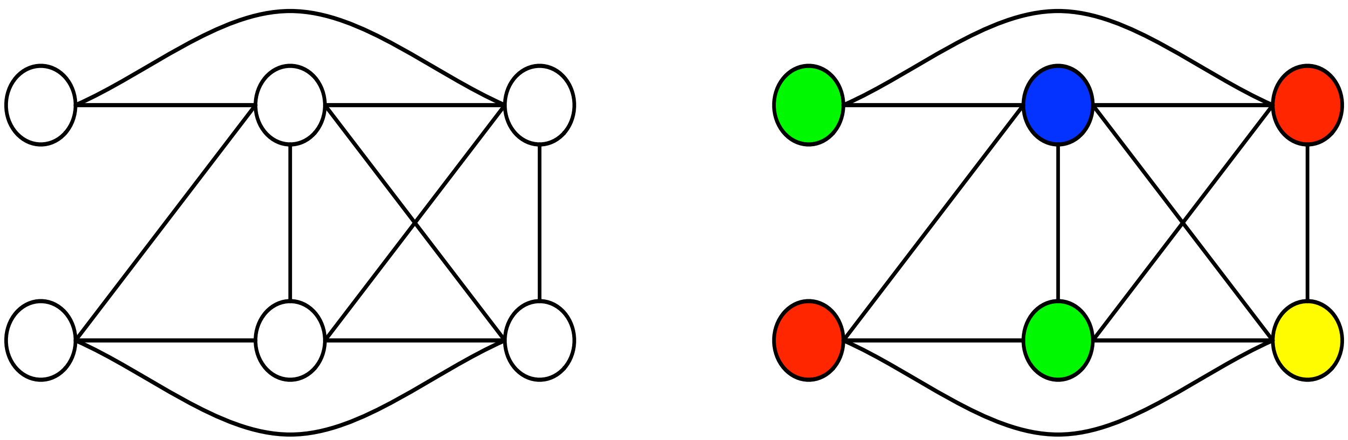
- $(A \vee B) \not\models A$ et $(A \vee B) \not\models \neg A$

Chapitre 5 : Logique

1. Logique des propositions
2. Sémantique
3. Satisfiabilité (SAT) et conséquence logique
4. **Modélisation**
5. Raisonnement
    - Model checking
    - Résolution

Modélisation : coloration de graphe

- Comment colorier les noeuds d’un graphe de telle sorte que deux noeuds adjacents ont toujours des couleurs différentes ?



Modélisation : coloration de graphe

- Etant donné
  - un graphe G=(V,E), où V est l'ensemble des noeuds et E l'ensemble des arcs
  - Un ensemble C de couleurs
- Définir les variables propositionnelles suivantes
  - couleur[v,c], avec $v \in V$ et $c \in C$
  - La variable couleur[v,c] est vraie si le noeud v est de couleur c. Elle est fausse sinon
  - Il y a donc #V x #C variables propositionnelles distinctes

Modélisation : coloration de graphe

Le modèle est compose d'une conjonction de formules

- Pour chaque arc $(v,w) \in E$, la formule
  ¬(couleur[v,c] ∧ couleur[w,c])
  empêche les noeuds adjacents d'avoir la même couleur
- Pour chaque noeud $v \in V$, la disjonction
  couleur[v,c]   sur toutes les couleurs $c \in C$
  assure que chaque noeud a au moins une couleur
- Pour chaque noeud $v \in V$, la conjonction
  ¬(couleur[v,c1] ∧ couleur[v,c2]) pour chaque paire de couleurs (c1,c2)
  assure que chaque noeud n'a jamais plus d'une seule couleur

Modélisation : coloration de graphe

- Un modèle pour la formule de coloration d'un graphe représente une solution pour ce problème (valeur des variables propositionnelles)
- Si la formule est non satisfaisable, le problème n'a pas de solution
- Résoudre le problème de coloration du graphe revient donc à déterminer si la formule est satisfaisable (et retourner le modèle le cas échéant)

Chapitre 5 : Logique

Raisonnement

Deux problèmes

- $p \models q$? Une formule q est-elle une **conséquence logique** d'une formule p ?
- $p \in \text{SAT}$? Une formule p est-elle satisfaisable ?

Le premier problème peut se réduire au second

- $p \models q$ ssi $(p \land \neg q) \notin \text{SAT}$

Raisonnement

Techniques de raisonnement

- Solveur SAT
  - Algorithmes de décision pour SAT
- Inférence
  - Méthodes formelles utilisant des règles d’inférence

Solveur SAT

Solveur SAT élémentaire basé sur le *model checking*

Donnée

- une formule *p* avec *n* variables propositionnelles

Algorithme

- Pour chaque interprétation *I* parmi les 2^n interprétations possibles de *p*
  - Si *p* est vraie dans cette interprétation *I*
  - Alors return <*true*,*I*> ($p \in$ SAT)
- Return <*false*, ∅> ($p \notin$ SAT)

Solveur SAT

La plupart des solveurs SAT travaillent sur une forme simplifiée des formules propositionelles : les formules sous forme normale conjonctive (CNF)

- Négation uniquement devant une variable propositionelle
- Que des disjonctions et des conjonctions
- La formule est une suite de conjonctions dont chaque élément est une disjonction de variables ou de négation de variables

$(\neg A \vee \neg C) \wedge (\neg A \vee D) \wedge (\neg B \vee \neg C) \wedge (\neg B \vee D) \wedge (A \vee B \vee C \vee \neg D)$

Forme Normale Conjonctive (CNF)

- Un *literal* est une variable propositionnelle (A) ou sa négation ($\neg$A).
- Une *clause* is a disjonction de literaux
- Une formule sous forme normal conjonctive (CNF) est une conjonction de clauses
  $c_1 \wedge \ldots \wedge c_n$
- Une formule sous forme CNF est habituellement représentée par l'ensemble
  $\{c_1 , \ldots , c_n\}$

Transformation en CNF

- Toute formule peut se représenter sous la forme d'une formule CNF équivalente
- Application des étapes suivantes
  - Eliminer les $\Leftrightarrow$ et $\Rightarrow$ en utilisant les équivalences présentées précédemment
  - Mettre les symboles de négation dans des literaux en utilisant la double negation et les équivalences de de Morgan
  - Utiliser la distributivité de $\vee$ sur $\wedge$

Exemple

- $(A \vee B) \Leftrightarrow (\neg C \wedge D)$
- $(\neg(A \vee B) \vee (\neg C \wedge D)) \wedge (\neg(\neg C \wedge D) \vee (A \vee B))$
- $((\neg A \wedge \neg B) \vee (\neg C \wedge D)) \wedge (C \vee \neg D \vee A \vee B)$
- $(\neg A \vee \neg C) \wedge (\neg A \vee D) \wedge (\neg B \vee \neg C) \wedge (\neg B \vee D) \wedge (A \vee B \vee C \vee \neg D)$

Sous la forme d'un ensemble de clauses

- $\{\neg A \vee \neg C, \neg A \vee D, \neg B \vee \neg C, \neg B \vee D, A \vee B \vee C \vee \neg D\}$

Chapitre 5 : Logique

1. Logique des propositions
2. Sémantique
3. Satisfiabilité (SAT) et conséquence logique
4. Modélisation
5. **Raisonnement**
   - Model checking
   - **Résolution**

Preuve par inference

- Transformations successives de formules propositionelles
- Application à chaque étape d'une règle d'inférence
- Chaque règle d'inférence garantit l'équivalence de la formule résultante à la formule initiale

Exemples de règle d'inférence

Equivalence

$$\frac{p \Leftrightarrow q \qquad q \Leftrightarrow r}{p \Leftrightarrow r}$$

Modus ponens

$$\frac{p \Rightarrow q \qquad p}{q}$$

$$\frac{\textit{prémices}}{\textit{conclusion}}$$

Soit un ensemble F = $\{p_1, \ldots, p_n\}$ de formules propositionnelles représentant la formule $p_1 \wedge \ldots \wedge p_n$

Si les prémices appartiennent à F,

alors on transforme F en F' en lui ajoutant la conclusion

- F et F' sont équivalents

Résolution

- Règle d'inférence unique généralisant le modus ponens
- Son utilisation permet de décider si un ensemble F de clauses est safisfaisable ou non
- Forme la plus simple de la résolution :
- Une table de vérité montre que tout modèle des prémices est aussi un modèle de la conclusion

$$\frac{\begin{array}{c} p \vee q \\ \neg p \vee r \end{array}}{q \vee r}$$

Règle de résolution

- Deux clauses prémices C_1 et C_2, la première contenant un litéral L_1=V et la seconde un litéral L_2= $\neg$V
- Une clause conclusion contenant tous les literaux de C_1 et de C_2, sauf les litéraux L_1 et L_2

Exemples

$$\frac{A \vee B \qquad \neg A}{B}$$

$$\frac{A \vee B \vee \neg C \qquad \neg D \vee \neg B \vee F}{A \vee \neg C \vee \neg D \vee F}$$

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

$$\frac{A \qquad \neg A}{\textit{false}}$$

Résolution

- Partir d'une formule CNF sous la forme d'un ensemble de clauses
- A chaque étape
  - Appliquer la règle de résolution sur deux clauses pour lesquelles la règle est applicable et dont la conclusion n'est pas une clause existante
  - Ajouter la clause conclusion à la formule CNF
- Si la clause *false* est ajoutée à une étape, alors la formule n'est pas satisfaisable
- Si la règle de résolution ne peut plus s'appliquer, alors la formule est satisfaisable

Exactitude de la résolution

- Chaque étape conduit à une formule CNF équivalente à la formule précédante
- Comme le nombre de clauses distinctes sur les variables de la formule est fini, la résolution se termine toujours
- Si une des clauses est la clause *false*, alors la formule n'est pas satisfaisable [évident]
- Si fin sans clause *false*, alors la formule est satisfaisable [non prouvé ici]

Résolution : résultat

- La résolution nous indique si une formule CNF appartient ou n'appartient pas à SAT
- Si elle appartient à SAT, la résolution ne donne pas de modèle comme résultat
- Résolution utilisée comme technique pour prouver $p \vDash q$
  - Transformer $(p \wedge \neg q)$ en CNF
  - Si résolution déduit *false* ,
    Alors $(p \wedge \neg q) \notin$ SAT , donc $p \vDash q$
  - Si résolution se termine sans déduire *false* ,
    Alors $(p \wedge \neg q) \in$ SAT , donc $p \nvDash q$

Résolution : exemple

- Soit la formule p sous forme CNF (ensemble de clauses)
  $\{A, \neg B, \neg A \vee \neg C \vee D, \neg E \vee C, B \vee C\}$
- Question $p \vDash D$?
- Appliquer la résolution à $p \cup \{\neg D\}$

$$\frac{\neg A \vee \neg C \vee D \quad \neg D}{\neg A \vee \neg C} \qquad \frac{\neg A \vee \neg C \quad A}{\neg C} \qquad \frac{\neg C \quad B \vee C}{B} \qquad \frac{\neg B \quad B}{\textit{false}}$$

- Donc $p \vDash D$