Résolution sémantique

Correction.

On se référera parfois au poly ; il s'agira toujours des versions au moins égales à 4 du cours.

La résolution *sémantique* est un raffinement de la résolution paramétrée par la donnée d'une interprétation de Herbrand $\mathcal{H}_0$.

On suppose qu'on a un algorithme $\mathcal{A}^+$ qui semi-décide la validité d'une clause donnée en entrée dans $\mathcal{H}_0$. Autrement dit : pour toute clause C, $\mathcal{A}^+(C)$ termine, retourne un booléen, et si ce booléen est "vrai", alors $\mathcal{H}_0 \models C$. En revanche, si $\mathcal{A}^+(C)$ retourne "faux", alors on ne sait pas si $\mathcal{H}_0 \models C$ ou $\mathcal{H}_0 \not\models C$. Par contraposition, si $\mathcal{H}_0 \not\models C$, alors $\mathcal{A}^+(C)$ doit retourner "faux".

De façon symétrique, on suppose qu'on a un algorithme $\mathcal{A}^-$ tel que si $\mathcal{A}^-(C)$ retourne "vrai", c'est que $\mathcal{H}_0$ rend fausse toute instance close de C. En d'autres termes, s'il existe une instance close $C\theta$ telle que $\mathcal{H}_0 \models C\theta$, alors $\mathcal{A}^-(C)$ doit retourner "faux".

La règle de *résolution sémantique* est :

$$\frac{C_1 \vee \pm A_1 \vee \ldots \vee \pm A_n \quad C' \vee \mp A'_1}{C_1\sigma \vee C'\sigma}$$

où $\pm$ désigne un signe, $+$ ou $-$, et $\mp$ désigne le signe opposé, et où les conditions suivantes sont vérifiées :

(i) $n \geq 1$;

(ii) $\sigma = \text{mgu}\,\{A_j \doteq A'_1 | 1 \leq j \leq n\}$;

(iii) $\mathcal{A}^+(C_1 \vee \pm A_1 \vee \ldots \vee \pm A_n)$ retourne "faux", et $A_1, \ldots, A_n$ sont maximaux dans $C_1 \vee \pm A_1 \vee \ldots \vee \pm A_n$;

(iv) $\mathcal{A}^-(C' \vee \mp A'_1)$ retourne "faux".

La maximalité est, comme d'habitude, comprise par rapport à un ordre strict $\succ$ stable.

1. Nous allons suivre l'argument de la démonstration du théorème 8 du poly, et montrer que la résolution sémantique est complète. Construisons l'interprétation I comme suit (je reprends les notations de la-dite démonstration).

   Appelons clause *génératrice* C_N, et par extension $C_N\theta_N$, toute clause telle que $\mathcal{H}_0 \not\models C_N\theta_N$. On peut écrire $C_N\theta_N$ de façon unique sous la forme $\pm_N H_N \vee \mathcal{V}_N \vee \mathcal{F}_N$, où $\mathcal{V}_N$ est la disjonction des littéraux (autres que $\pm_N H_N$) de $C_N\theta_N$ vrais dans $\mathcal{H}_0$, et $\mathcal{F}_N$ est celle de ceux (autres que $\pm_N H_N$) qui sont faux dans $\mathcal{H}_0$. Observer que C_N est génératrice si et seulement si $\mathcal{H}_0 \not\models \pm_N H_N$ et $\mathcal{V}_N$ est la disjonction vide, i.e., $C_N\theta_N = \pm_N H_N \vee \mathcal{F}_N$ avec $\mathcal{H}_0 \not\models \pm_N H_N$.

On construit alors une interprétation *partielle* I_k, c'est-à-dire un ensemble de littéraux clos ne contenant pas à la fois $+A$ et $-A$ pour aucun atome clos A, par récurrence sur k : I_0 est la fonction de domaine vide, et si I_k est déjà construite, on considère toutes les clauses génératrices C_N telles que $\pm_N H_N = \pm A^0_{k+1}$, où le signe $\pm$ est $-$ si $\mathcal{H}_0 \models A^0_{k+1}$, $+$ sinon ; s'il existe une telle clause génératrice telle que $I_k \not\models \mathcal{F}_N$, posons $I_{k+1} = I_k \cup \{\pm A^0_{k+1}\}$; sinon, $I_{k+1} = I_k \cup \{\mp A^0_{k+1}\}$, où $\mp$ est le signe opposé de $\pm$. Finalement, $I = I_n$.

Démontrer :

(I.1) Pour toute clause génératrice C_N telle que $I \not\models \mathcal{F}_N$, alors $I \models \pm_N H_N$.

(I.2) Si $I \models \pm H$ et $\mathcal{H}_0 \not\models \pm H$, alors il existe une clause génératrice C_N telle que $\pm_N = \pm$ et $H_N = H$. De plus, $I \not\models \mathcal{F}_N$.

(I.1) *Supposons $I \not\models \mathcal{F}_N$. Ecrivons $C_N\theta_N = \pm_N H_N \vee \mathcal{F}_N$, et posons k l'unique entier tel que $H_N = A^0_{k+1}$. Comme $\mathcal{F}_N$ ne contient que des atomes d'indices $\leq k$, et que I restreint aux atomes d'indices $\leq k$ est juste I_k, on a $I_k \not\models \mathcal{F}_N$. Par construction, I_{k+1} est nécessairement égal à $I_k \cup \{\pm_N H_N\}$, donc $I \models \pm_N H_N$, puisque I_{k+1} est égal à I restreint aux atomes d'indices $\leq k+1$ (donc coincide avec I sur $H_N = A^0_{k+1}$).*

(I.2) *Supposons $I \models \pm H$ et $\mathcal{H}_0 \not\models \pm H$. Ecrivons $H = A^0_{k+1}$, alors $I_{k+1} \models \pm A^0_{k+1}$. Par construction de I_{k+1}, il existe une clause génératrice C_N avec $C_N\theta_N = \pm_N H_N \vee \mathcal{F}_N$, $H_N = A^0_{k+1} = H$, et de plus $\pm_N$ est $-$ si $\mathcal{H}_0 \models A^0_{k+1}$, $+$ sinon. On a alors deux cas :*

- *Cas 1, $I_k \not\models \mathcal{F}_N$. On en déduit immédiatement $I \not\models \mathcal{F}_N$, c'est-à-dire la deuxième partie de* **(I.2)**. *De plus, par construction $I_{k+1} \models \pm_N H_N$, donc $I \models \pm_N H_N$, c'est-à-dire $I \models \pm_N H$; les signes $\pm_N$ et $\pm$ coincident donc, puisque $I \models \pm H$, ce qui finit de prouver la première partie de* **(I.1)**.
- *Cas 2, $I_k \models \mathcal{F}_N$. Alors $I_{k+1} \not\models \pm_N H_N$ par construction de I_{k+1}, donc $I \not\models \pm_N H_N$, donc $\pm_N$ est le signe opposé à $\pm$. En particulier $\mp H = \pm_N H_N$. Or $\mathcal{H}_0 \not\models \pm H$ par hypothèse, donc $\mathcal{H}_0 \models \mp H$, c'est-à-dire $\mathcal{H}_0 \models \pm_N H_N$. Mais ceci contredit le fait que C_N est génératrice, donc le cas 2 n'arrive jamais.*

2. *Prémisse principale.* Soit N_I le nœud d'échec correspondant à I. Montrer que l'on peut écrire C_{N_I} sous la forme $C' \vee \mp A'_1$, de sorte que *(iv)* soit vrai.

   Comme $C_{N_I}\theta_{N_I}$ est fausse en N_I, par (I.1) C_{N_I} n'est pas génératrice, donc par définition $\mathcal{H}_0 \models C_{N_I}\theta_{N_I}$, donc $\mathcal{A}^-(C_{N_I})$ retourne faux. De plus, comme $C_{N_I}\theta_{N_I} = \pm_{N_I} H_{N_I} \vee \mathcal{V}_{N_I} \vee \mathcal{F}_{N_I}$, où $\mathcal{V}_{N_I}$ contient au moins un littéral vrai dans $\mathcal{H}_0$. Soit $\mp A'_1$ un littéral de C_{N_I} tel que $\mp A'_1\theta_{N_I}$ soit vrai dans $\mathcal{H}_0$. On peut donc écrire C_{N_I} sous une forme telle que (iv) soit vrai.

3. *Prémisse auxiliaire.* Montrer qu'il existe alors nécessairement une clause génératrice C_N telle que $\pm_N = \pm$ et $H_N = A'_1\theta_{N_I}$. En déduire que C_N s'écrit sous la forme $C_1 \vee \pm A_1 \vee \ldots \vee \pm A_n$, de sorte que les conditions *(i)*, *(ii)*, et *(iii)* soient vérifiées ;

Comme $C_{N_I}\theta_{N_I}$ est fausse en N_I, $\mp A'_1\theta_{N_I}$ est faux dans I. Donc le littéral opposé $\pm A'_1\theta_{N_I}$ est à la fois vrai dans I et faux dans $\mathcal{H}_0$. Par (I.2), il existe une clause génératrice C_N telle que $\pm_N = \pm$ et $H_N = A'_1\theta_{N_I}$. Comme C_N est génératrice, $\mathcal{H}_0 \not\models C_N\theta_N$, donc $\mathcal{H}_0 \not\models C_N$, donc $\mathcal{A}^+(C_N)$ retourne "faux". Écrivons C_N sous la forme $C_1 \vee \pm A_1 \vee \ldots \vee \pm A_n$, où les $\pm A_i$ sont les littéraux de C_N dont les instances par θ_N sont égales à $\pm H_N = \pm A'_1\theta_{N_I}$. Clairement ils sont maximaux, ce qui démontre (iii).

Ensuite, en supposant sans perte de généralité que $C_1 \vee \pm A_1 \vee \ldots \vee \pm A_n$ et C_{N_I} n'ont aucune variable libre en commun, $\theta_{N_I} \cup \theta_N$ unifie A'_1 avec $A_1, \ldots, A_n$. Il existe donc un unificateur σ vérifiant (ii). La propriété (i) est claire.

4. Montrer que si $(T, C_\bullet, \theta_\bullet)$ est un arbre décoré pour un ensemble insatisfiable de clauses S, si $C_1\sigma \vee C'\sigma$ est une clause obtenue par résolution sémantique selon les lignes des questions précédentes, et si $(T', C'_\bullet, \theta'_\bullet)$ est un arbre décoré pour $S \cup \{C_1\sigma \vee C'\sigma\}$, alors $\mu(T, C_\bullet, \theta_\bullet)\ (>, (>_{mul})_{mul})_{lex}\ \mu(T', C'_\bullet, \theta'_\bullet)$. Autrement dit, l'arbre décoré décroît dans la mesure μ donnée dans le cours.

   On rappelle que $\mu(T, C_\bullet, \theta_\bullet) = (|T|, \mu^-(T, C_\bullet, \theta_\bullet))$, où la taille $|T|$ est le nombre de nœuds dans l'arbre T, $\mu^-(T, C_\bullet, \theta_\bullet)$ est le multi-ensemble des $\mu_1(C_N, \theta_N)$, N parcourant les nœuds d'échec de T, et $\mu_1(C_N, \theta_N)$ est le multi-ensemble contenant autant de fois l'entier i qu'il y a de littéraux $\pm A'$ de C_N tels que $A'\theta_N = A_i^0$.

   Exactement comme dans le cours, démonstration du théorème 8, fin.

5. En déduire que la résolution sémantique est complète.

   Partant d'un ensemble insatisfiable S de clauses, le processus des questions précédentes termine. Lorsque ceci termine, c'est qu'on a obtenu un arbre décoré dont la racine est un nœud d'échec, c'est-à-dire un ensemble de clauses contenant $\Box$. Il existe donc une dérivation finie de la clause vide depuis S par résolution sémantique.

6. Montrer que la résolution sémantique et la résolution ordonnée avec sélection ont un cas particulier en commun : pour la résolution sémantique, prendre $\mathcal{H}_0$ l'interprétation de Herbrand vide (qui rend tous les atomes faux ; définir les algorithmes $\mathcal{A}^+$ et $\mathcal{A}^-$ explicitement ici) ; pour la résolution ordonnée avec sélection, définir explicitement la fonction de sélection correspondante.

   Si $\mathcal{H}_0$ est l'interprétation de Herbrand vide, $\mathcal{H}_0 \models C$ si et seulement si $\mathcal{H}_0$ est une clause non positive, c'est-à-dire si et seulement si $\mathcal{H}_0$ contient au moins un littéral négatif. De façon équivalente, $\mathcal{H}_0 \not\models C$ si et seulement si C est une clause positive. On définit donc $\mathcal{A}^+(C)$ comme retournant "faux" si C est une clause positive, "vrai" sinon. Définissons d'autre part $\mathcal{A}^-(C)$ comme retournant toujours "faux".

   On obtient ainsi la règle

$$\frac{C_1 \vee +A_1 \vee \ldots \vee +A_n \quad C' \vee -A'_1}{C_1\sigma \vee C'\sigma}$$

   où les conditions suivantes sont vérifiées :

(i) $n \geq 1$ *;*

(ii) $\sigma = \text{mgu}\,\{A_j \doteq A'_1 | 1 \leq j \leq n\}$ *;*

(iii) $C_1 \vee +A_1 \vee \ldots \vee +A_n$ *est une clause positive et* $A_1, \ldots, A_n$ *sont maximaux dans* $C_1 \vee +A_1 \vee \ldots \vee +A_n$.

Ceci est exactement la règle de résolution ordonnée avec sélection, où $\text{sel}\,(C')$ *renvoie un singleton si* C' *n'est pas une clause positive, et* $\emptyset$ *sinon.*

7. Soit $S = S_0 \cup S_1$ un ensemble de clauses du premier ordre tel que l'on sait que S_0 est satisfiable (par exemple, un ensemble de clauses décrivant l'arithmétique, ou l'analyse). En utilisant la complétude de la résolution sémantique avec comme interprétation $\mathcal{H}_0$ n'importe quelle interprétation telle que $\mathcal{H}_0 \models S_0$, montrer que la règle de résolution ordonnée :

$$\frac{C_1 \vee \pm A_1 \vee \ldots \vee \pm A_n \quad C' \vee \mp A'_1}{C_1\sigma \vee C'\sigma}$$

où $\pm$ désigne un signe, $+$ ou $-$, et $\mp$ désigne le signe opposé, et où les conditions suivantes sont vérifiées :

(i') $n \geq 1$;

(ii') $\sigma = \text{mgu}\,\{A_j \doteq A'_1 | 1 \leq j \leq n\}$;

(iii') $A_1, \ldots, A_n$ sont maximaux dans $C_1 \vee \pm A_1 \vee \ldots \vee \pm A_n$ et $C_1 \vee \pm A_1 \vee \ldots \vee \pm A_n$ n'est pas dans S_0 ;

lue de sorte à ce que la conclusion $C_1\sigma \vee C'\sigma$ soit ajoutée à S_1, est complète. (Intuitivement, ceci exprime que l'on n'a pas besoin de résoudre deux clauses de S_0 ensemble, ceci ne pouvant mener à une contradiction ; mais ce n'est bien sûr pas un argument formel.) On notera que S_0 ne bouge pas, seul S_1 reçoit de nouvelles clauses.

Soit $\mathcal{H}_0$ *un modèle quelconque de* S_0*. Définissons l'algorithme* $\mathcal{A}^+$ *par :* $\mathcal{A}^+(C)$ *retourne "vrai" si* $C \in S_0$*, et "faux" sinon. (Ceci demande à ce que* S_0 *soit un ensemble récursif de clauses si l'on veut que ceci définisse un algorithme au sens usuel. Ceci est en général de toute façon appliqué sur des ensembles finis de clauses.) Clairement* $\mathcal{A}^+$ *vérifie les contraintes imposées sur* $\mathcal{A}^+$*. Quant à* $\mathcal{A}^-$*, il retourne toujours "faux". Les contraintes sur* $\mathcal{A}^-$ *sont vérifiées de façon triviale.*

8. La résolution sémantique est-elle toujours complète lorsqu'on élimine les tautologies au cours de la recherche de preuve ?

Oui, comme dans le cours, aucun nœud d'échec ne peut être étiqueté par une tautologie.

9. La résolution sémantique est-elle toujours complète lorsqu'on élimine les clauses linéairement subsumées au cours de la recherche de preuve ?

Oui, par exactement le même argument que dans le cours, puisque la mesure utilisée des arbres décorés est la même.