Deux raffinements de la résolution

On se référera parfois au poly ; il s'agira toujours des versions au moins égales à 4 du cours. Les questions les plus importantes, et donc les plus longues ou les plus difficiles, sont marquées d'une astérisque $(*)$

I. La résolution sémantique

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. $(*)$ En suivant l'argument de la démonstration du théorème 8 du poly, montrer que la résolution sémantique est complète. Indication : on y construira 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 une fonction qui à tout A_i^0, $1 \leq i \leq k$, associe "vrai" ou "faux", 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 $\pm_N H_N = \pm A_k^0$, où le signe $\pm$ est $-$ si $\mathcal{H}_0 \models A_k^0$, $+$ sinon ; s'il existe une telle clause génératrice telle que $I_k \not\models \mathcal{F}_N$, posons $I_{k+1} = I_k \cup \{\pm A_k^0\}$; sinon, $I_{k+1} = I_k \cup \{\mp A_k^0\}$, où $\mp$ est le signe opposé de $\pm$. Finalement, $I = I_n$.

On commencera par 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, $I \not\models \mathcal{F}_N$.

et on embraiera ensuite sur le reste de la démonstration de complétude. Notamment, la clause principale $C' \vee \mp A'_1$ sera trouvée comme la clause au nœud d'échec correspondant à l'interprétation I. (Il s'agit essentiellement de recopier la démonstration du cours, en effectuant, au fur et à mesure, toutes les adaptations nécessaires.)

2. 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.

3. 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.

II. La lock-résolution

La *lock-résolution* ressemble beaucoup à la résolution ordonnée. On commence par décorer chaque littéral de chaque clause par un entier, son *index*. Différentes occurrences du même littéral peuvent recevoir des index différents. Ensuite, on n'autorise à résoudre que sur des littéraux d'index minimaux dans les clauses.

Formellement, une *clause indexée* est une disjonction, vue comme un ensemble fini de littéraux ${}_n \pm A$, où A est un atome et $n \in \mathbb{N}$. Son *effacement* est la clause obtenue en effaçant tous les index, c'est-à-dire en remplaçant ${}_n \pm A$ par $\pm A$. La sémantique d'une clause indexée est celle de son effacement.

La règle de *lock-résolution* est :

$$\frac{C \vee {}_{i_1} + A_1 \vee {}_{i_2} + A_2 \vee \ldots \vee {}_{i_n} + A_n \quad C' \vee {}_j - A'}{C\sigma \vee C'\sigma} \tag{1}$$

où :

(i) $n \geq 1$;

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

(iii) $\min\{i_1, \ldots, i_n\}$ est l'indice minimal de la prémisse de gauche ;

(iv) j est l'indice minimal de la prémisse de droite.

1. On considère un nombre infini de symboles de prédicat $P^\pm[i]$, un pour chaque triplet formé d'un symbole de prédicat P, d'un signe $\pm$ (soit $+$ soit $-$) et d'un entier $i \in \mathbb{N}$. On suppose $P^\pm[i]$ différent de Q pour tout symbole de prédicat originel Q. On traduit chaque clause indexée en une clause ordinaire sur les $P[i]$ par

   $$({}_{i_1} \pm_1 P_1(t_1) \vee \ldots \vee {}_{i_n} \pm_n P_n(t_n))^* \quad = \quad +P_1^{\pm_1}[i_1](t_1) \vee \ldots \vee +P_n^{\pm_n}[i_n](t_n)$$

   Etant donné un ensemble fini S de clauses indexées, soit $S^* = \{C^* | C \in S\}$. Soit aussi Def l'ensemble de toutes les clauses

   $$-P^+[i_1](X) \vee \ldots \vee -P^+[i_n](X) \vee +P(X) \qquad - P^-[i](X) \vee -P(X)$$

   où P parcourt l'ensemble des symboles de prédicats, et $i, i_1, \ldots, i_n \in \mathbb{N}$, $n \geq 1$. Noter que Def est en général un ensemble infini de clauses.

   Montrer que la règle de résolution ordonnée avec sélection avec
   - l'ordre strict $\succ$ donné par $P[i](s) \succ Q[j](t)$ si et seulement si $i < j$, et $P(s) \succ Q[j](t)$ for every P, Q, s, t ;
   - sel $(-P^+[i_1](X) \vee \ldots \vee -P^+[i_n](X) \vee +P(X)) = \{-P^+[i_1](X), \ldots, -P^+[i_n](X)\}$, sel $(-P^-[i](X) \vee -P(X)) = \{-P^-[i](X)\}$, et sel $(C) = \emptyset$ pour toute autre clause

   simule la règle de lock-résolution, au sens où elle permet de déduire $(C\sigma \vee C'\sigma)^*$ à partir de $(C \vee {}_{i_1} + A_1 \vee {}_{i_2} + A_2 \vee \ldots \vee {}_{i_n} + A_n)^*$ et de $(C' \vee {}_j - A')^*$, ainsi que des clauses de Def.

2. En déduire que si la clause vide $\Box$ est déductible de S par lock-résolution, alors $\Box$ est aussi déductible de $S^* \cup \text{Def}$ par résolution ordonnée avec sélection.

3. $(*)$ Réciproquement, montrer que (intuitivement) si on peut déduire $(C'')^*$ à partir de $(C \vee\ _{i_1} + A_1 \vee\ _{i_2} + A_2 \vee \ldots \vee\ _{i_n} + A_n)^*$ et de $(C' \vee\ _j - A')^*$ par résolution ordonnée avec sélection, alors C'' est de la forme $C\sigma \vee C'\sigma$, où les conditions *(i)–(iv)* de la lock-résolution sont vérifiées.

   Formellement, soit $Star$ l'ensemble des clauses de la forme $(C'')^*$, pour n'importe quelle clause C'' (pas nécessairement dans S). Définissons inductivement les relations $E \vdash_1 C$ et $E \vdash C$, où $E \subseteq Star$ et C est une clause, par :
   - si $C \in E$, alors $E \vdash_1 C$;
   - si $E \vdash_1 C_1$, $E \vdash_1 C_2$, C est la conclusion d'une instance de la règle de résolution ordonnée avec sélection, partant des prémisses C_1 et C_2, et $C \notin Star$, alors $E \vdash_1 C$;
   - si $E \vdash_1 C_1$, $E \vdash_1 C_2$, C est la conclusion d'une instance de la règle de résolution ordonnée avec sélection, partant des prémisses C_1 et C_2, et $C \in Star$, alors $E \vdash C$.

   Autrement dit, $E \vdash C$ si et seulement si C est la première clause dans $Star$ obtenue après un nombre fini non nul d'applications de la règle de résolution ordonnée avec sélection, partant de l'ensemble de clauses E.

   On demande donc de démontrer que si $E \vdash (C'')^*$, où E consiste en deux clauses de $Star$, alors nécessairement ces deux clauses peuvent s'écrire $(C \vee\ _{i_1} + A_1 \vee\ _{i_2} + A_2 \vee \ldots \vee\ _{i_n} + A_n)^*$ et $(C' \vee\ _j - A')^*$ respectivement, de telle sorte que $C'' = C\sigma \vee C'\sigma$ et que les conditions *(i)–(iv)* de la lock-résolution sont vérifiées.

   On n'hésitera pas à poser clairement les lemmes intermédiaires nécessaires à prouver ce fait.

4. En déduire que la lock-résolution est complète : S est insatisfiable si et seulement si on peut déduire la clause vide à partir de S par lock-résolution.

5. Montrer qu'en revanche, l'élimination de tautologies (i.e., de clauses indexées dont l'effacement est une tautologie) n'est *pas* compatible avec la lock-résolution, autrement dit qu'éliminer les tautologies entraîne la perte de la propriété de complétude. Pour ceci, considérer l'exemple (clos) :

$$_1 + p \quad \vee \quad _2 + q \tag{2}$$
$$_3 - p \quad \vee \quad _4 - q \tag{3}$$
$$_5 + q \quad \vee \quad _6 - p \tag{4}$$
$$_7 - q \quad \vee \quad _8 + p \tag{5}$$

   En exhiber une dérivation de $\Box$ par lock-résolution, et montrer qu'il n'y en a pas si on élimine systématiquement toutes les tautologies.