Logique

Résumé des épisodes précédents

La Résolution et sa correction

La Complétude de la Résolution

Littéral : proposition atomique ou négation proposition atomique
Clause : disjonction de littéraux

Exemple : $\neg P(x) \vee P(S(x))$

Quantification universelle implicite
0 littéral : $\perp$
Disjonction implicitement AC1 (multiensembles)

Toute proposition peut être mise en forme clausale

Démontrer $\Gamma \vdash A$
Démontrer $\Gamma, \neg A \vdash$
Démontrer $\overline{\forall} C_1, \ldots, \overline{\forall} C_n \vdash$, où $C_1, \ldots, C_n$ forme clausale de $\Gamma, \neg A$

Recherche d'une contradiction ($\perp$, clause vide) à partir de $C_1, \ldots, C_n$ avec

$$\frac{P \vee C \quad \neg Q \vee C'}{\sigma(C \vee C')} \, \sigma = mgu(P, Q) \text{ Résolution}$$

$$\frac{L \vee L' \vee C}{\sigma(L \vee C)} \, \sigma = mgu(L, L') \text{ Factorisation}$$

Un exemple

$$P(0), \forall x\ (P(x) \Rightarrow P(S(x))) \vdash P(S(S(0)))$$

$$P(0)$$

$$\neg P(x) \vee P(S(x))$$

$$\neg P(S(S(0)))$$

$$\dfrac{\dfrac{\dfrac{P(0) \quad \neg P(x) \vee P(S(x))}{P(S(0))} \quad \neg P(x) \vee P(S(x))}{P(S(S(0)))} \quad \neg P(S(S(0)))}{\perp}$$

La correction de la Résolution

Si $\perp$ dérivable à partir de $C_1, ..., C_n$, alors $\overline{\forall} C_1, ..., \overline{\forall} C_n \vdash$ démontrable en calcul des séquents

Si $\perp$ dérivable à partir de $C_1, ..., C_n$, alors $\overline{\forall} C_1, ..., \overline{\forall} C_n \vdash$ valide dans tous les modèles

La complétude de la Résolution

Si $\overline{\forall} C_1, ..., \overline{\forall} C_n \vdash$ démontrable en calcul des séquents, alors $\perp$ dérivable à partir de $C_1, ..., C_n$

Si $\overline{\forall} C_1, ..., \overline{\forall} C_n \vdash$ valide dans tous les modèles, alors $\perp$ dérivable à partir de $C_1, ..., C_n$

Hélas : les deux méthodes sont utiles (généralisations de la Résolution)

Deux types de méthodes (deux écoles)

I. Dans les deux cas : R_0 et un lemme de relèvement

La règle de Résolution en deux étapes

$$\frac{P \vee C \quad \neg Q \vee C'}{\sigma(C \vee C')}\ \sigma = mgu(P, Q) \ \text{Résolution}$$

R_0

$$\frac{C}{(t/x)C}\ \text{Substitution}$$

$$\frac{P \vee C \quad \neg P \vee C'}{C \vee C'}\ \text{Résolution identique}$$

$$\frac{L \vee L \vee C}{L \vee C}\ \text{Factorisation identique}$$

Et un lemme de relèvement

Si $\perp$ dérivable à partir de $\mathcal{C}$ dans R_0, alors $\perp$ dérivable à partir de $\mathcal{C}$ dans R

De manière plus générale :
si $\mathcal{C}'$ copies (renommages) de clauses de $\mathcal{C}$ et θ substitution, telles que $\perp$ dérivable à partir de $\theta\mathcal{C}'$ dans R_0, alors $\perp$ dérivable à partir de $\mathcal{C}$ dans R

Récurrence sur la dérivation dans R_0
Substitution : on copie la clause et ajoute t/x à θ : hypothèse de récurrence
Résolution identique (ou Factorisation identique) : on a $\theta P = \theta Q$ donc $P = Q$ unifiable : mgu σ, $\theta = \eta \circ \sigma$, hypothèse de récurrence

Complétude et complétude

Démontrer la complétude de R_0 suffit pour démontrer celle de R

Si $\overline{\forall} C_1, \ldots, \overline{\forall} C_n \vdash$ démontrable en calcul des séquents (respectivement valide dans tous les modèles), alors $\perp$ dérivable à partir de $C_1, \ldots, C_n$ dans R_0 (complétude de R_0) et $\perp$ dérivable à partir de $C_1, \ldots, C_n$ dans R (relèvement)

On oublie R et on se concentre sur R_0

II. Dans les deux cas : un même lemme clé

Dans R_0

$\mathcal{C}$ ensemble de clauses, C_1 et C_2 clauses closes

Si D dérivable à partir de $\mathcal{C}, C_1$ alors D ou $D \vee C_2$ dérivable à partir de $\mathcal{C}, C_1 \vee C_2$ (Récurrence sur la dérivation de D, remarquez l'usage de la règle Factorisation identique)

Si $\perp$ dérivable à partir de $\mathcal{C}, C_1$ alors $\perp$ ou C_2 dérivable à partir de $\mathcal{C}, C_1 \vee C_2$

Si $\perp$ dérivable à partir de $\mathcal{C}, C_1$ et $\perp$ dérivable à partir de $\mathcal{C}, C_2$, alors $\perp$ dérivable à partir de $\mathcal{C}, C_1 \vee C_2$

Corollaire : si P atomique close, $\perp$ dérivable à partir de $\mathcal{C}, P$ et $\perp$ dérivable à partir de $\mathcal{C}, \neg P$ alors $\perp$ dérivable à partir de $\mathcal{C}$ (lemme clé + inutilité de $P \vee \neg P$)

III. La méthode syntaxique

Si $\overline{\forall} C_1, ..., \overline{\forall} C_n \vdash$ démontrable en calcul des séquents, alors $\perp$ dérivable dans R_0 à partir de $C_1, ..., C_n$

Plus généralement : si $\overline{\forall} C_1, ..., \overline{\forall} C_n \vdash P_1, ..., P_m$ démontrable en calcul des séquents, alors $\perp$ dérivable à partir de $C_1, ..., C_n, \neg P_1, ..., \neg P_m$

Par récurrence sur la structure d'une démonstration close et sans coupures de $\overline{\forall} C_1, ..., \overline{\forall} C_n \vdash P_1, ..., P_m$

Six règles possibles

Contraction-gauche, contraction-droite, $\neg$-gauche, axiome, $\forall$-gauche, $\vee$-gauche

Contraction-gauche, contraction-droite, $\neg$-gauche
Même ensemble de clauses
Hypothèse de récurrence

Et trois cas intéressants

- axiome : $(\overline{\forall} C_i) = P_j$, Résolution identique entre C_i et $\neg P_j$

- $\forall$-gauche, l'un des C_i remplacée par $(t/x)C_i$
  Hypothèse de récurrence : $\perp$ dérivable à partir de
  $C_1, ..., (t/x)C_i, ..., C_n, \neg P_1, ..., \neg P_m$
  $(t/x)C_i$ dérivable à partir de C_i (Substitution)
  $\perp$ dérivable à partir de $C_1, ..., C_i, ..., C_n, \neg P_1, ..., \neg P_m$

- $\vee$-gauche, l'un des C_i disjonction $D \vee D'$ de clauses closes
  Hypothèse de récurrence
  $\perp$ dérivable à partir de $C_1, \ldots, D, \ldots, C_n, \neg P_1, \ldots, \neg P_m$
  $\perp$ dérivable à partir de $C_1, \ldots, D', \ldots, C_n, \neg P_1, \ldots, \neg P_m$
  Lemme clé : $\perp$ dérivable à partir de $C_1, \ldots, C_i, \ldots, C_n, \neg P_1, \ldots, \neg P_m$

IV. Une digression : le théorème de Herbrand

La (non) commutation des règles du calcul des séquents

$$\cfrac{\cfrac{\cfrac{\cfrac{\dots}{P(0), \neg P(0) \lor P(S(0)), \neg P(S(0)) \lor P(S(S(0))), \neg P(S(S(0))) \vdash}}{P(0), \neg P(0) \lor P(S(0)), \forall x\ (\neg P(x) \lor P(S(x))), \neg P(S(S(0))) \vdash}}{P(0), \forall x\ (\neg P(x) \lor P(S(x))), \forall x\ (\neg P(x) \lor P(S(x))), \neg P(S(S(0))) \vdash}}{P(0), \forall x\ (\neg P(x) \lor P(S(x))), \neg P(S(S(0))) \vdash}$$

Impossible de commuter les règles contraction-gauche et $\forall$-gauche

Mais commutation dans l'autre sens (contraction vers le bas, $\forall$-gauche vers le haut)

Les séquents de la forme

$\overline{\forall} A_1, \ldots, \overline{\forall} A_n \vdash$, où A_1, ..., A_n sans quantificateurs (par exemple $\overline{\forall} C_1, \ldots, \overline{\forall} C_n \vdash$)

Une démonstration en trois phases :

1. des règles contraction-gauche
2. des règles $\forall$-gauche
3. des règles propositionnelles

Corollaire (Théorème de Herbrand)

Si

$$\overline{\forall} A_1, ..., \overline{\forall} A_n \vdash$$

démontrable
alors il existe θ_1^1, ..., $\theta_{k_1}^1$, ..., θ_1^n, ..., $\theta_{k_n}^n$ telles que

$$\theta_1^1 A_1, ..., \theta_{k_1}^1 A_1, ..., \theta_1^n A_n, ..., \theta_{k_n}^n A_n \vdash$$

(sans quantificateurs) démontrable

Corollaire (mais précurseur) du théorème d'élimination des coupures

Autre forme de la démonstration syntaxique de la complétude de la Résolution

Les instances avec Substitution puis Résolution propositionnelle (Résolution identique et Factorisation identique)

Le théorème de Herbrand à droite

Si

$$\vdash \overline{\exists} A_1, ..., \overline{\exists} A_n$$

démontrable
alors il existe θ_1^1, ..., $\theta_{k_1}^1$, ..., θ_1^n, ..., $\theta_{k_n}^n$ telles que

$$\vdash \theta_1^1 A_1, ..., \theta_{k_1}^1 A_1, ..., \theta_1^n A_n, ..., \theta_{k_n}^n A_n$$

(sans quantificateurs) démontrable

En particulier, si

$$\vdash \overline{\exists} A$$

démontrable
alors il existe θ_1, ..., θ_k telles que

$$\vdash \theta_1 A, ..., \theta_k A$$

démontrable
ou encore

$$\vdash \theta_1 A \vee ... \vee \theta_k A$$

démontrable

V. La méthode sémantique

Si $\overline{\forall} C_1, \dots, \overline{\forall} C_n \vdash$ valide dans tous les modèles, alors $\perp$ dérivable dans R_0 à partir de $C_1, \dots, C_n$

Si $\overline{\forall} C_1, \dots, \overline{\forall} C_n$ n'a pas de modèle, alors $\perp$ dérivable à partir de $C_1, \dots, C_n$

Si $\perp$ non dérivable à partir de $C_1, \dots, C_n$, alors $\overline{\forall} C_1, \dots, \overline{\forall} C_n$ a un modèle

Inspiration : démonstration du théorème de complétude de Gödel (troisième forme) : Si $\mathcal{T}$ cohérente, alors $\mathcal{T}$ a un modèle

Comme dans la démonstration du théorème de complétude de Gödel

On commence par saturer l'ensemble de clauses $\mathcal{C}$

Plus simple : pas de $\exists$, pas de témoins de Henkin (merci la Skolémisation)

Plus délicat : règles plus faibles
Au lieu de trois cas : $\mathcal{C}$ démontre A, $\mathcal{C}$ démontre $\neg A$, ou ni l'un ni l'autre
Une autre formulation : ajouter P ou ajouter $\neg P$ (P atomique close) à un ensemble de clauses préserve la cohérence (clause $\bot$ non dérivable)

La préservation de la cohérence

Si $\mathcal{C}$ cohérent, alors $\mathcal{C}, P$ cohérent ou $\mathcal{C}, \neg P$ cohérent

Contraposée du corollaire du lemme clé : si $\perp$ dérivable à partir de $\mathcal{C}, P$ et $\perp$ dérivable à partir de $\mathcal{C}, \neg P$, alors $\perp$ dérivable à partir de $\mathcal{C}$

La saturation de l'ensemble de clauses

Énumération des propositions atomiques closes $P_0, P_1, P_2 \ldots$

$\mathcal{U}_0 = \mathcal{C}$, cohérent

On suppose $\mathcal{U}_n$ cohérent
$\mathcal{U}_n, P_n$ cohérent ou $\mathcal{U}_n, \neg P_n$ cohérent
$\mathcal{U}_{n+1} = \mathcal{U}_n, P_n$ ou $\mathcal{U}_n, \neg P_n$, cohérent

$\mathcal{U} = \bigcup_i \mathcal{U}_i$ cohérent
Pour chaque proposition atomique close P, $P \in \mathcal{U}$ ou $\neg P \in \mathcal{U}$

La construction du modèle

Rien de nouveau

Domaine : termes clos

$\hat{f}$ trivial

$\hat{P}$ fonction qui à $t_1, ..., t_n$ associe 0 ou 1 selon que $\neg P(t_1, ..., t_n)$ ou $P(t_1, ..., t_n)$ appartient à $\mathcal{U}$

$\mathcal{M}$ modèle de $\mathcal{C}$

$C = L_1 \vee ... \vee L_n$ clause de $\mathcal{C}$
ρ valuation qui associe un terme clos à chaque variable de C (aussi une substitution)
$[\![L_1 \vee ... \vee L_n]\!]_\rho = 1$

$\perp$ a une dérivation à partir de $\rho C, \neg \rho L_1, ..., \neg \rho L_n$
donc ($\mathcal{U}$ cohérent) $\neg \rho L_1, ..., \neg \rho L_n$ pas tous dans $\mathcal{U}$
ρL_i dans $\mathcal{U}$
$[\![L_i]\!]_\rho = 1$
$[\![L_1 \vee ... \vee L_n]\!]_\rho = 1$

Donc

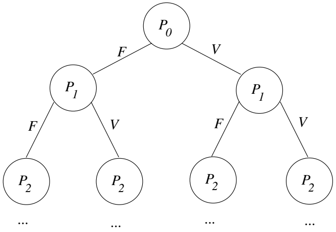
Si $\perp$ non dérivable à partir de $\mathcal{C}$, alors $\mathcal{C}$ a un modèle

Si $\overline{\forall} C_1, ..., \overline{\forall} C_n \vdash$ valide dans tous les modèles, alors $\perp$ dérivable à partir de $C_1, ..., C_n$

Variation sur la démonstration

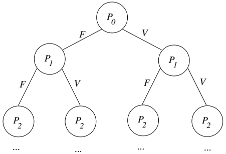
Contraposée : si $\mathcal{C}$ n'a pas de modèle, alors $\perp$ dérivable a partir de $\mathcal{C}$

Arbre sémantique : une fois les propositions atomiques closes énumérées P_0, P_1, P_2... un arbre infini



Saturation : choix d'un enfant à chaque nœud
Chaque branche infinie : modèle (domaine = ensemble des termes clos du langage)

Arbres et dérivations



$\mathcal{C}$ pas de modèle : dans chaque branche infinie une clause $L_1 \vee \ldots \vee L_n$ de $\mathcal{C}$ non valide

Une valuation ρ (substitution close) telle que $[\![L_1 \vee \ldots \vee L_n]\!]_\rho = 0$

Un nœud où $\neg\rho L_1$, ..., $\neg\rho L_n$ sur la branche : on élague

Un arbre fini : à chaque feuille, une dérivation de $\perp$ avec à partir de $\mathcal{C}, (\neg)P_0, \ldots, (\neg)P_m$

À chaque feuille : une dérivation de $\perp$ à partir de $\mathcal{C}, (\neg)P_0, \ldots, (\neg)P_m$

On remonte des feuilles à la racine en éliminant un littéral clos à chaque étape

(corollaire du lemme clé : si $\perp$ a une dérivation à partir de $\mathcal{D}, P$ et à partir de $\mathcal{D}, \neg P$, alors $\perp$ a une dérivation à partir de $\mathcal{D}$)

À la racine : une dérivation de la clause vide à partir de $\mathcal{C}$

La Résolution est correcte et complète

De nombreuses méthodes qui reviennent au même (démontrabilité = validité dans tous les modèles)

Un même système intermédiaire R_0, un même lemme clé

Mais qui se généralisent plus ou moins bien (ce qui explique leur existence)

La prochaine fois

La définissabilité