Induction sur les formules propositionnelles

Syntaxe du calcul propositionnel (rappel)

Soit $\mathcal{R}$ en ensemble dénombrable de lettres propositionnelles.

Définition : L'ensemble $\mathcal{F}_{prop}$ de formules du calcul propositionnel, est le plus petit ensemble t.q.

- $\mathcal{R} \subseteq \mathcal{F}_{prop}$
- Si $A \in \mathcal{F}_{prop}$, alors $\neg A \in \mathcal{F}_{prop}$.
- Si $A, B \in \mathcal{F}_{prop}$, alors $\vee(A, B)$, $\wedge(A, B)$, $\rightarrow (A, B) \in \mathcal{F}_{prop}$.

Exemple :	$\neg(p)$	$\vee(p, p)$	$\rightarrow (\wedge(p, q), \neg(r))$
Notation simplifiée :	$\neg p$	$p \vee p$	$(p \wedge q) \rightarrow \neg r$

Le calcul propositionnel en OCAML (rappel)

```
# type fprop = L of int | Neg of fprop |
               Ou of fprop * fprop |
               Et of fprop * fprop |
               Impl of fprop * fprop;;

# let f1 = Et(Ou(L(1),L(2)),Neg(L(3)));;
val f1 : fprop = Et (Ou (L 1, L 2), Neg (L 3))
```

Les formules comme des arbres

Les formules constituent un ensemble parametré par deux types `'a` et `'b`, où chaque étiquette d'une feuille est de type `'a` et chaque étiquette d'un nœud interne unaire ou binaire est de type `'b`.

Ceci donne une nouvelle définition du type `('a,'b) AbinII` :

L'ensemble `('a, 'b) AbinII` est le plus petit ensemble t.q.

- Si m est de type `'a`, alors $feuille(m) \in$ `('a, 'b) AbinII`
- Si $c \in$ `('a, 'b) AbinII` et o est de type `'b`, alors $noeud1(o, c) \in$ `('a, 'b) AbinII`.
- Si $c_1, c_2 \in$ `('a, 'b) AbinII` et o est de type `'b`, alors $noeud2(o, c_1, c_2) \in$ `('a, 'b) AbinII`.

Un type abstrait pour `('a, 'b) abinII`

Domaine :
`('a,'b) abinII`
Opérations de construction :
`cons_f` : `'a` $\rightarrow$ `('a,'b) abinII`
`cons_u` : `'b` $\times$ `('a,'b) abinII` $\rightarrow$ `('a,'b) abinII`
`cons_b` : `'b` $\times$ `('a,'b) abinII` $\times$ `('a,'b) abinII` $\rightarrow$ `('a,'b) abinII`
Opérations de test :
`est_f`, `est_u`,`est_b` : `('a,'b) abinII` $\rightarrow$ `booléen`
Opérations d'accès :
`etiquette_feuille` : `('a,'b) abinII` $\rightarrow$ `'a`
`etiquette_noeud` : `('a,'b) abinII` $\rightarrow$ `'b`
`fils_u`, `fils_g, fils_d` : `('a,'b) abinII` $\rightarrow$ `('a,'b) abinII`

Le calcul propositionnel en OCAML (deuxième possibilité)

```
# type ('a,'b) abinII =
  F of 'a |
  N1 of  'b * ('a,'b) abinII |
  N2 of 'b * ('a,'b) abinII * ('a,'b) abinII;;

# type op = Neg | Et | Ou | Impl;;

# let f1 = N2(Et,N2(Ou,F(1),F(2)),N1(Neg,F(3)));;
val f1 : (int, op) abinII =
    N2 (Et, N2 (Ou, F 1, F 2), N1 (Neg, F 3))
```

Fonctions récursives sur les formules

Formules $\subseteq$ Arbres, donc

pour définir une fonction sur les formules on peut utiliser l'un des schémas récursifs sur les arbres.

Schéma récursif pour les formules

$$\begin{aligned} \mathtt{f}(a) &= g_1(a, \mathtt{f}(\mathtt{fils\_u}(a))) \\ & \quad \text{Si } \mathtt{est\_u}(a) \\ \mathtt{f}(a) &= g_2(a, \mathtt{f}(\mathtt{fils\_g}(a)), \mathtt{f}(\mathtt{fils\_d}(a))) \\ & \quad \text{Si } \mathtt{est\_b}(a) \end{aligned}$$

Quelques fois g_1 et g_2 se “ressemblent” beaucoup.

Cas particulier : lors que $\mathtt{est\_f}(a)$

Exemple : nb de lettres d'une formule

```
# let rec nblettres f = match f with
      F(_)     -> 1
    | N1(_,a)   -> nblettres a
    | N2(_,a,b) -> nblettres a + nblettres b ;;
```

Exercice : Qui sont les fonctions g_1 et g_2 ?

Preuve de propriétés par induction sur les formules

Exemple : Montrer que toute formule A est équivalente à une formule A' où le connecteur $\neg$ se trouve uniquement à gauche d'une lettre propositionnelle.

Calculs des séquents

Définition : Un séquent est un couple de la forme $\Delta \triangleright \Gamma$, où Δ et Γ sont de multi-ensembles de formules.

Exemple :

$$\begin{array}{lll} p, p, p \to q & \triangleright & r, p \vee s \\ p \to q & \triangleright & \\ & \triangleright & p, s \\ & \triangleright & \end{array}$$

Définition d'un calcul des séquents

– On fixe des axiomes (des séquents particulièrs)

– On fixe des règles d'inférence de la forme $\dfrac{\Delta_1 \triangleright \Gamma_1 \ldots \Delta_n \triangleright \Gamma_n}{\Delta \triangleright \Gamma}$

Le système $\mathcal{G}$

Axiome : $\Delta, A \triangleright \Gamma, A$

Règles d'inférence logiques :

$$\frac{\Delta \triangleright \Gamma, A}{\Delta, \neg A \triangleright \Gamma}\ (\neg\ g) \qquad \frac{\Delta, A \triangleright \Gamma}{\Delta \triangleright \Gamma, \neg A}\ (\neg\ d)$$

$$\frac{\Delta \triangleright A, \Gamma \quad \Delta, B \triangleright \Gamma}{\Delta, A \to B \triangleright \Gamma}\ (\to\ g) \qquad \frac{\Delta, A \triangleright B, \Gamma}{\Delta \triangleright A \to B, \Gamma}\ (\to\ d)$$

$$\frac{\Delta, A, B \triangleright \Gamma}{\Delta, A \wedge B \triangleright \Gamma}\ (\wedge\ g) \qquad \frac{\Delta \triangleright A, \Gamma \quad \Delta \triangleright B, \Gamma}{\Delta \triangleright A \wedge B, \Gamma}\ (\wedge\ d)$$

$$\frac{\Delta, A \triangleright \Gamma \quad \Delta, B \triangleright \Gamma}{\Delta, A \vee B \triangleright \Gamma}\ (\vee g) \qquad \frac{\Delta \triangleright A, B, \Gamma}{\Delta \triangleright A \vee B, \Gamma}\ (\vee d)$$

Dérivation d'un séquent

Définition : La dérivation d'un séquent $\Gamma \triangleright \Delta$ à partir d'un ensemble de séquents Φ, notée $\Phi \vdash \Gamma \triangleright \Delta$, est un arbre fini tel que

– les nœuds sont des séquents
– chaque feuille est soit une formule de Φ, soit un axiome
– si S est le père des $S_1 \ldots S_n$, alors S est obtenu par l'application d'une règle d'inférence sur $S_1 \ldots S_n$.
– la racine de l'arbre est le séquent$\Gamma \triangleright \Delta$

Preuves et théorèmes

Définition : La preuve d'un séquent $\Gamma \triangleright \Delta$ est une dérivation de $\Gamma \triangleright \Delta$ à partir de l'ensemble vide de séquents. On dit dans ce cas que $\Gamma \triangleright \Delta$ est un théorème.

Conséquence logique (rappel)

Définition : Un multi-ensemble de formules Γ est conséquence logique d'un multi-ensemble de formules Δ, noté $\Delta \models \Gamma$, si toute interprétation qui satisfait toutes les formules de Δ satisfait au moins une formule de Γ.

Exemple :

$$p, p \to q \models q, r, s$$

Propriétés fondamentales du système $\mathcal{G}$

Théorème :(Correction) Le système $\mathcal{G}$ est correcte, i.e., si $\Delta \triangleright \Gamma$ est un théorème, alors $\Delta \models \Gamma$.

Théorème :(Complétude) Le système $\mathcal{G}$ est complet, i.e., si $\Delta \models \Gamma$, alors $\Delta \triangleright \Gamma$ est un théorème.

Donc, on peut utiliser $\mathcal{G}$ comme alternative aux tables de vérité. Cette approche peut produire des économies très importantes !

Premier exemple de dérivation dans $\mathcal{G}$

$$\dfrac{\dfrac{p \triangleright q}{\triangleright \neg p, q}\,(\neg\ d)}{\neg q \triangleright \neg p}\,(\neg\ g)$$

On a une dérivation de $\neg q \triangleright \neg p$ à partir de $p \triangleright q$: $p \triangleright q \vdash \neg q \triangleright \neg p$.

Donc, on sait que $p \triangleright q \models \neg q \triangleright \neg p$, sans besoin de construire une table de vérité, dont la taille dependrait du nombre de lettres propositionnelles en jeux.

Deuxième exemple de dérivation dans $\mathcal{G}$

$$\dfrac{\dfrac{p \triangleright \neg p}{\triangleright p \rightarrow \neg p}\,(\rightarrow\ d)}{\neg(p \rightarrow \neg p)\triangleright}\,(\neg\ g)$$

On a $p \triangleright \neg p \vdash \neg(p \rightarrow \neg p)\triangleright$ et donc aussi $p \triangleright \neg p \models \neg(p \rightarrow \neg p)\triangleright$

Comment transformer quelques dérivations dans $\mathcal{G}$

Théorème : (Affaiblissement) Si $\Delta \triangleright \Gamma$ est dérivable dans le système $\mathcal{G}$, alors $\Delta, A \triangleright \Gamma$ et $\Delta \triangleright A, \Gamma$ le sont aussi.

Théorème : (Contraction) Si $\Delta, A, A \triangleright \Gamma$ est dérivable dans le système $\mathcal{G}$, alors $\Delta, A \triangleright \Gamma$ l'est aussi. Si $\Delta \triangleright \Gamma, A, A$ est dérivable dans le système $\mathcal{G}$, alors $\Delta \triangleright \Gamma, A$ l'est aussi.

Premier exemple de théorème dans $\mathcal{G}$

Modus ponens

$$\dfrac{p \triangleright p, q\ (ax) \qquad p, q \triangleright q\ (ax)}{p, p \rightarrow q \triangleright q}\,(\rightarrow\ g)$$

On a $\vdash p, p \rightarrow q \triangleright q$, donc $p, p \rightarrow q \triangleright q$ est *valide*.

Deuxième exemple de théorème dans $\mathcal{G}$

Tiers exclu

$$\dfrac{\dfrac{p \triangleright p\ (ax)}{\triangleright p, \neg p}\,(\neg\ d)}{\triangleright p \vee \neg p}\,(\vee\ d)$$

On a $\vdash \triangleright p \vee \neg p$

Troisième exemple de théorème dans $\mathcal{G}$

Loi de Pierce

$$\dfrac{\dfrac{\dfrac{p \triangleright q, p\ (ax)}{\triangleright p \rightarrow q, p}\,(\rightarrow\ d) \qquad p \triangleright p\ (ax)}{(p \rightarrow q) \rightarrow p \triangleright p}\,(\rightarrow\ g)}{\triangleright ((p \rightarrow q) \rightarrow p) \rightarrow p}\,(\rightarrow\ d)$$

On a $\vdash \triangleright((p \rightarrow q) \rightarrow p) \rightarrow p$