Chapitre 4

Preuve de terminaison et de correction d'un algorithme.

1 Invariant de boucle.

Nous prouvons tout d'abord que l'algorithme s'arrête en montrant qu'une condition d'exécution de boucle finit par ne plus être réalisée. Nous exhibons alors un invariant de boucle, c'est-à-dire une propriété P qui, si elle est valide avant l'exécution d'un tour de boucle, est aussi valide après l'exécution du tour de boucle.
Nous vérifions alors que les conditions initiales rendent la propriété P vraie en entrée du premier tour de boucle. Nous en concluons que cette propriété est vraie en sortie du dernier tour de boucle. Un bon choix de la propriété P prouvera qu'on a bien produit l'objet recherché. La difficulté de cette méthode réside dans la détermination de l'invariant de boucle. Quand on l'a trouvé il est en général simple de montrer que c'est bien un invariant de boucle.

Exemple 1 : Établir la terminaison et la preuve l'algorithme suivant :

```
let division a b =
  let B = ref b in
  let R = ref a in
  let Q = ref 0 in
    while R >= B do
      R := !R - !B;
      Q := !Q+1
    done;
( !Q , !R );;
```

Exemple 2 : Établir la terminaison et la preuve l'algorithme suivant :

```
let puissance a n =
  let A = ref a in
  let N = ref n in
  let R = ref 1 in
    while !N >0 do
      if !N mod 2 = 0 then
        begin
        A := (!A)*(!A) ;
        N := !N/2
        end
      else
        begin
        R := (!R)*(!A) ;
        N := !N-1
        end
    done;
!R;;
```

2 Terminaison d'une fonction récursive

Que dire de la terminaison de la fonction suivante :
Conjecture de Collatz (problème de Syracuse)

```
let rec collatz n = match n with
| n when n <= 1 -> 0
| n when n mod 2 = 0 -> collatz (n/2)
| _ -> collatz (3*n+1);;
```

2.1 Ensemble ordonné :

Définition 1 :

Ordre bien fondé

Soit E un ensemble, et $\preceq$ une relation d'ordre sur E (pas nécessairement totale).
On note $\prec$ l'ordre strict correspondant :

$$\forall x \in E, x \prec y \Leftrightarrow (x \preceq y) \wedge (x \neq y)$$

On dit que l'ordre $\preceq$ est bien fondé s'il n'existe pas de suite d'éléments de E strictement décroissante. On parle alors aussi d'ensemble bien fondé.
Un ensemble est bien ordonné si, de plus, la relation d'ordre est totale.

Exemple 3 :

Exemple 4 : $\mathbb{N}^2$ muni de l'ordre lexicographique est bien fondé :

Définition 2 :

Soit un ensemble ordonné $(E, \preceq)$ et une partie $A \subset E$.
Soit $m \in A$.
On dit que m est minimal dans A lorsque :

$$\forall a \in A, a \preceq m \Rightarrow a = m$$

Remarque : Si l'ordre est total, m minimal dans $A \Leftrightarrow m = min(A)$.

Exemple 5 :

Propriété 1 :

Caractérisation d'un ordre bien fondé.
L'ordre $\preceq$ est bien fondé si et seulement si toute partie A non-vide de E possède un élément minimal.

Preuve

2.2 Terminaison :

Théorème 1 :

Justification de la terminaison d'une fonction récursive :
Soit $(E, \preceq)$ un ensemble muni d'un ordre bien fondé.
Soit A et B deux ensembles et $f : A \mapsto B$ une fonction récursive. Soit $\Phi : A \mapsto E$ une application. On note

$$M = \{x \in A / \Phi(x) \text{ est minimal dans } \Phi(A)\}$$

On fait les hypothèses suivantes :

- le calcul de $f(x)$ se termine pour tous les éléments $x \in M$;
- pour tout $x \in A$, le calcul de $f(x)$, n'utilise qu'un nombre fini de calculs $f(y_1), ..., f(y_k)$ où $\Phi(y_i) \prec \Phi(x)$.

Alors le calcul de $f(x)$ se termine pour toute valeur de $x \in A$.

Remarque : Lorsque $\Phi : A \mapsto (\mathbb{N}, \leqslant)$, on dit que Φ est une graduation.

Preuve

2.3 Preuve par induction :

Théorème 2 :

Induction sur un ensemble bien fondé :
Soit $(E, \preceq)$ un ensemble muni d'un ordre bien fondé.
Soit $\mathcal{P}$ un prédicat sur E (soit une application de E dans les booléens). On note M l'ensemble des éléments minimaux de E. On fait les hypothèses suivantes :

- $\forall x \in M$, $\mathcal{P}(x)$.
- $\forall x \in E \backslash M$, $(\forall y \prec x, \mathcal{P}(y)) \Rightarrow \mathcal{P}(x)$.

Alors , pour tout $x \in E$, $\mathcal{P}(x)$.

Preuve

2.4 Preuve de la correction :

Théorème 3 :

Justification de la correction d'une fonction récursive : :
Soit $(E, \preceq)$ un ensemble muni d'un ordre bien fondé.
Soit A et B deux ensembles et $f : A \mapsto B$ une fonction récursive. Soit $\Phi : A \mapsto E$ une application. On note

$$M = \{x \in A / \Phi(x) \text{ est minimal dans } \Phi(A)\}$$

Soit $\mathcal{P}_f$ un prédicat ;"f(x) donne bien la valeur demandée". On fait les hypothèses suivantes :

- $\forall x \in M$, $\mathcal{P}_f(x)$.
- $\forall x \in A$, le calcul de $f(x)$ n'utilise qu'un nombre fini de calculs de $f(y_1), ..., f(y_k)$ avec $\Phi(y_i) \prec \Phi(x)$ et $\mathcal{P}_f(y_1)$ et $\mathcal{P}_f(y_k) \Rightarrow \mathcal{P}_f(x)$

Alors , pour tout $x \in A$, $\mathcal{P}_f(x)$.