Introduction

On poursuit ici l'étude théorique des algorithmes entreprise dans le chapitre traitant de la complexité. On se pose maintenant la question de savoir si un algorithme donné répond bien au problème qu'il est censé traité dans sa spécification. *Il se pose alors deux grandes questions :*

1. *Se termine-t-il ? C'est la question de la* terminaison.
2. *Résout-il bien le problème qu'il est censé traiter ? C'est la question de la* correction.

Le but de ce chapitre est d'introduire les méthodologies qui permettent de traiter ces problèmes.

Source d'inspiration : cours de mon collègue Pierre Duclosson.

1 Terminaison d'algorithme

Objectif 1

Pour un algorithme ou une partie d'algorithme qui ne comporte pas de boucles ou seulement des boucles inconditionnelles, la question de la terminaison ne se pose, a priori, pas. Le cas des boucles conditionnelles est plus délicat : la condition est censée être vraie au départ (sinon c'est du code mort) et cette même condition doit finir par être fausse sinon les itérations ont lieu indéfiniment.

Exercice 1

Pour chacune des boucles déterminer si elle se termine ?

Boucle 1

```
x = 0
while x >= 0:
    x = x + 1
```

Boucle 2

```
x = 10
while x >= 0:
    x = x - 1
```

Boucle 3

```
x = 1
while x != 0:
    x = x - 0.1
```

Boucle 4

```
x = 1
while x > 0:
    x = x - 0.1
```

Point de cours 1 *Variant de boucle et terminaison d'algorithme*

- On appelle **itération** d'une boucle **une** exécution des instructions qui figure dans le corps de la boucle.
- Une boucle inconditionnelle `for` se termine nécessairement.
- Pour démontrer qu'une boucle conditionnelle (`while`) se termine, il suffit de déterminer une grandeur exprimée à l'aide des variables de l'algorithme qui vérifie les trois conditions suivantes :
  - Condition 1 : cette grandeur a une valeur entière avant la boucle ;
  - Condition 2 : une itération de boucle ne s'exécute que si la grandeur est positive ;
  - Condition 3 : chaque exécution d'une itération de boucle fait décroître strictement la grandeur et la maintient dans l'ensemble des entiers.

  Comme il n'existe pas de suite infinie à valeurs dans l'ensemble des entiers positifs qui soit strictement décroissante (pas de *descente infinie* dans l'ensemble des entiers naturels) cela prouve alors que la grandeur ne peut prendre qu'un nombre fini de valeurs positives et que le nombre d'itérations est fini.
- On appelle **variant** de la boucle une telle quantité.

Exercice 2

La fonction `division_euclidienne` ci-dessous calcule le quotient et le reste de la division euclidienne de a par b (avec $a \geqslant 0$ et $b > 0$).

```
def division_euclidienne(a, b):
    """Renvoie le quotient et le reste de la division euclidienne de a par
        b ."""
    assert (a >= 0) and (b > 0)
    q = 0
    r = a
    while r >= b :
        r = r - b
        q = q + 1
    return (q, r)
```

On numérote les itérations de boucles à partir de $k = 1$.
On définit la quantité $v_k = r_k - b$ où r_k est l'état de la variable r avant l'itération k de la boucle.
Démontrons que v_k est un **variant** de la boucle de `division_euclidienne` :

- Condition 1 : La valeur du variant avant exécution de la première itération de boucle est ....., c'est un .....
- Condition 2 : Supposons que v_k soit la valeur du variant avant l'itération k de la boucle. Cette itération s'exécute si et seulement si ..... c'est-à-dire v_k positif.
- Condition 3 : Supposons que l'itération k s'exécute et que la valeur v_k du variant soit entière avant l'itération k. À la fin de l'itération k, la valeur du variant est $v_{k+1} =$ .....

.....

.....

.....

.....

.....

.....

.....

Ainsi après exécution de l'itération k, on a v_{k+1} entière et $v_{k+1} < v_k$.

Les trois conditions caractéristiques d'un **variant** sont vérifiées, donc v_k est un variant de boucle et la boucle se termine.

Exercice 3

On considère l'algorithme implémenté par la fonction `boucle` ci-dessous.
À l'aide d'un variant de boucle, démontrer que l'algorithme se termine.

```
def boucle():
    x = 0
    while x < 10:
        x = x + 2
    return
```

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

2 Correction d'algorithme

Objectif 2

La terminaison d'un algorithme est une condition nécessaire mais pas suffisante. On souhaite s'assurer que lorsque l'algorithme se termine, le traitement effectué soit correctement réalisé.

Point de cours 2 *Invariant de boucle et correction d'algorithme*

Pour démontrer la **correction** d'un algorithme, les difficultés se posent dans les boucles (quel qu'en soit le type, conditionnelles ou inconditionnelles).

- ☞ Avant d'analyser la **correction** d'un algorithme, on démontre sa **terminaison** à l'aide d'un variant.
- ☞ Ensuite on associe à chaque itération i de boucle un **invariant**. C'est une propriété $\mathscr{P}_i$, évaluée avant l'itération i de boucle, qui doit vérifier deux caractéristiques :
  - **Initialisation :** la propriété est vraie avant la première itération de boucle, selon la façon de numéroter les itérations, cette première valeur de la propriété pourra être $\mathscr{P}_0$, $\mathscr{P}_1$ etc ...
  - **Transmission :** si $\mathscr{P}_k$ avant l'itération k et que celle-ci s'exécute alors $\mathscr{P}_{k+1}$ doit être vraie à la fin de l'itération donc avant une éventuelle itération $k+1$.
- ☞ Supposons que la boucle s'exécute n fois et que la dernière itération de boucle ait pour indice $n-1$, la correction s'obtient au terme d'une chaîne d'implications logiques :
  - $\mathscr{P}_0$ est vraie par *initialisation*;
  - itération 1 : $\mathscr{P}_0$ vraie donc $\mathscr{P}_1$ vraie par *transmission*;
  - ...
  - itération k : $\mathscr{P}_k$ vraie donc $\mathscr{P}_{k+1}$ vraie par *transmission*;
  - ...
  - itération $n-1$: $\mathscr{P}_{n-1}$ vraie donc $\mathscr{P}_n$ vraie par *transmission.*

  On en déduit que $\mathscr{P}_n$ est vraie.

  Si on a choisi judicieusement l'invariant, l'expression de $\mathscr{P}_n$ doit prouver la **correction** de l'algorithme.

Une preuve d'invariant est similaire à une preuve par récurrence en mathématiques.

Exercice 4

On considère la fonction `puissance(x, n)` définie ci-dessous.
L'algorithme contient une seule boucle `for` inconditionnelle donc il se termine.
On considère la propriété $\mathscr{P}_k$: « *La valeur de p avant l'itération k de la boucle est* x^{k-1} ».

1. Démontrer que $\mathscr{P}_k$ est un invariant de la boucle de la fonction `puissance(x, n)`.
2. En déduire que `puissance(x, n)` renvoie bien x^n et que l'algorithme est correct.

```
def puissance(x, n):
    """Renvoie x ** n, où x est un flottant et n un entier."""
    assert n >= 0
    p = 1
    for k in range(1, n + 1):
        p = p * x
    return p
```

Réponses :

1. La propriété $\mathscr{P}_k$ est un **invariant** de la boucle si et seulement si elle vérifie les deux propriétés caractéristiques d'un invariant. La première itération est numérotée par $k = 1$.

   - **Initialisation :** $\mathscr{P}_1$ se traduit par « La valeur de de p est $x^{1-1} = 1$ ». C'est vrai car on initialise p avec la valeur 1.
   - **Transmission :** On se place avant l'itération k et on suppose que la propriété $\mathscr{P}_k$ Par hypothèse la valeur de p avant l'exécution de l'itération k est x^{k-1}.

     .....

     .....

     .....

     La valeur de p à la fin de l'itération k est bien ..... donc la propriété $\mathscr{P}_{k+1}$ est vraie.
   - **Conclusion :** La propriété $\mathscr{P}_k$ est donc bien un **invariant** de la boucle de la fonction `puissance`.

   Ce schéma de preuve est similaire à une preuve par récurrence (programme de terminale spécialité mathématiques).

2. On sort de boucle après l'itération numéro n et avant l'itération $n+1$ donc l'expression $\mathscr{P}_{n+1}$ de l'invariant est vraie en sortie de boucle :

   .....

   .....

Exercice 5

Pour la fonction `division_euclidienne` de l'exercice 2, on numérote les itérations de boucle à partir de $k = 1$.
On définit la propriété $\mathscr{P}_k$: « $a_k = q_k \times b + r_k$ » où a_k, q_k et r_k sont les états des variables a, q et r avant l'itération k de la boucle.
On a démontré dans l'exercice 2 que l'algorithme se termine à l'aide d'un variant de boucle.

1. Démontrons que $\mathscr{P}_k$ est un invariant de la boucle de `division_euclidienne`.

   - **Initialisation :** $\mathscr{P}_1$ se traduit par .....
   - **Transmission :** On suppose que la propriété $\mathscr{P}_k$ est vraie avant l'exécution de l'itération k de la boucle.

     .....

     .....

     .....

     .....

     .....

     .....

   - **Conclusion :** La propriété $\mathscr{P}_k$ est donc bien un **invariant** de la boucle de l'algorithme de division euclidienne.

2. En déduire que cet algorithme est correct.

   .....

   .....

3 Terminaison et correction du tri par sélection.

Les algorithmes du programme : recherche linéaire de maximum dans un tableau, recherche dichotomique dans un tableau trié, tris par sélection ou insertion, se terminent et sont corrects. On va se limiter au cas du tri par sélection. Voir https://fjunier.forge.apps.education.fr/tnsi/Bac/C0_Algorithmes_de_r%C3%A9f%C3%A9rence/C0_Algorithmes_de_r%C3%A9f%C3%A9rence/ *pour les algorithmes de référence en NSI.*

Exercice 6 *Tri par sélection*

On suppose qu'on dispose de deux fonctions dont la terminaison et la correction sont prouvées :

- `recherche_index_min(t, i)` renvoie un index du minimum d'un tableau d'entiers `t` à partir de l'index `i < len(t)`.
- `echange(t, i, imin)` permute les éléments d'index `i` et `imin` dans un tableau d'entiers `t`.

La fonction `tri_selection(t)` trie en place par sélection un tableau d'entiers `t`.

```
def tri_selection(t):
    """Trie en place par sélection un tableau d'entiers."""
    for k in range(0, len(t)):
        imin = recherche_index_min(t, k)
        echange(t, i, imin)
```

1. Justifier la terminaison de l'algorithme implémenté par `tri_selection(t)`.

.....

.....

2. Pour tout indice `0 <= k < len(t)` on définit la propriété $\mathscr{P}_k$ vérifiée avant chaque itération d'indice k de la boucle. $\mathscr{P}_0$ désigne un état avant la première itération de boucle.

 *Ici on numérotes les itérations de boucle à partir de* 0.

$\mathscr{P}_k$:= *le sous-tableau* `t[0:k]` *est trié dans l'ordre croissant et si* `t[0:k]` *est non vide et* `t[k:]` *non vide alors* `t[k-1]` *est inférieur ou égal à tous les éléments de* `t[k:]`.

Démontrons que $\mathscr{P}_k$ est un invariant de boucle.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

La boucle se termine à la fin de l'itération d'indice `k = len(t) - 1` ***et avant l'itération d'indice*** `k = len(t)`***, donc*** $\mathscr{P}_{len(t)}$ ***est vraie ce qui se traduit par*** `t[0:len(t)]` ***est trié dans l'ordre croissant, ce qui prouve la correction de l'algorithme.***