Terminaison et correction

INFORMATIQUE COMMUNE - TP n° 2.1 - Olivier Reynet

À la fin de ce chapitre, je sais :

- ☞ programmer les algorithmes donnés en exemples.
- ☞ prouver la terminaison d'un algorithme simple.
- ☞ prouver la correction d'un algorithme simple.

A Terminaison

A1. Prouver la terminaison de l'algorithme 1 puis le traduire en Python.

Algorithme 1 Palindrome

```
Fonction PALINDROME(w)
    n ← la taille de la chaîne de caractères w
    i ← 0
    j ← n − 1
    tant que i < j répéter
        si w[i] = w[j] alors
            i ← i + 1
            j ← j − 1
        sinon
            renvoyer False
    renvoyer Vrai
```

A2. Prouver la terminaison de l'algorithme 2 puis le traduire en Python.

Algorithme 2 Est une puissance de deux

```
Fonction EST_PUISSANCE_DE_DEUX(n)
    si n < 2 alors
        renvoyer Faux
    sinon
        m ← n mod 2
        tant que m = 0 répéter
            n ← n//2
            m ← n mod 2
        renvoyer n = 1
```

Algorithme 3 Somme des n premiers entiers

```
Fonction INT_SUM(n)
    si n=0 alors
        renvoyer 0
    sinon
        renvoyer n + INT_SUM(n-1)
```

A3. Prouver la terminaison de l'algorithme récursif 3 puis le traduire en Python.

B Correction

B1. Prouver la correction partielle de l'algorithme 4 puis le traduire en Python en matérialisant l'invariant utilisé par des assertions.

Algorithme 4 Élément maximum d'un tableau

```
Fonction MAX(t)
    si t est vide alors
        renvoyer ∅
    sinon
        n ← la taille du tableau
        m = t[0]
        pour i = 1 à n − 1 répéter
            si m < t[i] alors
                m ← t[i]
        renvoyer m
```

B2. Prouver la correction partielle de l'algorithme de tri par sélection 5

Algorithme 5 Tri par sélection

```
Fonction TRIER_SELECTION(t)
    n ← taille(t)
    pour i de 0 à n − 1 répéter
        min_index ← i                          ▷ indice du prochain plus petit
        pour j de i + 1 à n − 1 répéter        ▷ pour tous les éléments non triés
            si t[j] < t[min_index ] alors
                min_index ← j                  ▷ c'est l'indice du plus petit non trié !
        échanger(t[i], t[min_index])           ▷ c'est le plus grand des triés !
```

B3. Prouver la correction de l'algorithme du tri par insertion 6.

C Algorithme d'Euclide du PGCD

On cherche à prouver la terminaison et la correction de l'algorithme d'Euclide 7. Dans ce but, on rappelle quelques éléments mathématiques importants.

Algorithme 6 Tri par insertion

```
Fonction INSERTION(t, i)
    à_insérer ← t[i]
    j ← i
    tant que t[j-1] > à_insérer et j>0  répéter
        t[j] ← t[j-1]                          ▷ faire monter les éléments
        j ← j-1
    t[j] ← à_insérer                           ▷ insertion de l'élément
Fonction TRIER_INSERTION(t)
    n ← taille(t)
    pour i de 1 à n-1 répéter
        INSERTION(t,i)
```

Algorithme 7 Algorithme d'Euclide (optimisé)

Fonction PGCD(a, b) ▷ On suppose pour simplifier que $a \in \mathbb{N}$, $b \in \mathbb{N}^\star$ et $b \leqslant a$.
    $r \leftarrow a \bmod b$
    tant que $r > 0$ **répéter** ▷ On connaît la réponse si r est nul.
        $a \leftarrow b$
        $b \leftarrow r$
        $r \leftarrow a \bmod b$
    renvoyer b ▷ Le pgcd est b

Théorème 1 — Division euclidienne . Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^\star$. Alors il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que les deux critères suivants sont vérifiés :

$$\begin{cases} a = bq + r \\ 0 \leqslant r < b \end{cases}$$

Démonstration.

1. Existence : a et b étant donné, on pose $q = \lfloor \frac{a}{b} \rfloor$. Par définition de partie entière, on a : $0 \leqslant \frac{a}{b} - \lfloor \frac{a}{b} \rfloor < 1$. En multipliant par b, on obtient : $0 \leqslant a - b \times \lfloor \frac{a}{b} \rfloor < b$. En choisissant donc $q = \lfloor \frac{a}{b} \rfloor$ et $r = a - b \times \lfloor \frac{a}{b} \rfloor$, on a bien :
$$\begin{cases} a = bq + r \\ 0 \leqslant r < b \end{cases}$$
2. Unicité : supposons que l'on ait deux couples (q, r) et (q', r') appartenant à $\mathbb{Z} \times \mathbb{N}$: $a = bq + r = bq' + r'$ avec $0 \leqslant r < b$ et $0 \leqslant r' < b$. Cela peut également s'écrire : $b(q' - q) = r - r'$. Or, on a l'encadrement $-b < r - r' < b$. On en conclut que $-b < b(q' - q) < b$ et donc que $-1 < q' - q < 1$. Mais q et q' sont des entiers d'après nos hypothèses de départ. Donc, on en déduit de $q' - q = 0$. Il s'en suit que $q = q'$ et que $r = r'$. Il s'agit donc bien du même couple.

■

Théorème 2 — Existence du PGCD. Parmi tous les diviseurs communs de deux entiers a et b non nuls, il y en a **un** qui est le plus grand. Ce dernier est nommé plus grand commun diviseur de a et de b. On le note PGCD(a, b).

Démonstration. Soit $a \in \mathbb{N}^\star$. Tous les diviseurs de a sont bornés par $|\, a\,|$. On peut tenir le même raisonnement pour ceux de b. Donc, parmi les diviseurs de a et de b, il y en a donc un plus grand. ■

Théorème 3 — Propriété du PGCD. Soit a et b deux entiers.

1. Si $b = 0$, alors $\text{PGCD}(a, b) = a$.
2. Si $b \neq 0$, alors $\text{PGCD}(a, b) = \text{PGCD}(b, a \mod b)$.

Démonstration. Démonstration de l'égalité de l'ensemble $\mathcal{D}_{ab}$ des diviseurs de a et de b et de l'ensemble $\mathcal{D}_{br}$ des diviseurs de b et de r par double inclusion.

$\mathcal{D}_{ab} \subset \mathcal{D}_{br}$: La division euclidienne étant unique comme nous l'avons montré au théorème 1, il existe un entier q tel que $a = qb + r$. Ce qui peut s'écrire : $a - qb = r$. Si γ est un diviseur de a et de b, alors on peut écrire : $a - bq = \gamma a' + \gamma b' q = \gamma(a' - b' q) = r$. On a donc montrer qu'un diviseur de a et de b est un diviseur de r.

$\mathcal{D}_{br} \subset \mathcal{D}_{ab}$: De même, si η est un diviseur de b et de r, alors on a : $a = bq + r = \eta(b'q + r')$, ce qui signifie que η est un diviseur de a.

Donc, $\mathcal{D}_{ab} = \mathcal{D}_{br}$. Ceci est vrai, y compris pour le plus grand des diviseurs de a et de b. ■

■ **Définition 1 — Suite des restes de la division euclidienne.** Soient a et b des entiers. On définit la suite des restes de la division euclidienne comme suit :

$$r_0 = |\, a\,| \tag{1}$$
$$r_1 = |\, b\,| \tag{2}$$
$$q_k = \lfloor r_{k-1} / r_k \rfloor, 1 \leqslant k \leqslant n \tag{3}$$

Alors on a :

$$r_{k-1} = q_k r_k + r_{k+1} \tag{4}$$
$$r_{k+1} = r_{k-1} \mod r_k \tag{5}$$

Théorème 4 — Stricte décroissance de $(r_n)_{n\in\mathbb{N}}$. La suite des restes de la division euclidienne est positive, strictement décroissante et minorée par zéro.

C1. Coder l'algorithme 7 en Python.

C2. Grâce au théorème 3, coder une version récursive de l'algorithme du PGCD.

```python
def rec_pgcd(a, b):
    if b == 0:
        return a
    else:
        return rec_pgcd(b, a % b)
```

C3. Donner une preuve du théorème 4.

C4. Montrer que r est un variant de boucle pour l'algorithme d'Euclide.

C5. Prouver la correction de l'algorithme d'Euclide.