

Correction TD1

MP2I Lycée Pierre de Fermat

Exercice 1.

Q1. ...

Q2. Soit $a \in \mathbb{N}^*$.

- Si a est pair, alors il existe $k \in \mathbb{N}^*$ tel que $a = 2k$. On a $\lfloor \frac{a}{2} \rfloor = \frac{a}{2} = k$, et $k < 2k = a$ car $k > 0$.
- Si a est impair, alors il existe $k \in \mathbb{N}^*$ tel que $a = 2k + 1$. On a $\lfloor \frac{a}{2} \rfloor = \frac{a-1}{2} = k$, et $k < 2k + 1 = a$.

D'où le résultat attendu.

Q3. Montrons que N est **positive**, **entière** et **strictement décroissante** lors de l'exécution de la boucle.

On pose $(N_k)_{k \in \mathbb{N}}, (r_k)_{k \in \mathbb{N}}, (X_k)_{k \in \mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ les suites définies par : pour tout $k \in \mathbb{N}$, N_k est la valeur prise par N après k tours de boucle (idem pour r_k et X_k). Notons que x et n sont des constantes lors de l'algorithme car elles ne sont jamais modifiées.

- Positive et entière : montrons par récurrence que $\forall k \in \mathbb{N}, P(k)$: “Si la boucle fait k passages, $N_k \in \mathbb{N}$.”
 - Initialisation ($k = 0$) : $N_0 = n \in \mathbb{N}$ par précondition de l'algorithme. D'où $P(0)$
 - Hérédité : soit $k \in \mathbb{N}$ tel que $P(k)$. On suppose que la boucle fait $k + 1$ passages. Alors $N_k > 0$ par condition de boucle. De plus, $N_{k+1} = \lfloor \frac{N_k}{2} \rfloor$, donc N_{k+1} est un entier, et est positive car N_k l'est (par HR). D'où $P(k + 1)$.

Par récurrence, N reste bien entière positive au long de la boucle.

- Décroissance stricte : Pour $k \in \mathbb{N}$ tel que la boucle fait au moins $k + 1$ tours, on a $N_k > 0$ par condition de boucle, et $N_{k+1} = \lfloor \frac{N_k}{2} \rfloor$. En appliquant la Q2, on a directement que $N_{k+1} < N_k$.

Ainsi, N est bien un variant de la boucle, et l'algorithme termine.

Q4. La correction de l'algorithme peut s'exprimer par : “A la fin de l'exécution, $r = x^n$.”

Q5. Ce n'est pas un invariant de boucle : par exemple pour $x = 2$ et $n = 9$, en entrée de boucle on a $r = 1 \neq 512 = x^n$.

Q6. On propose $rX^N = x^n$. On peut voir dans le tableau d'exécution que le terme X^N est toujours exactement le facteur qui manque pour avoir $r = x^n$.

Q7. Montrons par récurrence que $\forall k \in \mathbb{N}, P(k)$: “Si la boucle fait k passages, $r_k X_k^{N_k} = x^n$.”

- Initialisation ($k = 0$) : Les valeurs initiales des variables sont :

- $r_0 = 1$
- $X_0 = x$
- $N_0 = n$

On a bien $r_0 X_0^{N_0} = x^n$.

— Hérédité : Soit $k \in \mathbb{N}$ tel que $P(k)$. On suppose que l'on fait $k + 1$ tours de boucles. Alors, on distingue deux cas :

- Si N_k est pair, alors :

$$\circ r_{k+1} = r_k \qquad \circ X_{k+1} = X_k^2 \qquad \circ N_{k+1} = \frac{N_k}{2}$$

Ainsi :

$$\begin{aligned} r_{k+1} X_{k+1}^{N_{k+1}} &= r_k (X_k^2)^{\frac{N_k}{2}} \\ &= r_k X_k^{N_k} \\ &= x_n \end{aligned} \quad \text{par HR}$$

- Si N_k est impair, alors :

$$\circ r_{k+1} = r_k X_k \qquad \circ X_{k+1} = X_k^2 \qquad \circ N_{k+1} = \frac{N_k - 1}{2}$$

Ainsi :

$$\begin{aligned} r_{k+1} X_{k+1}^{N_{k+1}} &= r_k X_k (X_k^2)^{\frac{N_k - 1}{2}} \\ &= r_k X_k^{1 + N_k - 1} \\ &= r_k X_k^{N_k} \\ &= x_n \end{aligned} \quad \text{par HR}$$

Finalement, dans les deux cas, $P(k + 1)$ est vraie.

Par récurrence, $r X^N = x^n$ est bien un invariant de la boucle.

Q8. En particulier, l'invariant montré à la question précédente reste vrai en sortie de boucle. A ce moment, on a $N \leq 0$ par condition de boucle, mais on sait que $N \geq 0$ car c'est un variant. Donc, $N = 0$, et alors $r X^0 = x^n$, soit $r = x^n$.

L'algorithme est bien totalement correct

Exercice 2.

Q1. ...

Q2. Aucun des deux n'est un variant de boucle. n décroît un tour sur 2, et pareil pour N .

Q3. Pour $k \in \mathbb{N}$ un nombre de tours valide, posons N_k la valeur de N après k tours de boucle, et n_k celle de n . Montrons par récurrence que $\forall k \in \mathbb{N}, N_k \geq n_k$:

— Initialisation ($k = 0$) : $N_0 = n_0 + 1 \geq n_0$, la propriété est vraie pour $k = 0$.

— Hérédité : Soit $k \in \mathbb{N}$ tel que $N_k \geq n_k$ et tel que l'on fait un $k + 1$ -ème passage. On distingue deux cas :

- Si $n_k = N_k$, alors $n_{k+1} = n_k - 1$ et $N_{k+1} = N_k$.

Donc, $N_{k+1} = N_k \geq n_k \geq n_k - 1 = n_{k+1}$.

- Sinon, alors $n_k \neq N_k$, et comme par HR $N_k \geq n_k$, on a même $N_k > n_k$.

Dans ce cas, $n_{k+1} = n_k$ et $N_{k+1} = N_k - 1$. Donc :

$N_{k+1} = N_k - 1 > n_k - 1$, et comme ce sont des entiers, $N_{k+1} \geq n_k = n_{k+1}$.

La propriété se conserve au rang $k + 1$.

Q4. Il est clair n et N sont entières, car leurs valeurs initiales sont entières et que l'on ne leur applique que des opérations entières. Donc $n + N$ est un **entier**.

De plus, nous avons vu que n et N décroissent un tour sur deux, en alternant. Autrement dit, pour $k \in \mathbb{N}$ tel que $k+1$ est un nombre valide de tours, on a $n_{k+1} + N_{k+1} = n_k + N_k - 1$. Donc $n + N$ est **strictement décroissant**.

Enfin, puisque n décroît d'au plus 1 à chaque tour, et que la condition de boucle est $n > 0$, on a toujours $n \geq 0$ tout au long de l'exécution. Comme on sait aussi que $N \geq n$ est un invariant de boucle, cela assure que $n + N \geq 2n \geq 0$: $n + N$ est **positif**.

$n + N$ est bien un variant de boucle.

Exercice 3.

Montrons que $b + c - i$ est un variant de boucle.

- Entier : a, b, c étant des entiers, et i prenant les valeurs $a, a + c, a + 2c, \dots$, il est clair que $b + c - i$ reste entier tout au long de la boucle.
- Strictement décroissant : i est strictement croissant car il augmente de c à chaque tour, et b, c sont des constantes. Donc $b + c - i$ est strictement décroissant.
- Positivité : Soit k le plus petit entier tel que $a + kc > b$. La valeur maximale prise par i est précisément $a + kc$, suite à quoi la condition de boucle devient fausse. De plus, par définition de k , on a $a + (k - 1)c \leq b$, d'où $a + kc \leq b + c$. Donc, $i \leq b + c$ est un invariant de boucle, i.e. $b + c - i \geq 0$.

La boucle admet un variant, elle termine bien.

Exercice 4.

Q1. Ne pas oublier les assertions !

```
1  /* Renvoie le plus grand commun diviseur à a et b.
2     a et b doivent être positifs, et au moins l'un
3     doit être non-nul */
4  int pgcd(int a, int b){
5     assert(a >= 0 && b >= 0); // positifs
6     assert(a != 0 || b != 0); // entrée différente de (0, 0)
7     int A = a;
8     int B = b;
9     while (B != 0){
10        int r = A % B;
11        A = B;
12        B = r;
13    }
14    return A;
15 }
```

Q2. ..

Q3. Si on veut faire très proprement cette question, il faut se rendre compte que A et B sont liées, et qu'on ne peut pas juste montrer que r est un entier positif, il faut montrer

que A et B le sont, en même temps !

Posons, pour $k \in \mathbb{N}$, A_k la valeur de A après k tours de boucles, et B_k celle de B (lorsque c'est bien défini).

- Entier : montrons par récurrence que $\forall k \in \mathbb{N}$, $P(k)$: “ A_k et B_k sont des entiers.”
 - Initialisation : $A_0 = a$, $B_0 = b$, donc par précondition ce sont bien des entiers.
 - Hérédité : Soit $k \in \mathbb{N}$ tel que $P(k)$. Supposons que l'on fait $k + 1$ passages de boucle. On a $A_{k+1} = B_k$ et $B_{k+1} = A_k \bmod A_k$. Par HR, A_k et B_k sont des entiers, donc A_{k+1} et B_{k+1} aussi.
- Positif : une récurrence analogue à la précédente montre que A et B restent positifs au cours de la boucle.
- Strictement décroissant : Nous avons noté que pour $k \in \mathbb{N}$ tel que la boucle fait $k + 1$ tours, $B_{k+1} = A_k \bmod B_k < B_k$ (par définition du reste euclidien). Donc B prend des valeurs strictement décroissantes.

B est bien un variant de boucle, assurant la terminaison.

Q4. Montrons que “ $\mathbf{PGCD}(A, B) = \mathbf{PGCD}(a, b)$ ” est un IdB. On montre donc par récurrence que pour $k \in \mathbb{N}$, on a $\mathbf{PGCD}(A_k, B_k) = \mathbf{PGCD}(a, b)$.

- Initialisation ($k = 0$) : $A_0 = a$ et $B_0 = b$, donc $P(0)$ est trivialement vraie.
- Hérédité : soit $k \in \mathbb{N}$ tel que $P(k)$, et tel que la boucle fait $+1$ passages. Alors $B_k \neq 0$ par condition de boucle, et est positif car c'est un variant, donc le reste modulo B_k est bien défini, et on a $A_{k+1} = B_k$ et $B_{k+1} = A_k \bmod B_k$. D'après la propriété donnée dans l'énoncé de la question, on a donc $\mathbf{PGCD}(A_{k+1}, B_{k+1}) = \mathbf{PGCD}(A_k, B_k)$, et par HR on aussi $\mathbf{PGCD}(A_k, B_k) = \mathbf{PGCD}(a, b)$, d'où $P(k + 1)$.

Finalement, $\mathbf{PGCD}(A, B) = \mathbf{PGCD}(a, b)$ est bien un invariant. En particulier, en sortie de boucle, on a $B = 0$, ce qui donne $\mathbf{PGCD}(A, B) = \mathbf{PGCD}(a, b)$, soit $A = \mathbf{PGCD}(a, b)$. Or l'algorithme renvoie A , il correspond donc bien à la spécification attendue. Comme de plus il termine, il est totalement correct.

Exercice 5.

Q1. En suivant les indications données, on teste tous les éléments en gardant en mémoire l'indice du plus petit :

Algorithme 1 : indice_min($n, x_0, \dots, x_{n-1}$)

Entrée(s) : $n \in \mathbb{N}^*$, $x_0, \dots, x_{n-1} \in R$

Sortie(s) : $i_0 \in \llbracket 0, n - 1 \rrbracket$ tel que $x_{i_0} = \min\{x_0, \dots, x_{n-1}\}$

```

1  $i_0 \leftarrow 0$  // indice du min
2  $i \leftarrow 1$  // indice de parcours
3 tant que  $i < n$  faire
4   si  $x_i < x_{i_0}$  alors
5      $i_0 \leftarrow i$ ;
6    $i \leftarrow i + 1$ ;
7 retourner  $i_0$ 
```

Q2. La boucle Tant Que est en réalité une boucle “Pour i allant de 1 à $n - 1$ ”, et termine donc forcément. Alternativement, on peut dire que $n - i$ est un variant de boucle.

Q3. A chaque fois que l'on passe sur la condition de boucle, on a essayé tous les éléments entre 0 et $i - 1$ (on n'a pas encore testé i). De plus, i_0 est sensé être l'indice du plus petit élément vu jusqu'à maintenant. Si l'on exprime cela plus mathématiquement, on obtient un bon invariant :

$$\forall j \in \llbracket 0, i - 1 \rrbracket, x_j \geq x_{i_0}$$

Reste à le montrer. On pose, pour $k \in \mathbb{N}$, i^k la valeur de i après k passages de boucles, et i_0^k celle de i_0 (on note les indices de suites en exposant pour éviter la confusion entre i^0 et i_0

Montrons par récurrence que pour tout $k \in \mathbb{N}$, on a $P(k)$: si la boucle fait k passages, alors :

$$\forall j \in \llbracket 0, i^k - 1 \rrbracket, x_j \geq x_{i_0^k}$$

- Initialisation : $i^0 = 1$ et $i_0^0 = 0$. L'intervalle $\llbracket 0, i^0 - 1 \rrbracket$ est réduit à $\{0\}$, et la propriété est donc vérifiée : on a bien $x_0 \leq x_0$.
- Hérédité : Soit $k \in \mathbb{N}$, supposons que $P(k)$ est vraie et que l'on fait un $k + 1$ -ème passage. On a $i^{k+1} = i^k + 1$, et on distingue deux cas :

- Si $x_{i^k} < x_{i_0^k}$, alors $i_0^{k+1} = i^k$. Soit $j \in \llbracket 0, i^{k+1} - 1 \rrbracket$.
 - Si $j < i^k$, alors par HR, $x_j \geq x_{i_0^k}$, donc $x_j \geq x_{i^k} = x_{i_0^{k+1}}$.
 - Si $j = i^k$, alors clairement $x_j \geq x_{i^k} = x_{i_0^{k+1}}$.

Dans tous les cas, $x_j \geq x_{i_0^{k+1}}$, d'où $P(k + 1)$.

- Sinon, alors $x_{i^k} \geq x_{i_0^k}$, et $i_0^{k+1} = i_0^k$. Soit $j \in \llbracket 0, i^{k+1} - 1 \rrbracket$.
 - Si $j < i^k$, alors par HR, $x_j \geq x_{i_0^k} = x_{i_0^{k+1}}$.
 - Si $j = i^k$, alors $x_j \geq x_{i_0^k} = x_{i_0^{k+1}}$.

Dans tous les cas, $x_j \geq x_{i_0^{k+1}}$, d'où $P(k + 1)$.

D'où l'hérédité.

L'invariant annoncé a bien été montré. En sortie de boucle, on a $i = n$, et l'invariant dit alors exactement que x_{i_0} est inférieur ou égal à $x_0, x_1, \dots, x_{n-1}$. C'est bien l'élément minimal.

Exercice 6.

Q1. Les valeurs les plus simples ici sont $q \leftarrow 0$ et $r \leftarrow a$. Par précondition, on sait que $a \geq 0$, et on a bien $a = qb + r$.

Q2. Si les propriétés A et B proposées sont bien des invariants, alors il ne manque qu'une seule condition pour que le couple (q, r) soit bien la division euclidienne : il faut que $r < b$. On peut donc ajouter la condition opposée à la boucle :

```
1 tant que  $r \geq b$  faire
2    $\lfloor \dots$ ;
```

En sortie, la condition deviendra fausse, garantissant que la spécification est suivie.

Q3. Dans le corps de la boucle, on sait que $r \geq b$. Afin que r soit un variant, on souhaite pouvoir la faire décroître à chaque tour de boucle. On pourrait donc faire $r \leftarrow r - b$, ce qui préservera aussi le fait que r est positive. Pour compenser, il faut faire augmenter q de 1 :

```
1 tant que  $r \geq b$  faire
2    $r \leftarrow r - b$ ;
3    $q \leftarrow q + 1$ ;
```

Alors, r est bien un variant de boucle (positif, entier, strictement décroissant), et l'invariant A est clairement préservé car on a exactement compensé q et r .

Les preuves ne sont pas compliquées, on ne les détaille pas ici.