

VI. Invariants de boucles

1 Variants de boucles

Définition 1. On appelle variant d'une boucle une expression dont la valeur varie à chacune des itérations de la boucle.

Exemple 1. Calcul de la plus petite puissance de deux supérieure ou égale à un entier n .

Entrée: variable entière n
Sortie: variable entière p dont la valeur est égale à la plus petite puissance de deux supérieure ou égale à n

Début
 | $p \leftarrow 1$
 | **TantQue** $p < n$ **faire**
 | | $p \leftarrow 2p$
 | **FinTantQue**
Fin

Dans l'algorithme ci-dessus, p est un variant de la boucle **TantQue** car sa valeur (non nulle) est multipliée par 2 à chacune des itérations.

Un variant de boucle bien choisi permet de prouver qu'une boucle *tant que* se termine.

Exemple 2. Dans l'algorithme précédent, le variant de boucle non nul p est multiplié par 2 à chaque itération, il finit donc par devenir supérieur ou égal à n et la boucle **TantQue** se termine.

Exercice 1. On considère la fonction suivante qui permet de tester si une chaîne de caractères est un palindrome :

Fonction: $palindrome(m)$
Action: Teste si une chaîne de caractères m est un palindrome

Début
 | $i \leftarrow 0$
 | $j \leftarrow \text{longueur}(m) - 1$
 | **TantQue** $i \leq j$ **faire**
 | | **Si** $m_i = m_j$ **alors**
 | | | $i \leftarrow i + 1$
 | | | $j \leftarrow j - 1$
 | | **sinon**
 | | | **Renvoyer** *Faux*
 | | **FinSi**
 | **FinTantQue**
 | **Renvoyer** *Vrai*
Fin

1. Décrire au moyen d'un tableau indiquant l'évolution des valeurs des variables le fonctionnement de l'algorithme précédent pour la chaîne de caractères "sauras" puis pour la chaîne de caractères "radar".
2. Montrer que $\delta = j - i$ est un variant de la boucle **TantQue**.
3. En déduire que la boucle **TantQue** se termine.

2 Invariants de boucles

Définition 2. On appelle invariant d'une boucle une propriété qui si elle est vraie avant l'exécution d'une itération le demeure après l'exécution de l'itération.

Exemple 3. Calcul de 2^n .

Entrée: variable entière n
Sortie: variable entière p dont la valeur est égale à 2^n
Début
 | $p \leftarrow 1$
 | **Pour** k allant de 1 à n faire
 | | $p \leftarrow 2p$
 | **FinPour**
Fin

Dans l'algorithme ci-dessus, la propriété $p = 2^k$ est un invariant de la boucle Pour :

valeur de k	valeur de p
i	2^i
$i + 1$	$2 \times 2^i = 2^{i+1}$

Un invariant de boucle bien choisi permet de prouver qu'une boucle produit le résultat attendu.

Exemple 4. Dans l'algorithme précédent, p vaut $2 \times 1 = 2^1$ après la première itération, la propriété $p = 2^k$ est donc vraie après la première itération et le demeure donc après l'exécution de la n -ième itération, on en déduit qu'à la fin de l'algorithme p vaudra 2^n .

Remarque 1. Cette preuve est en fait un raisonnement par récurrence avec initialisation, hérédité et conclusion.

Exercice 2. On considère la fonction suivante qui permet de calculer le quotient et le reste de la division euclidienne d'un entier positif par un entier strictement positif :

Fonction: $\text{division}(a, b)$
Action: Calcul du quotient q et du reste r de la division euclidienne de l'entier a par l'entier b
Début
 | $q \leftarrow 0$
 | $r \leftarrow a$
 | **TantQue** $r \geq b$ faire
 | | $q \leftarrow q + 1$
 | | $r \leftarrow r - b$
 | **FinTantQue**
 | **Renvoyer** q, r
Fin

1. Décrire le fonctionnement de l'algorithme pour l'entrée ($a = 17, b = 5$) au moyen d'un tableau indiquant l'évolution des valeurs des variables au fil des itérations.
2. Montrer que la boucle TantQue se termine en utilisant un variant de boucle.
3. Montrer que la propriété $a = bq + r$ est un invariant de la boucle TantQue, en déduire que l'algorithme produit le résultat attendu.

Exercices supplémentaires

Exercice 3. *Écrire un algorithme utilisant une boucle TantQue permettant d'afficher les carrés inférieurs ou égaux à un entier n donné puis montrer que la boucle TantQue se termine.*

Exercice 4. *Prouver que la boucle TantQue de l'algorithme de recherche par dichotomie dans un tableau trié se termine.*

Exercice 5. *Écrire un algorithme utilisant une boucle Pour permettant de calculer $n!$ puis montrer que l'algorithme produit le résultat attendu.*

Exercice 6. *Écrire un algorithme utilisant une boucle Pour permettant de calculer la somme des valeurs d'un tableau de nombres puis montrer que l'algorithme produit le résultat attendu.*

Exercice 7. *Prouver que la fonction palindrome de l'exercice 1 produit le résultat attendu.*

Exercice 8. *Prouver que l'algorithme de recherche par dichotomie dans un tableau trié produit le résultat attendu.*

Exercice 9. *Écrire un algorithme utilisant une boucle TantQue permettant de déterminer si un entier n strictement positif donné est une puissance entière de 2. Montrer que la boucle TantQue se termine puis que l'algorithme produit le résultat attendu.*

Réponses

1)	m	$i \leq j$	$m_i = m_j$	i	j
	sauras			0	5
		Vrai	Vrai	1	4
		Vrai	Vrai	2	3
	Vrai	Faux			

m	$i \leq j$	$m_i = m_j$	i	j
radar			0	4
	Vrai	Vrai	1	3
	Vrai	Vrai	2	2
	Vrai	Vrai	3	1
	Faux			

À chaque itération δ diminue de 2, il finit donc par devenir strictement négatif et la boucle *TantQue* se termine :

valeur de i	valeur de j	valeur de $\delta = j - i$
x	y	$y - x$
$x + 1$	$y - 1$	$(y - 1) - (x + 1) = y - x - 2$

2) •	q	r	$r \geq 5$
	0	17	Vrai
	1	12	Vrai
	2	7	Vrai
	3	2	Faux

- Le variant de boucle entier r diminue strictement à chaque itération car $b > 0$, il finit donc par devenir strictement inférieur à b et la boucle *TantQue* se termine.
- La valeur de $bq + r$ ne varie pas lors d'une itération :

valeur de q	valeur de r	valeur de $bq + r$
x	y	$bx + y$
$x + 1$	$y - b$	$b(x + 1) + (y - b) = bx + y$

De plus avant l'exécution de la boucle $bq + r$ vaut a , on en déduit qu'à la fin de l'algorithme $bq + r$ vaudra encore a avec $r < b$. En outre, la condition de la boucle *TantQue* impose également que r demeure positif ou nul.

3)

Entrée: variable entière n
Sortie: affichage des carrés inférieurs ou égaux à n
Début
 $k \leftarrow 0$
TantQue $k^2 \leq n$ **faire**
 Afficher k^2
 $k \leftarrow k + 1$
FinTantQue
Fin

Le variant de boucle entier k^2 augmente strictement à chaque itération, il finit donc par devenir strictement supérieur à n et la boucle *TantQue* se termine.

4)

Fonction: Indice(v, t)
Action: Détermination d'un indice d'occurrence d'une valeur v dans un tableau de nombres t trié en ordre croissant
Début
 $a \leftarrow 0$
 $b \leftarrow \text{longueur}(t) - 1$
TantQue $a \leq b$ **faire**
 $c \leftarrow \lfloor \frac{a+b}{2} \rfloor$
 Si $t_c = v$ **alors**
 Renvoyer c
 sinon
 Si $t_c < v$ **alors**
 $a \leftarrow c + 1$
 sinon
 $b \leftarrow c - 1$
 FinSi
 FinSi
FinTantQue
Renvoyer -1
Fin

En remarquant que pour x, y entiers avec $x \leq y$ on a $x \leq \lfloor \frac{x+y}{2} \rfloor \leq y$, on montre que le variant de boucle entier $b - a$ diminue strictement à chaque itération, il finit donc par devenir strictement négatif et la boucle *TantQue* se termine :

valeur de a	valeur de b	valeur de c	valeur de $b - a$
x	y	$\lfloor \frac{x+y}{2} \rfloor$	$y - x$
$\lfloor \frac{x+y}{2} \rfloor + 1$	y	$\lfloor \frac{x+y}{2} \rfloor$	$y - \lfloor \frac{x+y}{2} \rfloor - 1 \leq y - x - 1 < y - x$
valeur de a	valeur de b	valeur de c	valeur de $b - a$
x	y	$\lfloor \frac{x+y}{2} \rfloor$	$y - x$
x	$\lfloor \frac{x+y}{2} \rfloor - 1$	$\lfloor \frac{x+y}{2} \rfloor$	$\lfloor \frac{x+y}{2} \rfloor - 1 - x \leq y - 1 - x < y - x$

```

Entrée: variable entière  $n$ 
Sortie: variable entière  $p$  dont la valeur est égale à  $n!$ 
Début
5) |  $p \leftarrow 1$ 
    | Pour  $k$  allant de 1 à  $n$  faire
    | |  $p \leftarrow p \times k$ 
    | FinPour
    | Fin
    
```

On montre qu'à la fin de chaque itération p vaut $\prod_{i=1}^{i=k} i$.

```

Fonction: somme( $t$ )
Action: Calcul de la somme  $s$  des valeurs d'un tableau de nombres  $t$ 
Début
6) |  $s \leftarrow 0$ 
    | Pour  $k$  allant de 0 à longueur( $t$ ) - 1 faire
    | |  $s \leftarrow s + t_k$ 
    | FinPour
    | Renvoyer  $s$ 
    | Fin
    
```

On montre qu'à la fin de chaque itération s vaut $\sum_{i=0}^{i=k} t_i$.

- 7) On montre que $i + j$ demeure égal à longueur(m) - 1 puis que pour tout $k \in \llbracket 0; i - 1 \rrbracket$ on a m_k qui vaut $m_{\text{longueur}(m)-1-k}$.
- 8) On montre que la propriété « la valeur v est présente parmi les éléments de t d'indices compris entre a et b » est un invariant de boucle.

Si la boucle *TantQue* se termine, deux cas se présentent lors de la dernière étape :

- $c + 1 > b$ soit $c \geq b$ d'où a vaut b et donc v n'était pas présente dans le tableau.
- $c - 1 < a$ soit $c \leq a$ d'où a vaut b et donc v n'était pas présente dans le tableau.

```

Fonction: PuissanceDeux( $n$ )
Action: Détermine si l'entier  $n$  strictement positif est une puissance entière de 2
Début
9) |  $d \leftarrow n$ 
    | TantQue  $d$  divisible par 2 faire
    | |  $d \leftarrow \frac{d}{2}$ 
    | FinTantQue
    | Si  $d = 1$  alors
    | | Renvoyer Vrai
    | sinon
    | | Renvoyer Faux
    | FinSi
    | Fin
    
```

On considère comme variant de boucle l'exposant e de 2 dans la décomposition de d en produit de facteurs premiers. Si n est pair e est un entier non nul qui diminue de 1 à chaque itération, il finit donc par s'annuler donc d devient impair et la boucle *TantQue* se termine.

Si on note ϵ l'exposant de 2 dans la décomposition de n en produit de facteurs premiers, on vérifie que $d2^{\epsilon-e}$ demeure égal à n donc à la fin de l'algorithme comme e vaut 0 on en déduit que $d2^\epsilon$ vaut n or la valeur de d est impaire donc n est une puissance entière de 2 si et seulement si d vaut 1.