# Module EA4 – Éléments d'Algorithmique II Outils pour l'analyse des algorithmes

Dominique Poulalhon dominique.poulalhon@irif.fr

Université Paris Cité L2 Informatique & DL Bio-Info, Jap-Info, Math-Info Année universitaire 2023-2024

algorithme = méthode systématique pour résoudre un problème

algorithme = méthode systématique pour résoudre un problème

nécessite une preuve de correction : pour chaque entrée, l'algorithme doit terminer en produisant la bonne sortie

algorithme = méthode systématique pour résoudre un problème

nécessite une preuve de correction : pour chaque entrée, l'algorithme doit terminer en produisant la bonne sortie

il peut exister plusieurs algorithmes pour le même problème

algorithme = méthode systématique pour résoudre un problème

nécessite une preuve de correction : pour chaque entrée, l'algorithme doit terminer en produisant la bonne sortie

il peut exister plusieurs algorithmes pour le même problème

pour les comparer, il faut étudier leur complexité, à la fois en temps et en espace

suite définie par :  $F_0=0, \qquad F_1=1 \qquad \text{et} \qquad \forall n\geqslant 2, \ F_n=F_{n-1}+F_{n-2}$ 

suite définie par :  $F_0=0, \qquad F_1=1 \qquad \text{et} \qquad \forall n\geqslant 2, \ F_n=F_{n-1}+F_{n-2}$ 



suite définie par :  $F_0=0, \qquad F_1=1 \qquad \text{et} \qquad \forall n\geqslant 2, \ F_n=F_{n-1}+F_{n-2}$ 

Préambule: à quel point est-ce gros? 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, ...

• la suite  $(F_n)$  est positive, (preuve par récurrence)

suite définie par :  $F_0=0, \qquad F_1=1 \qquad \text{et} \qquad \forall n\geqslant 2, \ F_n=F_{n-1}+F_{n-2}$ 

- la suite  $(F_n)$  est positive, (preuve par récurrence)
- donc croissante :  $\forall n \geqslant 2, F_n = F_{n-1} + \underbrace{F_{n-2}}_{\geqslant 0} \geqslant F_{n-1}$

suite définie par :  $F_0=0$ ,  $F_1=1$  et  $\forall n\geqslant 2, \; F_n=F_{n-1}+F_{n-2}$ 

- la suite  $(F_n)$  est positive, (preuve par récurrence)
- donc croissante :  $\forall n \geqslant 2, F_n = F_{n-1} + F_{n-2}$  et  $F_{n-2} \geqslant 0$  donc  $F_n \geqslant F_{n-1}$
- donc:  $\forall n \ge 2$ ,  $F_n = F_{n-1} + F_{n-2} \ge 2F_{n-2}$

suite définie par :  $F_0 = 0$ ,  $F_1 = 1$  et  $\forall n \ge 2$ ,  $F_n = F_{n-1} + F_{n-2}$ 

- la suite  $(F_n)$  est positive, (preuve par récurrence)
- donc croissante :  $\forall n \geqslant 2, F_n = F_{n-1} + F_{n-2}$  et  $F_{n-2} \geqslant 0$  donc  $F_n \geqslant F_{n-1}$
- donc:  $\forall n \ge 2$ ,  $F_n = F_{n-1} + F_{n-2} \ge 2F_{n-2}$





suite définie par :  $F_0=0$ ,  $F_1=1$  et  $\forall n\geqslant 2, \ F_n=F_{n-1}+F_{n-2}$ 

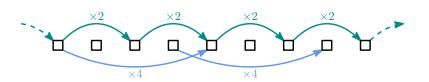
- la suite  $(F_n)$  est positive, (preuve par récurrence)
- donc croissante :  $\forall n \ge 2, F_n = F_{n-1} + F_{n-2}$  et  $F_{n-2} \ge 0$  donc  $F_n \ge F_{n-1}$
- donc:  $\forall n \ge 2$ ,  $F_n = F_{n-1} + F_{n-2} \ge 2F_{n-2}$





suite définie par :  $F_0 = 0$ ,  $F_1 = 1$  et  $\forall n \ge 2$ ,  $F_n = F_{n-1} + F_{n-2}$ 

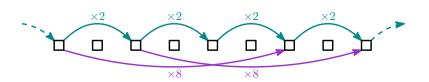
- la suite  $(F_n)$  est positive, (preuve par récurrence)
- donc croissante :  $\forall n \geqslant 2, F_n = F_{n-1} + F_{n-2}$  et  $F_{n-2} \geqslant 0$  donc  $F_n \geqslant F_{n-1}$
- donc:  $\forall n \ge 2$ ,  $F_n = F_{n-1} + F_{n-2} \ge 2F_{n-2}$





suite définie par :  $F_0 = 0$ ,  $F_1 = 1$  et  $\forall n \ge 2$ ,  $F_n = F_{n-1} + F_{n-2}$ 

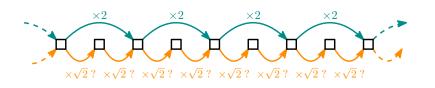
- la suite  $(F_n)$  est positive, (preuve par récurrence)
- donc croissante :  $\forall n\geqslant 2, F_n=F_{n-1}+F_{n-2}$  et  $F_{n-2}\geqslant 0$  donc  $F_n\geqslant F_{n-1}$
- donc:  $\forall n \ge 2$ ,  $F_n = F_{n-1} + F_{n-2} \ge 2F_{n-2}$





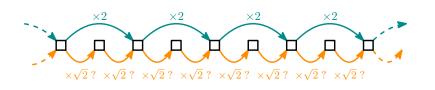
suite définie par :  $F_0=0$ ,  $F_1=1$  et  $\forall n\geqslant 2, \ F_n=F_{n-1}+F_{n-2}$ 

- la suite  $(F_n)$  est positive, (preuve par récurrence)
- donc croissante :  $\forall n \geqslant 2, F_n = F_{n-1} + F_{n-2}$  et  $F_{n-2} \geqslant 0$  donc  $F_n \geqslant F_{n-1}$
- donc:  $\forall n \ge 2$ ,  $F_n = F_{n-1} + F_{n-2} \ge 2F_{n-2}$



suite définie par :  $F_0=0$ ,  $F_1=1$  et  $\forall n\geqslant 2$ ,  $F_n=F_{n-1}+F_{n-2}$ 

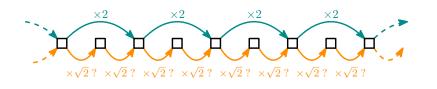
- la suite  $(F_n)$  est positive, (preuve par récurrence)
- donc croissante :  $\forall n \geqslant 2, F_n = F_{n-1} + F_{n-2}$  et  $F_{n-2} \geqslant 0$  donc  $F_n \geqslant F_{n-1}$
- donc :  $\forall n \ge 2$ ,  $F_n = F_{n-1} + F_{n-2} \ge 2F_{n-2}$
- (or  $F_6=8=2^{6/2}$  et  $F_7=13\geqslant 2^{7/2}$ ) donc :  $\forall n\geqslant 6,\ F_n\geqslant 2^{n/2}$





suite définie par :  $F_0=0$ ,  $F_1=1$  et  $\forall n\geqslant 2,\ F_n=F_{n-1}+F_{n-2}$ 

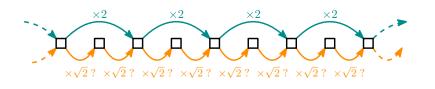
- la suite  $(F_n)$  est positive, (preuve par récurrence)
- donc croissante :  $\forall n \geqslant 2, F_n = F_{n-1} + F_{n-2}$  et  $F_{n-2} \geqslant 0$  donc  $F_n \geqslant F_{n-1}$
- donc:  $\forall n \ge 2$ ,  $F_n = F_{n-1} + F_{n-2} \ge 2F_{n-2}$
- (or  $F_6 = 8 = 2^{6/2}$  et  $F_7 = 13 \ge 2^{7/2}$ ) donc :  $\forall n \ge 6$ ,  $F_n \ge 2^{n/2}$
- donc  $\forall n \geq 6$ ,  $F_n$  a *au moins*  $\frac{n}{2}$  *chiffres* (en binaire)





suite définie par :  $F_0=0$ ,  $F_1=1$  et  $\forall n\geqslant 2, \; F_n=F_{n-1}+F_{n-2}$ 

- la suite  $(F_n)$  est positive, (preuve par récurrence)
- donc croissante :  $\forall n \geqslant 2, F_n = F_{n-1} + F_{n-2}$  et  $F_{n-2} \geqslant 0$  donc  $F_n \geqslant F_{n-1}$
- donc:  $\forall n \ge 2$ ,  $F_n = F_{n-1} + F_{n-2} \ge 2F_{n-2}$
- (or  $F_6 = 8 = 2^{6/2}$  et  $F_7 = 13 \ge 2^{7/2}$ ) donc :  $\forall n \ge 6$ ,  $F_n \ge 2^{n/2}$
- donc  $\forall n \ge 6$ ,  $F_n$  a *au moins*  $\frac{n}{2}$  *chiffres* (en binaire)
- similairement,  $F_n \leq 2^n$ , donc a *au plus* n *chiffres* (en binaire)





suite définie par :  $F_0=0$ ,  $F_1=1$  et  $\forall n\geqslant 2, \; F_n=F_{n-1}+F_{n-2}$ 

Préambule: à quel point est-ce gros? 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, ...

- la suite  $(F_n)$  est positive, (preuve par récurrence)
- donc croissante :  $\forall n \geqslant 2, F_n = F_{n-1} + F_{n-2}$  et  $F_{n-2} \geqslant 0$  donc  $F_n \geqslant F_{n-1}$
- donc:  $\forall n \ge 2$ ,  $F_n = F_{n-1} + F_{n-2} \ge 2F_{n-2}$
- (or  $F_6 = 8 = 2^{6/2}$  et  $F_7 = 13 \ge 2^{7/2}$ ) donc :  $\forall n \ge 6$ ,  $F_n \ge 2^{n/2}$
- donc  $\forall n \geq 6$ ,  $F_n$  a *au moins*  $\frac{n}{2}$  *chiffres* (en binaire)
- similairement,  $F_n \leq 2^n$ , donc a *au plus* n *chiffres* (en binaire)

Donc  $F_{1\,000\,000}$  a entre 500 000 et 1 000 000 chiffres en binaire, soit (environ) entre 150 000 et 300 000 chiffres en décimal



suite définie par :  $F_0=0$ ,  $F_1=1$  et  $\forall n\geqslant 2, \; F_n=F_{n-1}+F_{n-2}$ 

Préambule: à quel point est-ce gros? 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, ...

- la suite  $(F_n)$  est positive, (preuve par récurrence)
- donc croissante :  $\forall n \geqslant 2, F_n = F_{n-1} + F_{n-2}$  et  $F_{n-2} \geqslant 0$  donc  $F_n \geqslant F_{n-1}$
- donc:  $\forall n \ge 2$ ,  $F_n = F_{n-1} + F_{n-2} \ge 2F_{n-2}$
- (or  $F_6 = 8 = 2^{6/2}$  et  $F_7 = 13 \ge 2^{7/2}$ ) donc :  $\forall n \ge 6$ ,  $F_n \ge 2^{n/2}$
- donc  $\forall n \geq 6$ ,  $F_n$  a *au moins*  $\frac{n}{2}$  *chiffres* (en binaire)
- similairement,  $F_n \leq 2^n$ , donc a *au plus* n *chiffres* (en binaire)

Donc  $F_{1\,000\,000}$  a entre 500 000 et 1 000 000 chiffres en binaire, soit (environ) entre 150 000 et 300 000 chiffres en décimal

Plus précisément, on peut montrer (admis):

$$F_n \sim \varphi^n$$
, avec  $\varphi = \frac{1+\sqrt{5}}{2} \approx 1.618$  (« nombre d'or »)



suite définie par :  $F_0=0, \qquad F_1=1 \qquad \text{et} \qquad \forall n\geqslant 2, \ F_n=F_{n-1}+F_{n-2}$ 

suite définie par :  $F_0=0, \qquad F_1=1 \qquad \text{et} \qquad \forall n\geqslant 2, \ F_n=F_{n-1}+F_{n-2}$ 

1 utiliser directement la définition par récurrence

```
def fibo_1(n) :
   if n <= 0 : return 0
   if n <= 2 : return 1
   return fibo_1(n-1) + fibo_1(n-2)</pre>
```



suite définie par :  $F_0=0, \qquad F_1=1 \qquad \text{et} \qquad \forall n\geqslant 2, \ F_n=F_{n-1}+F_{n-2}$ 

1 utiliser directement la définition par récurrence

```
def fibo_1(n) :
   if n <= 0 : return 0
   if n <= 2 : return 1
   return fibo_1(n-1) + fibo_1(n-2)</pre>
```

#### Preuve de terminaison : par récurrence (forte)

- cas de base : si  $n \leq 2$ , fibo\_1(n) termine
- hérédité: soit n ≥ 2 t.q. fibo\_1(k) termine pour tout k < n</li>
   alors fibo\_1(n-1) et fibo\_1(n-2) terminent, donc fibo\_1(n)
   termine

donc fibo\_1(n) termine pour tout n

suite définie par :  $F_0=0, \quad F_1=1 \quad \text{et} \quad \forall n\geqslant 2, \ F_n=F_{n-1}+F_{n-2}$ 

1 utiliser directement la définition par récurrence

```
def fibo_1(n) :
   if n <= 0 : return 0
   if n <= 2 : return 1
   return fibo_1(n-1) + fibo_1(n-2)</pre>
```

#### Preuve de correction : par récurrence (forte)

- cas de base : si  $n \le 2$ , fibo\_1(n) retourne  $F_n$
- hérédité: soit n ≥ 2 t.q. fibo\_1(k) retourne F<sub>k</sub> pour tout k < n alors fibo\_1(n) retourne</li>
   fibo\_1(n-1) + fibo\_1(n-2) = F<sub>n-1</sub> + F<sub>n-2</sub> = F<sub>n</sub>

donc fibo\_1(n) retourne  $F_n$  pour tout n



suite définie par :  $F_0=0, \qquad F_1=1 \qquad \text{et} \qquad \forall n\geqslant 2, \ F_n=F_{n-1}+F_{n-2}$ 

1 utiliser directement la définition par récurrence

```
def fibo_1(n) :
   if n <= 0 : return 0
   if n <= 2 : return 1
   return fibo_1(n-1) + fibo_1(n-2)</pre>
```

(gros) inconvénient : recalcul permanent de valeurs déjà calculées



suite définie par :  $F_0=0, \qquad F_1=1 \qquad \text{et} \qquad \forall n\geqslant 2, \ F_n=F_{n-1}+F_{n-2}$ 

- 1 utiliser directement la définition par récurrence
- 2 garder un tableau de toutes les premières valeurs

```
def fibo_2(n) :
   if n <= 0 : return 0
   liste = [0, 1] + [0] * (n-1)
   for i in range(2, n+1) :
      liste[i] = liste[i-1] + liste[i-2]
   return liste[n]</pre>
```

(on appelle cette technique « programmation dynamique »)

suite définie par :  $F_0=0, \qquad F_1=1 \qquad \text{et} \qquad \forall n\geqslant 2, \ F_n=F_{n-1}+F_{n-2}$ 

- 1 utiliser directement la définition par récurrence
- 2 garder un tableau de toutes les premières valeurs
- 3 garder seulement les deux dernières valeurs

```
def fibo_3(n) :
   if n <= 0 : return 0
   previous, last = 0, 1
   for i in range(2, n+1) :
      previous, last = last, previous + last
   return last</pre>
```



suite définie par :  $F_0=0, \qquad F_1=1 \qquad \text{et} \qquad \forall n\geqslant 2, \ F_n=F_{n-1}+F_{n-2}$ 

- 1 utiliser directement la définition par récurrence
- 2 garder un tableau de toutes les premières valeurs
- 3 garder seulement les deux dernières valeurs

```
def fibo_3(n) :
   if n <= 0 : return 0
   previous, last = 0, 1
   for i in range(2, n+1) :
      previous, last = last, previous + last
   return last</pre>
```

Preuve de terminaison : n-1 tours de boucle



suite définie par :  $F_0=0, \qquad F_1=1 \qquad \text{et} \qquad \forall n\geqslant 2, \ F_n=F_{n-1}+F_{n-2}$ 

- 1 utiliser directement la définition par récurrence
- 2 garder un tableau de toutes les premières valeurs
- 3 garder seulement les deux dernières valeurs

```
def fibo_3(n) :
   if n <= 0 : return 0
   previous, last = 0, 1
   for i in range(2, n+1) :
      previous, last = last, previous + last
   return last</pre>
```

```
Preuve de correction : à l'aide de l'invariant : 

« après le tour de boucle d'indice i, previous = F_{i-1} et last = F_i »
```



suite définie par : 
$$F_0=0$$
,  $F_1=1$  et  $\forall n\geqslant 2, \; F_n=F_{n-1}+F_{n-2}$ 

- 1 utiliser directement la définition par récurrence
- 2 garder un tableau de toutes les premières valeurs
- 3 garder seulement les deux dernières valeurs

$$\textbf{4} \text{ utiliser}: \forall n \geqslant 2, \ \begin{bmatrix} F_n \\ F_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} F_{n-1} \\ F_{n-2} \end{bmatrix}$$



suite définie par : 
$$F_0=0$$
,  $F_1=1$  et  $\forall n\geqslant 2, \; F_n=F_{n-1}+F_{n-2}$ 

- 1 utiliser directement la définition par récurrence
- 2 garder un tableau de toutes les premières valeurs
- 3 garder seulement les deux dernières valeurs

$$\textbf{4} \text{ utiliser}: \forall n \geqslant 2, \begin{bmatrix} F_n \\ F_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} F_{n-1} \\ F_{n-2} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{n-1} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$



suite définie par : 
$$F_0=0$$
,  $F_1=1$  et  $\forall n\geqslant 2, \; F_n=F_{n-1}+F_{n-2}$ 

- 1 utiliser directement la définition par récurrence
- 2 garder un tableau de toutes les premières valeurs
- 3 garder seulement les deux dernières valeurs

$$\textbf{4} \text{ utiliser}: \forall n \geqslant 2, \ \begin{bmatrix} F_n \\ F_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} F_{n-1} \\ F_{n-2} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{n-1} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

ou encore : 
$$\forall n\geqslant 2, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{n-1} = \begin{bmatrix} F_n & F_{n-1} \\ F_{n-1} & F_{n-2} \end{bmatrix}$$



suite définie par : 
$$F_0=0$$
,  $F_1=1$  et  $\forall n\geqslant 2, \; F_n=F_{n-1}+F_{n-2}$ 

- 1 utiliser directement la définition par récurrence
- 2 garder un tableau de toutes les premières valeurs
- 3 garder seulement les deux dernières valeurs

4 utiliser: 
$$\forall n \geqslant 2$$
,  $\begin{bmatrix} F_n \\ F_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} F_{n-1} \\ F_{n-2} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{n-1} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ 

ou encore :  $\forall n\geqslant 2,\; \begin{bmatrix}1&1\\1&0\end{bmatrix}^{n-1}=\begin{bmatrix}F_n&F_{n-1}\\F_{n-1}&F_{n-2}\end{bmatrix}$ 

```
def fibo_4(n) :
   if n <= 0 : return 0
   M = puissance_matrice_2_2 ([ [1, 1], [1, 0] ], n-1)
   return M[0][0]</pre>
```

suite définie par : 
$$F_0=0$$
,  $F_1=1$  et  $\forall n\geqslant 2, \; F_n=F_{n-1}+F_{n-2}$ 

- 1 utiliser directement la définition par récurrence
- 2 garder un tableau de toutes les premières valeurs
- 3 garder seulement les deux dernières valeurs
- 4 calculer  $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{n-1}$  par exponentiation binaire

suite définie par : 
$$F_0=0$$
,  $F_1=1$  et  $\forall n\geqslant 2, \; F_n=F_{n-1}+F_{n-2}$ 

- 1 utiliser directement la définition par récurrence
- 2 garder un tableau de toutes les premières valeurs
- 3 garder seulement les deux dernières valeurs
- 4 calculer  $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{n-1}$  par exponentiation binaire

Lemme: les 4 algorithmes sont corrects



suite définie par : 
$$F_0=0$$
,  $F_1=1$  et  $\forall n\geqslant 2, \; F_n=F_{n-1}+F_{n-2}$ 

- 1 utiliser directement la définition par récurrence
- 2 garder un tableau de toutes les premières valeurs
- 3 garder seulement les deux dernières valeurs
- 4 calculer  $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{n-1}$  par exponentiation binaire

Lemme: les 4 algorithmes sont corrects

Quelle est la meilleure méthode?



# Complexité en espace

= quantité de mémoire nécessaire pour effectuer le calcul

# Complexité en espace

= quantité de mémoire nécessaire pour effectuer le calcul

mémoire *incompressible* : nécessaire pour stocker les données et le résultat

mémoire *auxiliaire* : pour les calculs intermédiaires

#### Complexité en espace

= quantité de mémoire nécessaire pour effectuer le calcul

mémoire *incompressible* : nécessaire pour stocker les données et le résultat

mémoire *auxiliaire* : pour les calculs intermédiaires

pour comparer entre eux des algorithmes résolvant le même problème, seule la mémoire *auxiliaire* est pertinente

```
def fibo_2(n) :
   if n <= 0 : return 0
   liste = [0, 1] + [0] * (n-1)
   for i in range(2, n+1) :
     liste[i] = liste[i-1] + liste[i-2]
   return liste[n]</pre>
```

utilise un *tableau de* n *(grands) entiers* pour en calculer un seul (plus un (petit <sup>1</sup>) entier comme indice de boucle)

<sup>1.</sup> petit = valeur de l'ordre de n vs grand = de l'ordre de n chiffres

```
def fibo_2(n) :
   if n <= 0 : return 0
   liste = [0, 1] + [0] * (n-1)
   for i in range(2, n+1) :
     liste[i] = liste[i-1] + liste[i-2]
   return liste[n]</pre>
```

utilise un *tableau de* n *(grands) entiers* pour en calculer un seul (plus un (petit <sup>1</sup>) entier comme indice de boucle)

donc la place nécessaire est (à peu près) la somme des tailles des n valeurs calculées, donc (supérieure à)  $\sum_{i=0}^n \frac{i}{2} = \frac{n(n+1)}{4}$  bits

(soit à peu près 250 000 000 000 bits pour  $n = 1\,000\,000$ , c'est-à-dire 30 Go)

<sup>1.</sup> petit = valeur de l'ordre de n vs grand = de l'ordre de n chiffres

```
def fibo_3(n) :
   if n <= 0 : return 0
   previous, last = 0, 1
   for i in range(2, n+1) :
     previous, last = last, previous + last
   return last</pre>
```

utilise seulement une variable auxiliaire de type (grand) entier (plus un (petit) entier comme indice de boucle)

```
def fibo_3(n) :
   if n <= 0 : return 0
   previous, last = 0, 1
   for i in range(2, n+1) :
     previous, last = last, previous + last
   return last</pre>
```

utilise seulement une variable auxiliaire de type (grand) entier (plus un (petit) entier comme indice de boucle)

 $\implies$  on peut envisager d'utiliser fibo\_3 pour calculer  $F_{106}$ , contrairement à fibo\_2

# Complexité en temps

= temps nécessaire pour mener le calcul à son terme

#### Complexité en temps

= temps nécessaire pour mener le calcul à son terme

plus difficile à quantifier précisément, essentiellement car ce temps dépend de la machine utilisée

#### Complexité en temps

= temps nécessaire pour mener le calcul à son terme

plus difficile à quantifier précisément, essentiellement car ce temps dépend de la machine utilisée

convention : on estime ce temps par le *nombre d'opérations élémentaires effectuées* : sur une machine donnée, le temps d'exécution sera (à peu près) proportionnel à ce nombre

opération élémentaire = opération dont le temps d'exécution peut être considéré comme constant

exemple : affectation, comparaison, opération arithmétique (sur des nombres de taille bornée)...

Nombre de cycles effectués par un processeur monocœur à 1 GHz :

en 1 seconde	109
en 1 heure	$3 \cdot 10^{12}$
en 1 jour	9 · 10 <sup>13</sup>
en 1 an	3 · 10 <sup>16</sup>
en $13, 8 \cdot 10^9$ années	4 · 10 <sup>26</sup>

(pour un quadricœur à 2.5GHz, rajouter juste un zéro)



n	10	100	10 <sup>3</sup>	10 <sup>6</sup>	109	10 <sup>12</sup>
log <sub>2</sub> n	4	7	10	20	30	40
10n	100	10 <sup>3</sup>	10 <sup>4</sup>	10 <sup>7</sup>	1010	10 <sup>13</sup>
n log <sub>2</sub> n	34	665	10 <sup>4</sup>	2 · 10 <sup>7</sup>	3 · 10 <sup>10</sup>	$4 \cdot 10^{13}$
n <sup>2</sup>	100	10 <sup>4</sup>	10 <sup>6</sup>	10 <sup>12</sup>	10 <sup>18</sup>	10 <sup>24</sup>
$n^3$	10 <sup>3</sup>	10 <sup>6</sup>	109	10 <sup>18</sup>	10 <sup>27</sup>	10 <sup>36</sup>
2 <sup>n</sup>	10 <sup>3</sup>	10 <sup>30</sup>	10 <sup>301</sup>	•••	•••	•••

(rappel : en 1 an, un processeur à 1 GHz effectue  $3 \cdot 10^{16}$  cycles)

n	10	100	10 <sup>3</sup>	10 <sup>6</sup>	109	10 <sup>12</sup>
log <sub>2</sub> n	4	7	10	20	30	40
10n	100	10 <sup>3</sup>	10 <sup>4</sup>	10 <sup>7</sup>	1010	10 <sup>13</sup>
n log <sub>2</sub> n	34	665	10 <sup>4</sup>	2 · 10 <sup>7</sup>	3 · 10 <sup>10</sup>	$4 \cdot 10^{13}$
n <sup>2</sup>	100	10 <sup>4</sup>	10 <sup>6</sup>	10 <sup>12</sup>	10 <sup>18</sup>	10 <sup>24</sup>
n <sup>3</sup>	10 <sup>3</sup>	10 <sup>6</sup>	109	10 <sup>18</sup>	10 <sup>27</sup>	10 <sup>36</sup>
2 <sup>n</sup>	10 <sup>3</sup>	10 <sup>30</sup>	10 <sup>301</sup>	•••	•••	•••

n	10	100	10 <sup>3</sup>	10 <sup>6</sup>	109	10 <sup>12</sup>
log <sub>2</sub> n	4	7	10	20	30	40
10n	100	10 <sup>3</sup>	10 <sup>4</sup>	10 <sup>7</sup>	1010	10 <sup>13</sup>
n log <sub>2</sub> n	34	665	10 <sup>4</sup>	2 · 10 <sup>7</sup>	3 · 10 <sup>10</sup>	4 · 10 <sup>13</sup>
n <sup>2</sup>	100	10 <sup>4</sup>	10 <sup>6</sup>	10 <sup>12</sup>	10 <sup>18</sup>	10 <sup>24</sup>
n <sup>3</sup>	10 <sup>3</sup>	10 <sup>6</sup>	109	10 <sup>18</sup>	10 <sup>27</sup>	10 <sup>36</sup>
2 <sup>n</sup>	10 <sup>3</sup>	10 <sup>30</sup>	10 <sup>301</sup>		•••	•••

n	10	100	10 <sup>3</sup>	10 <sup>6</sup>	109	10 <sup>12</sup>
log <sub>2</sub> n	4	7	10	20	30	40
10n	100	10 <sup>3</sup>	104	10 <sup>7</sup>	1010	10 <sup>13</sup>
n log <sub>2</sub> n	34	665	104	2 · 10 <sup>7</sup>	3 · 10 <sup>10</sup>	$4 \cdot 10^{13}$
n <sup>2</sup>	100	10 <sup>4</sup>	10 <sup>6</sup>	10 <sup>12</sup>	10 <sup>18</sup>	10 <sup>24</sup>
$n^3$	10 <sup>3</sup>	10 <sup>6</sup>	109	10 <sup>18</sup>	10 <sup>27</sup>	10 <sup>36</sup>
2 <sup>n</sup>	10 <sup>3</sup>	10 <sup>30</sup>	10 <sup>301</sup>			•••

n	10	100	10 <sup>3</sup>	10 <sup>6</sup>	109	10 <sup>12</sup>
log <sub>2</sub> n	4	7	10	20	30	40
10n	100	10 <sup>3</sup>	10 <sup>4</sup>	10 <sup>7</sup>	1010	10 <sup>13</sup>
n log <sub>2</sub> n	34	665	10 <sup>4</sup>	2 · 10 <sup>7</sup>	3 · 10 <sup>10</sup>	$4 \cdot 10^{13}$
n <sup>2</sup>	100	10 <sup>4</sup>	106	10 <sup>12</sup>	10 <sup>18</sup>	10 <sup>24</sup>
n <sup>3</sup>	10 <sup>3</sup>	10 <sup>6</sup>	109	10 <sup>18</sup>	10 <sup>27</sup>	10 <sup>36</sup>
2 <sup>n</sup>	10 <sup>3</sup>	10 <sup>30</sup>	10 <sup>301</sup>			•••

n	10	100	10 <sup>3</sup>	10 <sup>6</sup>	109	10 <sup>12</sup>
100 log <sub>2</sub> n	400	700	10 <sup>3</sup>	$2 \cdot 10^3$	$3 \cdot 10^{3}$	$4 \cdot 10^3$
100 n	10 <sup>3</sup>	104	10 <sup>5</sup>	10 <sup>8</sup>	10 <sup>11</sup>	10 <sup>14</sup>
100 n log <sub>2</sub> n	$3 \cdot 10^{3}$	7 · 10 <sup>4</sup>	106	2 · 109	3 · 10 <sup>12</sup>	$4\cdot 10^{15}$
100 n <sup>2</sup>	10 <sup>4</sup>	10 <sup>6</sup>	10 <sup>8</sup>	10 <sup>14</sup>	10 <sup>20</sup>	10 <sup>26</sup>
100 n <sup>3</sup>	10 <sup>5</sup>	108	10 <sup>11</sup>	10 <sup>20</sup>	10 <sup>29</sup>	10 <sup>38</sup>
100 2 <sup>n</sup>	10 <sup>5</sup>	10 <sup>32</sup>	10 <sup>303</sup>	•••		•••

### NOTATIONS UTILISÉES

$$\mathsf{f} \in \mathsf{O}(\mathsf{g}) \iff \mathsf{f} \; \texttt{``ne grandit } \textit{\textit{pas plus vite}} \; \mathsf{que} \; \texttt{``g} \; \; \; \; (\texttt{``grand O``)})$$

$$f \in \Theta(g) \iff \text{f et } g \text{ « grandissent à la même vitesse »} \qquad (\text{« Th\'eta »})$$

(on s'intéresse uniquement à des fonctions positives et croissantes)



#### Notations utilisées

$$f \in O(g) \iff f$$
 « ne grandit  $pas \ plus \ vite$  que »  $g$  («  $grand \ O$  »)

« (pour  $m \leqslant n$  assez grands) si  $g(n) \leqslant \alpha g(m)$ , alors  $f(n) \leqslant \alpha f(m)$  »

$$f \in \Theta(g) \iff f \ \text{et} \ g \ \text{ \ensuremath{\text{w}}} \ \text{grandissent \ a la même vitesse} \ \text{\ensuremath{\text{w}}} \ \ \text{\ensuremath{\text{(}}\ $\it{w}$ } \ \text{\ensuremath{\text{m}}} \ \text{\ensuremath{\text{e}}} \ \text{\ensuremath{e}} \ \text{\ensuremath{\text{e}}} \ \text{\ensuremath{e}} \ \text{\ensuremat$$

(on s'intéresse uniquement à des fonctions positives et croissantes)



#### Notations utilisées

$$f \in O(g) \iff f \text{ "ne grandit } pas plus \ vite \ que "g" ( "grand O "))$$

« (pour  $m \leqslant n$  assez grands) si  $g(n) \leqslant \alpha g(m)$ , alors  $f(n) \leqslant \alpha f(m)$  »

$$\mathsf{f} \in \Omega(\mathsf{g}) \iff \mathsf{f} \mathrel{ \lessdot } \mathsf{grandit} \mathrel{ \textit{au moins aussi vite} } \mathsf{que} \mathrel{ \lor } \mathsf{g} \mathrel{ ( \lessdot Om\acute{e}\mathit{ga} \mathrel{ \lor })} \; | \;$$

« (pour  $m \le n$  assez grands) si  $g(n) \ge \alpha g(m)$ , alors  $f(n) \ge \alpha f(m)$  »

(on s'intéresse uniquement à des fonctions positives et croissantes)



#### Notations utilisées

# Définition (grand O, grand Oméga, grand Théta)

Soit f et g deux fonctions de  $\mathbb N$  dans  $\mathbb N$ . On dit que :

• 
$$f \in O(g)$$
 (ou  $f(n) \in O(g(n))$ , ou  $f(n) = O(g(n))$ ) si:

$$\exists c > 0, \ \exists n_0 \in \mathbb{N}, \quad \forall n \geqslant n_0, \quad f(n) \leqslant c \cdot g(n)$$

•  $f \in \Omega(g)$  (ou  $f(n) \in \Omega(g(n))$ ) si:

$$\exists c>0, \ \exists n_0 \in \mathbb{N}, \quad \forall n \geqslant n_0, \quad f(n) \geqslant c \cdot g(n)$$

•  $f \in \Theta(g)$  (ou  $f(n) \in \Theta(g(n))$ ) si:

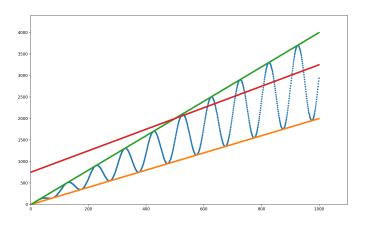
$$f \in O(g)$$
 et  $f \in \Omega(g)$ 

autrement dit:

$$\exists c_1, c_2 > 0, \ \exists n_0 \in \mathbb{N}, \quad \forall n \geqslant n_0, \quad c_1 \cdot g(n) \leqslant f(n) \leqslant c_2 \cdot g(n)$$

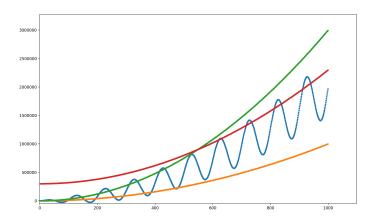


# EXEMPLES



Fonctions appartenant à  $\Theta(n)$ 

# EXEMPLES



Fonctions appartenant à  $\Theta(\mathfrak{n}^2)$ 



# Complexité des calculs de F<sub>n</sub>

#### utilisation naïve de la récurrence

```
\implies \Theta(\phi^n) additions
```

```
def fibo_1(n) :
   if n <= 2 : return 1
   return fibo_1(n-1) + fibo_1(n-2)</pre>
```

### Complexité des calculs de Fn

utilisation naïve de la récurrence

```
\implies \Theta(\varphi^n) additions
```

calcul itératif des n premières valeurs

```
\implies \Theta(n) additions
```

```
def fibo_3(n) :
  previous, last = 1, 1
  for i in range(2, n+1) :
    previous, last = last, previous + last
  return last
```

### Complexité des calculs de Fn

utilisation naïve de la récurrence  $\implies \Theta(\varphi^n)$  additions  $\Longrightarrow \Theta(n)$  additions calcul itératif des n premières valeurs calcul de  $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$  par exponentiation binaire  $\Longrightarrow$ ? def fibo\_4(n) : if  $n \le 0$  : return 0 M = puissance\_matrice\_2\_2 ([ [1, 1], [1, 0] ], n-1) return M[0][0]

```
def puissance(a, n) : # 1ère version récursive
  if n == 0 : return 1  # une comparaison
  tmp = puissance(a, n//2)  # une division par 2, un appel récursif
  carre = tmp * tmp  # une multiplication
  if n%2 == 0 : return carre  # une comparaison modulo 2
  else : return a * carre  # une multiplication
```

```
def puissance(a, n) : # 1ère version récursive
  if n == 0 : return 1  # une comparaison
  tmp = puissance(a, n//2)  # une division par 2, un appel récursif
  carre = tmp * tmp  # une multiplication
  if n%2 == 0 : return carre  # une comparaison modulo 2
  else : return a * carre  # une multiplication
```

### Preuve de correction : par récurrence (forte) sur n

- cas de base : si n = 0, puissance(a, n) retourne a<sup>n</sup> = 1 pour tout a (convention usuelle pour 0°)
- hérédité : soit  $n \ge 1$  t.q. puissance(a, k) retourne  $a^k$  pour tout k < n comme n//2 < n, puissance(a, n//2) retourne  $a^{n//2}$ , donc :
  - si n est pair : puissance(a,n) retourne  $a^{n/2} \times a^{n/2} = a^n$
  - si n est impair : puissance(a, n) retourne  $a^{(n-1)/2} \times a^{(n-1)/2} \times a = a^n$

donc puissance (a, n) retourne  $a^n$  pour tout n



```
def puissance(a, n) : # 1ère version récursive
  if n == 0 : return 1  # une comparaison
  tmp = puissance(a, n//2)  # une division par 2, un appel récursif
  carre = tmp * tmp  # une multiplication
  if n%2 == 0 : return carre  # une comparaison modulo 2
  else : return a * carre  # une multiplication
```

#### Calcul de complexité:

- chaque appel récursif effectue (au plus) 2 multiplications, une division par 2, une comparaison et une comparaison modulo 2
- à chaque appel récursif, le paramètre n est divisé par 2 (avec arrondi inférieur), avec n=0 comme cas terminal; donc le nombre total d'appels est h+2 si  $n=2^h$ , et plus généralement si  $2^h \le n < 2^{h+1}$ , c'est-à-dire si  $h=\lfloor \log_2 n \rfloor$ .
- $\implies \Theta(\log_2 n)$  multiplications de la forme  $a^k \cdot a^{\ell}$ ,  $k \in \{1, \ell\}$

# Complexité

 $\Theta(\log_2 n)$  multiplications de la forme  $\alpha^k \cdot \alpha^\ell$ 

c'est le cas avec l'arithmétique modulaire ou l'arithmétique flottante utilisées usuellement : tous les nombres sont codés sur exactement 32 (ou 64) bits, donc le coût d'une multiplication est constant

# Complexité

 $\Theta(\log_2 n)$  multiplications de la forme  $\alpha^k \cdot \alpha^\ell$ 

si ces multiplications ont un coût constant, *i.e.* si les opérandes ont une taille constante, complexité en  $\Theta(\log_2 n)$ 

c'est le cas avec l'arithmétique modulaire ou l'arithmétique flottante utilisées usuellement : tous les nombres sont codés sur exactement 32 (ou 64) bits, donc le coût d'une multiplication est constant

# Complexité

 $\Theta(\log_2 n)$  multiplications de la forme  $\alpha^k \cdot \alpha^\ell$ 

si ces multiplications ont un coût constant, *i.e.* si les opérandes ont une taille constante, complexité en  $\Theta(\log_2 n)$ 

c'est le cas avec l'arithmétique modulaire ou l'arithmétique flottante utilisées usuellement : tous les nombres sont codés sur exactement 32 (ou 64) bits, donc le coût d'une multiplication est constant

**sinon** il faut tenir compte du coût de ces multiplications; par exemple en arithmétique exacte sur des entiers :

valeur	taille (en bits)	coût du calcul naïf du carré	
а	log <sub>2</sub> α	$\Theta((\log_2 a)^2)$	
$a^k$	$a^k \qquad k \cdot \log_2 a \qquad \Theta(k^2 \cdot (\log_2 a))$		

# Complexité des calculs de Fn

utilisation naïve de la récurrence  $\implies \Theta(\phi^n)$  additions calcul itératif des n premières valeurs  $\implies \Theta(n)$  additions calcul de  $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{n-1} \implies \Theta(\log_2 n)$  multiplications... de matrices  $2 \times 2$  (chacune impliquant 4 additions et 8 multiplications d'entiers)

# Complexité des calculs de Fn

utilisation naïve de la récurrence

$$\implies \Theta(\varphi^n)$$
 additions

calcul itératif des n premières valeurs

$$\implies \Theta(n)$$
 additions

calcul de 
$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{n-1}$$
  $\implies \Theta(\log_2 n)$  multiplications...  $extit{de matrices } 2 \times 2$ 

(chacune impliquant 4 additions et 8 multiplications d'entiers)

**MAIS...** comme  $F_n \in \Theta(\phi^n)$ , les opérations arithmétiques se font sur des entiers de **taille**  $\Theta(n)$  (c'est-à-dire de  $\Theta(n)$  chiffres)

 $\implies$  additions en  $\Theta(n)$  opérations élémentaires, multiplications en  $O(n^2)$  (coût de l'algo naïf)

