Des problèmes “difficiles”

François Schwarzentruber
ENS Cachan – Antenne de Bretagne

Problème indécidable

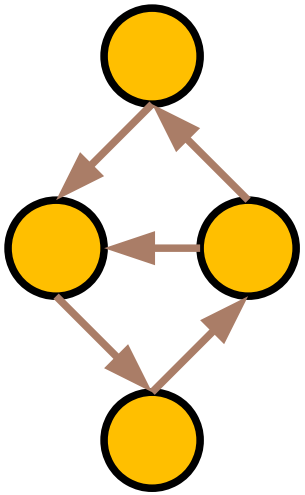
```
Procédure truc()
    Pendant que 1 = 1
        x := 1
```

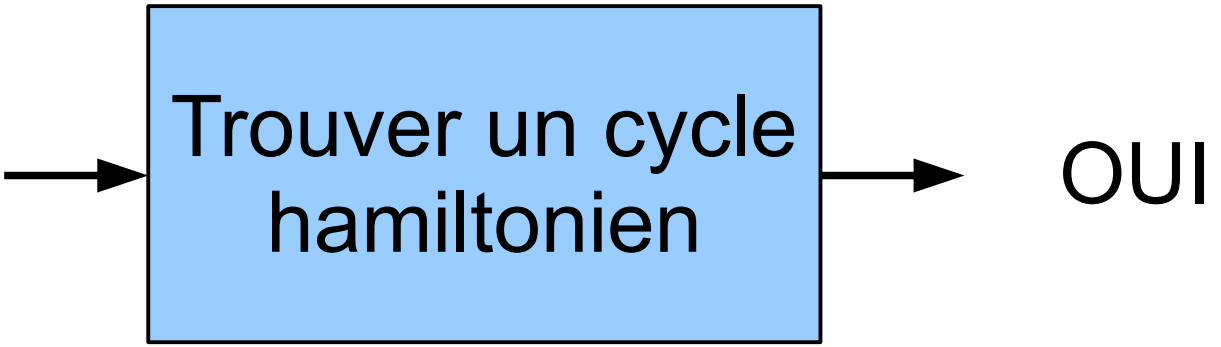
OUI

Tester si
un programme
s'arrête

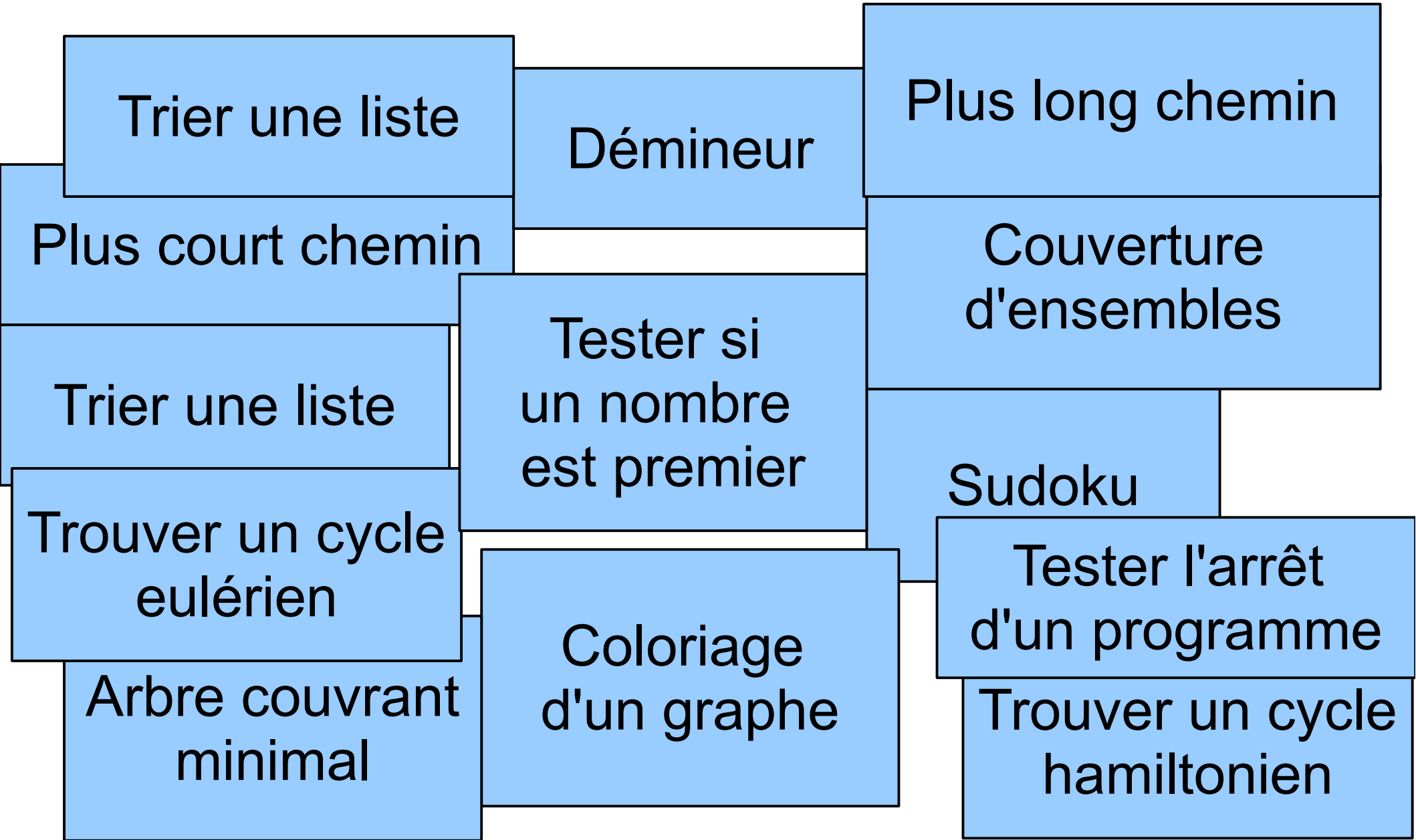
pub : cours de logique et calculabilité

Problème de décision





Besoin de classer



Besoin de classer les problèmes

Savoir quand :

- s'attendre à un temps de réponse long
- un algorithme approximatif (glouton ?)
- une réduction...

Problème décidable

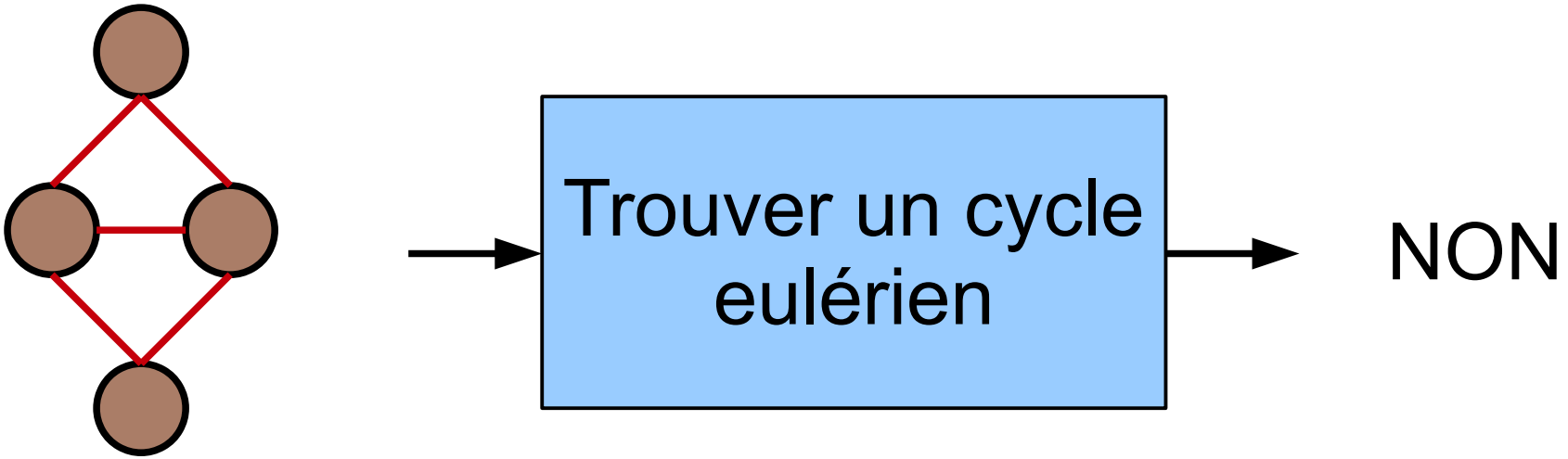
19 →  → OUI

Tester si
un nombre
est premier

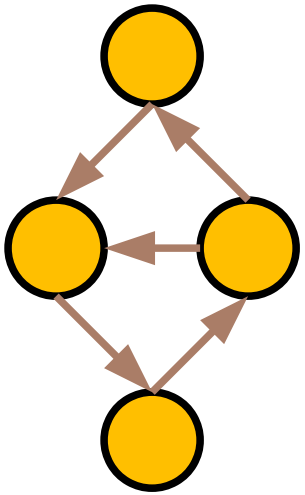
Plan du cours

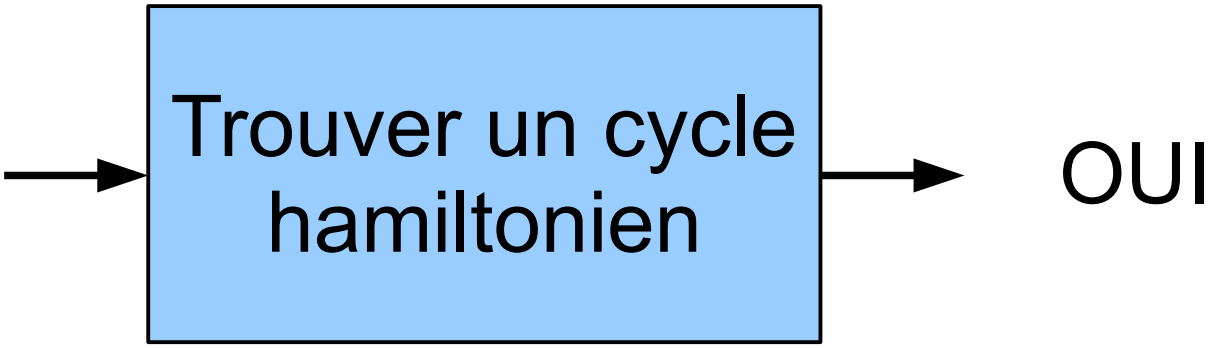
- Définir un classement des problèmes
  - Définitions intuitives
  - Machines de Turing pour définir P et NP
  - Réduction pour définir la difficulté
- Le pouvoir de la logique propositionnelle
  - Introduction à la logique
  - La puissance du problème SAT
- Des réductions pour montrer la NP-compéltude

Un problème facile



Un problème qui semble “difficile”

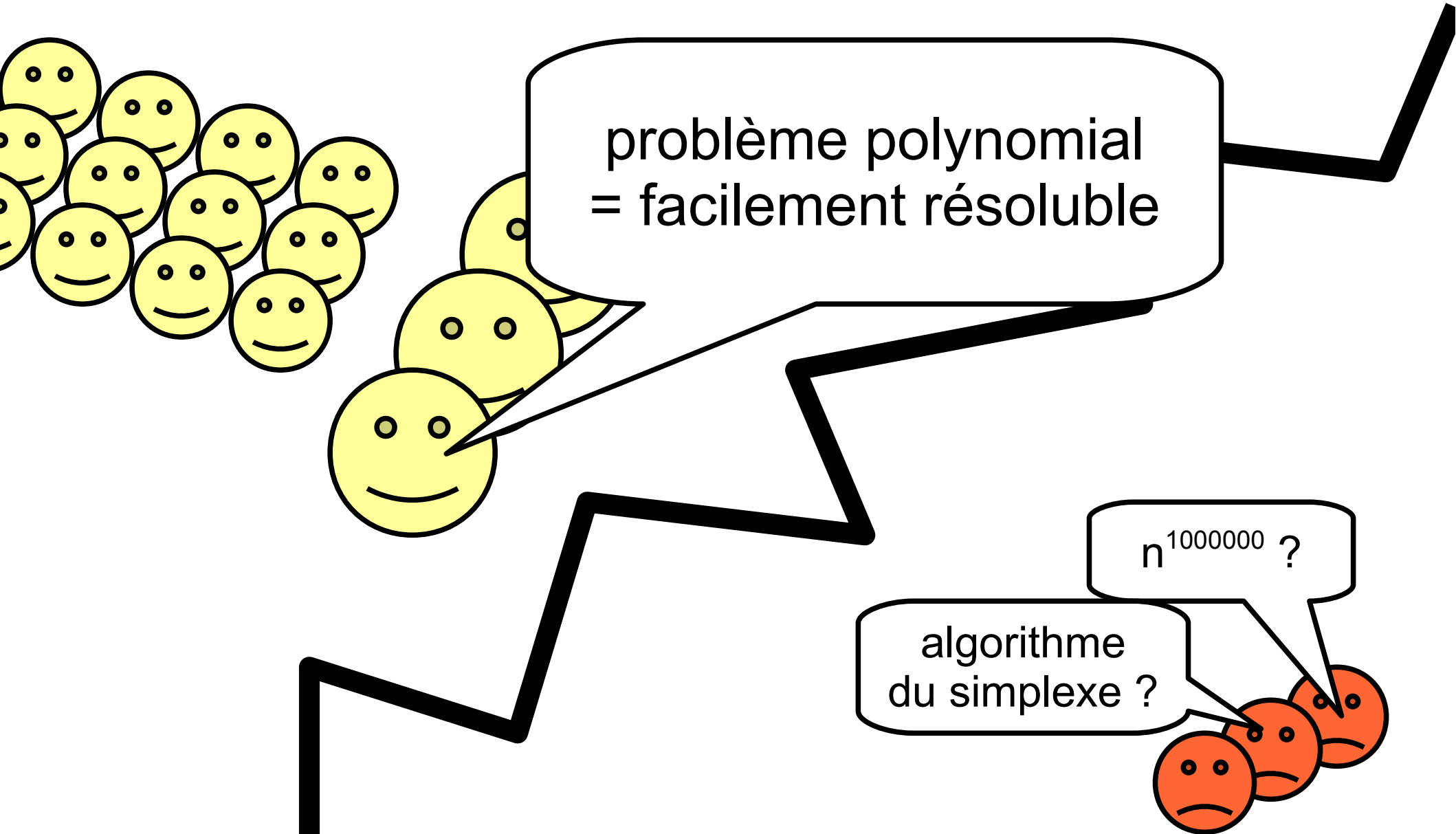




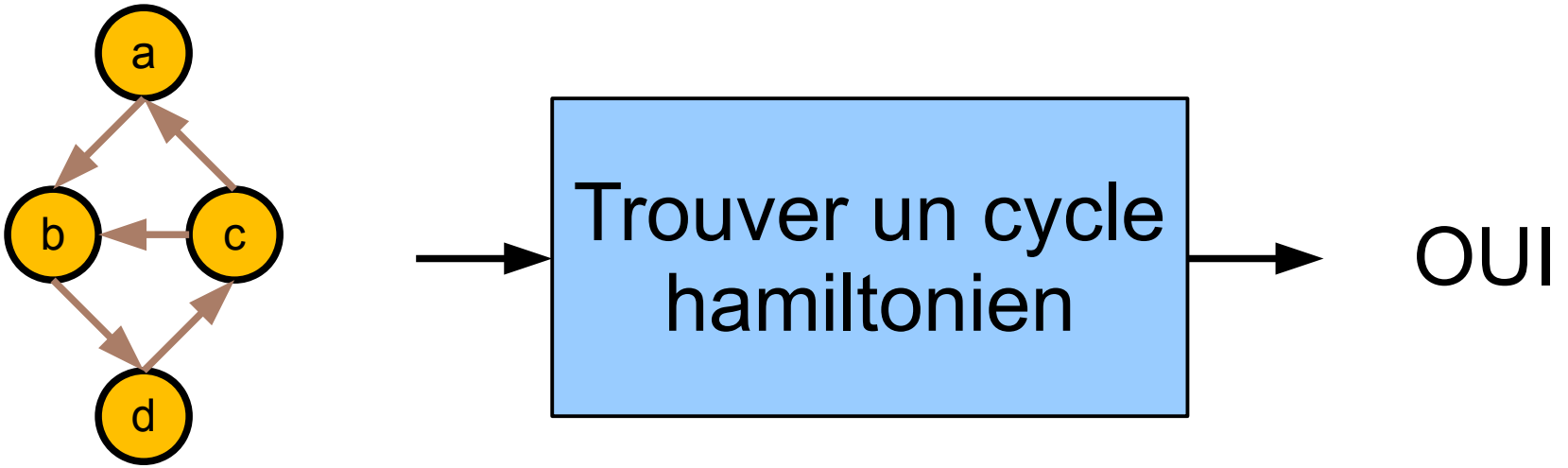
Les seuls algorithmes qu'on connaisse...

- **pire cas** en **temps exponentiel**

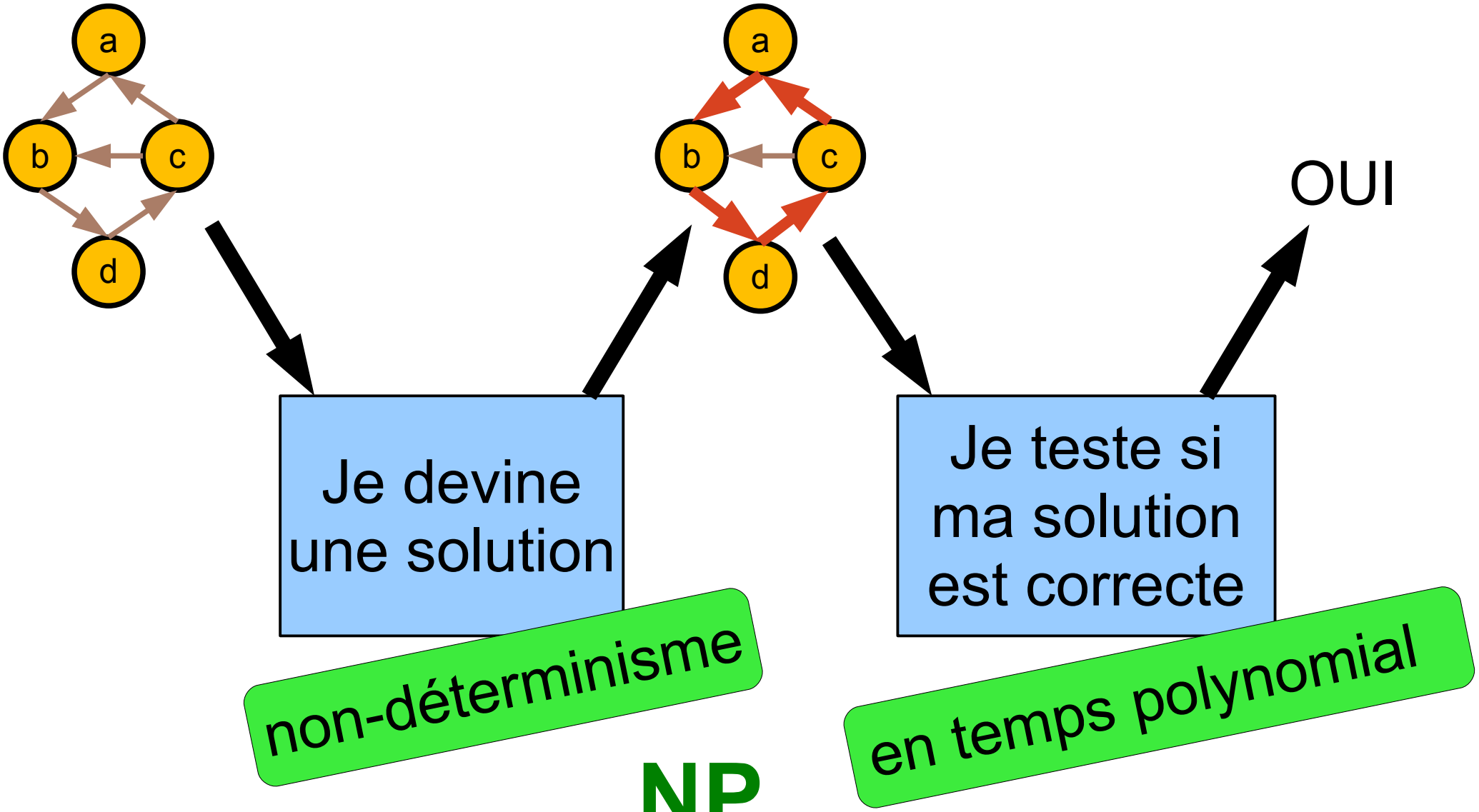
Thèse de Cobham-Edmonds



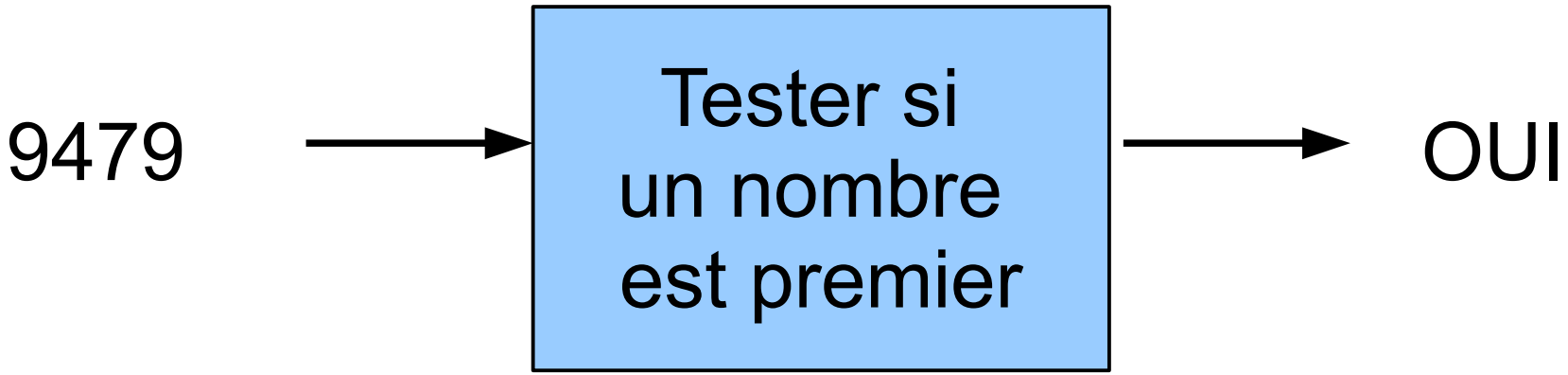
Un problème qui a l'air "difficile"



Deviner et tester

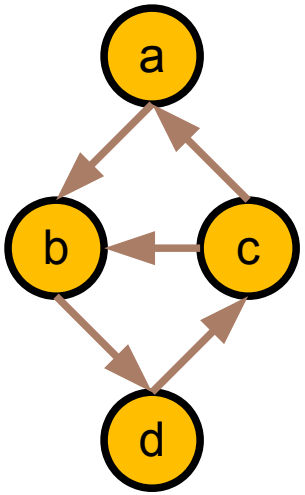


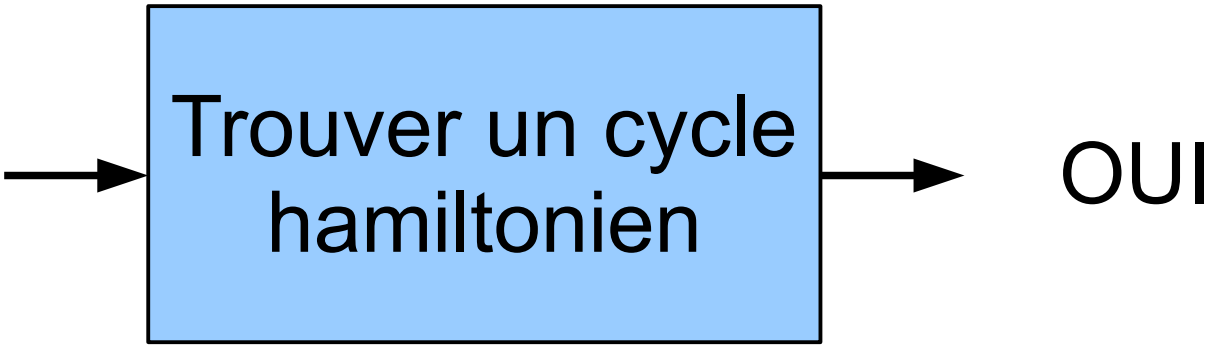
Un problème de décision ~ un langage



pub : cours de langage formel

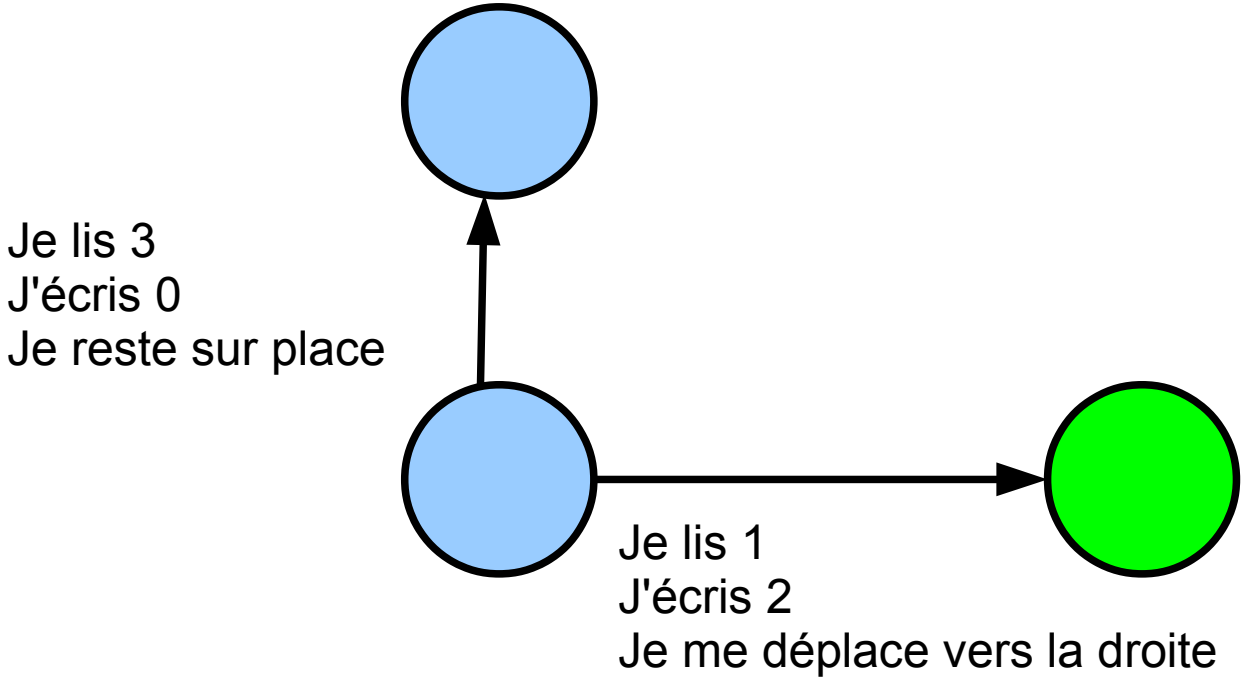
Un problème de décision ~ un langage

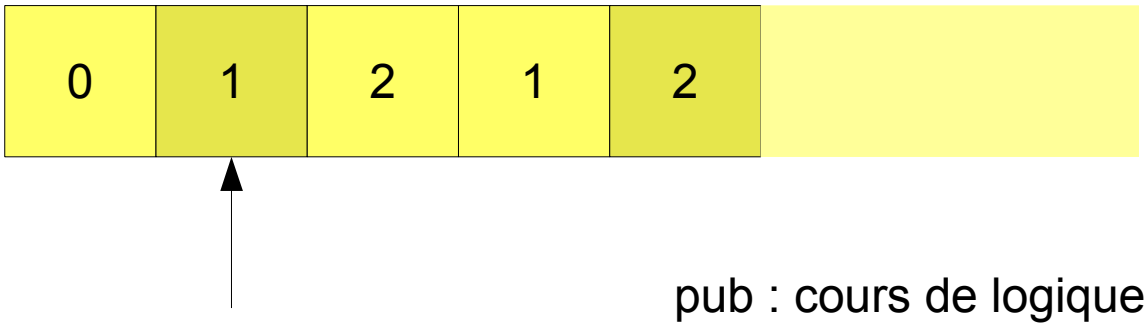




“a(b)b(d)c(ab)d(c)”

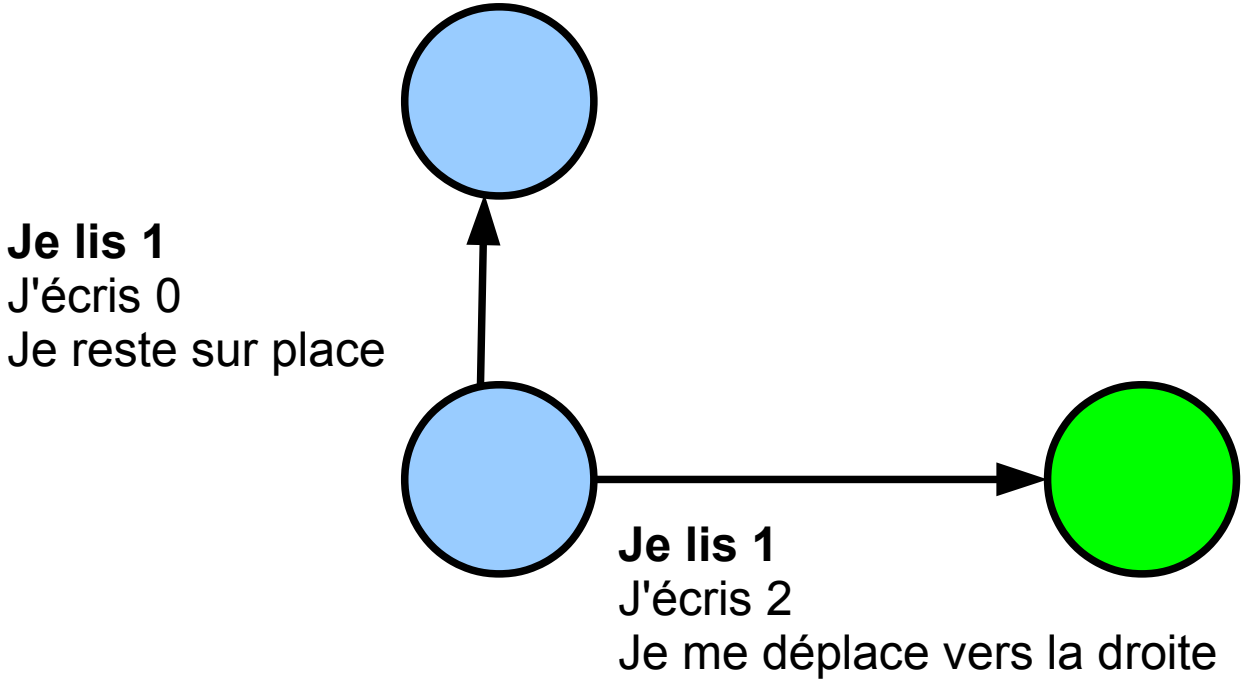
Besoin : parler d'algo formellement... machine de Turing

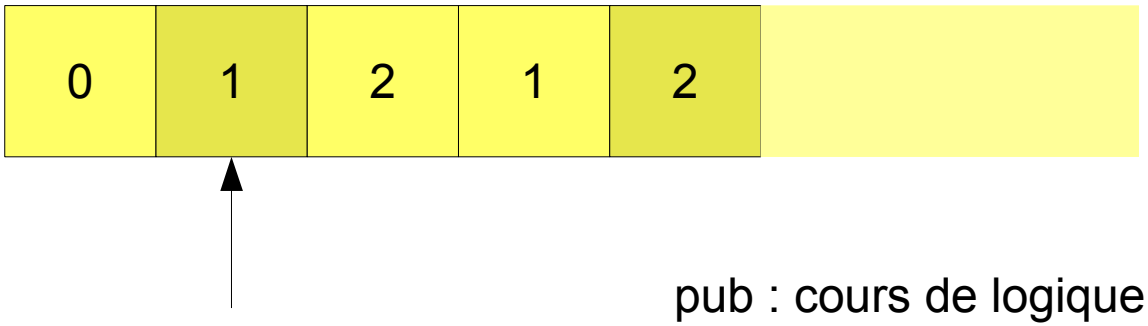




pub : cours de logique et calculabilité
ALGO2, CVFP

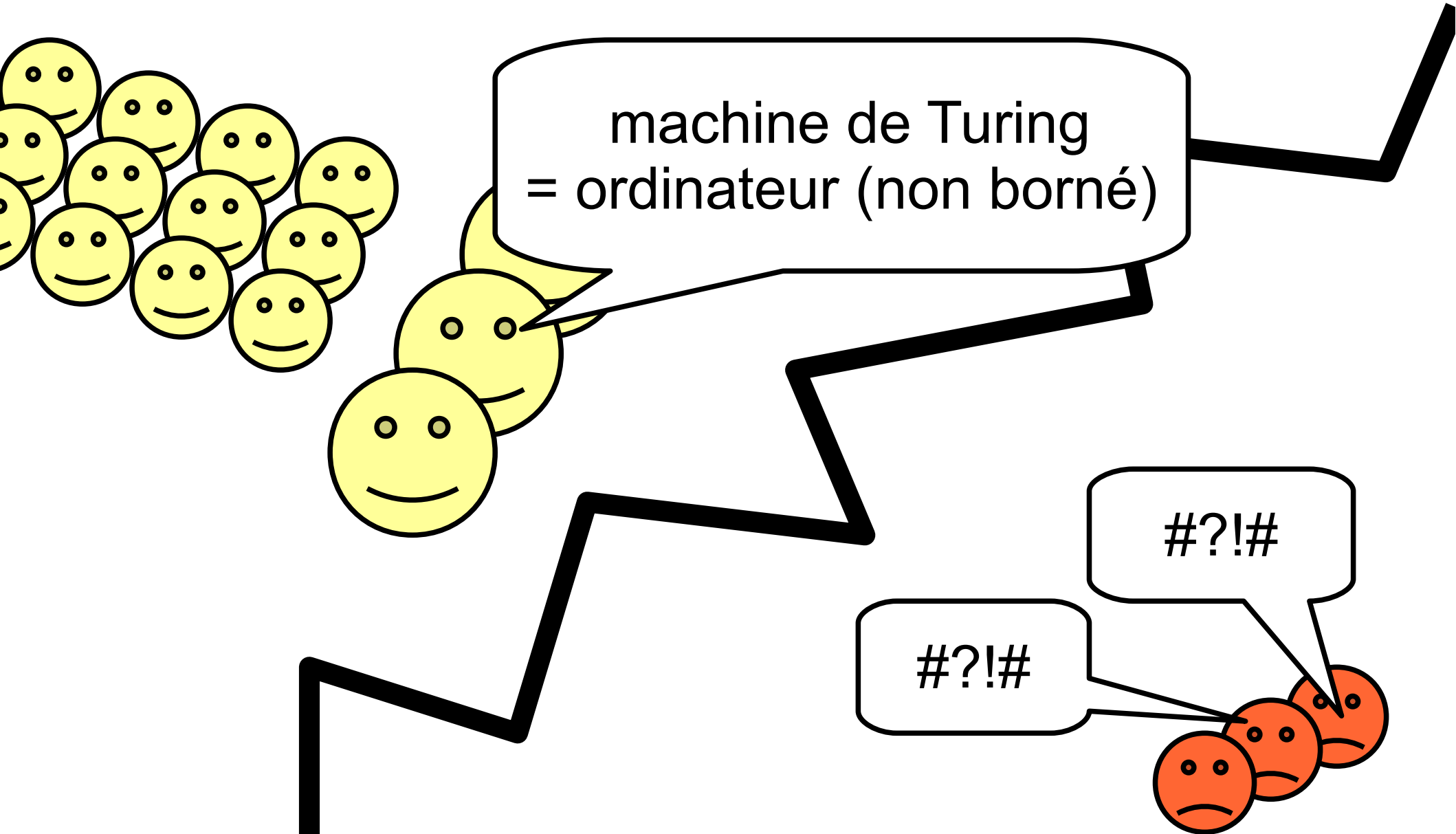
Machine de Turing **non déterministe**



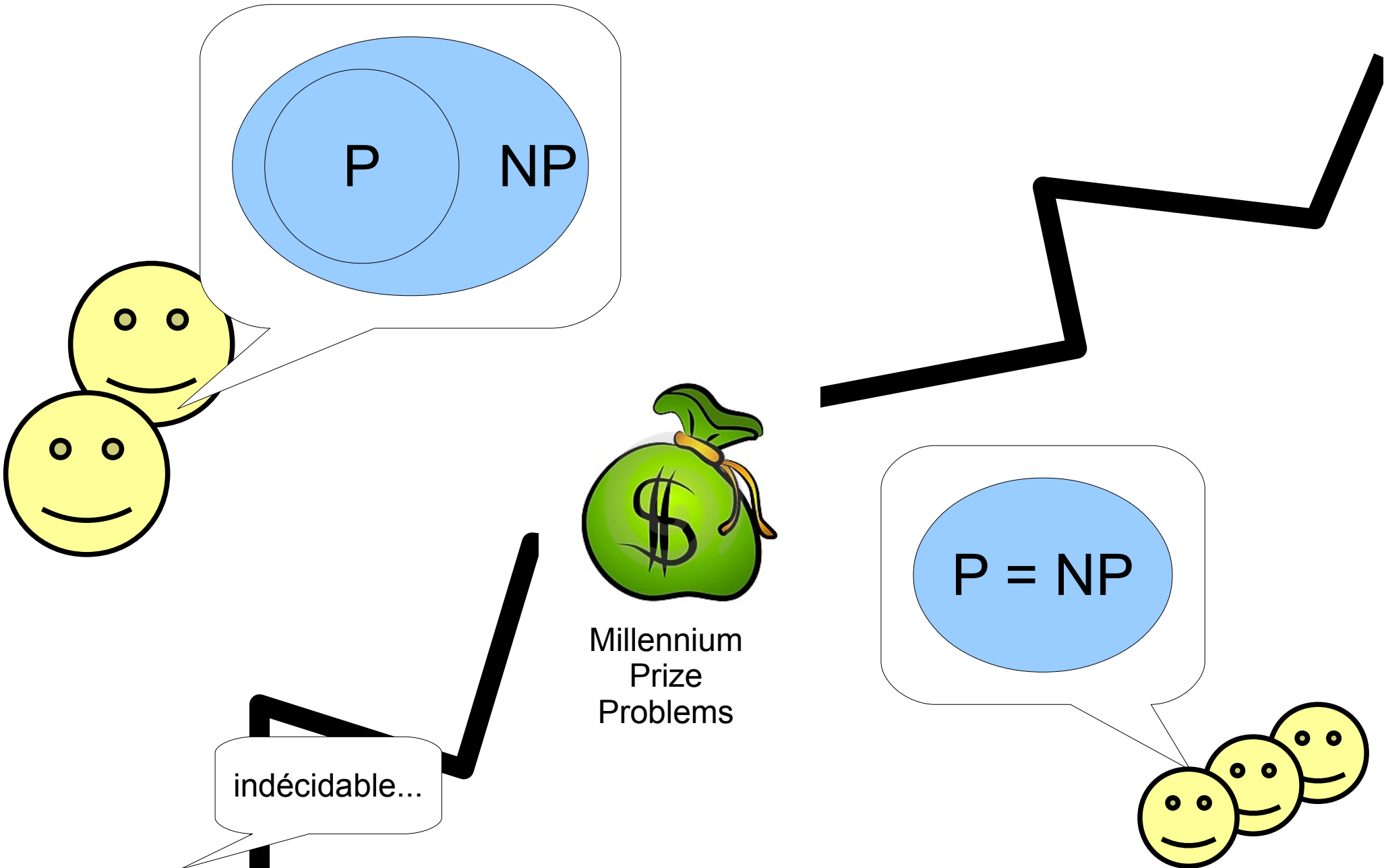


pub : cours de logique et calculabilité
ALGO2, CVFP

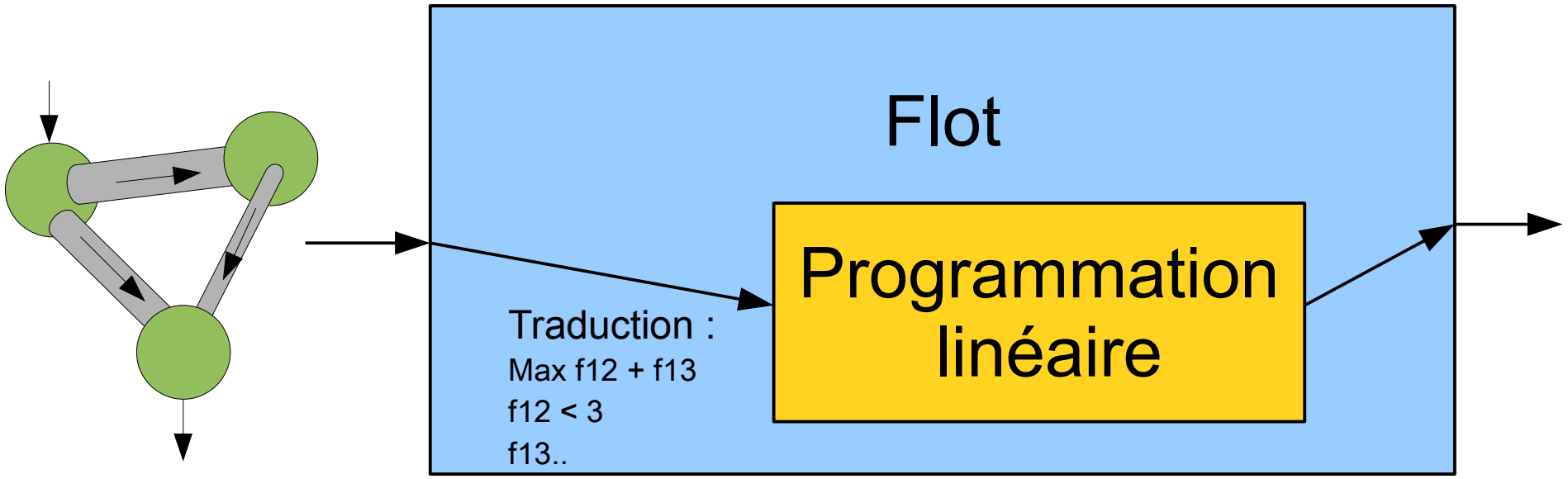
Thèse de Church



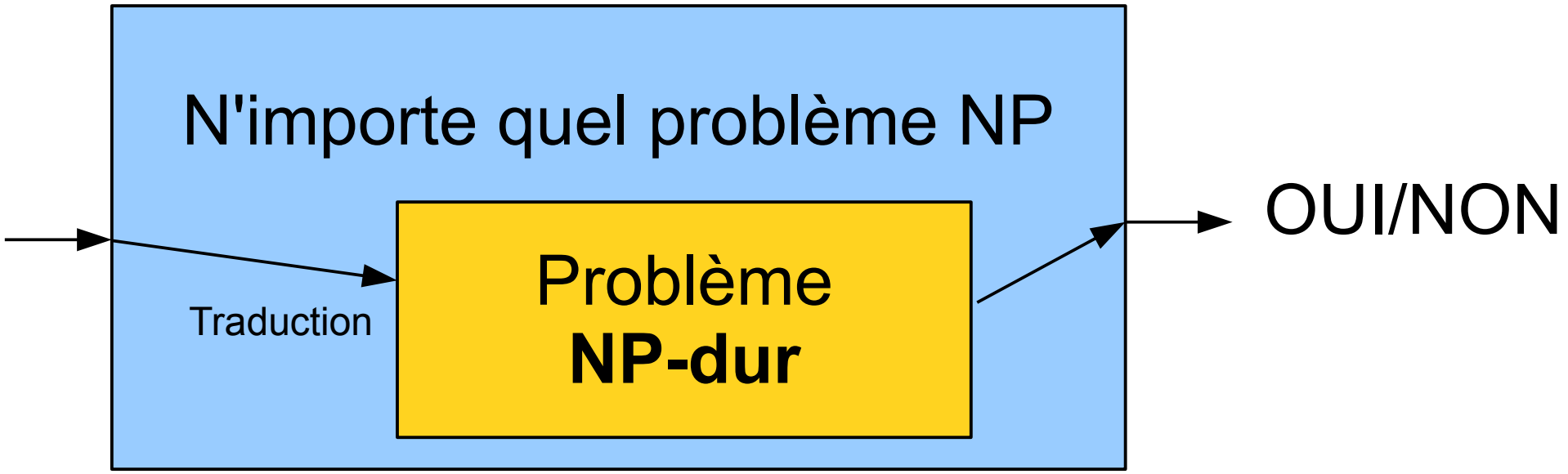
Problème ouvert



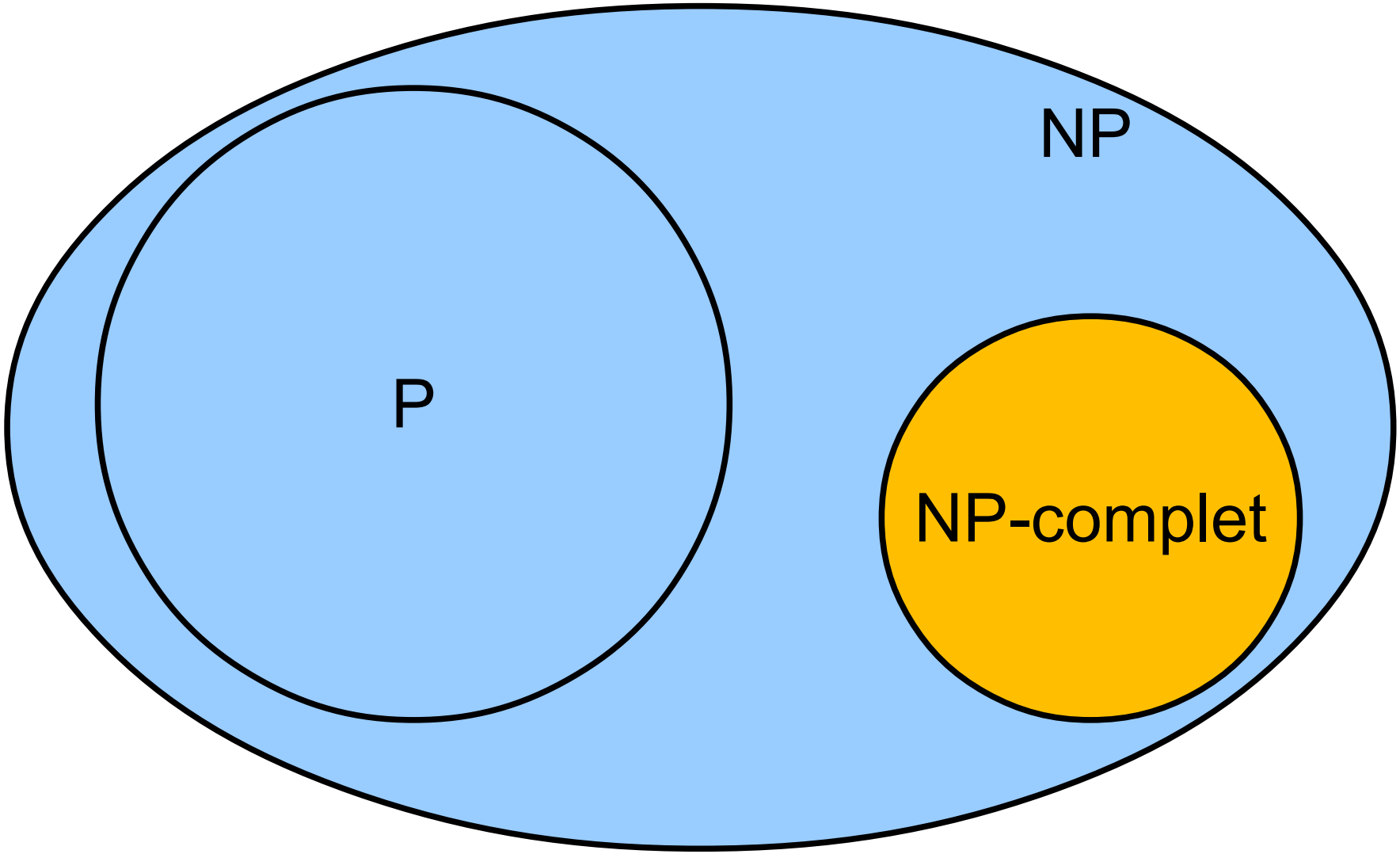
Réduction... flashback...



Réduction pour définir la difficulté



Conclusion



Le pouvoir de la logique propositionnelle

Logique propositionnelle

((p ou q) → r) et (non r) et p

pub : cours de logique et calculabilité !

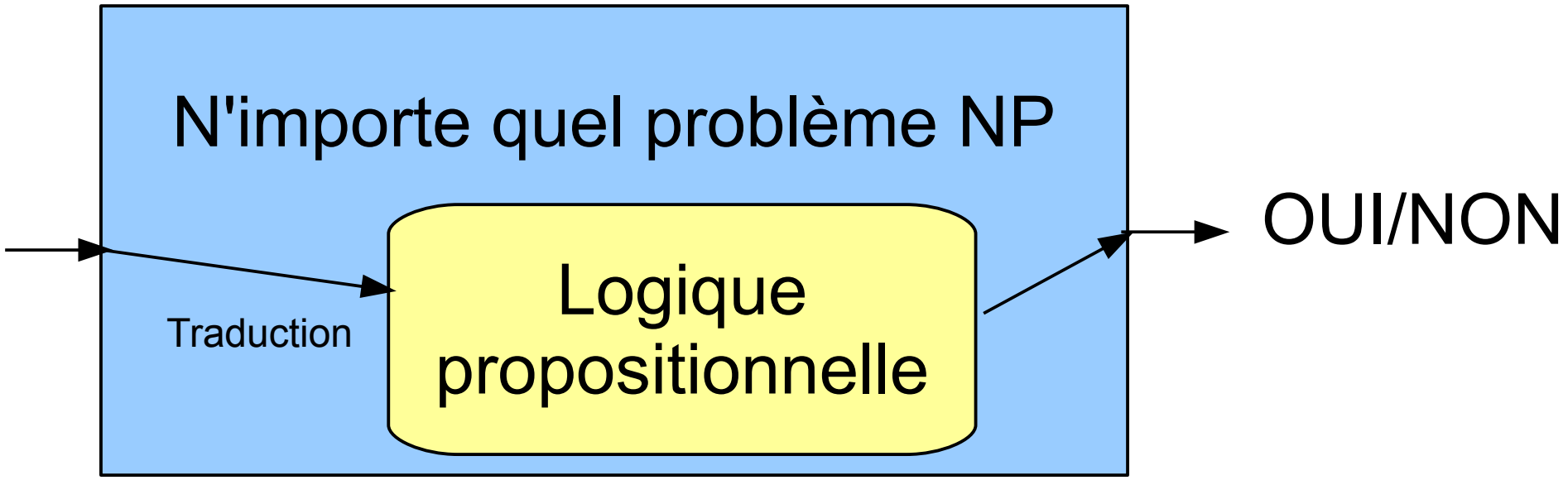
Le problème SAT

Pourquoi parler de logique ?

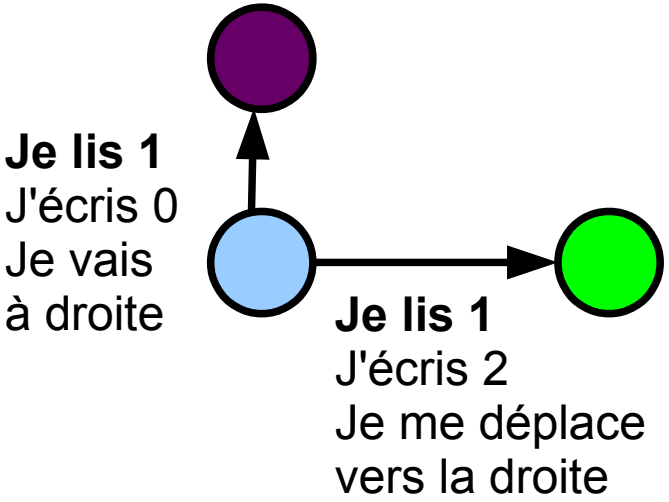
	4		1					
		3	5				1	9
					6			3
		7			5			8
	8	1				9	6	
9			2			7		
6			9					
8	1				2	4		
					4		9	

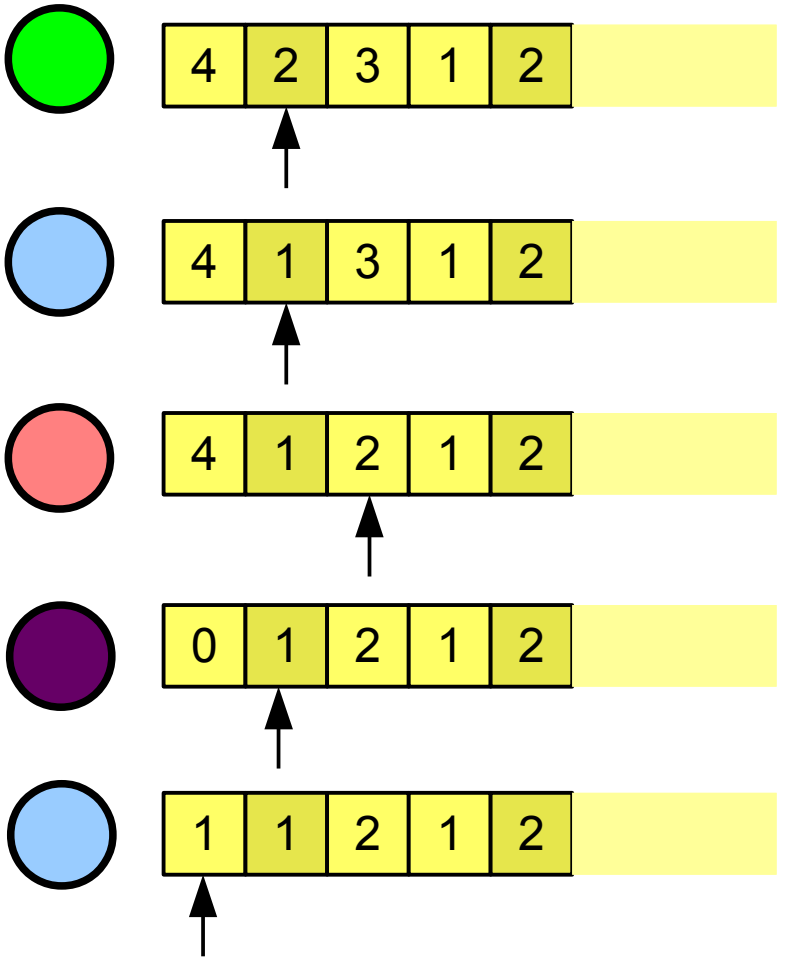
SAT

Théorème de Cook : SAT est NP-dur

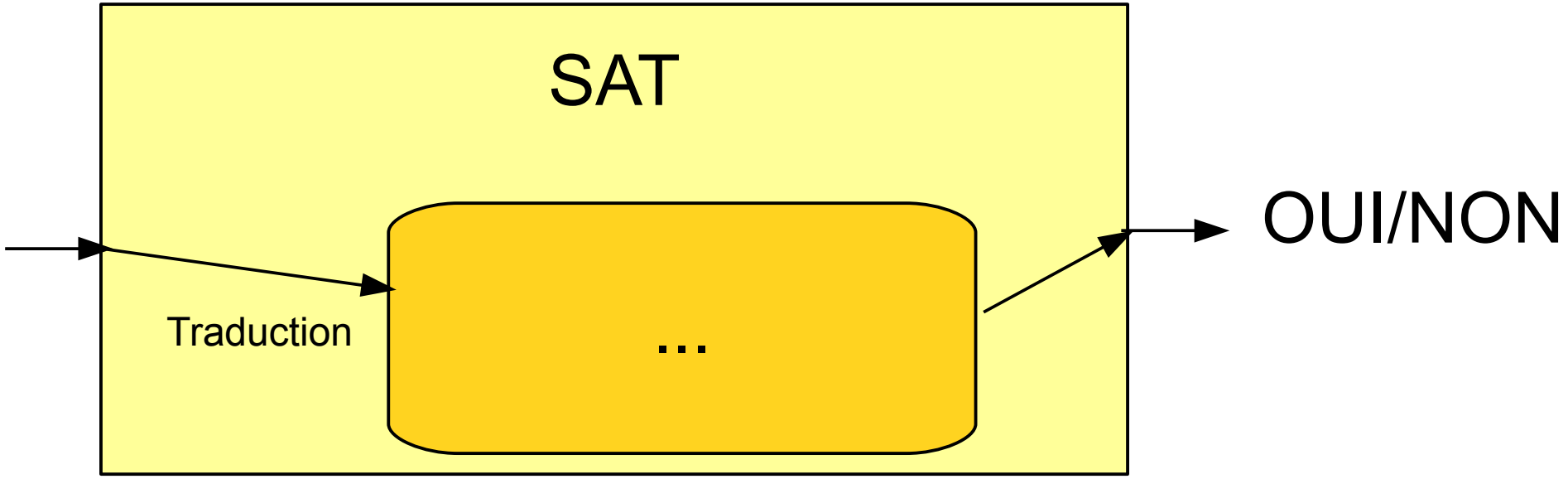


SAT encode une machine de Turing non-déterministe

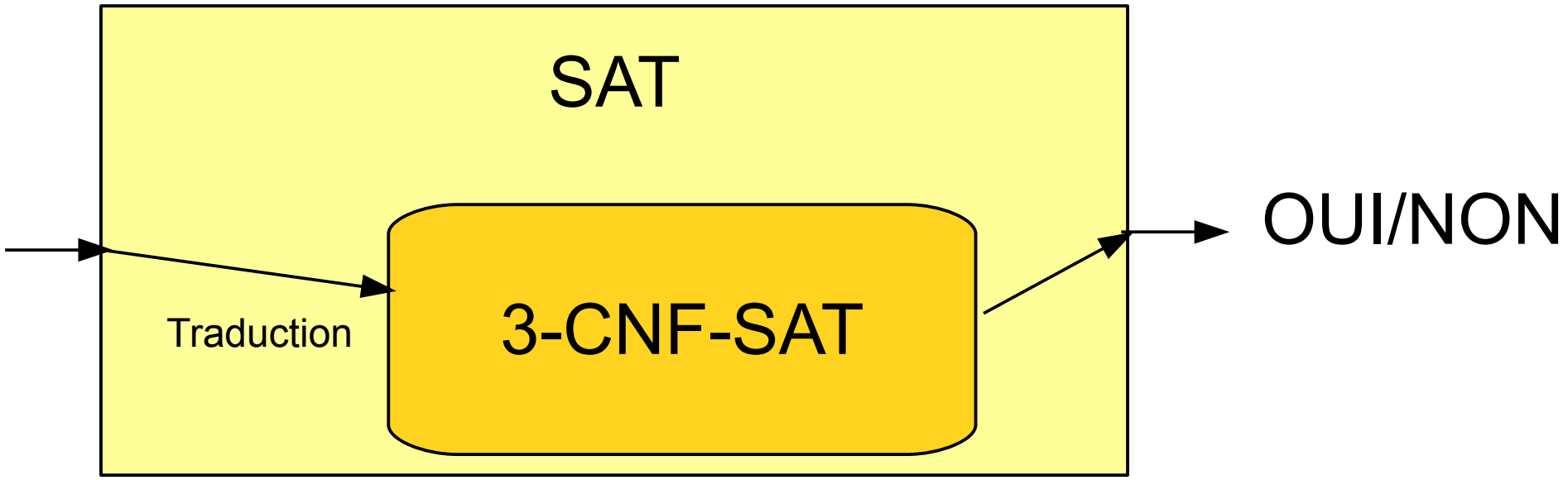




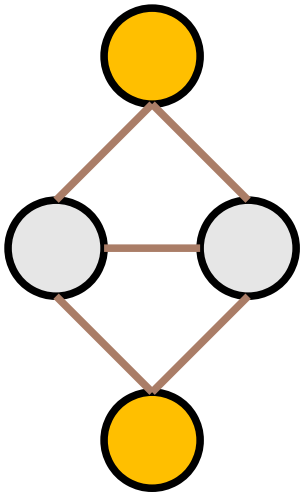
Réductions pour montrer la difficulté

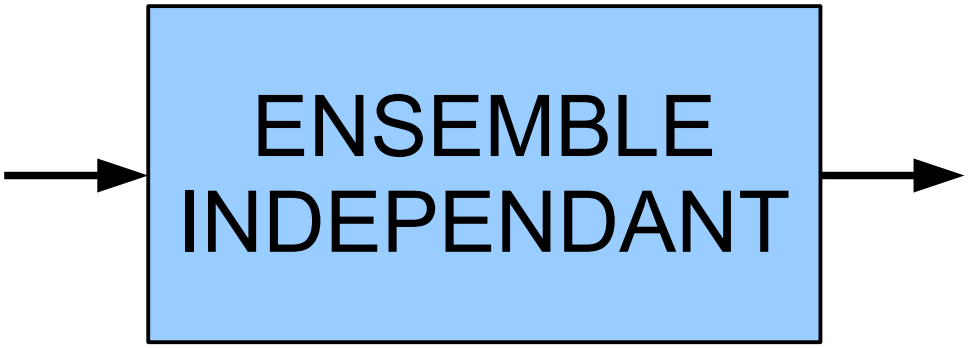


Variante plus fine : 3-CNF-SAT



Problème de l'ensemble indépendant

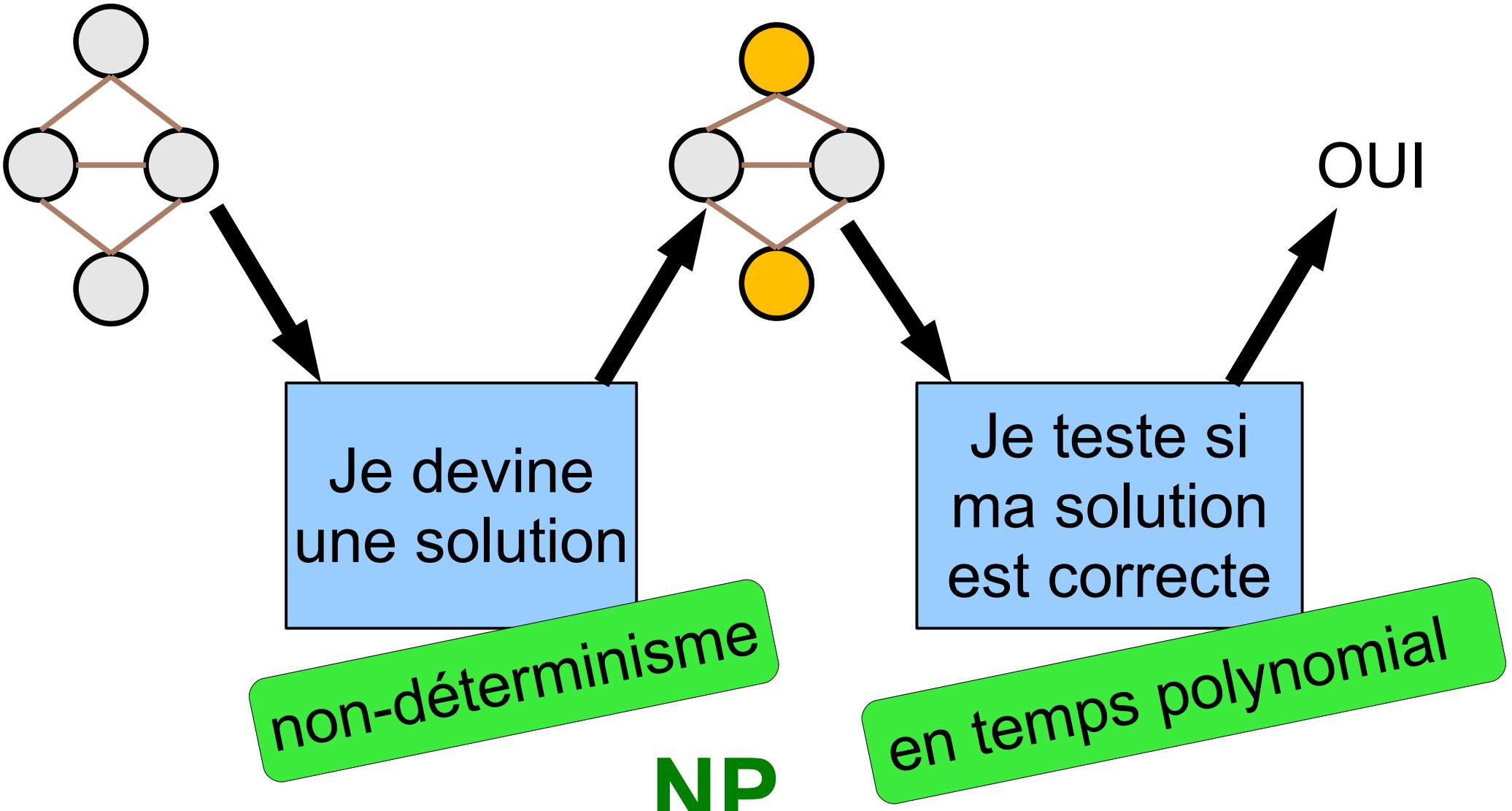




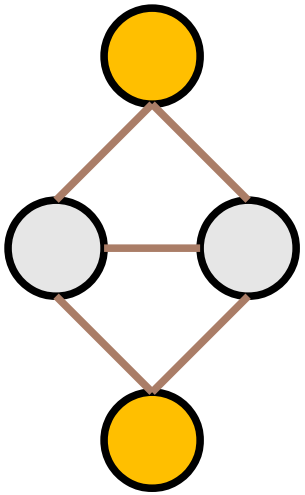
OUI,
il y a
un k-ens
indépendant

k = 2

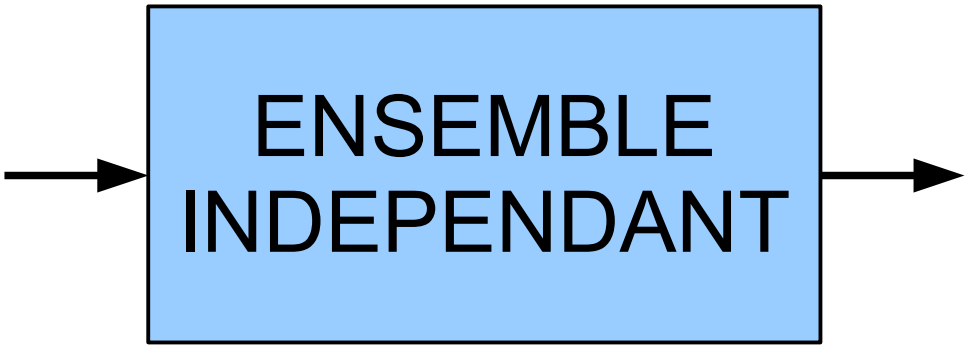
ENS INDEPENDANT est dans NP



ENS INDEPENDANT est NP-dur ?

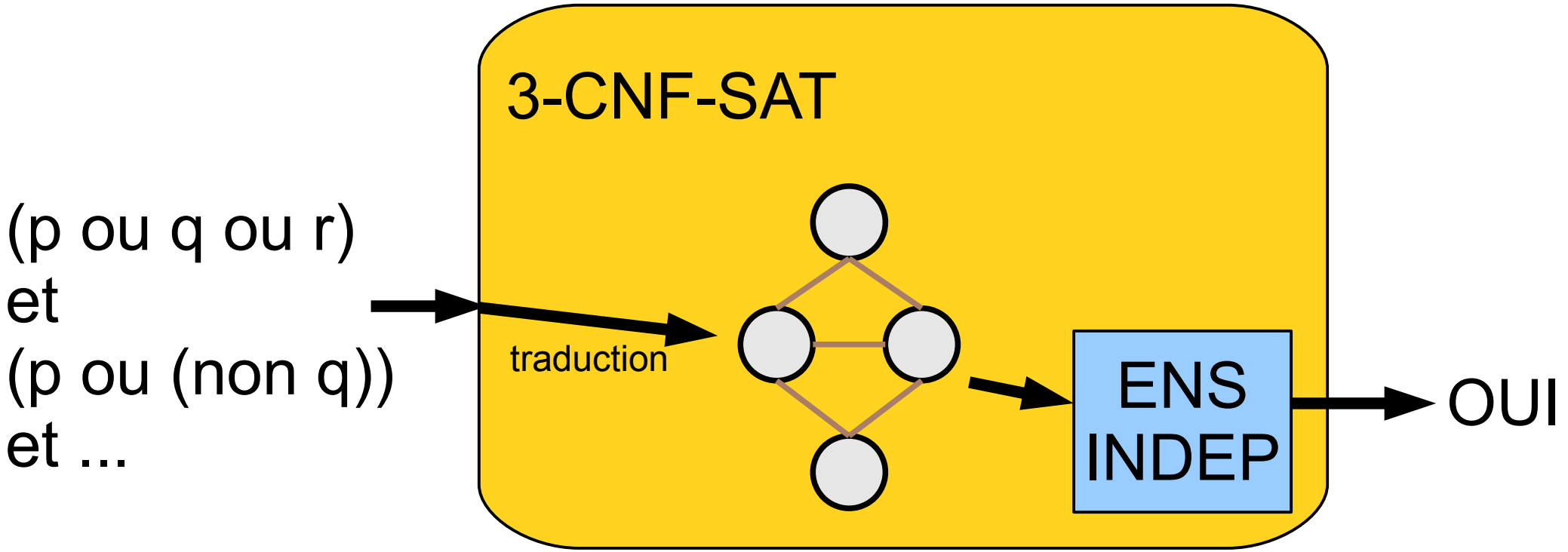


k = 2

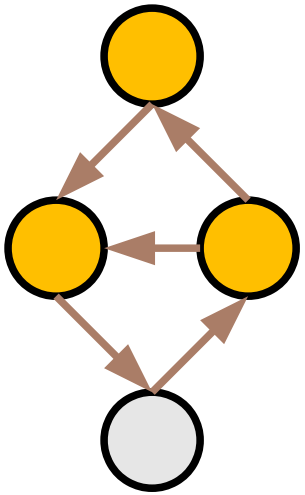


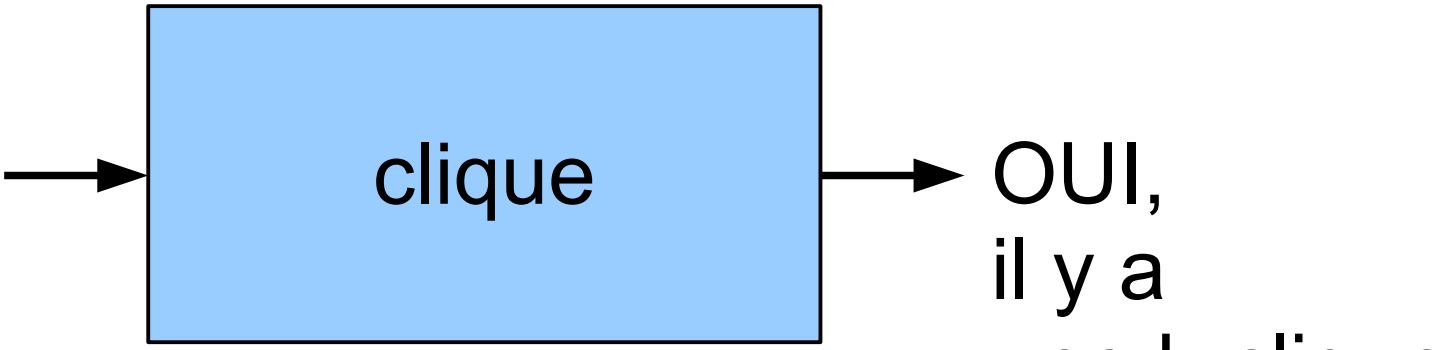
OUI,
il y a
un k-ens
indépendant

ENS INDEPENDANT est NP-dur ?



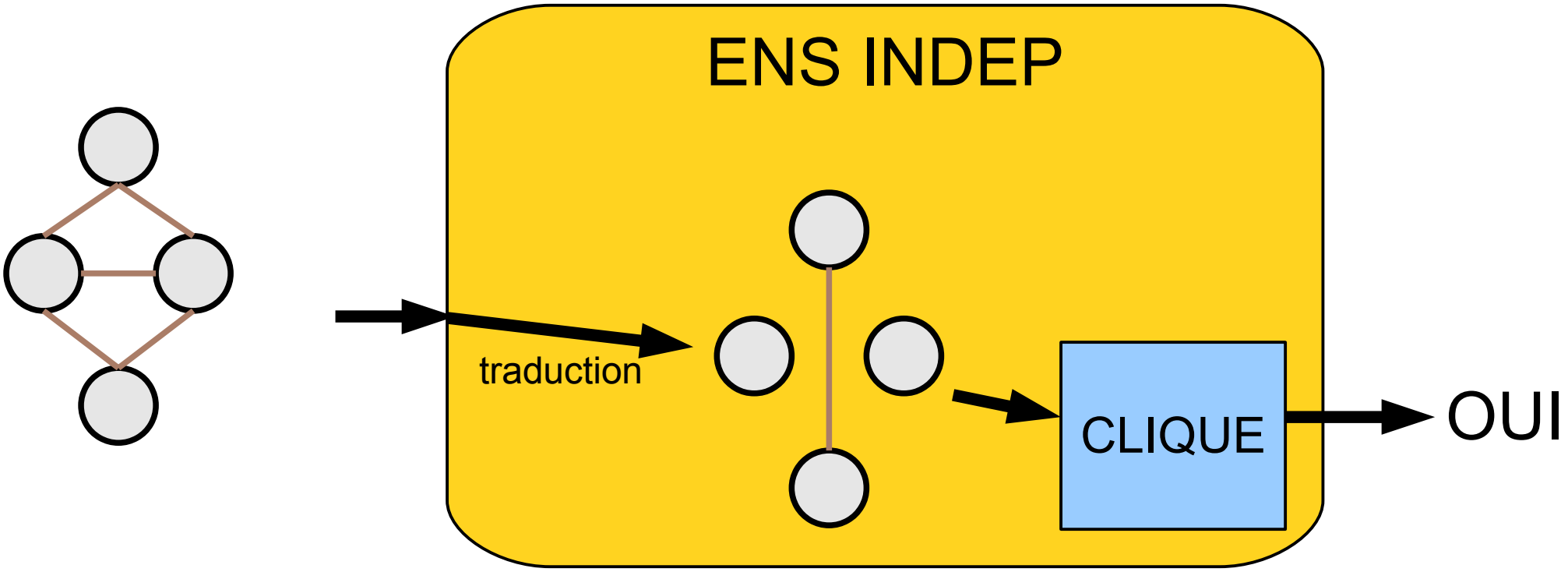
Problème de la clique



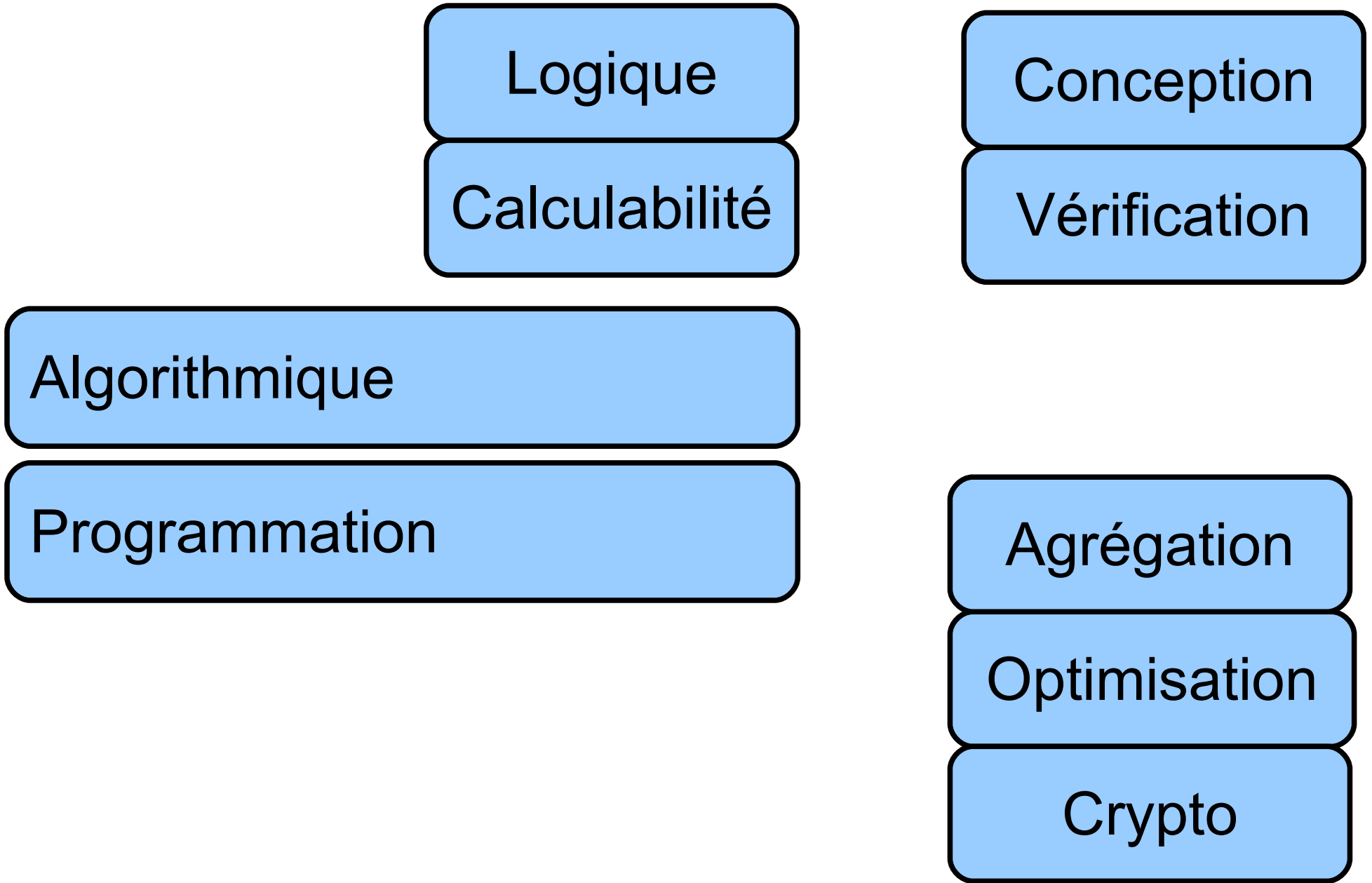


k = 3

Réduction !



A Rennes...


Logique
Calculabilité
Conception
Vérification
Algorithmique
Programmation
Agrégation
Optimisation
Crypto

Autre manière de voir les choses