Les classes
P et NP

Nous utiliserons un formalisme simple, adapté au traitement des problèmes de décision, forme à laquelle il est presque toujours possible de se ramener. La façon standard d′énoncer un problème sera composée de trois parties :

- le nom du problème
- les données du problème (description complète, codage inclus)
- une question n′admettant comme réponse que oui ou non.

NOM : **KNAPSACK** (sac à dos)

DONNEES : un ensemble fini d'objets, E, avec deux fonctions entières, v et p, associant à chaque objet une valeur et un poids. Un poids total autorisé P et une valeur totale minimale V.

QUESTION : peut-on choisir des objets (à mettre dans le sac) de manière à ne pas dépasser le poids total autorisé, et que le total des valeurs soit supérieur ou égal à V ?

La réduction polynomiale

P_1 et P_2 deux problèmes.

On dira que le problème P_1 peut être *réduit* au problème P_2 s′il existe une transformation associant à chaque instance Π de P_1 une instance $f(\Pi)$ de P_2, de manière que la réponse à Π est oui si et seulement si la réponse à $f(\Pi)$ est oui.

On utilise le terme *réduction*, car en disposant d'une telle transformation, si on sait résoudre le problème P_2, alors on sait aussi résoudre le problème P_1 (on le transforme, puis on répond à la question par oui ou non).

Notons le paradoxe linguistique que P_1 se réduit en un problème plus dur P_2. Si, de plus, la transformation est polynomiale (peut se faire en temps polynomial) alors la réduction est dite polynomiale. On notera $P_1 \propto P_2$.

NOM : **CHAINEHAM** (chaîne hamiltonienne)

DONNEES : un graphe fini G(V,E), représenté sous forme de listes d'adjacence.

QUESTION : est-ce que le graphe admet une chaîne hamiltonienne (une chaîne passant une fois et une seule par tous les sommets) ?

NOM : **CYCLEHAM** (cycle hamiltonien)

DONNEES : un graphe fini G(V,E), représenté sous forme de listes d′adjacence.

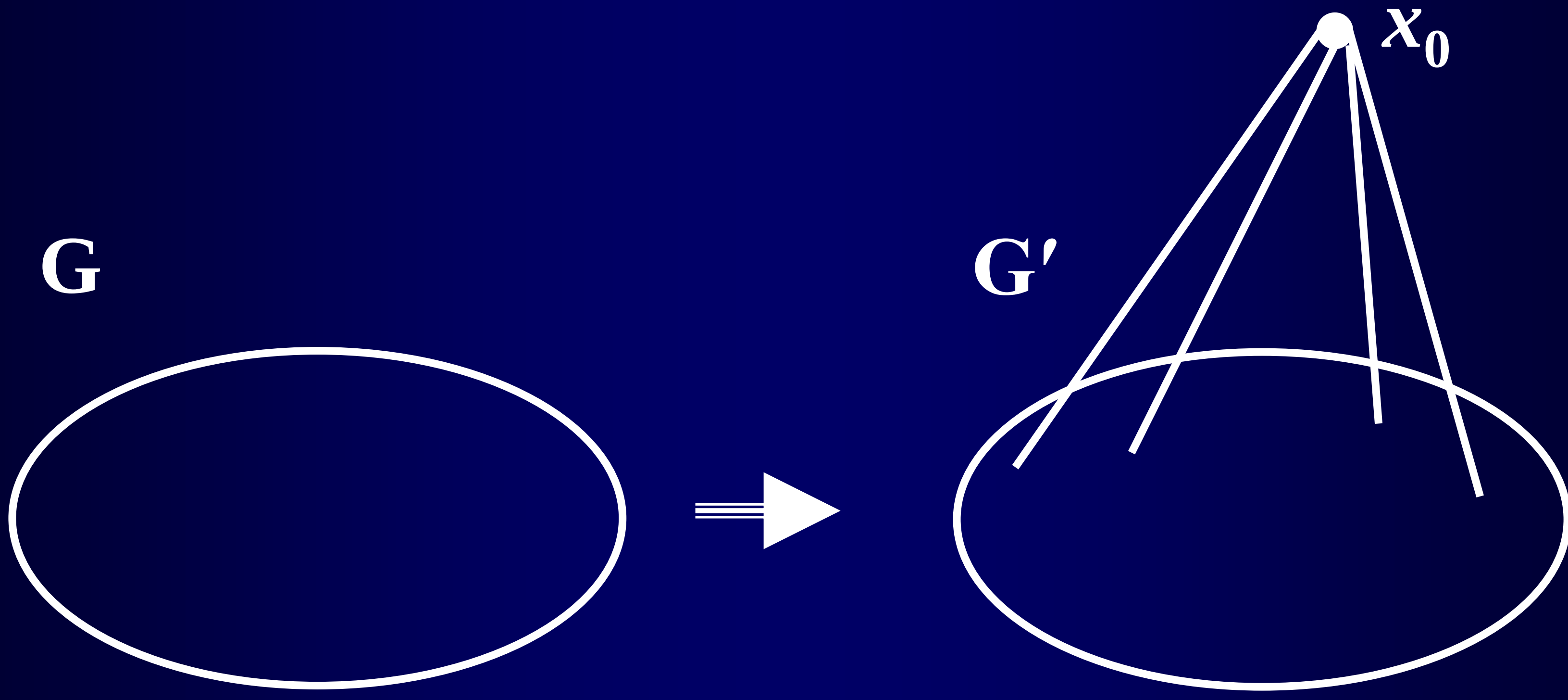
QUESTION : est-ce que le graphe admet un cycle hamiltonien (un cycle passant une fois et une seule par tous les sommets) ?

Montrons que **CHAINEHAM** $\propto$ **CYCLEHAM**.

La transformation :

le graphe $G'(V',E')$ pour le problème **CYCLEHAM** est obtenu en rajoutant au graphe $G(V,E)$ donné pour le problème **CHAINEHAM** un sommet relié à tous les autres sommets.

Cette transformation peut se faire en temps polynomial.


G
G′
x_0

Cette transformation polynomiale est une réduction. Il faut montrer que G(V,E) admet une chaîne hamiltonienne si et seulement si G′(V′,E′) admet un cycle hamiltonien.

Si : G′(V′,E′) admet un cycle hamiltonien. Soient $x_1,x_2,\ldots,x_n$ les sommets de V et x_0 le sommet rajouté pour obtenir G′. Le cycle hamiltonien moins le sommet x_0 constitue une chaîne hamiltonienne dans G.

Seulement si : G admet une chaîne hamiltonienne. Cette chaîne, avec le sommet x_0 et les deux arêtes qui le relient aux deux extrémités de la chaîne constitue en G′ un cycle hamiltonien.

Une remarque

On peut remarquer que la relation $\propto$ est une relation d′ordre.

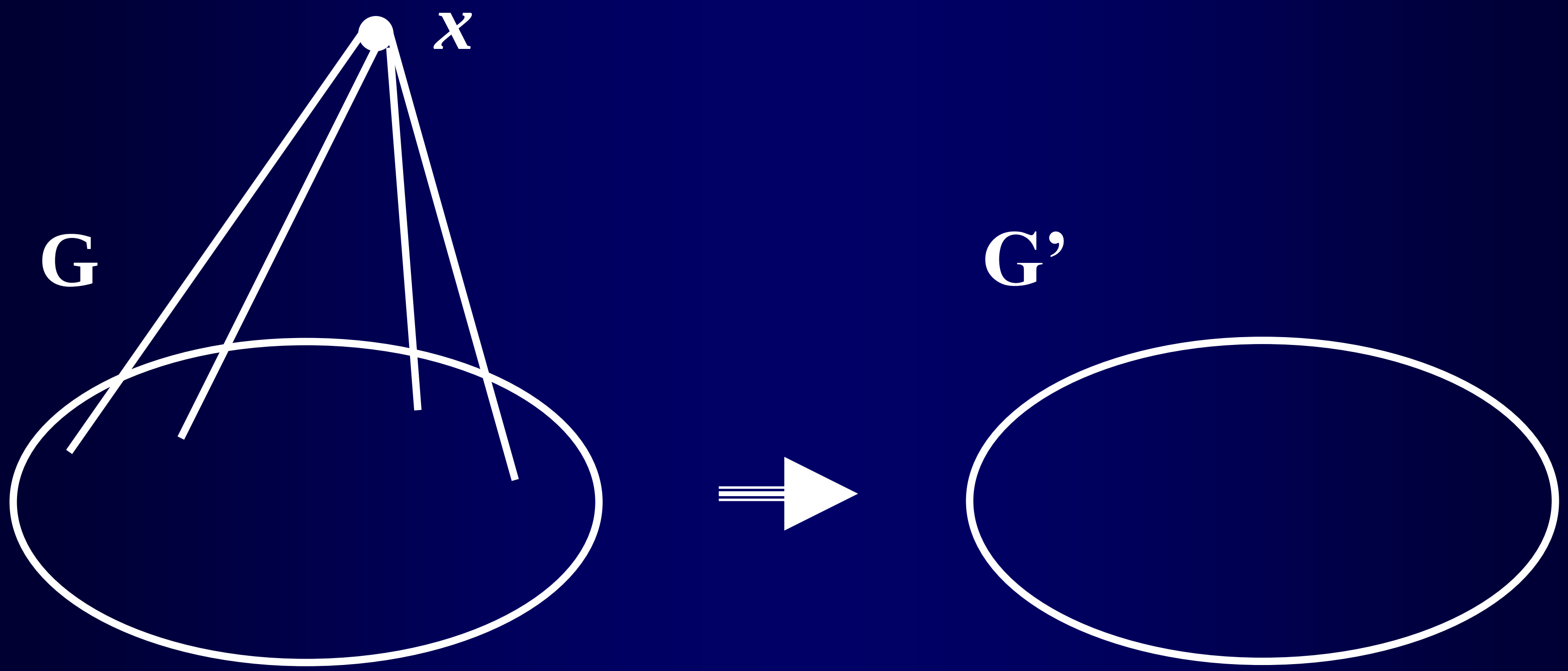
On notera par $\approx$ l′équivalence associée :

$$P_1 \approx P_2 \text{ si et seulement si } P_1 \propto P_2 \text{ et } P_2 \propto P_1.$$

Montrons que **CYCLEHAM** $\propto$ **CHAINEHAM**.

La transformation : le graphe G'(V',E') pour le problème **CHAINEHAM** est obtenu en supprimant dans le graphe G(V,E) donné pour le problème **CYCLEHAM** un sommet.

Cette transformation peut se faire en temps polynomial.


x
G
G'

Il faut montrer que G(V,E) admet une chaîne hamiltonienne si et seulement si G'(V',E') admet un cycle hamiltonien.

Si : G(V,E) admet un cycle hamiltonien. Soient $x_1, x_2, \ldots, x_n$ les sommets de V. Le cycle hamiltonien moins un sommet x_i constitue une chaîne hamiltonienne dans G'.

Seulement si : G' admet une chaîne hamiltonienne. Cette chaîne, avec le sommet *x* peut constituer en G un cycle hamiltonien, à condition que ses deux extrémités soient des voisins de *x*.

ET SINON ??????????????????????????

P et NP

Définition : P est la classe des problèmes qu'on sait résoudre en temps polynomial sur une machine de Turing déterministe *(vu les résultats du chapitre précédent, il n'est pas nécessaire de préciser le nombre de bandes)*.

Définition : NP est la classe des problèmes qu'on sait résoudre en temps polynomial sur une machine de Turing non-déterministe.

Remarque

Attention : bien souvent les gens pensent que P veut dire polynomial et NP non-polynomial ! C'est une erreur !!!!!!!!!

Une observation

Proposition : Tous les problèmes inclus dans P sont polynomialement équivalents.

Preuve : Soient P_1 et P_2 deux problèmes dans P.

Montrons que $P_1 \propto P_2$. On choisit deux instances de P_2, Π_O pour laquelle la réponse est oui et Π_N pour laquelle la réponse est non.

La transformation se fait en deux étapes :

1) On résout l'instance donnée de P_1.
2) Selon la réponse, le résultat de la transformation sera soit Π_O soit Π_N.

Et encore …

Proposition : P est inclus dans NP.

Preuve : comme on a vu qu'une machine déterministe peut être considérée comme une machine non-déterministe avec un choix unique pour chaque transition, la conclusion est évidente.

Le GRAND problème

Problème : est-ce que l'inclusion de P dans NP est stricte ?

L'Institut Clay propose un prix de 1.000.000 $ pour une réponse à cette question (voir http://www.claymath.org/prizeproblems/pvsnp.htm**)**

Telegraph.co.uk

Computer scientist Vinay Deolalikar claims to have solved maths riddle of P vs NP

A computer scientist claims to have solved one of the world's most complex and intractable mathematical problems by proving that P≠NP.

Forbes

Lee Gomes
DIGITAL TOOLS
MY PROFILE | MY HEADLINE GRABS

Aug. 12 2010 - 1:44 pm | 2,686 views | 0 recommendations | 5 comm

How To Think Like A Mathematician

The New York Times

Step 1: Post Elusive Proof. Step 2: Watch Fireworks.

By JOHN MARKOFF
Published: August 16, 2010

On en est ou avec $P \neq NP$ (ou $P=NP$)?

semaine 10-17/8/2010

IBN Live
A NETWORK18 VENTURE

Can man solve practical problems? Math riddle holds clue

Mise à jour 04:33
LE FIGARO·fr

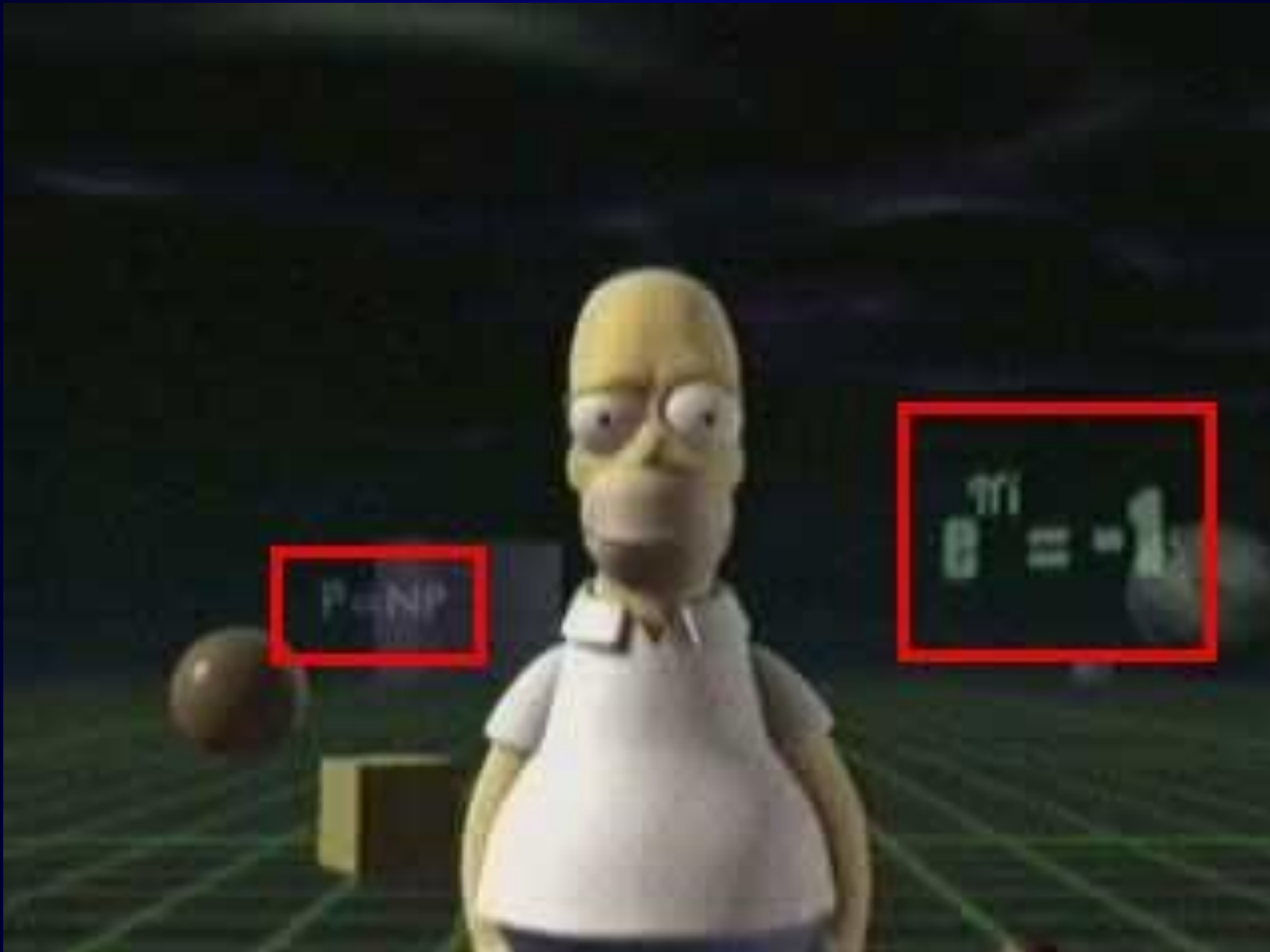
Un problème mathématique à un million de dollars résolu?

האם החידה הגדולה ביותר של מדעי המחשב נפתרה?

nana10

חוקר טוען שפתר את חידת ה-P!=NP המפורסמת, ואנחנו מסבירים לכם במה בכלל מדובר. לפרק את הבייט

IBM


P = NP
$e^{\pi i} = -1$


P=NP
$e^{\pi i} = -1$


PF'03
I WISH P≠NP WAS FINALLY PROVED!
BY ME, OF COURSE!
POOR FELLOW! HE DOESN'T KNOW IT'S EQUAL INDEED, CONSIDER THE TRAVELLING DOG PROBLEM...*
P.P.
* SORRY, THIS CARTOON IS TOO SMALL TO CONTAIN THE PROOF

La dernière ….

The Register®

Biting the hand that feeds IT

Science

P≠NP proof fails, Bonn boffin admits

Norbert Blum says his proposed solution doesn't work

By Thomas Claburn in San Francisco 31 Aug 2017 at 19:16

La NP-complétude

Le pourquoi

Si on savait que $P \neq NP$, on pourrait dire que des problèmes dans P sont « faciles » ou « solvables », alors que les problèmes qui sont dans NP et ne sont pas dans P ne le sont pas.

Hélas, nous ne savons pas !

La réduction polynomiale nous fournit un outil intéressant : en effet tous les problèmes de P sont polynomialement équivalents.

Et dans NP, il peut y avoir, éventuellement, d'autres classes d'équivalence.

Et parmis les différentes classes d'équivalence, il peut y avoir une classe des plus difficiles ! (un maximum, dans l'ordre quotient).

Ce maximum est dans NP mais pas dans P – sauf si P=NP !!!!!!!!!

Cette classe d’équivalence s’appelle la classe des problèmes NP-complètes.

Formellement

Définition : un problème Π est dit NP-complet,

si :

- Π est dans NP

et

- tout problème Π' de NP peut être réduit polynomialement à Π.

Ceci paraît très difficile à prouver !!!!!

Heureusement …

COOK, a prouvé qu’un problème (connu sous le nom SAT) est NP-complet.

D’autres ont prouvé que d’autres problèmes sont NP-complets.

Nous pouvons utiliser tout cela, car il suffit de prouver qu’un problème déjà connu comme NP-complet se réduit à notre problème.

Problèmes connus
3DM

NOM : 3DM (Couplage en 3 dimensions)

DONNEES : un ensemble M de triplets (w,x,y), avec w, x et y des éléments de trois ensembles W, X, Y de même cardinalité q.

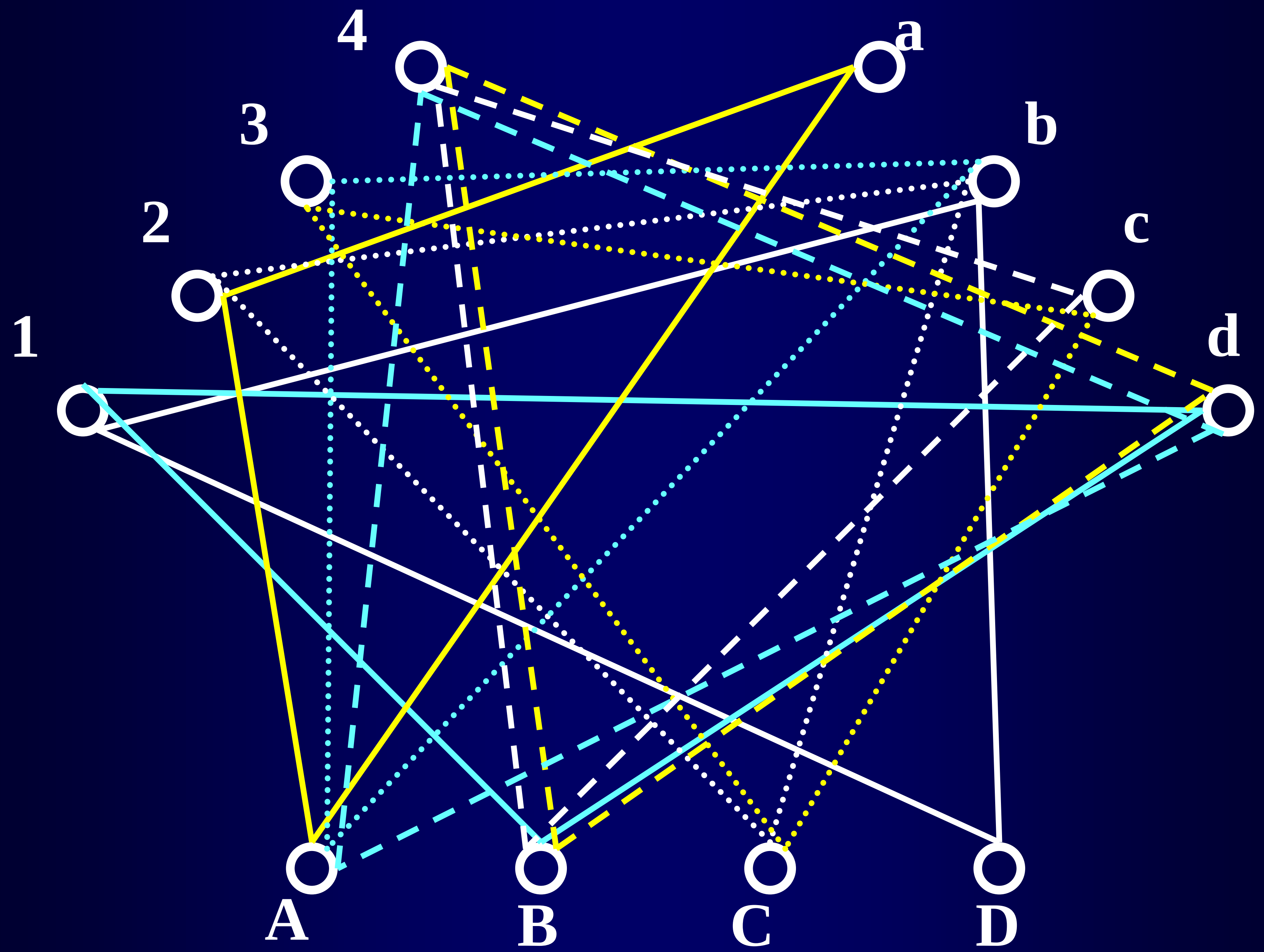
QUESTION : est-ce que M contient un couplage (un sous-ensemble de triplets contenant tous les éléments une fois et une seule) ?

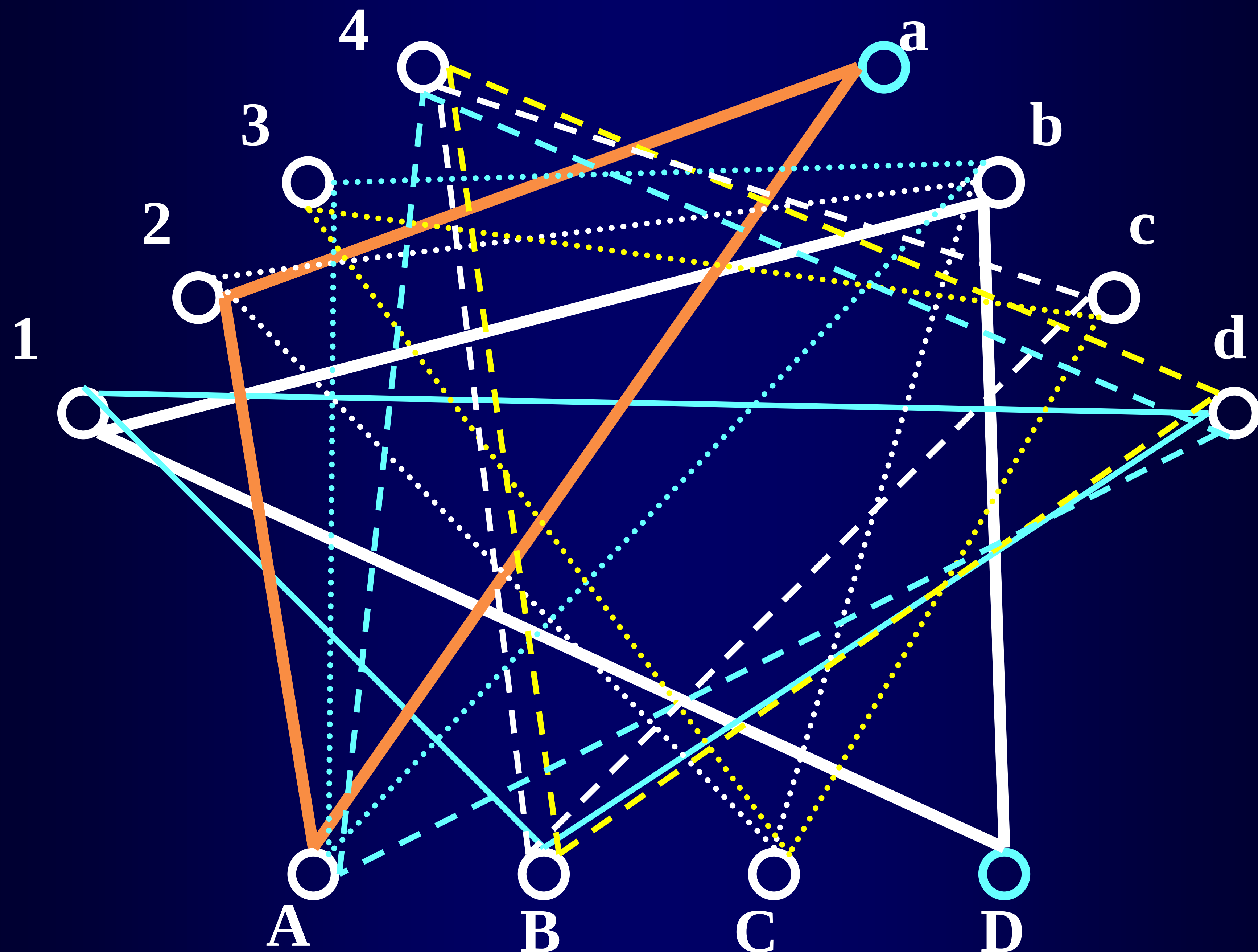
Un exemple de 3DM

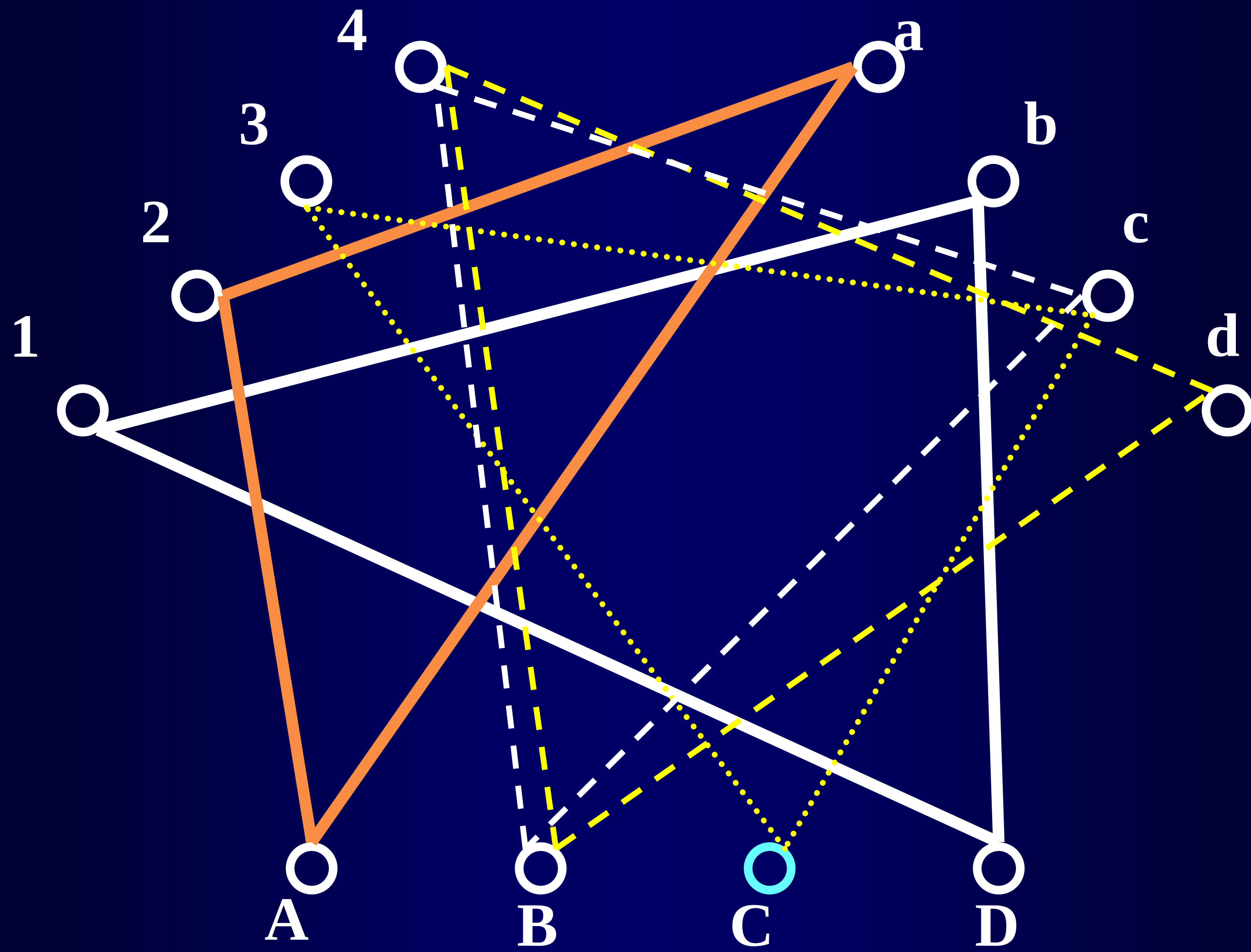
W={1,2,3,4}   X={a,b,c,d}   Y={A,B,C,D}

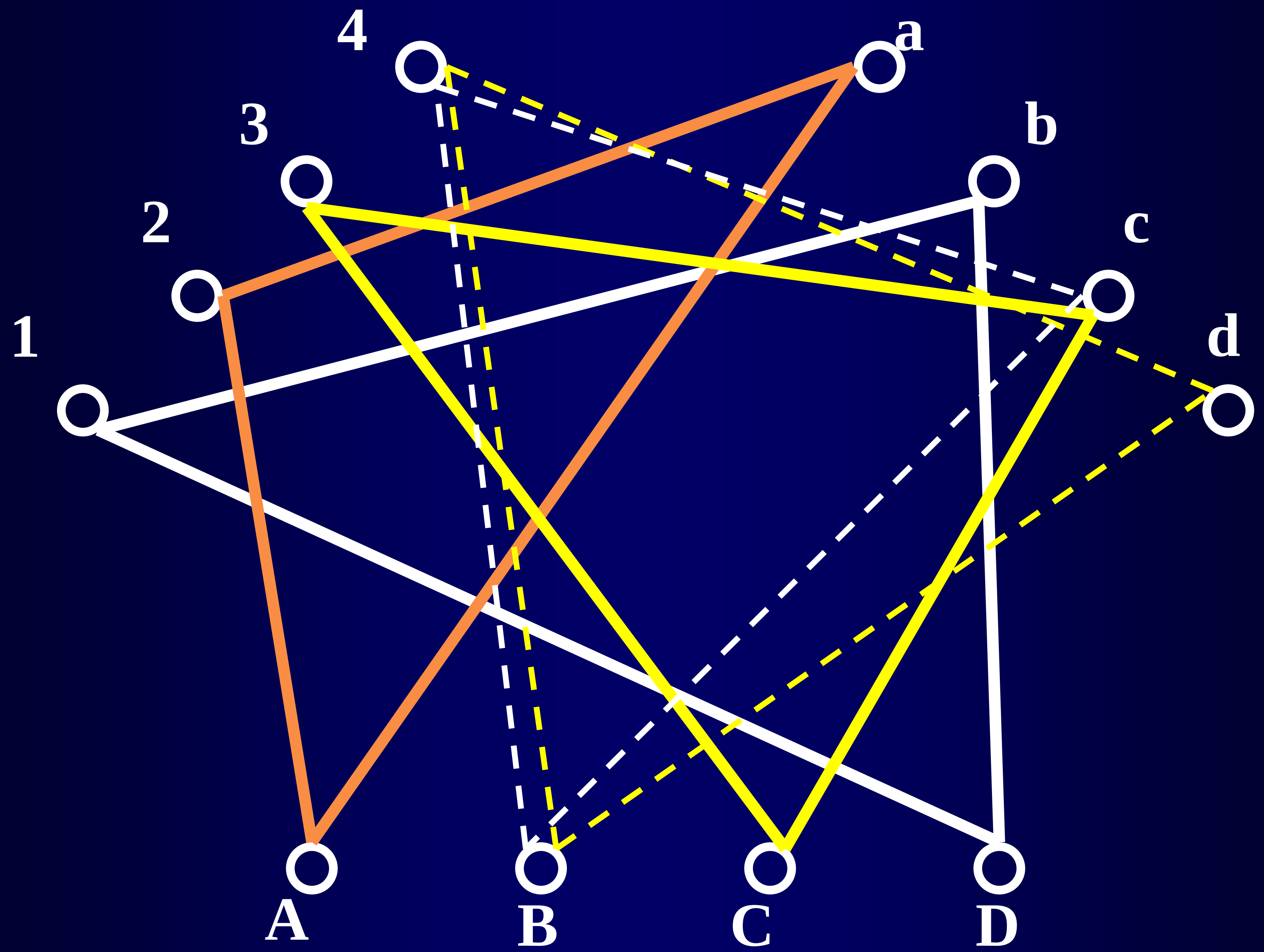
M={(1,b,D), (1,d,B), (2,a,A), (2,b,C), (3,b,A), (3,c,C), (4,d,A), (4,c,B), (4,d,B)}

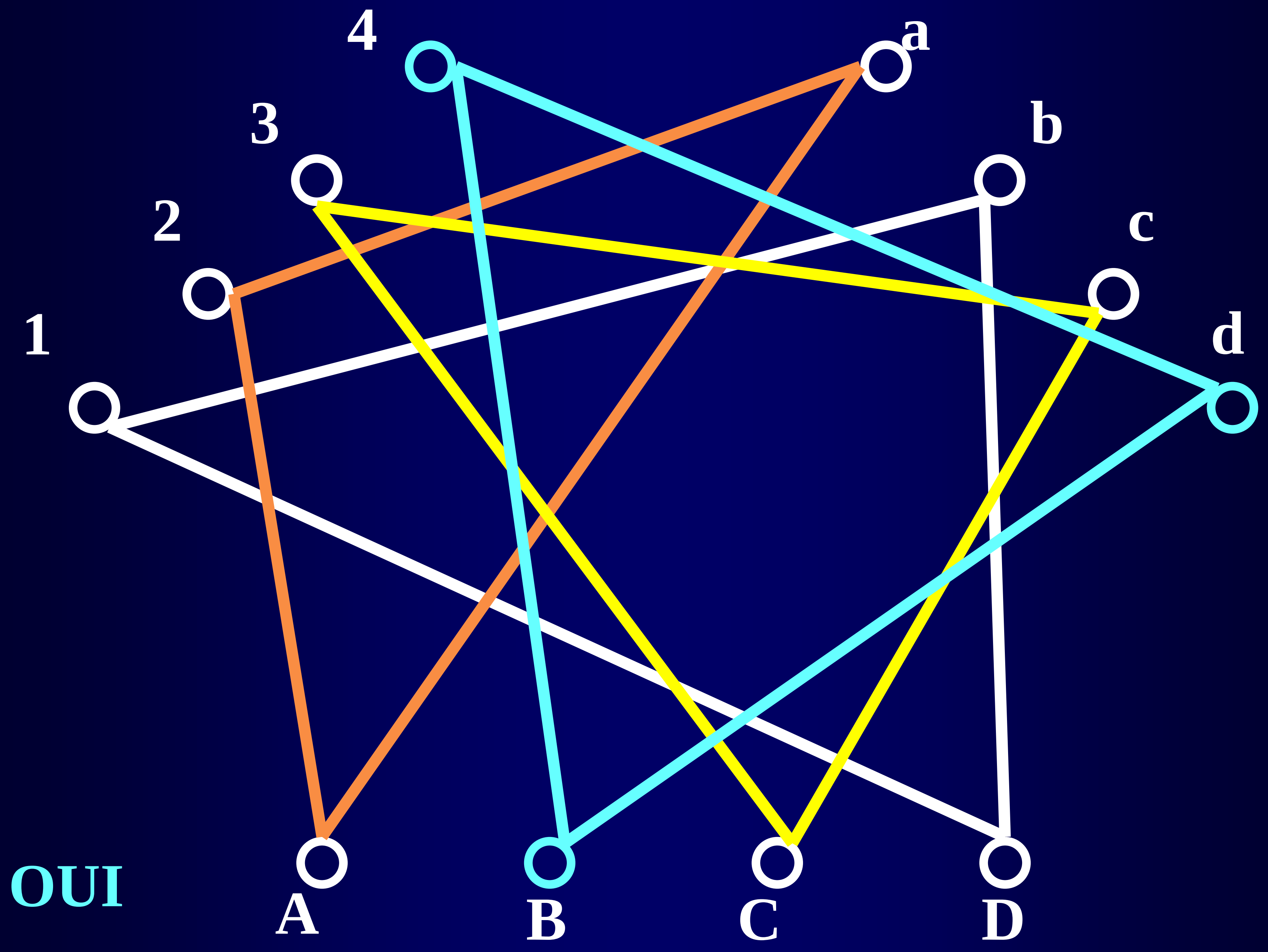
M'={(1,b,D), (2,a,A), (3,c,C), (4,d,B)}


4
a
3
b
2
c
1
d
A
B
C
D


4
a
3
b
2
c
1
d
A
B
C
D


4
a
3
b
2
c
1
d
A
B
C
D


4
a
3
b
2
c
1
d
A
B
C
D


4
a
3
b
2
c
1
d
OUI
A
B
C
D

Problèmes connus
VC

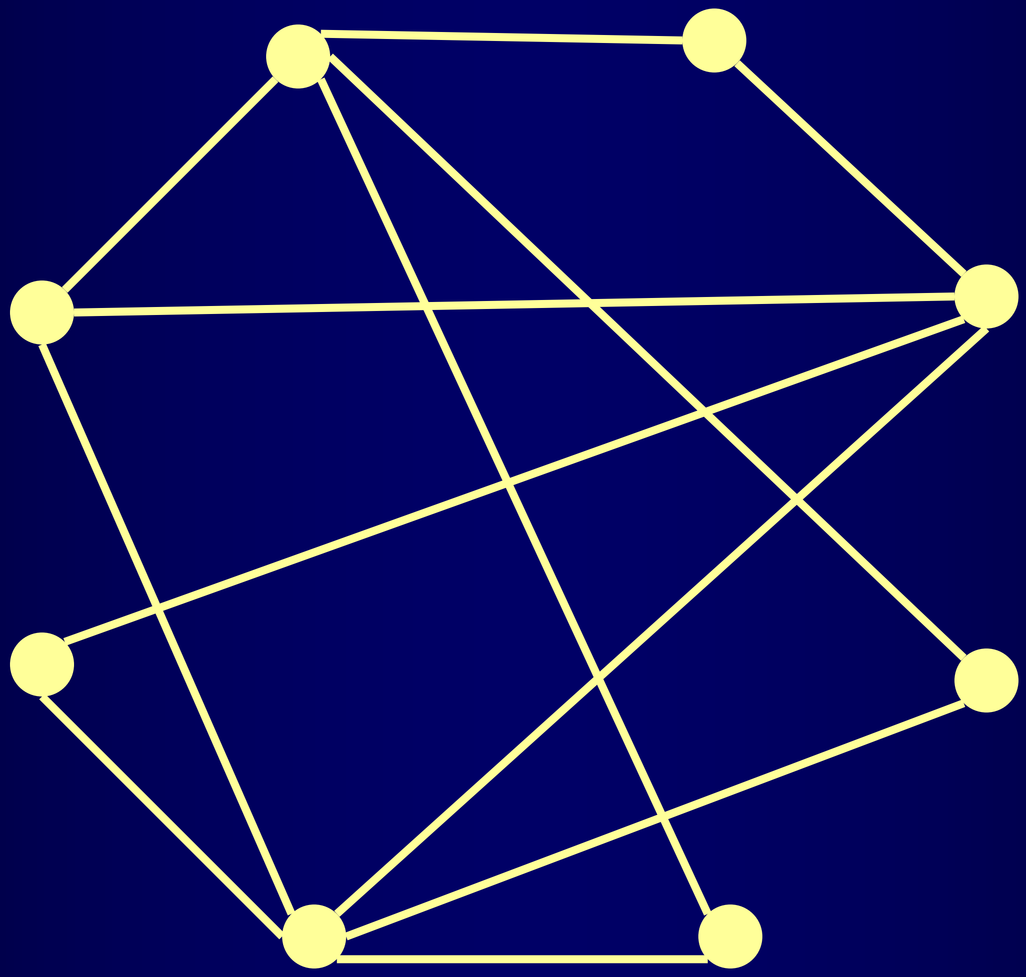
NOM : VC (transversal)

DONNEES : un graphe fini G(V,E), et un entier positif $K \leq |V|$

QUESTION : est-ce que le graphe admet un transversal (un ensemble de sommets contenant au moins une extrémité de toute arête) de cardinalité au plus K ?

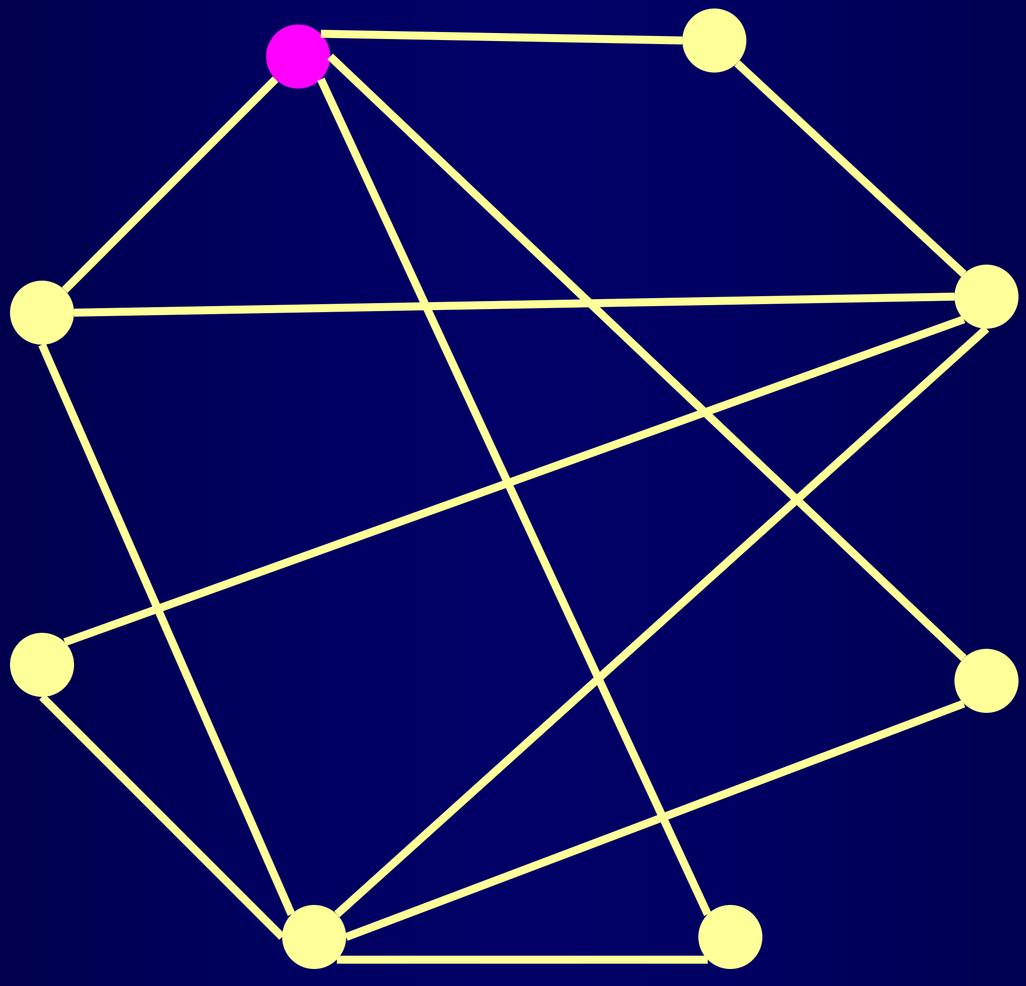
Un exemple VC

K=3



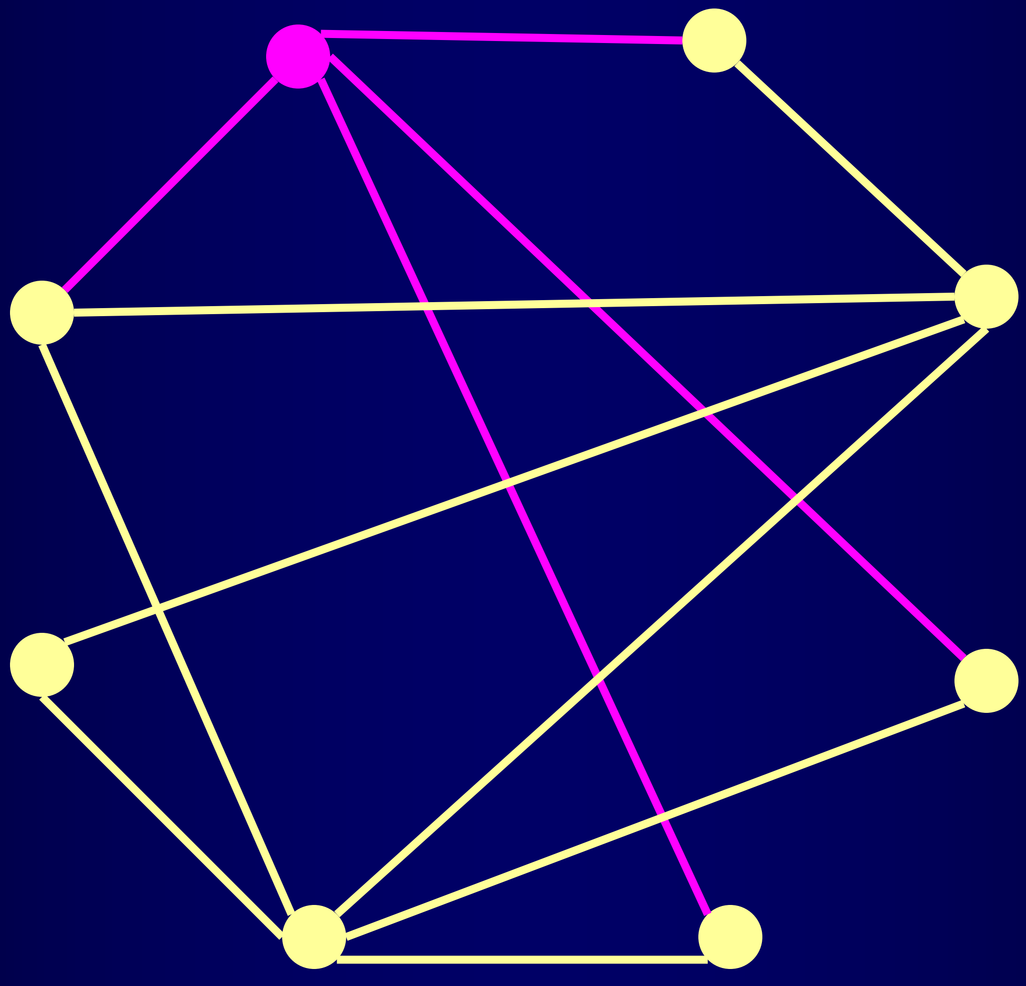
Un exemple VC

K=3



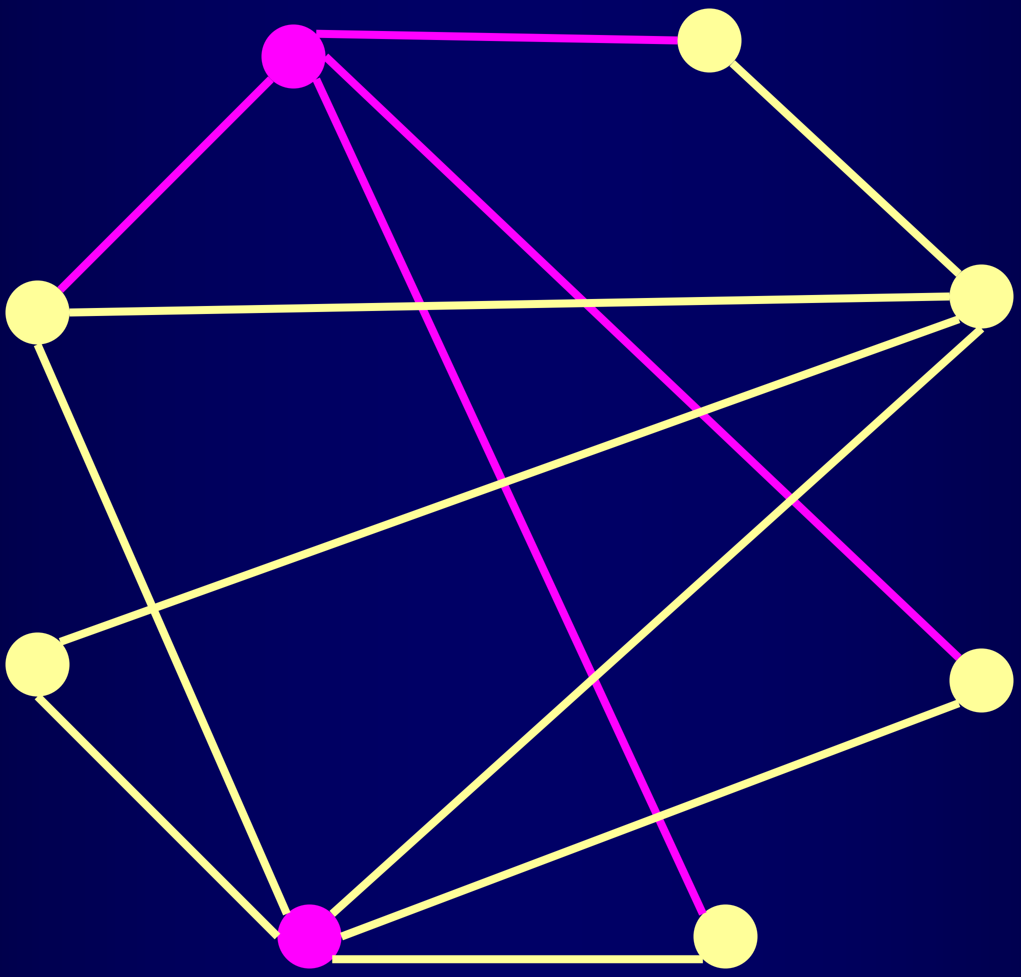
Un exemple VC

K=3



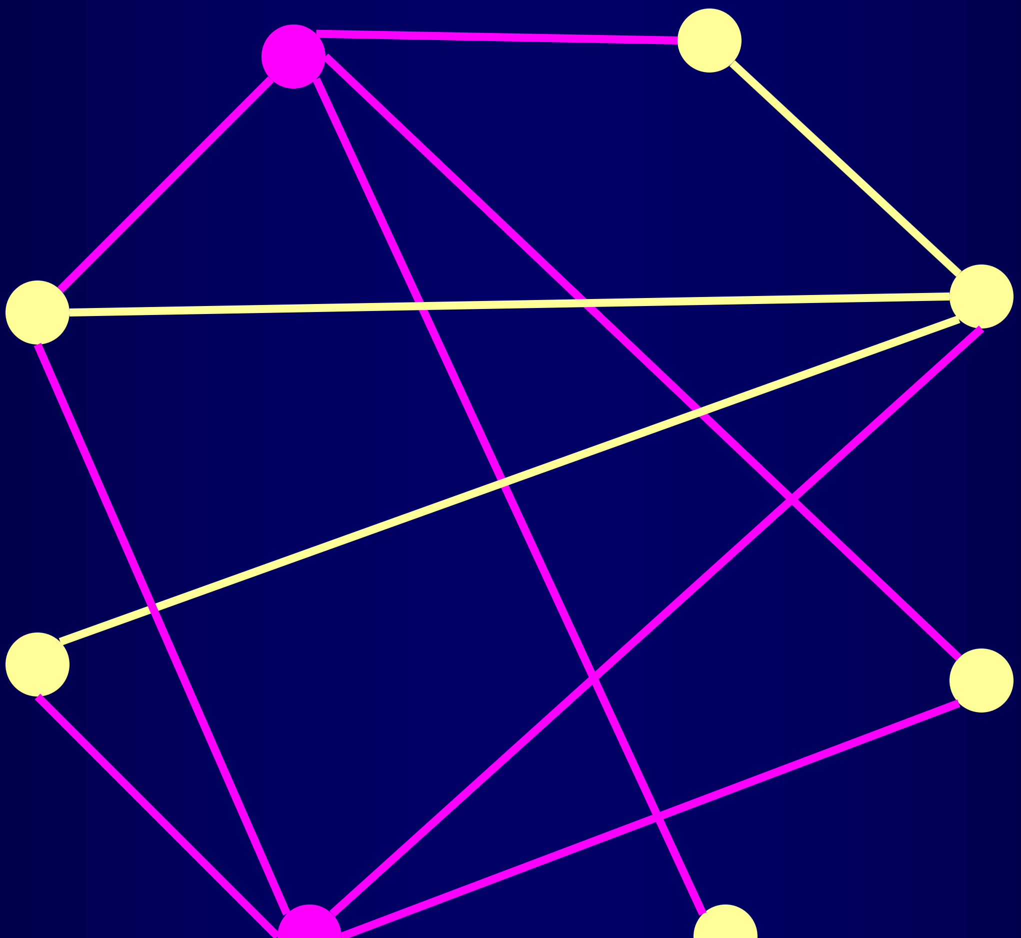
Un exemple VC

K=3



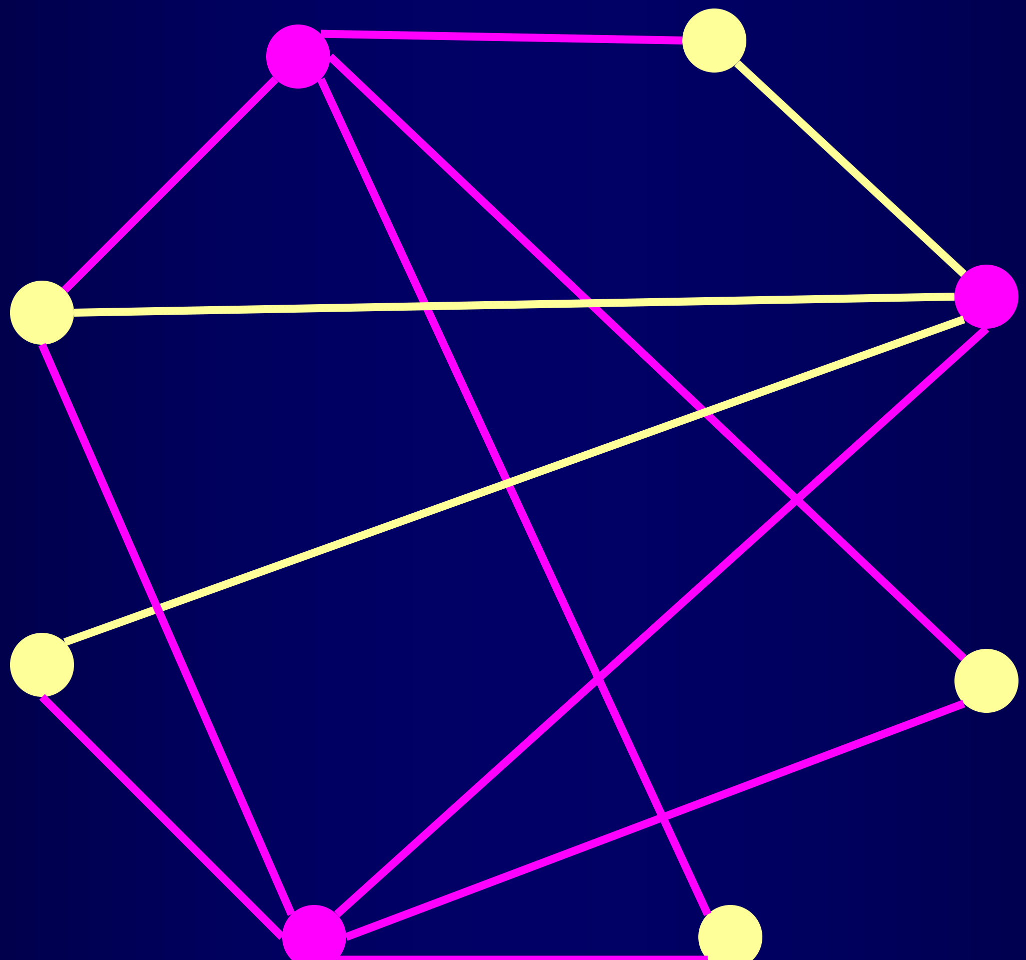
Un exemple VC

K=3



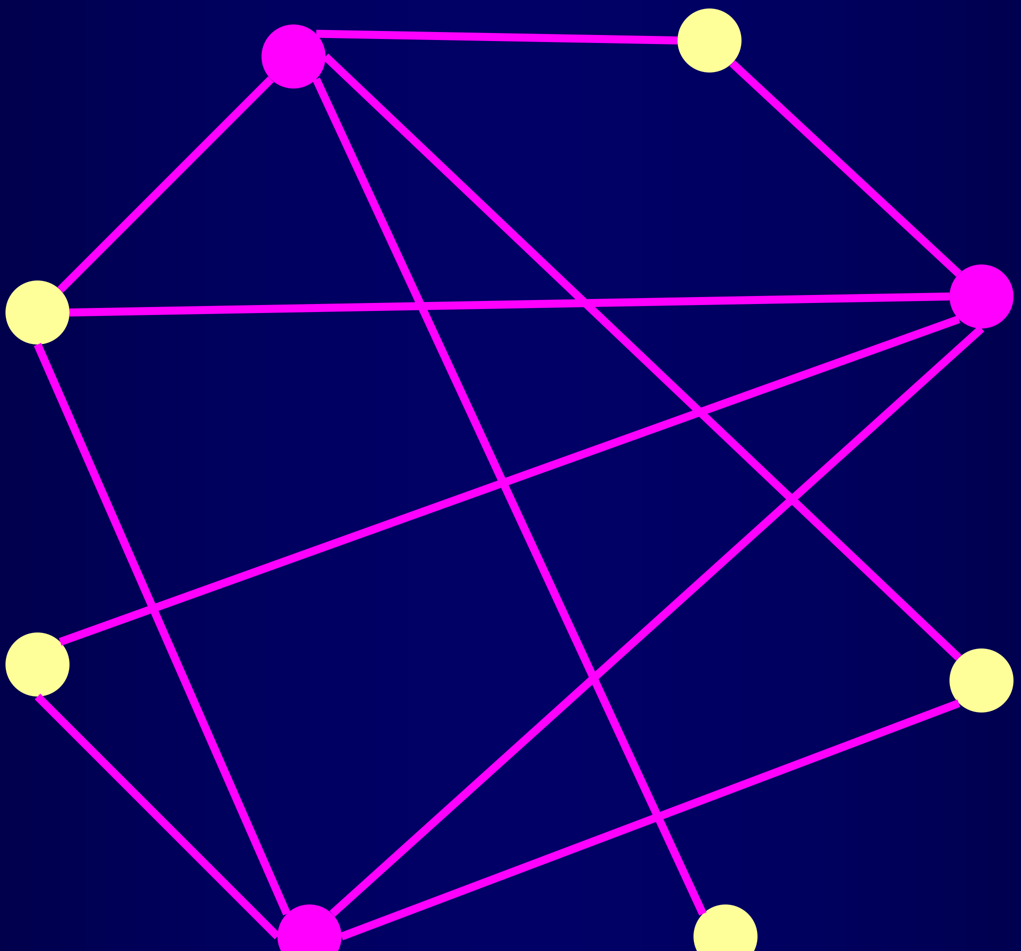
Un exemple VC

K=3



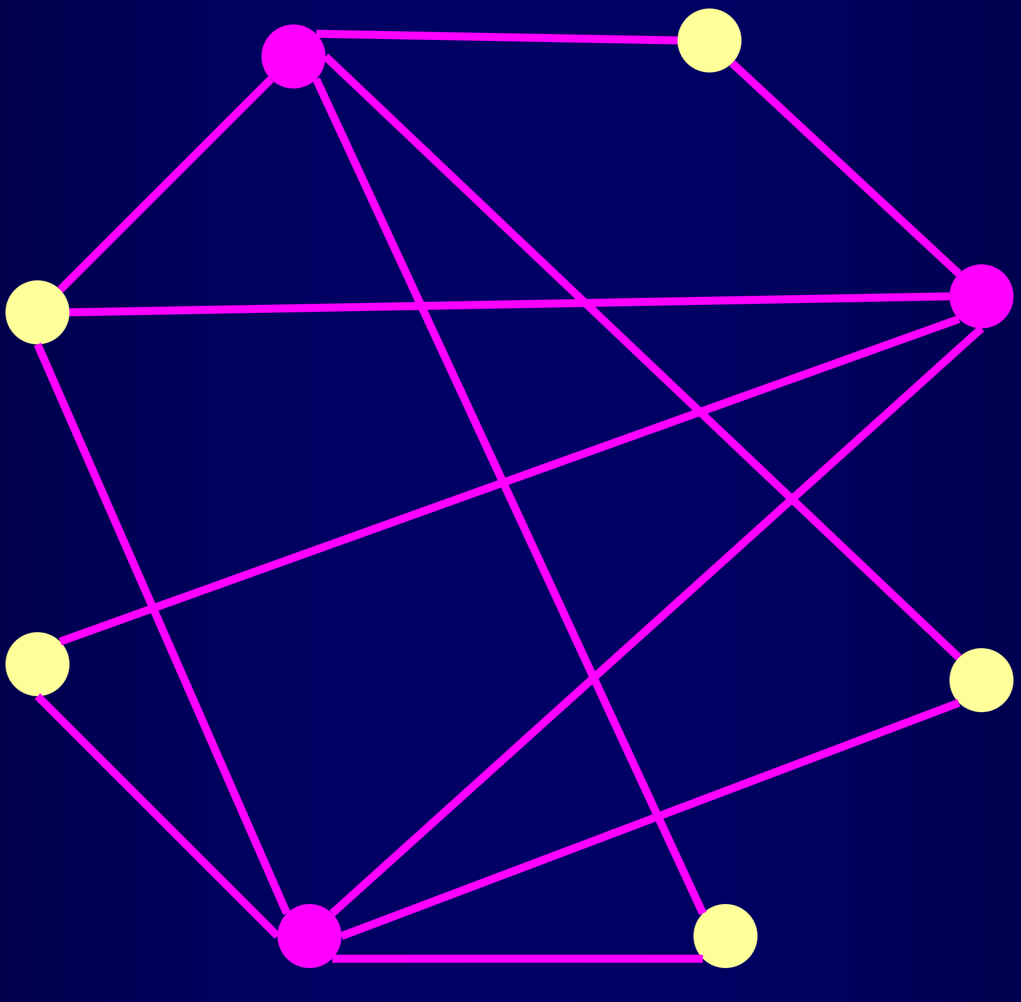
Un exemple VC

K=3



Un exemple VC

K=3



OUI

Problèmes connus
CLIQUE

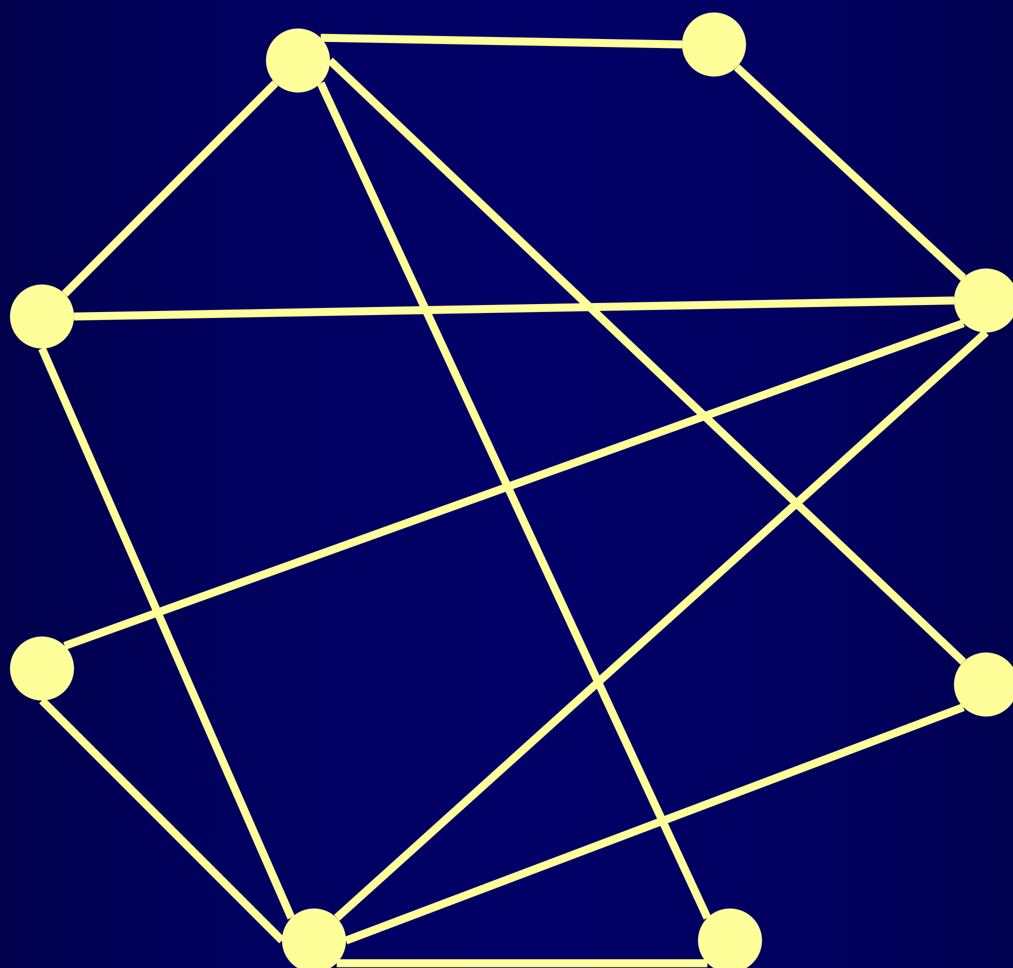
NOM : CLIQUE

DONNEES : un graphe fini G(V,E), et un entier positif $C \leq |V|$

QUESTION : est-ce que le graphe admet un clique (sous-graphe complet) de cardinalité au moins C ?

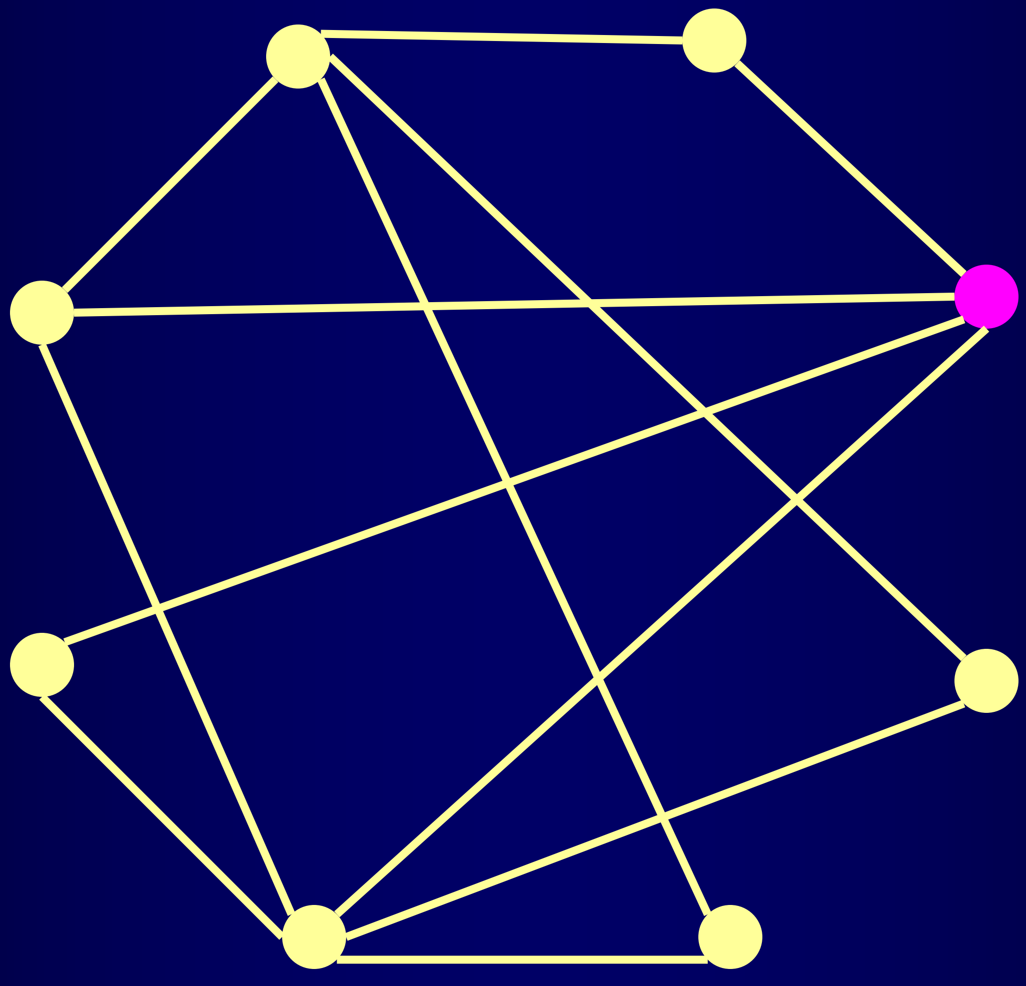
Un exemple CLIQUE

K=3



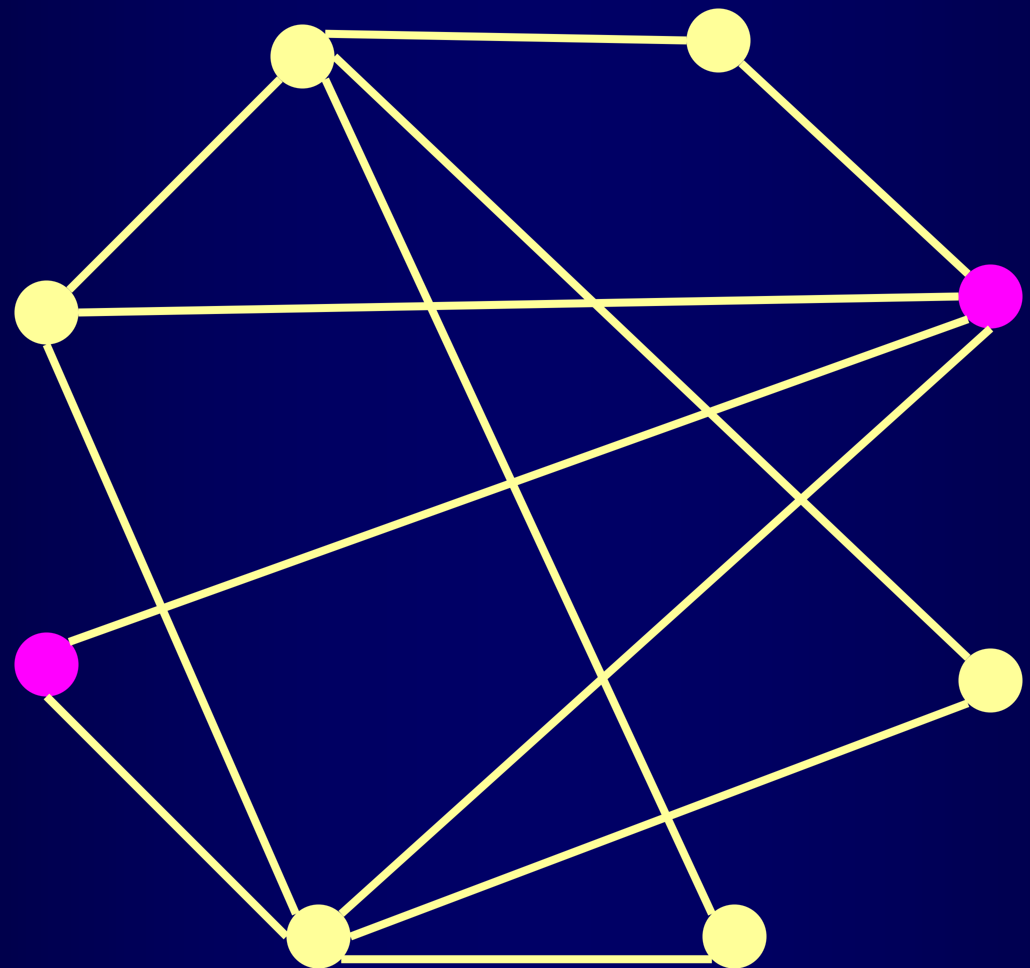
Un exemple CLIQUE

K=3



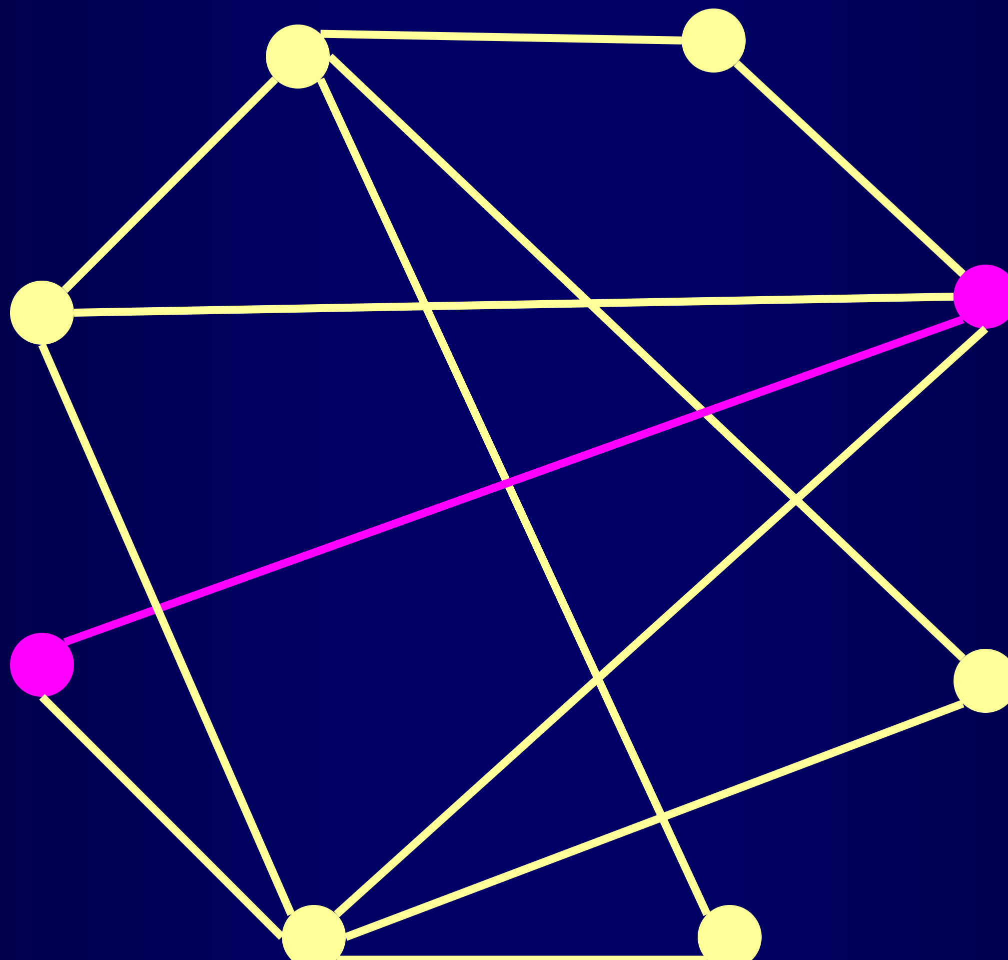
Un exemple CLIQUE

K=3



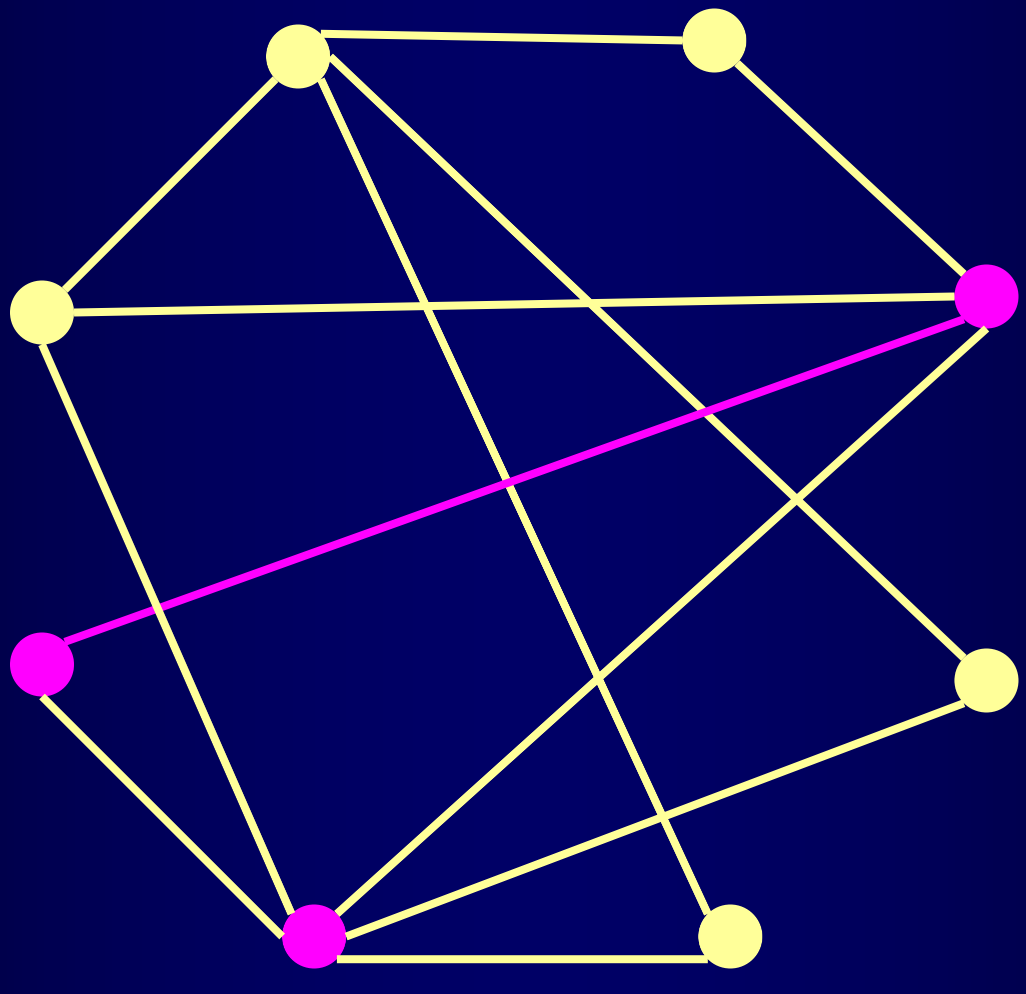
Un exemple CLIQUE

K=3



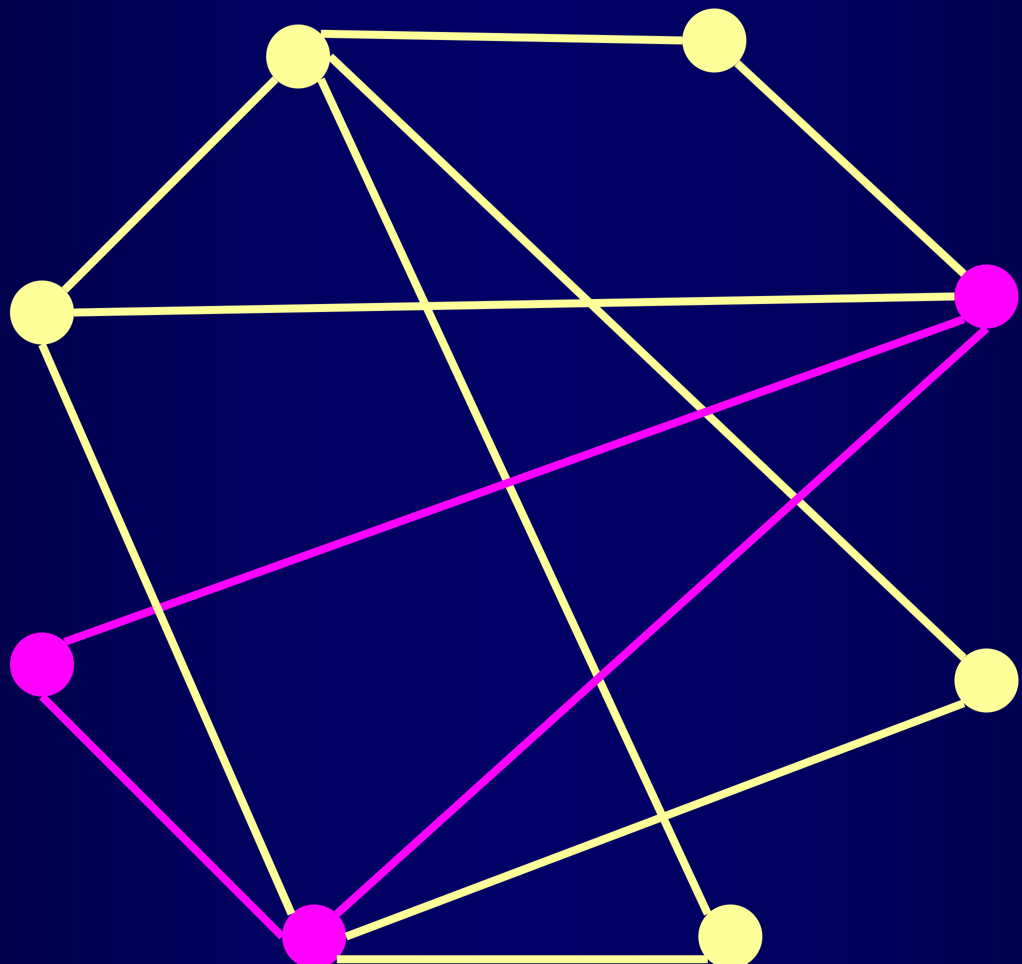
Un exemple CLIQUE

K=3



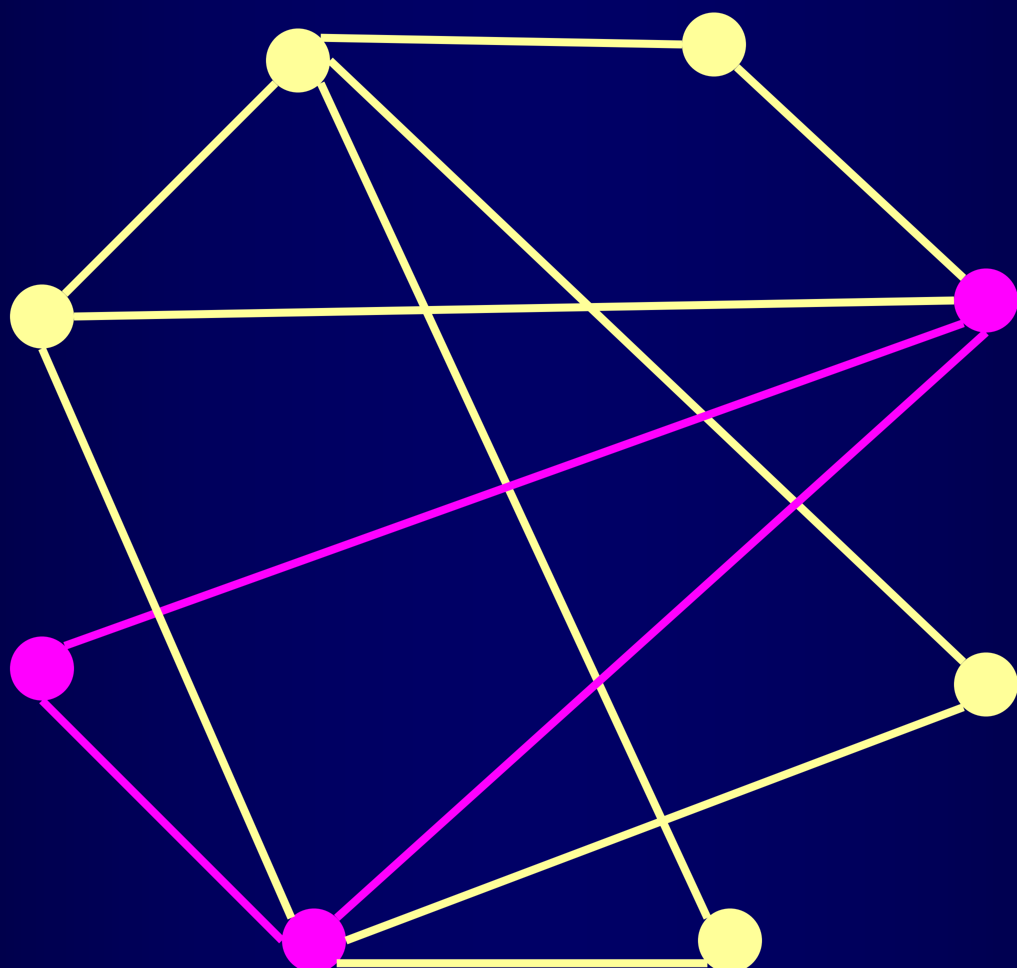
Un exemple CLIQUE

K=3



Un exemple CLIQUE

K=3



OUI

Problèmes connus (9)
STABLE

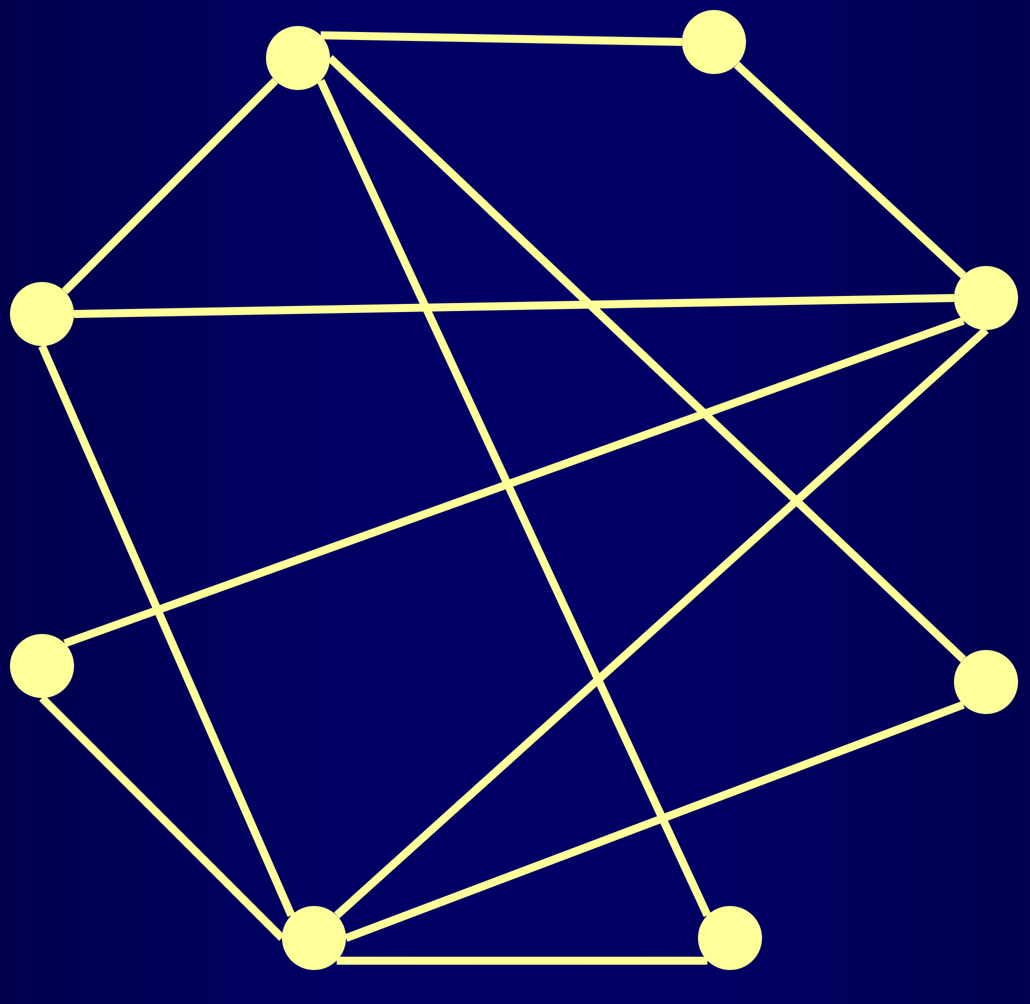
NOM : STABLE

DONNEES : un graphe fini G(V,E), et un entier positif $J \leq |V|$

QUESTION : est-ce que le graphe admet un stable (sous-graphe vide) de cardinalité au moins J ?

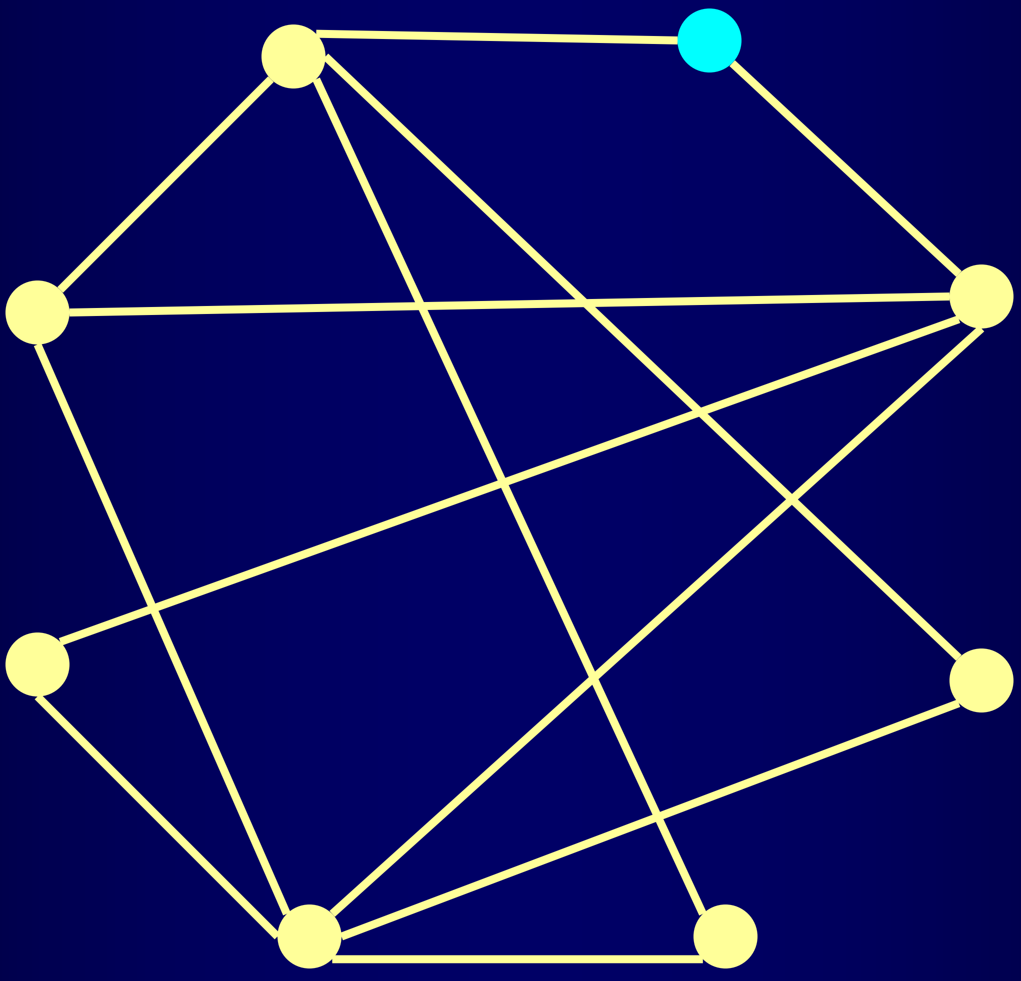
Un exemple STABLE

J=5



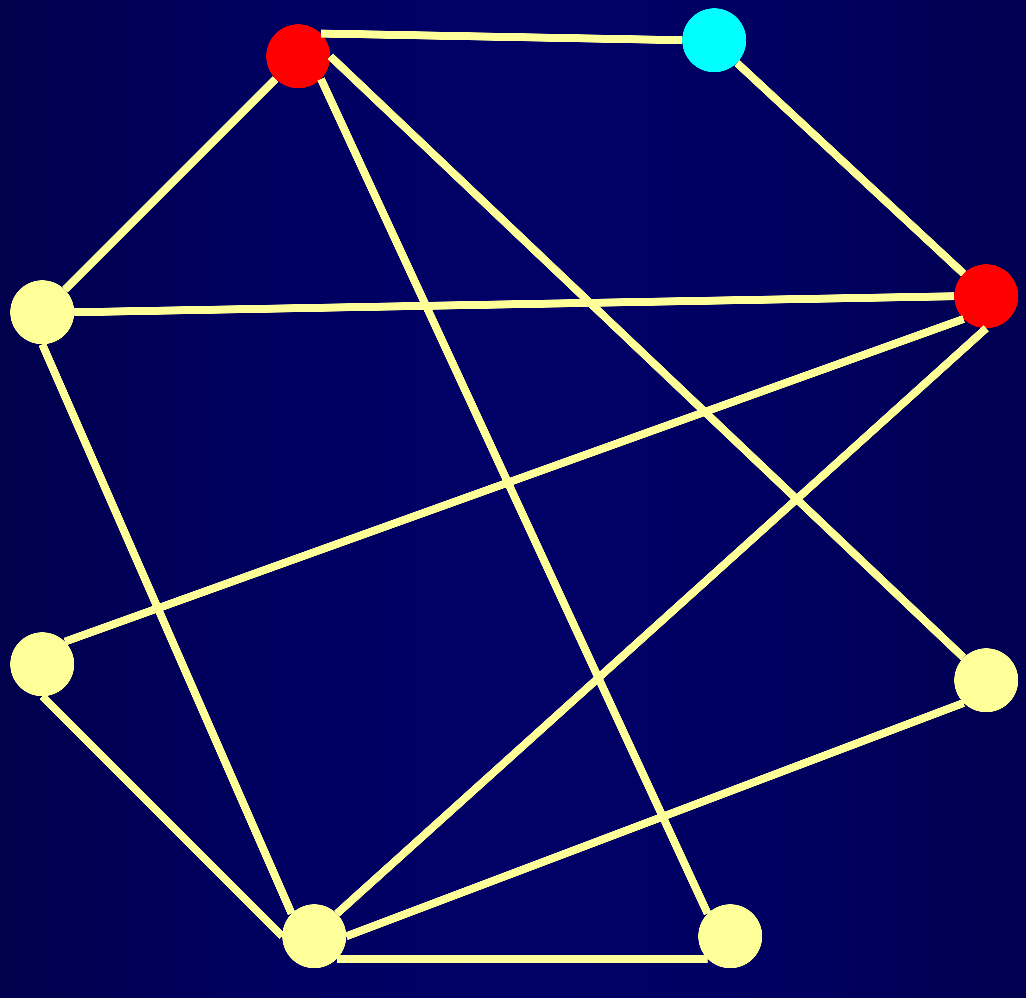
Un exemple STABLE

J=5



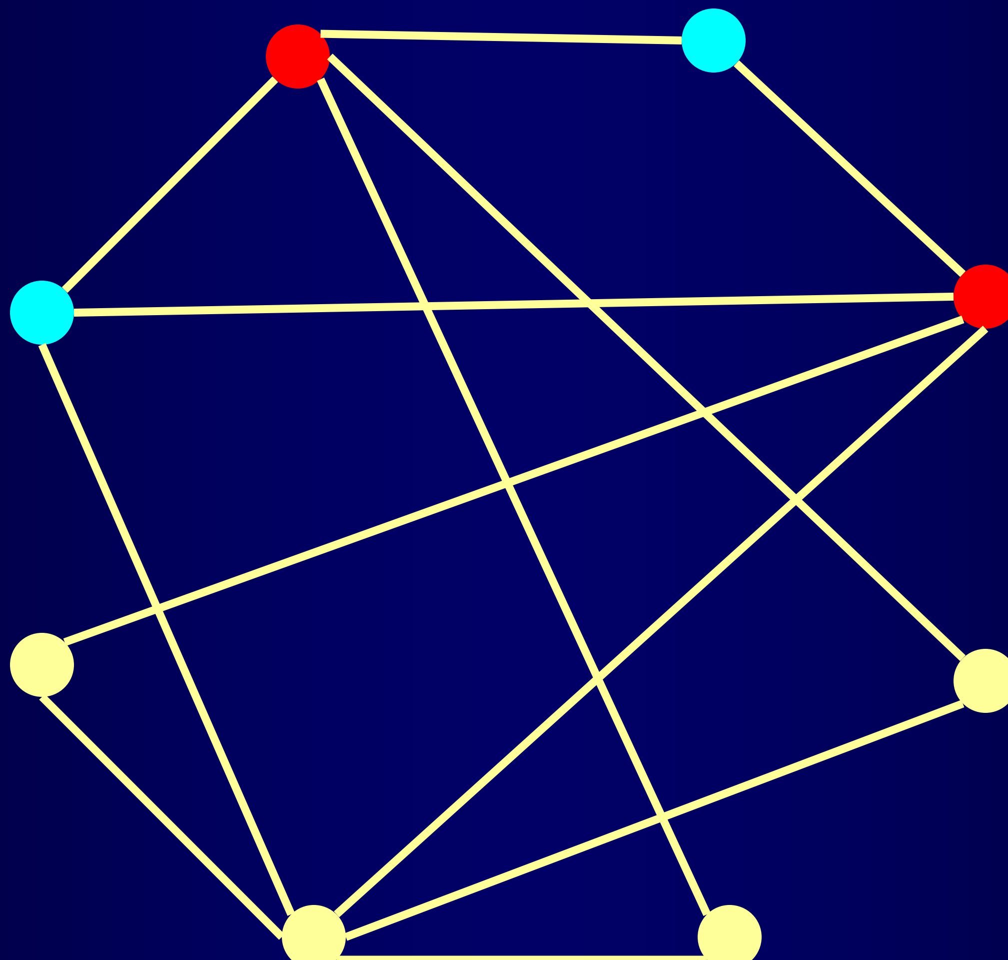
Un exemple STABLE

J=5



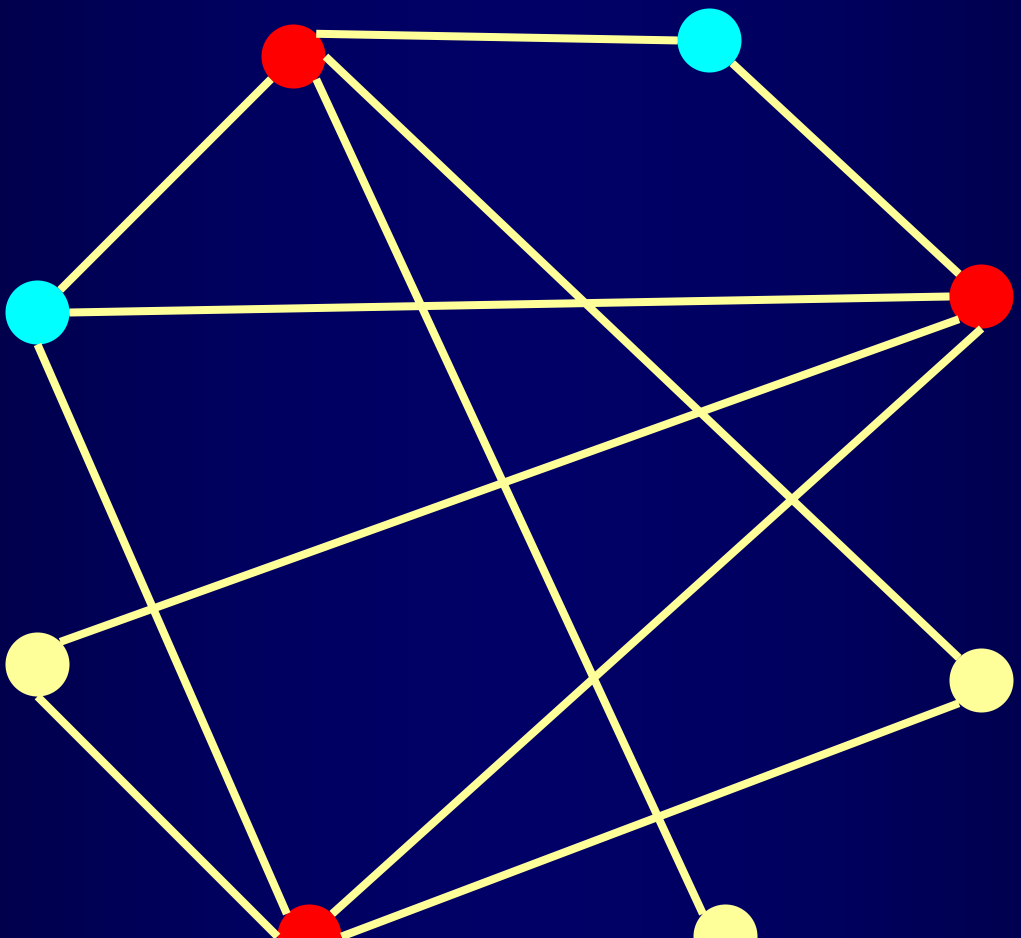
Un exemple STABLE

J=5



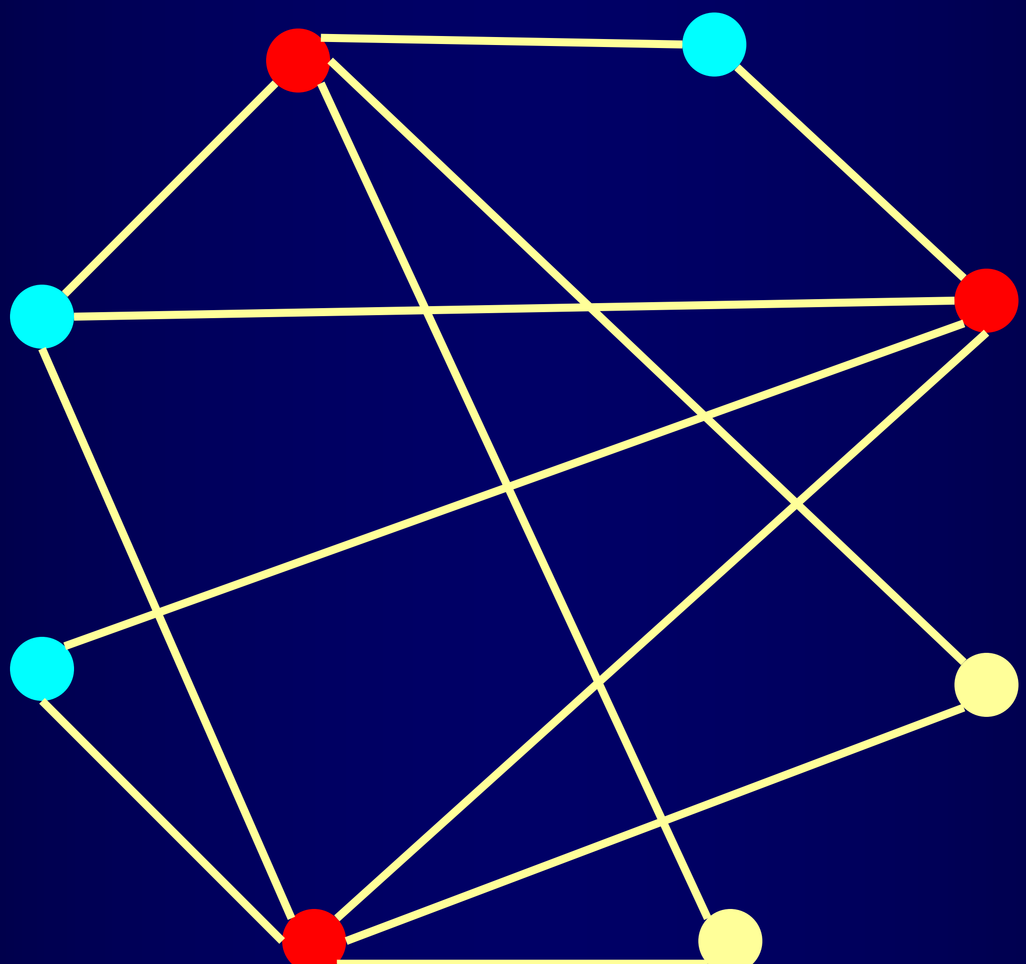
Un exemple STABLE

J=5



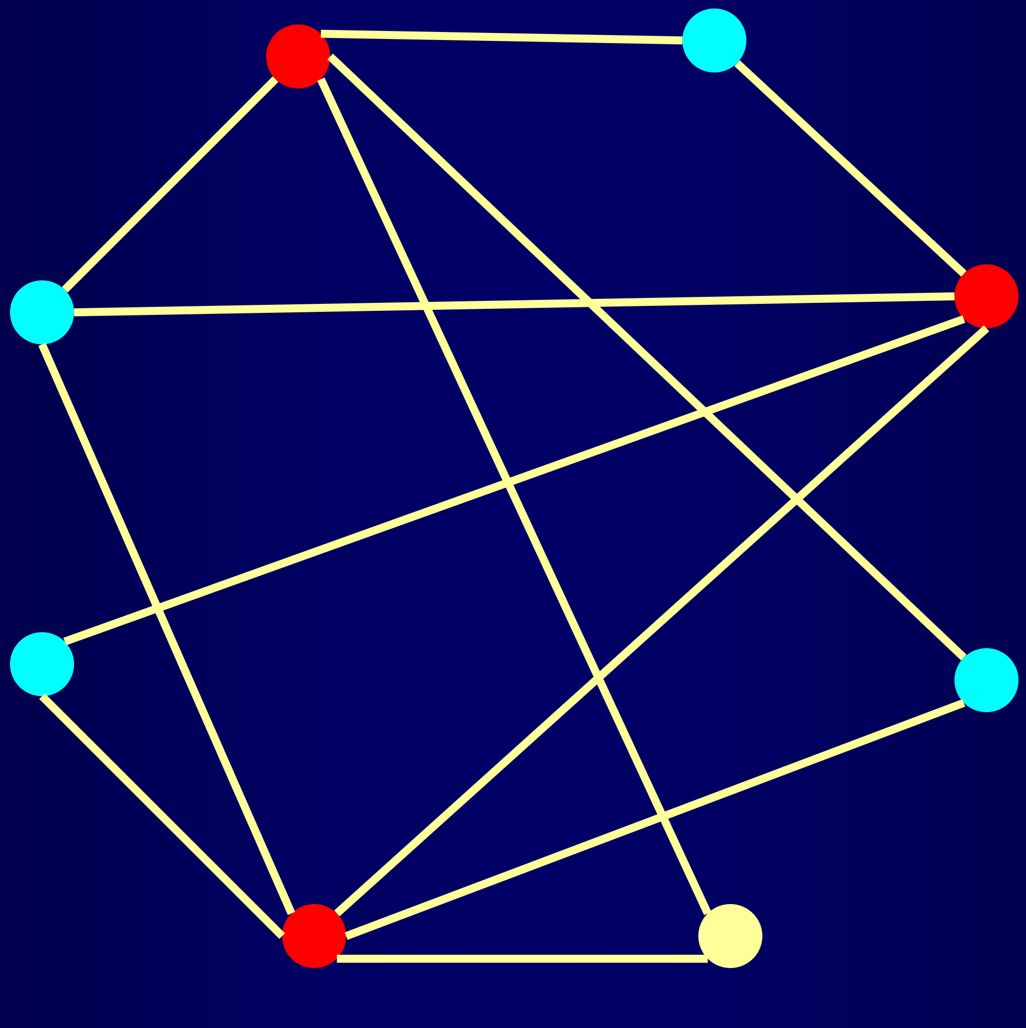
Un exemple STABLE

J=5



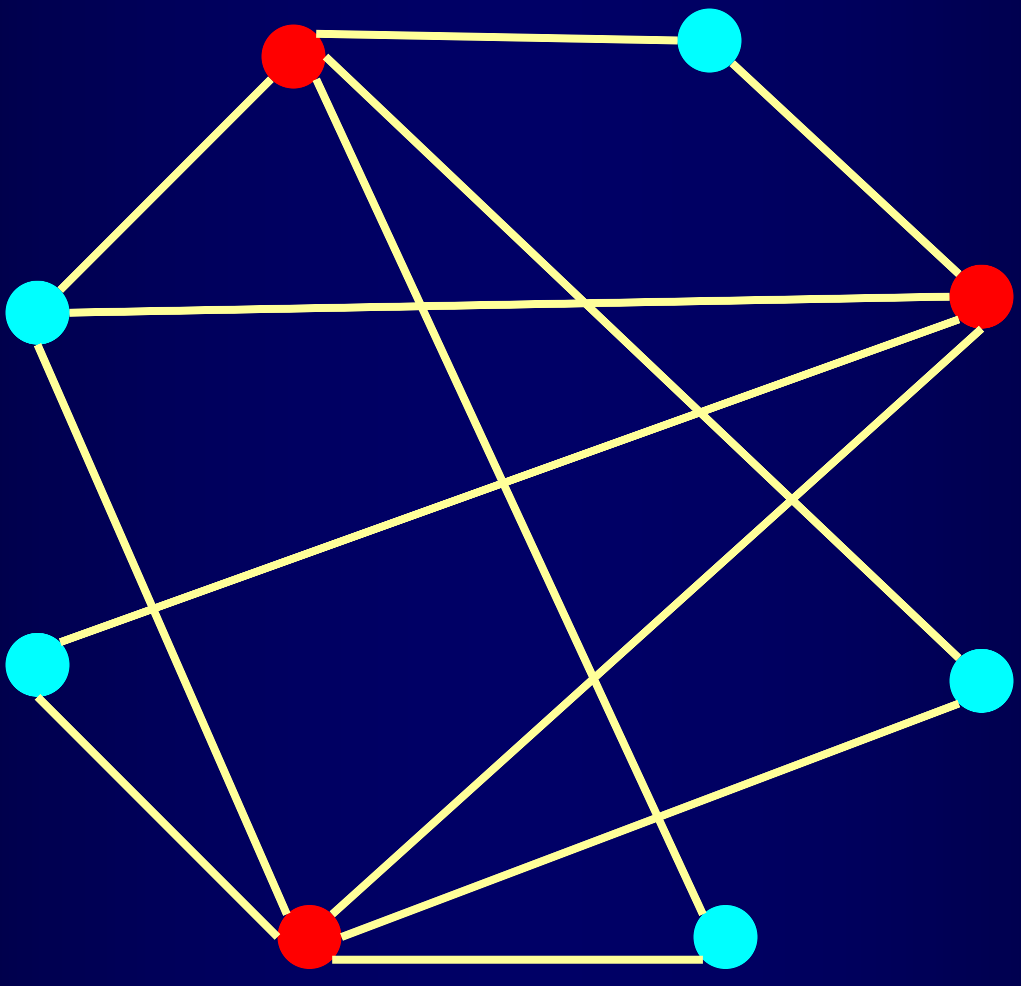
Un exemple STABLE

J=5



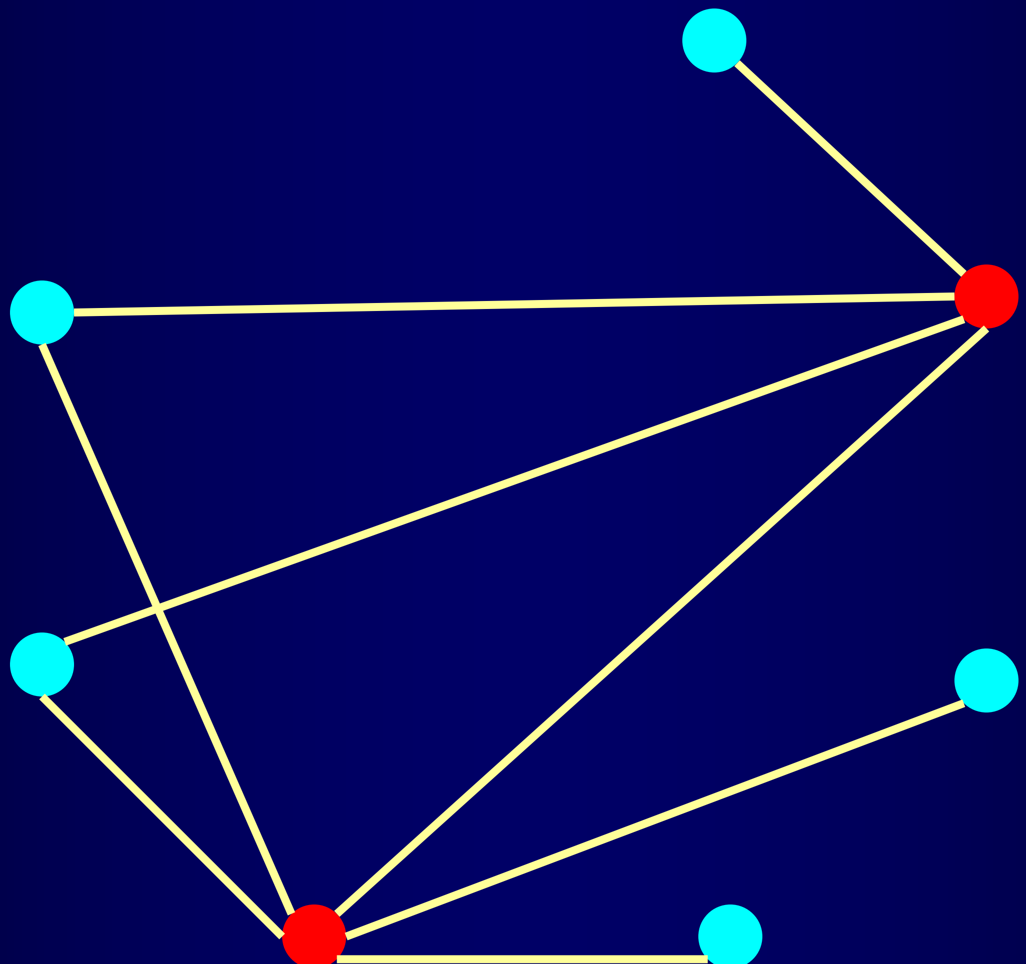
Un exemple STABLE

J=5



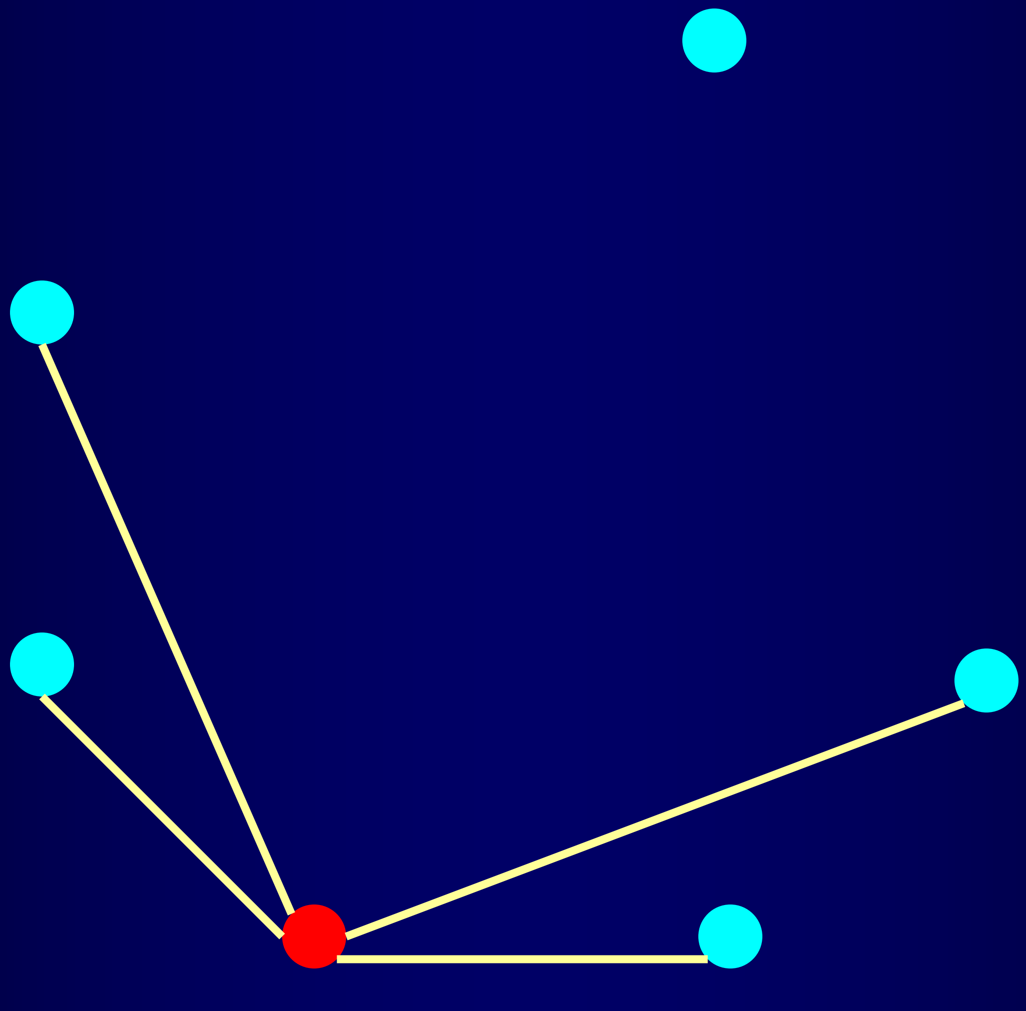
Un exemple STABLE

J=5



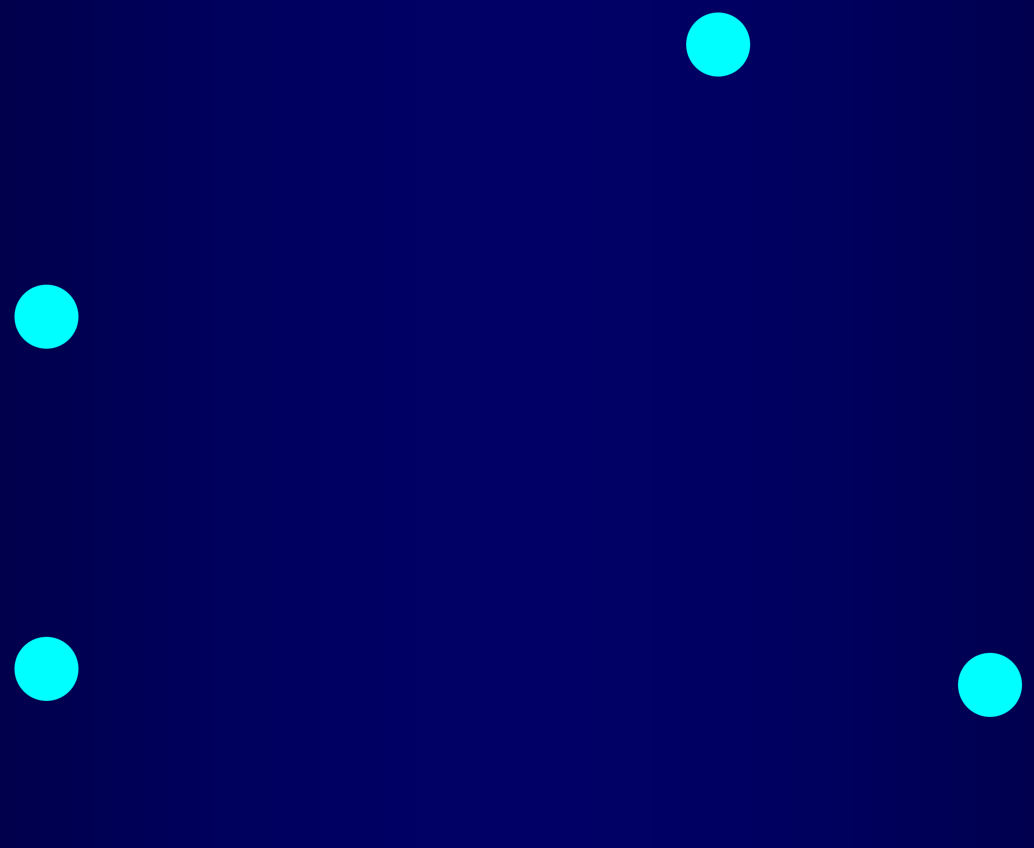
Un exemple STABLE

J=5



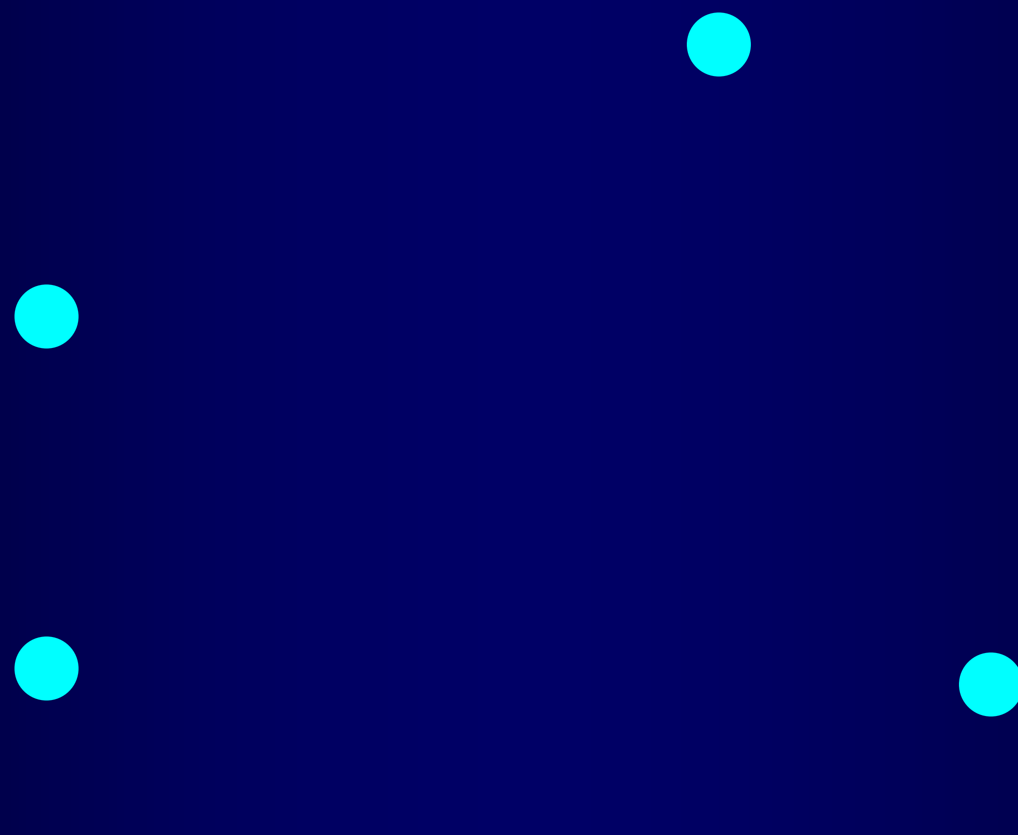
Un exemple STABLE

J=5



Un exemple STABLE

J=5



OUI

Problèmes connus

PARTITION

NOM : PARTITION

DONNEES : un ensemble fini d'entiers non-négatifs A

QUESTION : est-ce qu'il existe une partition de A en deux ensembles A' et A", telle que la somme des éléments de A' soit égale à la somme des éléments de A" ?

Un exemple PARTITION

A={1, 3, 5, 11, 23, 38, 49}

La réponse est : OUI

A' ={1, 3, 23, 38}

A''={5, 11, 49}

Problèmes connus

CYCLEHAM

NOM : CYCLEHAM (cycle hamiltonien)

DONNEES : un graphe fini G(V,E), sous forme de liste d'adjacence

QUESTION : est-ce que le graphe admet un cycle hamiltonien ?

Problèmes connus

Le problème SAT

NOM : SAT (satisfiabilité)

DONNEES : une formule sous FNC

QUESTION : est-ce que la formule est satisfiable ?

Rappels de logique

- Une ***variable logique*** est une variable qui peut prendre une des deux valeurs vrai ou faux.
- Un ***littéral*** est une variable ou la négation d'une variable
- Une ***formule logique*** est une expression contenant des variables, reliées par les opérations de négation, conjonction et disjonction.
- Une ***clause*** est la disjonction de littéraux.
- Le ***degré*** de la clause est le nombre de littéraux qu'elle contient.
- Une formule en **forme normale conjonctive** (**FNC**) est une conjonction de clauses.

Exemple de formule en FNC

$$(x_1 \vee \neg x_2 \vee x_3) \wedge (\neg x_1 \vee x_4 \vee \neg x_5) \wedge$$
$$(x_2 \vee \neg x_4 \vee x_5) \wedge (x_2 \vee \neg x_3 \vee \neg x_5) \wedge$$
$$(x_1 \vee x_4 \vee x_5) \wedge (x_1 \vee \neg x_2 \vee \neg x_3) \wedge$$
$$(x_1 \vee x_2 \vee x_3) \wedge (x_2 \vee \neg x_3 \vee x_4)$$

¼ des valuations satisfont la formule (8/32)

X1	X2	X3	X4	X5	X1 v ¬X2 v X3	¬X1 v X4 v ¬X5	X2 v ¬X4 v X5	X2 v ¬X3 v ¬X5	X1 v X4 v X5	X1 v ¬X2 v ¬X3	X1 v X2 v X3	X2 v ¬X3 v X4
V	V	V	V	V	V	V	V	V	V	V	V	V
V	V	V	V	F	V	V	V	V	V	V	V	V
V	V	V	F	F	V	V	V	V	V	V	V	V
V	V	F	V	V	V	V	V	V	V	V	V	V
V	V	F	V	F	V	V	V	V	V	V	V	V
V	V	F	F	F	V	V	V	V	V	V	V	V
V	F	F	V	V	V	V	V	V	V	V	V	V
V	F	F	F	F	V	V	V	V	V	V	V	V