Cpts 515. 11/16/2020

Reminder: you have a hw to do.
(HW5). if you need extension,
text me 509 338 5089

A is NP-complete if

(1). $A \in NP$

(2). $\forall B \in NP$, $B \leq_m A$.

First NP-complete problem,

Thm. SAT is NP-complete.

SAT: Given a Boolean formula $f(x_1, \ldots, x_k)$

Question: $\exists$ Boolean values $x_1, \ldots, x_k$ s.t.

$f(x_1 \ldots x_k)$ is true ?

$x_1 \vee \overline{x_2}$ is satisfiable,

$x_1 \wedge \overline{x_1}$ is not satisfiable.

How to prove a problem X is NP-complete:

(1). $\delta \leq_m X$

a known NP-complete.

(2). $X \in NP$. // Design a nondet. poly-time alg.

Remark: A subproblem can be harder than the whole, can be easier than the whole problem.

3SAT. (3CNF).

We can write any Boolean formula into CNF (Conjunctive Normal form):

$$\_\_\_\_ \wedge \_\_\_\_ \wedge \_\_\_\_ \wedge \ldots$$

each is $(\_ \vee \_ \vee \_ \vee \ldots)$

each is a Bool var or its negation.

3CNF Example:

$$\_\_\_ \wedge \_\_\_ \wedge \_\_\_ \wedge \_\_\_ \ldots$$

$$(\_ \vee \_ \vee \_)$$

is a Boolvar or its negation.

Example,

$$(x_1 \vee \overline{x_2} \vee x_3) \wedge (\overline{x_1} \vee x_2 \vee x_3) \wedge (\ldots) \wedge \ldots$$

3SAT: Given: a Boolean formula $f(x_1 \ldots x_k)$ in the form of 3CNF,

Question: $\exists x_1, \ldots, x_k$, $f(x_1 - x_k)$ is true?

Remark: 3SAT is a subproblem of SAT.

Thm. 3SAT is NP-complete.

Proof. (1). 3SAT $\in$ NP. We design a nondet. poly-time alg for 3SAT:

input $f(x_1 - x_k)$.

Guess bool values $x_1 \ldots x_k$

det. poly-time $\{$ Check $f(x_1 \ldots x_k)$ is indeed true.

if yes, ret yes

crash.

(2). SAT $\leq_m$ 3SAT. We need demonstrate a translation from Boolean formula F to 3CNF Boolean formula F' s.t.

F is sat. iff F' is sat.

Let $F = \bigwedge F_i$ each F_i is a disjunction of literals. Then $F' = \bigwedge F_i'$ where F_i', which is a ~~a~~ conjunction of disjunctions over 3 literals, are obtained as follows.

Example: $(x_1 \vee x_2 \vee \bar{x}_3 \vee \bar{x}_4 \vee x_5 \vee \bar{x}_6)$

$\Rightarrow (x_1 \vee x_2 \vee y_1) \wedge (\bar{y}_1 \vee \bar{x}_3 \vee y_2) \wedge (\bar{y}_2 \vee \bar{x}_4 \vee y_3) \wedge$
$(\bar{y}_3 \vee x_5 \vee \bar{x}_6)$

Independent Set

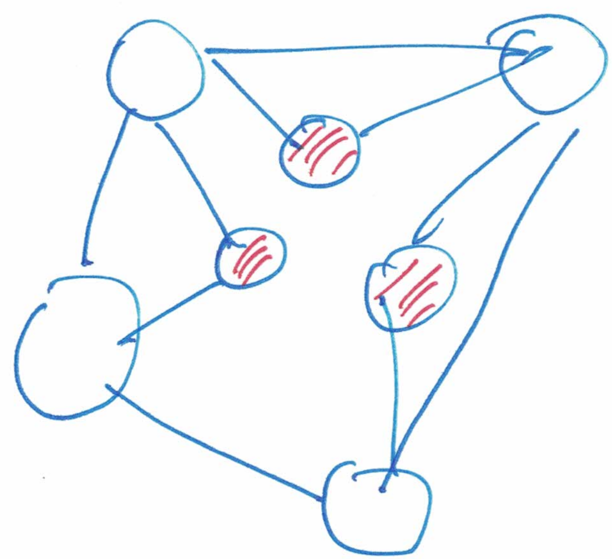
Given: an undirected graph $G = (V, E)$

a number k

Question: $\exists$ a set $I \subseteq V$ s.t.

$|I| = k$ and for each $v, v' \in I$,

$(v, v') \notin E$?



$k = 3$.

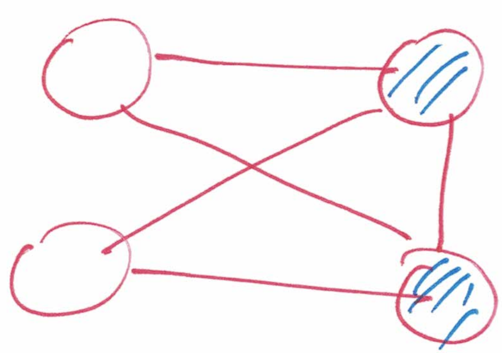
Thm. IDSet is NP-complete.

Proof. 5.16.

Vertex Cover.

Given: $G=(V,E)$, a number k

Question: $\exists C \subseteq V$ s.t. $|C| = k$ and for all $(v, v') \in E$, at least one of v and v' must be in C?



$k=2$.

Thm. VC is NP-complete.

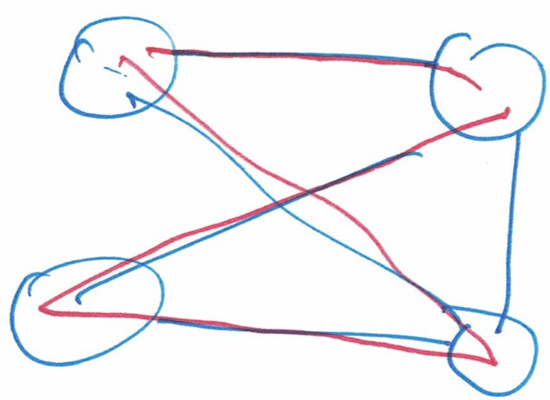
Proof. 516.

Hamiltonian Circuit.

Given: a graph G

Question: Is there a walk that covers every node exactly once?

Example:



Thm. HC is NP-complete.

Proof. Skip. This is considered to be one of the trickiest proof in CS!

NP-complete problem Example: SAT, 3SAT, IDSet, VC, HC.

Famous NP-complete problems:

ILP is NP-complete.

↳ Given: a system of linear inequalities

Question: Any integer solutions to the system?

Remark. LP is in P. (Dantzig's Alg).

Interesting Examples.

① Graph Isomorphism. $\leftarrow$ machine learning on structured data

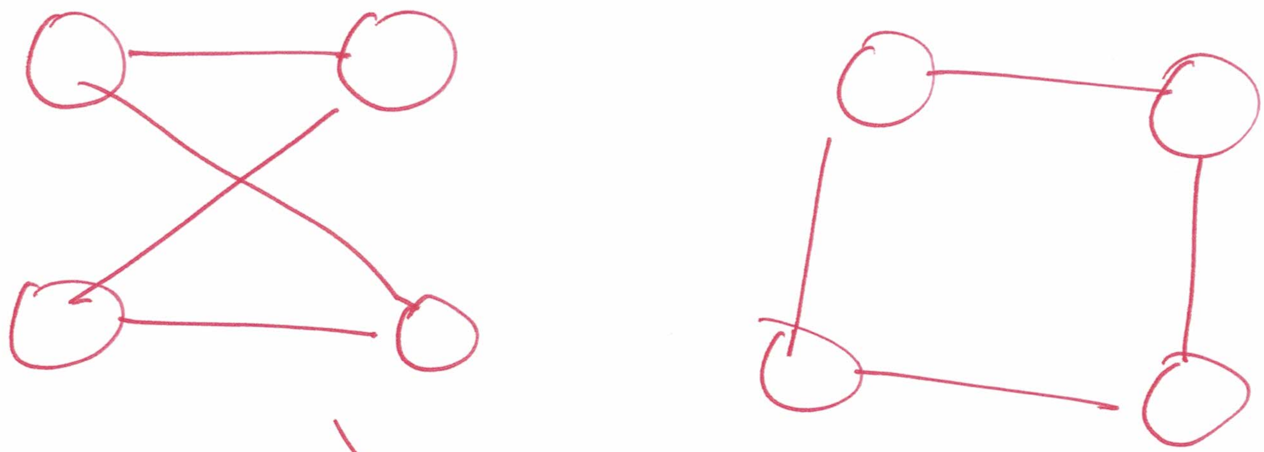
② large number factorization. $\leftarrow$ security (RSA).

Definition. Let $G_1 = (V_1, E_1)$ and $G_2 (V_2, E_2)$ be two graphs. We say that $G_1 \equiv G_2$ if $\exists$ a 1-1 mapping f s.t.

$\forall v, v' \in V$, we have

$$(v, v') \in E_1 \text{ iff } (f(v), f(v')) \in E_2.$$

Example:



are isomorphic!

GI: Given: G_1, G_2

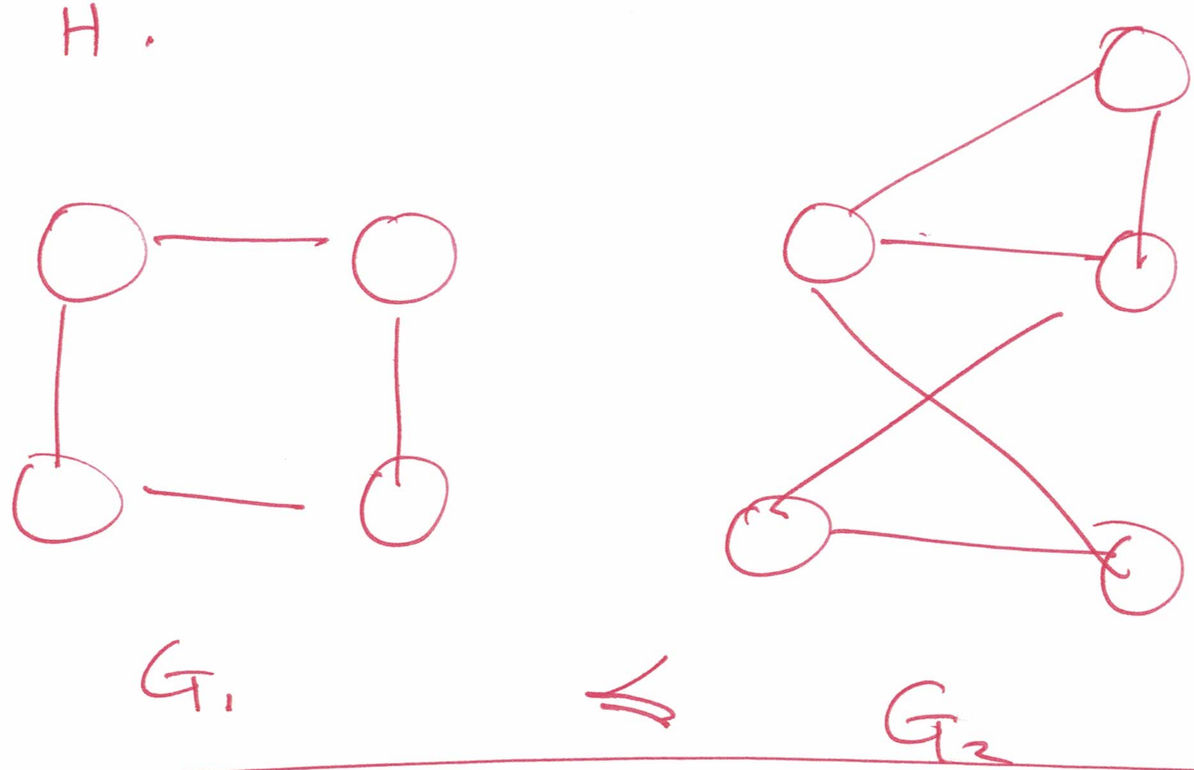
Question: $G_1 \cong G_2$?

Subgraph ~~Isoph~~ Isomorphic problem:

Let G_1 and G_2 be two graphs. We say that $G_1 \preceq G_2$ if there is a subgraph H of G_2

s.t. $G_1 \equiv H$.

Example:



Thm. Subgraph Isomorphism is NP-complete.

Proof. We know HC is NP-complete.

(1). SI $\in$ NP. We show a nondet. polytime alg:

input G_1, G_2

Guess a subgraph H of G_2 and guess a 1-1 mapping from G_1 to H

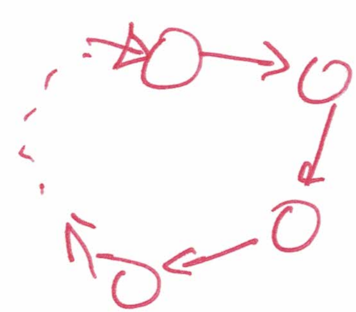
Check the mapping witnesses $H \equiv G_1$,
if yes, ret yes
crash.

---

(2). $HC \leq_m SI$. To show this, we need a translation from an instance of HC to an instance of SI:

G has n nodes $\Longrightarrow$ G_1, G_2

$G_1 =$



n-node ring

$G_2 = G$

Obviously, the translation is efficient and notice that

G has HC iff $G_1 \leq G_2 = G$.

GI: currently, we don't know GI is NP-cmplete or not, even though $GI \in NP$.

(Look at papers by Babai at U. Chicago).

Practical way to test "$G_1 \equiv G_2$?"

(1). Do lapalacian of G_1, G_2.

(2). Get all the eigenvalues (called spectrum) & compare them.

Remark: those eigenvalues of Lapalacian are all nonnegative reals