ProblemSet11

$\forall u \in V(G) \to \{u,u'\} + u_{mid}$:= path enforcement

---

5

if(G is undirected){
$f(G) = G - \{st\} = G'$
$H_c \in G \implies H_p \in G'$ (s->...->t->s remove t->s => s->t)
$H_p \in G' \implies H_c \in G$ (just add s->t)
Removing an edge is $f(G) \in O(1)$
}else if(G directed){
$f(G) = (G - \{st\}) + \forall u \in V(G) \to \{u,u'\} + u_{mid} = G'$
$H_c \in G \implies H_p \in G$\` $(s \to \ldots \to t \to s \implies s \to u \to u_{mid} \to u' \to \ldots t)$
$H_p \in G' \implies H_c \in G$ (Combine u's together add {st})
$f(G) \in O(n)$ path enforcement $\forall v$
}
$\implies$ HAMCYCLE $\leq_p$ st-HAMPATH

6

P1 = HAMPATH = {G$|H_p \in G\}$
P2 = MAXDEG-SPANNINGTREE = {(G,k)$|T_s \in G$ s.t $\Delta(T_s) = k\}$

1. f(G)=(G,1) $\Delta(T_s) = 1$
2. $G \in P_1 \implies H_c \in G \implies T_s \in (G,1)$ s.t $\Delta(T_s) = 1 \implies (G,1) \in P_2$
   (Hc uses all the edges and every edge has degree 1)
3. $(G,1) \in P_2 \implies T_s \in (G,1)$ s.t $\Delta(T_s) = 1 \implies H_c \in G \implies G \in P_1$
   (A T_s of all degree 1 is a path connecting all vertices)
4. $f(G) \in O(1)$
   $\implies$ HAMPATH $\leq_p$ MAXDEG-SPANNINGTREE

7.

P1 = HAMPATH = {G$|H_p \in G\}$
P2 = MAXLEAF-SPANNINGTREE = {(G,k)$|T_s \in G$ s.t numLeaves(T_s)=k}

1. f(G)=(G,2)
2. if G in P1 => has an HP => G has a ST of 2 leaves (the start and the end of the HP) because HP includes every vertex of G and it is a path (not Cycle). It has 2 vertices deg 1 and all the others deg 2 => 2 leaves => f(G)=(G,2) is in P2;
3. if (G,2) in P2 => has ST of 2 leaves => you have a path which contains every vertex of G (from connectivity of ST) which is a HP of G => G has a HP.
4. f(G) in O(1)

8

L = FACTORIZATION = {(m,t)|∃d s.t d|m and $1 < d \leq t$}
a)
witness = give divisor d |d|≤|(m,t)|
verification in P (just division and check)
- $1 < d \leq t$
- d|m

=> FACTORIZATION in NP

b)
~L = {(m,t)|∄d s.t d|m and $1 < d \leq t$} = {(m,t)|∀d d∤m or $d > t$ or d=1}
witness = prime factor of m s.t $\neq$ to 1 and $\leq$ t |m|≤|mt|
verification{
-check if the factor is a prime (in P)
-check if factor|m (in P)
} => (in P)
=> ~L in NP
L and ~L in NP => L in coNP

c) $P = NP \cap coNP$ => [if L in NP and L in coNP => L in P]
~FACTORIZATOIN in NP and in coNP => ~FACTORIZATION in P

PRIMES $\leq_p$ ~FACTORIZATION
f(p)=(m=p,t=p+1)
=>:
p in PRIMES => p a prime => ∄d s.t d|p and $1 < d \leq p+1$ => (p,p+1) in ~FACTORIZATION
<=:
(p,p) in ~FACTORIZATION => ∄d s.t d|p and $1 < d \leq p+1$ => p is a prime => p in PRIMES
RT:
f(p) in O(1)

=> PRIMES in P => RSA can be decrypted fast.

9