

(3) (10 points) The transactions in a blockchain ledger can be modeled as a directed acyclic graph  $G = (V, E)$  whose vertex set is partitioned into subsets  $V_1, V_2, \dots, V_p$ , where  $V_i$  represents the set of transactions pertaining to user  $i$ , and an edge  $(u, v)$  can be interpreted as meaning that transaction  $u$  is a predecessor of transaction  $v$ . The graph  $G$  and its partition  $V_1, \dots, V_p$  are assumed to satisfy the following property:

(\*) For  $i = 1, \dots, p$ ,  $V_i$  contains a node  $r_i$  that has no incoming edges in  $G$ . For every other  $v \in V_i$  there is at least one  $u \in V_i$  such that  $(u, v) \in E$ .

A set of transactions,  $S$ , is called *compatible* if it satisfies the following two properties.

1. For all  $(u, v) \in E$ , if  $v \in S$  then  $u \in S$ .
2. For all  $i = 1, 2, \dots, p$ , if  $V_i$  contains three distinct nodes  $u, v, w$  such that  $u$  has edges to both  $v$  and  $w$  in  $G$ , then  $v$  and  $w$  cannot both belong to  $S$ .

The first constraint can be interpreted as stating that a transaction cannot be accepted unless all of its predecessors are accepted. The second constraint prevents each user  $i$  from “double-spending.”

Consider the decision problem COMPAT defined as follows. An input instance consists of a directed acyclic graph  $G = (V, E)$ , a partition of  $V$  into subsets  $V_1, \dots, V_p$  satisfying property (\*), and a positive integer  $k \leq |V|$ . It is a ‘Yes’ instance of COMPAT if and only if there exists a compatible set of at least  $k$  transactions. Prove that COMPAT is NP-complete.

Not sure.