

Due: Monday, December 5, 8AM EST

NOTE change of due date!

This assignment is worth 15% of final grade. If you have no idea how to answer a question (or part of a question), you will receive 20% of the credit for that question (or subquestion) by stating “I do not know how to answer this question”. If your answer makes no sense, you will not receive any credit. Any answer that shows some understanding of the question will receive some credit.

1. (10 points) Show that there is a polynomial time transformation that transforms an instance of the $(k + 1)$ -SAT problem to an instance of the k -SAT problem for $k \geq 3$.

Hint: $z \equiv x \vee y$ can be represented by a 3CNF formula.

2. (20 points)

Assume $P = NP$. How would you solve the following optimization problem in polynomial time. Note: time is measured as a function of the length of the encoding of the input so it is good to first estimate the length (say in binary) of the encoding of an input instance. Integer weights are represented in binary.

Given a vertex weighted graph $G = (V, E, w)$ with $w : V \rightarrow \{1, 2, \dots, 2^k\}$, output an independent set V' in G that maximizes $\sum_{v_i \in V'} w(v)$.

3. (10 points) Suppose you and your business partner both have public keys for each to use to send RSA encrypted messages to each other. But it is possible that someone else knows your friend’s public key so that they can send a false message to your business partner and pretend it is coming from you. Can you think of some way to use RSA encoding and decoding so that you can sign your message and your business partner can now be sure the message is coming from you?

4. (10 points)

The following is a thought question. Using the terminology of graphs/networks and using your own experience, How would you define a “community” of friends in a social network? Provide some justification for your answer. Your definition should just be based on graph properties and not information contained in the nodes of the social network. More specifically, justify how your definition hopefully corresponds to your intuitive sense of a community.