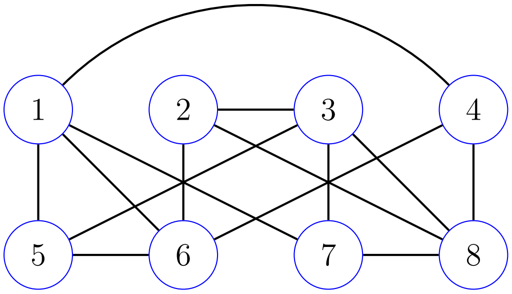
CECS 329, Learning Outcome Assessment 2, February 8th, Spring 2024, Dr. Ebert

Problems

LO1. Answer the following.

(a) Provide the definition of what it means to be a mapping reduction from problem A to problem B.

(b) Suppose $(G, k = 3)$ is an instance of the `Clique` decision problem, where G is drawn below. Draw $f(G, k)$, where f is the mapping reduction from `Clique` to the `Half Clique` decision problem.



(c) Verify that f is valid for input (G, k) in the sense that both (G, k) and $f(G)$ are either both positive instances or both negative instances of their respective problems. Defend your answer.

LO2. An instance of the `Quadratic Residue (QR)` decision problem is a triple (a, c, m) of positive integers, where $a, c \leq m$, and the problem is to decide if there is an $1 \leq x \leq c$ for which $x^2 \equiv a \bmod m$. For example, $(3, 7, 11)$ is a positive instance of `QR` since $x = 6 \leq 7$ and $6^2 \equiv 3 \bmod 11$. Hint: $x \equiv y \bmod m$ iff x and y both yield the same remainder when divided by m.

(a) For a given instance (a, c, m) of `QR`, describe a certificate in relation to (a, c, m).

(b) Provide a semi-formal verifier algorithm that takes as input i) an instance (a, c, m), and ii) a certificate for (a, c, m) as defined in part a, and decides if the certificate is valid for (a, c, m).

(c) Suppose m is a b-bit number, explain why b is a more appropriate size parameter than m. Hint: think about the definition of the **size** of a problem instance.

(d) Use the b size parameter to describe the running time of your verifier from part b. Hint: think about the big-O number of steps required for certain arithmetic operations.