Exercise sheet 2

Exercise 2.1. Recall that two graphs G and H are *isomorphic* if the vertices of G can be renamed so that G becomes identical to H. Let $\mathsf{Iso} = \{\langle G, H\rangle \mid \text{The graph } G \text{ is isomorphic to } H\}$. Show that $\mathsf{Iso} \in \text{NP}$.

Exercise 2.2. Let $\mathsf{Factoring} = \{\langle n, m\rangle \mid n \text{ has a factor } k \text{ such that } 1 < k \leq m\}$, where n and m are encoded in binary.

(a) Show that $\mathsf{Factoring} \in \text{NP}$.

Consider the following algorithm for Factoring:

for $k = 2$ to m **do**
  if k divides n **then**
    return 1
return 0

(b) Why does this algorithm **not** show that Factoring is in P?

Exercise 2.3. Suppose that $A, B \in \text{NP}$. Can we conclude that $A \cup B \in \text{NP}$? that $A \cap B \in \text{NP}$?

Exercise 2.4. Prove the "universality of CNF", i.e., for any Boolean function $f\colon \{0,1\}^n \to \{0,1\}$, there exists a CNF formula ϕ on n variables, and of size at most $n \cdot 2^n$, such that

$$\phi(x_1, \ldots, x_n) \text{ is true} \Leftrightarrow f(x_1, \ldots, x_n) = 1.$$

Hint: First consider a single tuple $(a_1, \ldots, a_n) \in \{0,1\}^n$ such that $f(a_1, \ldots, a_n) = 0$ and find a clause $C(x_1, \ldots, x_n)$ such that $C(x_1, \ldots, x_n)$ is false iff $x_i = a_i$ for $1 \leq i \leq n$.

Exercise 2.5. Show that $\mathsf{SAT} \leq_p \mathsf{3SAT}$.

More problems Let $G = (V, E)$ be an undirected graph.

- A *clique* in G is a subset $S \subseteq V$ such that for all $u, v \in S$, $u \neq v$, we have $\{u, v\} \in E$.
- A *vertex cover* in G is a subset $S \subseteq V$ such that every edge in E has at least one vertex in S. More formally, $|\{u, v\} \cap S| > 0$ for every $\{u, v\} \in E$.
- A *dominating set* in G is a subset $S \subseteq V$ such that every vertex $v \in V$ is either in S or has a neighbour in S.

We consider the following decision problems:

$$\mathsf{Clique} = \{\langle G, k\rangle \mid \text{the graph } G \text{ has a clique of size} \geq k\}$$

$$\mathsf{VertexCover} = \{\langle G, k\rangle \mid \text{the graph } G \text{ has a vertex cover of size} \leq k\}$$

$$\mathsf{DomSet} = \{\langle G, k\rangle \mid \text{the graph } G \text{ has a dominating set of size} \leq k\}$$

Exercise 2.6. Show that Clique, VertexCover, DomSet $\in$ NP.

Exercise 2.7. Prove that Clique is NP-hard.

Exercise 2.8. Prove that Clique $\leq_p$ VertexCover.

Exercise 2.9. Prove that VertexCover $\leq_p$ DomSet.

Exercise 2.10. (★) A k-colouring of a graph $G = (V, E)$ is an assignment $c\colon V \to \{1, 2, \ldots, k\}$ such that if $\{u, v\} \in E$, then $c(u) \neq c(v)$. Let k-Col $= \{\langle G \rangle \mid G$ has a k-colouring$\}$.

▷ Prove that 3SAT $\leq_p$ 3-Col.

Hint: The colours correspond to True, False, and Other.

- Introduce two special vertices v_f and v_o and add an edge between them to force them to take different colours. The colours of these two vertices will indicate False and Other, respectively.
- For each variable x of the 3-CNF formula, introduce two vertices v_x and v'_x and add an edge between them. Also add an edge from each of these two vertices to the vertex v_o. Then, v_x will either take the same colour as v_f, indicating that x should be set to False, or it will take the colour different from v_f and v_o, representing the value True.
- For each clause, introduce additional vertices and edges to force at least one literal to become true in each clause.

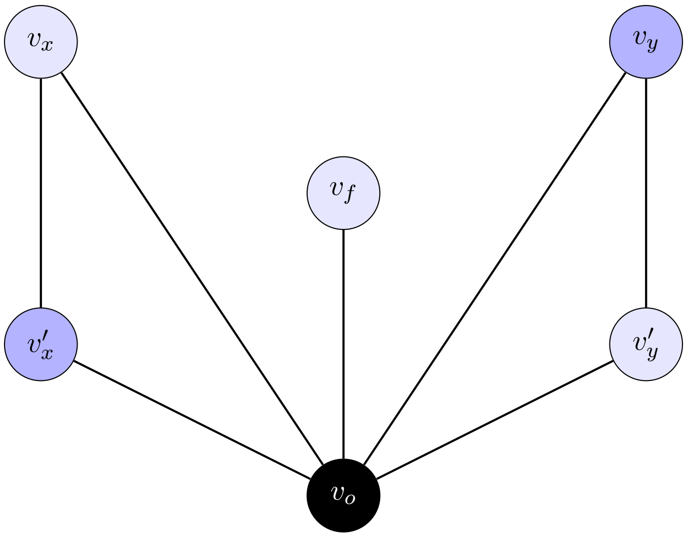

Figure 1: Example with two variables x and y and assigned colours. x is False and y is True.

Exercise 2.11. (★) Let Primes $= \{\langle n \rangle \mid n$ is a prime$\}$. The Agrawal–Kayal–Saxena (AKS) primality test algorithm was announced in 2002 and shows that Primes $\in$ P. Without using this result, show that Primes $\in$ NP.

Use the following fact from number theory: A number n is prime iff for every prime factor q of $n-1$, there exists a number $a \in \{2, 3, \ldots, n-1\}$ such that $a^{n-1} \equiv 1 \pmod{n}$ but $a^{(n-1)/q} \not\equiv 1 \pmod{n}$.