Université Gustave Eiffel
M2 – Semester 1 – 2025/2026

Complexity - Exercise Sheet 2

CHAU Dang Minh

Exercise 2.2. Let Factoring $= \{\langle n, m\rangle \mid, n$ has a factor k such that $1 < k \leq m\}$.

(a) Show that Factoring $\in$ NP.

(b) Consider the following algorithm for Factoring

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

Why does this algorithm not show that Factoring $\in$ P?

Solution. Let $|n|$ be the length of the binary representation of n. We have an encoding of the pair $\langle n, m\rangle$ such that the length of the encoding is also $O(\log(n))$. Firstly, encode m and n as usual, separated by #. Then encode again $0 \mapsto 00$, $1 \mapsto 01$ and $\# \mapsto 11$. Indeed, $|\langle m, n\rangle| \in O(2\log n) = O(\log n) = O(|n|)$. Therefore, it is enough to measure complexity with respect to $|n|$.

(a) Let the verifier V accept input $\langle n, m\rangle$ and certificate k if $1 < k \leq m$ and k divides n. It runs standard division on binaries to check if k divides n, which takes time in $O(|n|)$. Therefore, Factoring $\in$ NP.

(b) The algorithm above runs in time $O(m)$, which is $O(2^{|n|})$ when m is chosen to be in $O(n)$. Therefore, this algorithm does not show that Factoring $\in$ P.

Exercise 2.5. Show that Clique, VertexCover and DomSet are in NP.

Solution. The length of the encoding of a graph G is $O(|E|) = O(|V|^2)$. The natural number for the minimal size of the cliques, the maximal size of the vertex covers and the maximal size of dominating sets are all bounded by $|V|$. Therefore, it is enough to measure complexity with respect to $|V|$.

The certificate for each element $\langle G, k\rangle$ in Clique is a clique S. The verifier checks if

1. $S \subseteq V$ in $O(k|V|) \subset O(|V|^2)$, by searching each vertex in S in V;
2. $|S| \geq k$ in $O(k) \subset O(|V|)$;
3. all vertices in S are pairwise connected in $O(k^2 \cdot |E|) \subset O(|V|^4)$, by searching for each pair of vertices in S if there is the corresponding edge in E.

Therefore, the running time is polynomial in $|V|$, or Clique is in NP.

The certificate for each element $\langle G, k\rangle$ in VertexCover is a vertex cover S. The verifier checks if

1. $S \subseteq V$ and $|S| \leq k$ in polynomial of $|V|$ similarly to above;
2. all edges in G are covered by S in $O(|E| \cdot k) \subset O(|V|^3)$, by searching for each edge in E if at least one of its endpoints is in S.

Therefore, we also have that VertexCover is in NP.

The certificate for each element $\langle G, k\rangle$ in DomSet is a dominating set S. The verifier checks if

1. $S \subseteq V$ and $|S| \leq k$ in polynomial of $|V|$ similarly to above;
2. all vertices in G are dominated by S in $O(|V| \cdot k \cdot |V| \cdot k) \subset O(|V|^4)$, by searching in worst case if a vertex is not in S and adjacent to all $|V| - 1$ other vertices.

Therefore we also have that DomSet is in NP.

Exercise 2.6. Show that $\textsc{Clique}$ is NP-hard.

Solution. Using the fact that the independent set problem $\textsc{IndSet}$ is NP-hard, we will show that

$$\textsc{IndSet} \leq_P \textsc{Clique}.$$

Let $G = (V, E)$ be a graph. We define the complement graph $\overline{G} = (V, \overline{E})$ where $\overline{E} = \{\{u, v\} \mid u, v \in V, u \neq v, \{u, v\} \notin E\}$. We have that

$$S \text{ is an independent set in } G \iff S \text{ is a clique in } \overline{G}.$$

Indeed, if S is an independent set in G, then for all $u, v \in S$, $\{u, v\} \notin E$. Therefore, $\{u, v\} \in \overline{E}$ and S is a clique in $\overline{G}$. The converse is similar. Hence, $\langle G, k\rangle \in \textsc{IndSet} \iff \langle \overline{G}, k\rangle \in \textsc{Clique}$.

Next, we show that there is a transformation f such that $f(\langle G, k\rangle) = \langle \overline{G}, k\rangle$ that is computable in polynomial time of $|V|$. In particular, the computation is in $O(|V|^2 \cdot |E|) \subset O(|V|^4)$, by traversing all pairs of vertices in V and checking if there is the corresponding edge in E.

Therefore, $\textsc{IndSet} \leq_P \textsc{Clique}$, or $\textsc{Clique}$ is harder than every problem in NP. Therefore, $\textsc{Clique}$ is NP-hard.

Exercise 2.7. Show that $\textsc{Clique} \leq_P \textsc{VertexCover}$.

Solution. Let $G = (V, E)$ be a graph. We have that

$$S \text{ is a clique in } G \iff S \text{ is an independent set in } \overline{G} \iff V \setminus S \text{ is a vertex cover in } \overline{G}.$$

The first equivalence is shown in Exercise 2.6. For the second equivalence, if S is an independent set in $\overline{G}$, then for all $u, v \in S$, $\{u, v\} \notin \overline{E}$. Therefore, $\{u, v\} \in E$ and at least one of u, v is in $V \setminus S$. Hence, $V \setminus S$ is a vertex cover in $\overline{G}$. The converse is similar. Hence, $\langle G, k\rangle \in \textsc{Clique} \iff \langle \overline{G}, |V| - k\rangle \in \textsc{VertexCover}$, or $\langle G, k\rangle \in \textsc{Clique} \iff \langle \overline{G}, |V| - k\rangle \in \textsc{VertexCover}$.

The polynomial-time computable transformation f such that $f(\langle G, k\rangle) = \langle \overline{G}, |V| - k\rangle$ is defined as follows. Transforming G to $\overline{G}$ is in polynomial time as in Exercise 2.6 and computing $|V| - k$ is in $O(1)$.

Therefore, $\textsc{Clique} \leq_P \textsc{VertexCover}$.

Exercise 2.8. Show that $\textsc{VertexCover} \leq_P \textsc{DomSet}$.

Solution. Let $G = (V, E)$ be a graph. We construct a graph $G' = (V', E')$ as follows such that

$$\begin{aligned}
V' &= V \cup \{v_e \mid e \in E\}, \\
E' &= E \cup \{\{u, v_e\}, \{v, v_e\} \mid e = \{u, v\} \in E\}.
\end{aligned}$$

We will show that

$$S \text{ is a vertex cover in } G \iff S \text{ is a dominating set in } G'.$$

If S is a vertex cover in G, then for all $e = \{u, v\} \in E$, at least one of u, v is in S. Therefore, v_e is adjacent to at least one vertex in S in G'. Hence, all vertices in $V' \setminus S$ are adjacent to at least one vertex in S, or S is a dominating set in G'. The converse is similar. Hence, $\langle G, k\rangle \in \textsc{VertexCover} \iff \langle G', k\rangle \in \textsc{DomSet}$.

The polynomial-time computable transformation f such that $f(\langle G, k\rangle) = \langle G', k\rangle$ is defined as follows. Constructing V' from V is in $O(|V| + |E|) \subset O(|V|^2)$ and constructing E' from E is in $O(|E|) \subset O(|V|^2)$.

Therefore, $\textsc{VertexCover} \leq_P \textsc{DomSet}$.

Extra Exercises

Exercise 2.1. Show that the problem $\textsc{Iso} = \{\langle G, H\rangle \mid G \text{ is isomorphic to } H\}$ is in NP.

Solution. The length of the encoding of a graph G is $O(|E|) = O(|V|^2)$. Using the same argument as in Exercise 2.2, the length of the encoding of the pair $\langle G, H\rangle$ is also $O(|V|^2)$. Therefore, it is enough to measure complexity with respect to $|V|$.

The certificate to be fed in the verifier for each element $\langle G, H\rangle$ in $\textsc{Iso}$ is a bijection $f : V_G \to V_H$. The verifier firstly transforms E_G to E'_G following f in $O(|V|^2)$. Then it compares E'_G with E_H in $O(|V|^4)$ (by comparing the length of these lists, then search for each element in E'_G in E_H). Therefore, the running time is polynomial in $|V|$, or $\textsc{Iso}$ is in NP.

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

Solution. By the assumption, there are two polynomial-time verifiers V_A and V_B for A and B respectively. We will construct two polynomial-time verifiers $V_\cup$ and $V_\cap$ for $A \cup B$ and $A \cap B$ respectively.

Note that each certificate c of either A or B is also a certificate for $A \cup B$. For $V_\cup$, on input x and certificate c, it runs as follows.

1. Runs V_A on input x and certificate c. If V_A accepts, then $V_\cup$ accepts;
2. Otherwise, it runs V_B on input x and certificate c. If V_B accepts, then $V_\cup$ accepts;
3. Otherwise, it rejects.

The running time of $V_\cup$ is at most the sum V_A and V_B, which is bounded by polynomial in $|x|$. Therefore, the running time of $V_\cup$ is polynomial in $|x|$. Moreover, if $x \in A \cup B$, then there is a certificate such that either V_A or V_B accepts, which is the certificate such that $V_\cup$ accepts.

For $V_\cap$, on input x and certificate (c_A, c_B), it runs as follows such that c_A is a certificate for A and c_B is a certificate for B, it runs as follows.

1. Runs V_A on input x and certificate c_A. If V_A rejects, then $V_\cap$ rejects;
2. Otherwise, it runs V_B on input x and certificate c_B. If V_B rejects, then $V_\cap$ rejects;
3. Otherwise, it accepts.

Similarly to above, the running time of $V_\cap$ is polynomial in $|x|$.

Therefore, both $A \cup B$ and $A \cap B$ are in NP.