

Class NP

Exercise sheet 8 (solutions)

Exercise 8.1. Prove that the following problems are in NP:

- (a) $\{\langle G, s, t, k \rangle \mid \text{graph } G \text{ contains a simple path from } s \text{ to } t \text{ visiting at least } k \text{ vertices}\};$
- (b) $\text{SUBSET-SUM} = \{\langle a_1, \dots, a_m, t \rangle \in \mathbb{N}^{m+1} \text{ in binary} \mid \exists I \subseteq \{1, \dots, m\} : \sum_{i \in I} a_i = t\};$
- (c) $3\text{COLOUR} = \{G \mid \text{graph } G \text{ has a proper colouring using at most three colours}\}.$

Solution. In each part, the verifier first checks that the input is a well-formed encoding of an instance of the problem. If it is not, the verifier rejects. It also rejects any certificate that does not have the format specified below.

- (a) The certificate is a list of vertices $(v_1, \dots, v_\ell)$ of G . The verifier checks that $v_1 = s$, $v_\ell = t$, and $\ell \geq k$; that no vertex occurs twice; and that each consecutive pair v_i, v_{i+1} is an edge of G . Thus, it accepts exactly when the list describes a simple path from s to t visiting at least k vertices. Such a path has at most $|V(G)|$ vertices, so the certificate has polynomial length. All the checks take polynomial time.
- (b) The certificate is a bit string $b_1 \dots b_m$, with one bit for each input number. The verifier adds the numbers a_i for which $b_i = 1$ and checks whether the sum is t . The certificate has length m , which is at most the input length. The sum has polynomially many bits, so binary addition and comparison take polynomial time.
- (c) The certificate gives one of three colours to each vertex of G . The verifier checks that there is exactly one colour for each vertex and that the endpoints of every edge have different colours. The certificate has polynomial length, and these checks take polynomial time.

□

Exercise 8.2. Suppose $L_1, L_2 \in \text{NP}$. Is it true that $L_1 \cup L_2 \in \text{NP}$? Is it true that $L_1 \cap L_2 \in \text{NP}$?

Solution. Yes in both cases. Let V_1, V_2 be polynomial-time verifiers for L_1, L_2 , and let $p_1(n), p_2(n)$ bound the lengths of their certificates on inputs of length n .

For $L_1 \cup L_2$, the certificate specifies an index $i \in \{1, 2\}$ and includes a certificate s for V_i . The verifier checks the index and runs V_i on (w, s) . An accepted certificate exists exactly when $w \in L_1 \cup L_2$. The certificate length is at most $1 + \max\{p_1(|w|), p_2(|w|)\}$, so it is polynomial.

For $L_1 \cap L_2$, the certificate is a pair (s_1, s_2) , where s_i is a certificate for V_i . The verifier runs V_1 on (w, s_1) and V_2 on (w, s_2) , and accepts exactly when both accept. An accepted pair exists exactly when $w \in L_1$ and $w \in L_2$. The certificate length is at most $p_1(|w|) + p_2(|w|)$, up to the polynomial overhead for encoding the pair, and is therefore polynomial. □

Exercise 8.3. * Suppose that $P = NP$. Prove that a polynomial-time algorithm can find a clique of size at least k in a given graph G , if one exists, and report that none exists otherwise.

Solution. Since $CLIQUE \in NP$ and $P = NP$, we have a polynomial-time algorithm that decides whether a graph has a clique of size at least k . First run it on (G, k) ; if it answers no, report that no such clique exists.

Otherwise, maintain a graph H and a target j , initially G and k . While $j > 0$, choose a vertex v of H and ask whether $H - v$ has a clique of size at least j . If yes, replace H by $H - v$. If no, every such clique in H must contain v : add v to the answer, replace H by the subgraph induced by the neighbours of v , and decrease j by one. This preserves the invariant that H contains a clique of size at least j . When $j = 0$, the selected vertices form the required clique.

Each step removes at least one vertex from H , so there are at most $|G|$ steps. Each uses one call to the polynomial-time decision algorithm, and the graphs passed to it have polynomial size. The full search therefore takes polynomial time. $\square$

Exercise 8.4. Recall that $L^* = \{w_1 \cdots w_r \mid r \geq 0, w_i \in L\}$. Suppose $L \in NP$. Is it true that $L^* \in NP$?

Solution. Pending $\square$