

Luennolla esitettiin kysymys, ovatko kaikki ei-rekursiiviset kielet NP-kovia. Tietysti jos $P = NP$, niin vastaus on kyllä, koska harjoitustehtävän 8.2(a) mukaan kaikki muut kielet kuin \emptyset ja Σ^* ovat tällöin NP-kovia. Kysymys on siis kiinnostava vain, jos oletetaan, että $P \neq NP$.

Jos $P \neq NP$, niin ei itse asiassa ole mitään erityistä syytä olettaa, että kaikki ratkeamattomat ongelmat olisivat NP-kovia. Merkinnän " $A \leq_m^p B$ " lukeminen " B on ainakin yhtä vaikea kuin A ", mitä luennoilla on tullut käytetyksi, on sikäli harhaanjohtava, että ongelmien vaikeudet eivät asetu millenkään täysin järjestetylle asteikolle. Jos esim. A on NP-täydellinen ja B ratkeamaton, voidaan perustellusti sanoa, että B on vaikeampi kuin A . Tästä ei kuitenkaan millään ilmeisellä tavalla seuraa $A \leq_m^p B$, sillä B voi olla "eri tavalla vaikea" kuin A . Osoitamme nyt diagonalisointikonstruktiolla, että tosiaan voi olla $A \not\leq_m^p B$.

Merkitään funktion $f: \Sigma^* \rightarrow \Sigma^*$ arvojoukkoa $\text{Ran}(f) = \{ f(w) \mid w \in \Sigma^* \}$. Todetaan ensin, että yleisyyttä rajoittamatta voidaan palautuksissa olettaa palautusfunktion arvojoukko äärettömäksi. Olkoon nimittäin f palautus $A \leq_m^p B$ millä tahansa A ja B . Selvästi sama f on myös palautus $A \leq_m^p B'$, missä $B' = B \cap \text{Ran}(f)$. Jos $\text{Ran}(f)$ on äärellinen, niin myös B' on äärellinen. Tällöin erityisesti $B' \in P$, ja siis myös $A \in P$.

Siis jos f on palautus $A \leq_m^p B$, missä $A \notin P$, niin $\text{Ran}(f)$ on ääretön.

Oletetaan nyt $P \neq NP$, ja valitaan jokin $A \in NP - P$ (esim. $A = \text{SAT}$). Olkoon nyt (f_1, f_2, \dots) jono, joka sisältää jossain järjestyksessä kaikki polynomisessa ajassa laskettavat funktiot f_i , joilla $\text{Ran}(f)$ on ääretön. Huomaa, että oletettavasti tätä jonoa ei voida tuottaa mitenkään algoritmisesti, mutta sillä ei ole jatkossa väliä. Edellä esitetyn perusteella $A \leq_m^p B$, jos ja vain jos f_i on palautus $A \leq_m^p B$ jollain $i \geq 1$.

Tarkastellaan ensin, miten diagonalisoimalla muodostetaan B , jolla tämä ei päde. Emme vielä tässä vaiheessa huolehdi konstruoitavan kielen B rekursiivisuudesta.

Määritellään induktiivisesti jono joukkoja $C_0 \subset C_1 \subset C_2 \subset \dots$, missä $|C_i| = i$. Aluksi siis asetetaan $C_0 = \emptyset$. Vaiheessa i valitaan alkioksi v_i joukon $\text{Ran}(f_i) - C_{i-1}$ leksikografisesti ensimmäinen alkio. Koska C_{i-1} on äärellinen ja $\text{Ran}(f_i)$ on ääretön, tällainen on aina olemassa. Valitaan lisäksi jokin $u_i \in \Sigma^*$, jolla $f_i(u_i) = v_i$.

Joukoksi B valitaan nyt

$$B = \{ v_i \mid u_i \notin A \}.$$

Siis jos $u_i \notin A$, niin $f_i(u_i) = v_i \in B$. Toisaalta $v_i \neq v_j$ kun $i \neq j$, joten

jos $u_i \in A$, niin $f_i(u_i) = v_i \notin B$. Täten $u_i \in A$, jos ja vain jos $f_i(u_i) \notin B$, joten erityisesti f_i ei ole palautus $A \leq_m^p B$. Koska tämä pätee kaikilla i , niin $A \not\leq_m^p B$.

Intuitiivisesti ei tuntuisi olevan syytä olettaa, että edellä konstruoitu B olisi rekursiivinen. Joukon B ei-rekursiivisuutta voi kuitenkin olla vaikea todistaa. Teemme siksi konstruktion uudelleen, ja lisäämme siihen toisen diagonalisaation, joka varmistaa ei-rekursiivisuuden. Tätä jälkimmäistä diagonalisaatiota varten olkoon (M_1, M_2, \dots) jono, joka sisältää kaikki Turingin koneet jossain järjestyksessä (esim. $M_i = M_{w_i}$ luennoilla esitetyn indeksoinnin mukaan, missä w_i on aakkoston $\{0, 1\}^*$ merkkijono numero i leksikografisessa järjestyksessä).

Määritellään taas induktiivisesti jono äärellisiä joukkoja $C_0 \subset C_1 \subset C_2 \subset \dots$. Taas $C_0 = \emptyset$. Vaiheessa i valitaan ensin joukosta $\text{Ran}(f_i) - C_{i-1}$ leksikografisesti ensimmäinen alkio v_i , ja lisäksi jokin u_i , jolla $f(u_i) = v_i$. Lisäksi otetaan joukosta Σ^* alkioita x_i leksikografisesti seuraava alkio ja merkitään sitä x_i . Joukkoon C_i tulee nyt joukon Σ^* leksikografisesti ensimmäiset alkio alkioon x_i asti (tämä mukaanlukien).

Joukko B määritellään nyt seuraavasti:

- $v_i \in B$, jos $u_i \notin A$,
- $x_i \in B$, jos $x_i \notin L(M_i)$, ja
- joukkoon B ei tule muita alkioita.

Jälleen $u_i \in A$, jos ja vain jos $v_i = f_i(u_i) \notin B$, joten ei ole olemassa polynomista palautusta $A \leq_m^p B$. Lisäksi $v_i \in B$, jos ja vain jos $v_i \notin L(M_i)$, joten B ei ole $L(M_i)$ millään i , ja siis B ei ole rekursiivinen (eikä edes rekursiivisesti lueteltava).