20 - Számításelmélet

Dr. Gazdag Zsolt kiadott jegyzete alapján

2009. június 22.

Kiszámíthatóság

Alapfogalmak

- Számítási problémának nevezünk egy matematikai nyelven megfogalmazott, számítógéppel megoldandó feladatot.
- Egy probléma és a probléma egy bemenete alkotja a probléma egy példányát.
- Válaszként a probléma megoldását kapjuk. Speciális esetben a válasz igen/nem lehet. Ezeket a problémákat eldöntésproblémának nevezzük.

Formális definíciók

- Egy $F : A \to B$ parciális függvényt számítási problémának nevezünk. A parciálisság szükséges, mert a problémának lehetnek olyan példányai amik algoritmikusan nem számolhatók ki.
- F kiszámítható, ha létezik olyan algoritmus, mellyel $\forall x \in A$-ra véges sok lépésben kiszámolható $F(X) \in B$.
- Ha egy probléma által meghatározott függvény kiszámítható, akkor a problémát megoldhatónak nevezzük.
- Ha egy eldöntés probléma kiszámítható, akkor azt speciálisan eldönthetőnek nevezzük.

Church-Turing tézis

A kiszámíthatóság ismert matematikai modelljei ekvivalensek az effektíven kiszámítható függvények osztályával(, azaz nem ismerünk a Turing gép által reprezentált algoritmus modellnél erősebb eszközt). A tézis nem tétel, mert elemeit nem tudjuk formálisan definiálni.

A Turing-gép, mint algoritmus modell, a rekurzív és rekurzívan felsorolható nyelvek

A Turing-gép

A Turing-gép fogalma

A Turing-gép egy véges sok állapotú diszkrét ütemskálás eszköz.

Részei:

- Egyik irányban végtelen, egyforma mezőkre osztott szalag.

- Író olvasó fej, mely a szalagon fut.
- Véges sok belső állapottal rendelkező vezérlő egység.

Indításkor a gép szalagján csak a bemenő szó van, ezen kívül minden jel az úgynevezett 'szóköz'. A fej a szalag bal szélén tartózkodik és a gép pedig a kezdőállapotban van.

Egy ütemében a gép kiolvassa a fej alatti jelet és az állapotától függően: új jelet ír a szalagra, valamely irányban elmozdítja a fejet és új állapotot vesz fel.

Formális definíció

$M = \{Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n\}$ rendszer, ahol

- Q az állapotok véges, nem üres halmaza
- Σ a bemenő jelek ábécéje
- Γ a szalagábácé; $\Sigma \subset \Gamma$, de $\Gamma \backslash \Sigma$ mindig tartalmaz (legalább) egy speciális jelet, a szóközt
- $q_0, q_i, q_n \in Q$ rendre: kezdőállapot, elfogadó- és elutasító állapot.
- $\delta : \ (Q \backslash \{q_i, q_n\}) \times \Gamma \rightarrow Q \times \Gamma \times \{L, R\}$ átmeneti függvény, ahol L,R a fej mozgásának irányait jelölik.

Konfiguráció

A Turing-gép konfigurációját egy uqv hármas írja le, ahol $q \in Q$, $u, v \in \Gamma$ és $v \neq \varepsilon$. Ekkor a szalagon uv szó található, a gép q állapotban van és a fej v első jelére mutat. Ha $q \in \{q_i, q_n\}$, akkor megállási konfigurációról beszélünk. $q = q_i$ esetén elfogadó, $q = q_n$ esetén elutasító a konfiguráció.

Kezdőkonfigurációnak nevezzük a $q_0 u \bigsqcup$ konfigurációt, ha $u \in \Sigma^*$.

Konfigurációátmenet

Legyen $uqav$ egy konfiguráció, ahol $a \in \Gamma$ és $u, v \in \Gamma^*$.

- $\delta(q, a) = (r, b, R)$ esetén $uqav \vdash ubrv'$, ahol $v = v'$, ha $v \neq \varepsilon$, különben $v' = \bigsqcup$.
- $\delta(q, a) = (r, b, L)$ esetén, ha $u \neq \varepsilon$, akkor $uqav \vdash u'rcbv'$, ahol $c \in \Gamma$ és $u'c = u$, egyébként $uqav \vdash urbv$.

M véges sok lépésben eljut C konfigurációból C'-be (jelölés: $C \vdash^* C'$), ha van olyan $n \geq 0$ és $C_1, C_2, ..., C_n$ konfiguráció sorozat, melyre $C_1 = C$ és $C_n = C'$ és minden $1 \leq i < n$-re $C_i \vdash C_{i+1}$.

Különböző Turing-gép változatok

Mindkét irányban végtelen szalagú Turing-gép

Ez a változat annyiban tér el az eredtitől, hogy a szalagja mindkét irányban végtelen, így korlátlanul lépkedhet rajta jobbra és balra.

K-szalagos Turing-gép

Az eredeti modelltől eltérően ennek k darab szalagja van. Mindegyiken külön olvasófejjel, melyek mozgása független a többitől. Formálisan csak az átmenetfüggvénye tér el az eredeti modelltől a következők szerint:

$\delta : \ (Q - \{q_i, q_n\}) \times \Gamma^k \rightarrow Q \times \Gamma^k \times \{L, R\}^k$, ami értelemszerű kiterjesztése az egyszalagos esetnek.

Nemdeterminisztikus Turing-gép

A nemdeterminisztikus autómatákhoz hasonló kiterjesztése a Turing-gép modellnek.

Tétel: A fenti modellek mindegyikéhez konstruálható velük ekvivalens félszalagos Turing-gép.

A rekurzív és rekurzívan felsorolható nyelvek

Az M által felismert nyelv azoknak az $u \in \Sigma^*$ szavaknak a halmaza, melyekre: $uq_0 \sqcup \vdash^* xq_iy$, ahol $x, y \in \Gamma^*$ és $y \neq \varepsilon$.

Egy $L \in \Sigma^*$ nyelv felismerhető, vagy rekurzívan felsorolható, ha létezik olyan M Turing-gép, melyre $L = L(M)$. A rekurzívan felsorolható nyelveket RE-vel jelöljük.

Továbbá, ha $L \in \Sigma^*$-hez létezik olyan M Turing-gép, mely a nyelv összes szavára megállási konfigurációba jut és felismeri L-et, akkor a nyelvet eldönthetőnek, vagy rekurzívnak nevezzük. A rekurzív nyelvek osztályát R-rel jelöljük.

Algoritmikusan eldönthető és eldönthetetlen problémák

Egy nem rekurzív felsorolható nyelv

Legyen a nyelv olyan (M, ω) párok halmaza, melyre M egy megfelelően elkódolt {0,1} ábécé feletti Turing-gép, mely elfogadja ω-t. Ezt a nyelvet L_u-nak nevezzük. Párja az $L_{átló}$ nyelv, mely azon {0,1} ábécé feletti Turing-gépek kódjait tartalmazza, melyek nem fogadják el saját kódjukat.

Formálisan: $L_u = \{\omega_i 111 \omega_j | i, j \geq 1,\ \omega_j \in L(M_i)\}$ és $L_{átló} = \{\omega_i | i \geq 1,\ \omega_i \notin L(M_i)\}$

Tételek

Egy L nyelv rekurzívan felsorolható, ha létezik olyan M Turing-gép, amelyre L=L(M). Ha M minden bemenetre megáll, akkor L rekurzív, azaz eldönthető.

- Tétel: L_u rekurzívan felsorolható, de nem rekurzív. $L_{átló}$ nem rekurzívan felsorolható.
- Tétel: Ha egy nyelv rekurzív, akkor a komplementere is rekurzív.
- Tétel: Ha egy nyelv és komplementere rekurzívan felsorolható, akkor a nyelv rekurzív.
- Tétel: A megállási probléma, azaz az L_{halt} nyelv rekurzívan felsorolható, de nem eldönthető

Ha P rekurzív nyelvek egy halmaza, akkor azt a rekurzív nyelvek egy tulajdonságának nevezzük. Triviális a tulajdonság, ha $P = \emptyset$, vagy $P = RE$. Egy L nyelv rendelkezik P tulajdonsággal, ha $L \in P$.

- Tétel: Eldönthetetlen, hogy egy M Turing-gép *üres/véges/reguláris/környezetfüggetlen* nyelvet ismer-e fel.

Problémák egymásra való visszavezethetősége

Legyen Σ és Δ két ábécé és f egy Σ^*-ból Δ^*-ba képező függvény. Azt mondjuk, hogy f kiszámítható, ha van olyan M Turing-gép, hogy M-et $\omega \in \Sigma^*$szóval a bemenetén indítva, M úgy áll meg, hogy a szalagján $f(\omega)$ szó lesz.

Legyen $L_1 \in \Sigma^*$és $L_2 \in \Delta^*$ két nyelv. Azt mondjuk, hogy L_1 visszavezethető L_2-re, ha van olyan $f: \Sigma^* \to \Delta^*$ függvény, hogy minden $\omega \in \Sigma^*$ szóra, ha $\omega \in L_1 \leftrightarrow f(\omega) \in L_2$.

Tétel: Legyen L_1, L_2 két eldöntésprobléma és L_1 legyen visszavezethető L_2-re. Ekkor

- Ha L_1 eldönthetetlen, akkor L_2 is az.
- Ha $L_1 \notin RE$, akkor $L_2 \notin RE$ is igaz.

Idő- és tárbonyolultsági osztályok

Legyen $f(n): \mathbb{N} \to \mathbb{N}$függvény.

$TIME(f(n)) = \{L | L \text{ eldönthető } \mathcal{O}(f(n)) \text{ időigényű } Turing - géppel\}$

$P = \bigcup_{k>1} TIME(n^k)$

$NTIME(f(n)) = \{L | L \text{ eldönthető } \mathcal{O}(f(n)) \text{ időigényű } nemdeterminisztikus\ Turing - géppel\}$

$NP = \bigcup_{k>1} NTIME(n^k)$

Tipikus P-beli probléma az úgynevezett *elérhetőség* probléma, melynek bemenete egy G gráf, illetve két kitüntetett pontja. Válaszként megmondja van e út a két pont között.

Az NP-beli problémák közös tulajdonsága, hogy egy probléma egy példányának ellenőrzése polinom időben elvégezhető. Ennek megfelelően a nemdeterminisztikus Turing-gép általában „megsejt" egy megoldást és leellenőrzi azt.

A definíciókból következik, hogy $P \subseteq NP$. Sejtés, hogy a tartalmazás valódi.

Polinomiális idejű visszavezetések

Legyen Σ és Δ két ábécé és f egy Σ^*-ból Δ^*-ba képező függvény. Azt mondjuk, hogy f *polinom időben* kiszámítható, ha van olyan *polinom időigényű* M Turing-gép, hogy M-et $\omega \in \Sigma^*$szóval a bemenetén indítva, M úgy áll meg, hogy a szalagján $f(\omega)$ szó lesz.

Legyen $L_1 \in \Sigma^*$és $L_2 \in \Delta^*$ két nyelv. Azt mondjuk, hogy L_1 *polinom időben* visszavezethető L_2-re, ha van olyan $f: \Sigma^* \to \Delta^*$ polinom időben kiszámítható függvény, hogy minden $\omega \in \Sigma^*$ szóra, ha $\omega \in L_1 \leftrightarrow f(\omega) \in L_2$.

Tétel: Legyen L_1, L_2 két eldöntésprobléma és $L_1 \leq_p L_2$. Ekkor, ha L_2

- P-beli, akkor $L_1$is.
- NP-beli, akkor L_1 is.

Egy probléma NP-teljes, ha NP-beli és minden más NP-beli probléma polinom időben visszavezethető rá.

Tétel: Ha L NP-teljes és $L \in P$, akkor $P = NP$.

Tétel: Legyen L_1 NP-teljes és L_2 NP-beli. Ekkor, ha $L_1 \leq_p L_2$, akkor L_2 is NP-teljes.

NP-teljes problémák

SAT=$\{(\O)\,|\O$ kielégíthető, konjunktív normálformában adott formula$\}$

Legyen $k \geq 1$. kSAT=$\{(\O)\,|\O \in$SAT és minden tagjában k literál található$\}$

Tétel: SAT és 3SAT NP-teljes.

Teljes részgráf: (G,k) párok, melyekre G gráfban van k csúcsú teljes részgráf.

Független csúcshalmaz: (G,k) párok, melyekre G gráfban van k darab csúcs melyek között sehol nem vezet él.

Csúcselfedés: (G,k) párok, melyekre G gráfban van olyan k elemű csúcshalmaz, mely a G-beli élek közül mindegyiknek legalább egyik végpontját tartalmazza.

Tétel: Az előző három probléma NP-teljes.