Automaták irányítása II.

Iván Szabolcs

2009. október 6.

Tartalom

Véges automaták

Automata

Automata: egy $M = (Q, A, \delta)$ hármas, ahol

- Q a véges, nemüres állapothalmaz;
- A a véges, nemüres input ábécé;
- $\delta : Q \times A \to Q$ az átmenetfüggvény.

$q \cdot u$

A szokott módon δ kiterjeszthető egy $\delta : Q \times A^* \to Q$ leképezéssé. $\delta(p, u)$ helyett egyszerűen $p \cdot u$ vagy pu szerepel majd, ha δ egyértelműen kiderül a környezetből.

Pu

Ha $P \subseteq Q$ és $u \in A^*$, legyen $Pu = \{pu : p \in P\}$.

Irányítás (J. Černý, 1964.)

Irányító szó

Az $M = (Q, A, \delta)$ automatának $u \in A^*$ irányító szava, ha $|Qu| = 1$.
Vagyis ha $\forall p, q: \; pu = qu$.
M irányítható, ha van irányító szava.

$d(M), d(n)$

$d(M)$

Ha M irányítható, legyen

$$d(M) = \min\{|u| : u \text{ irányítja } M\text{-et}\}.$$

$$d(n) = \max\{d(M) : M \text{ irányítható, } n\text{-állapotos automata}\}.$$

Ismert:

$$(n-1)^2 \leq d(n) \leq \frac{n^3 - n}{6}.$$

A Černý-sejtés

$$d(n) \stackrel{?}{=} (n-1)^2$$

Tartalom

Általánosítás

Rang

Legyen az u szó rangja $|Qu|$.

A sejtés átfogalmazása...

Ha van 1 rangú szó, akkor van legfeljebb $(n-1)^2$ hosszú 1 rangú szó is.

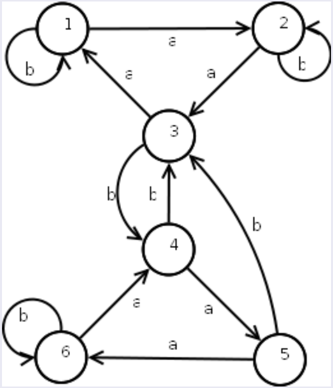
...és általánosítása (Pin, 1978)

Ha van k rangú szó, akkor van legfeljebb $(n-k)^2$ hosszú k rangú szó is.

Ez igaz $k = n-1, n-2, n-3$-ra.

Ellenpélda

Ellenpélda az általános sejtésre (Kari, 2001)



Egy legrövidebb 2 rangú szó: *baababababaabbabaab*, hossza $17 > 16 = (6-2)^2$!
Sőt: ez az automata szintén „Černý-i” automata.

Tartalom

Részeredmények

A sejtés (legalábbis $d(n) = O(n^2)$) igaz, ha az automata...

- ...állapotszáma prím és van ciklikusan permutáló betűje (Pin, 1981)
- ...rendelkezik ciklikusan permutáló betűvel (Dubuc, 1998)
- ...euleri (Kari, 2002)
- ...aperiodikus (Trahtman, 2007)
- ...gyengén monoton (Volkov, 2009) (január)
- ...egy-klaszteres (Béal-Perrin, 2009) (július)
- ...

Mik ezek?

Euleri automata

Az $M = (Q, A, \delta)$ automata euleri, ha összefüggő és átmenet(multi)gráfja euleri:

$$\forall p \in Q : |\{(q, a) : qa = p\}| = |A|.$$

Aperiodikus automata

Az $M = (Q, A, \delta)$ automata aperiodikus, ha minden $u \in A^+$, $k > 0$ és $p \in Q$ esetén

$$pu^k = p \;\Rightarrow\; pu = p.$$

Egy-klaszteres automata

Az $M = (Q, A, \delta)$ automata egy-klaszteres, ha van olyan $a \in A$ betű, amire a $p \mapsto pa$ transzformáció gráfjában csak egy kör van.

A gyengén monoton automatákat később definiáljuk.
Higgyük el egyelőre, hogy minden aperiodikus automata gyengén monoton.

Mindent bebizonyítunk??

(Vázlatosan) belátjuk a Černý-sejtést a következő esetekre:

- euleri automatára;
- egy-klaszteres automatára;
- gyengén monoton automatára.

Az első két esetet együtt fogjuk kezelni.

A továbbiakban rögzítsünk egy $M = (Q, A, \delta)$ irányítható automatát és legyen $Q = \{1, \dots, n\}$.

Valszám

(Véges tartójú) valószínűségi mérték (avagy VM)...

...egy olyan $P : A^* \to \mathbb{R}_0^+$ leképezés, amire csak véges sok szó képe nemnulla és $\sum_{w \in A^*} P(w) = 1$.

Tartója a $\mathrm{dom}(P) = \{w \in A^* : P(w) > 0\}$ halmaz.

A P_1 és P_2 szorzata...

$P_1 P_2$, ahol $P_1 P_2(w) = \sum_{uv=w} P_1(u) P_2(v)$.

Vegyük észre, hogy $P_1 P_2$ is VM és $\mathrm{dom}(P_1 P_2) = \mathrm{dom}(P_1)\mathrm{dom}(P_2)$.

w mint VM

Ha $w \in A^*$ egy szó, akkor legyen $\mathbf{w}$ az a VM, ami w-hez rendel 1-et (minden máshoz pedig nullát).

Mátrixok

M_P

Ha P egy VM, definiálhatjuk a következő $M_P \in \mathbb{R}^{n\times n}$ mátrixot:

$$M_P(p,q) \; = \; \sum_{pw=q} P(w).$$

Vegyük észre: $M_{P_1P_2} = M_{P_1}M_{P_2}$.

M_w

Speciálisan $M_{\mathbf{w}}$ az a (bináris) mátrix, amire $M_{\mathbf{w}}(p,q) = 1 \;\Leftrightarrow\; pw = q$.

Vektorok

$[S]$

Ha $S \subseteq Q$ állapotok egy halmaza, legyen $[S] \in \mathbb{R}^{1\times n}$ az S karakterisztikus (sor)vektora: $S(p) = 1 \;\Leftrightarrow\; p \in S$.

Sw^{-1}

Ha $S \subseteq Q$ és $w \in A^*$, legyen $Sw^{-1} = \{p \in Q : pw \in S\}$.

Összefüggés

Tetszőleges $w \in A^*$-ra és $S \subseteq Q$-ra,

$$M_{\mathbf{w}}[S]^T \;=\; [Sw^{-1}]^T.$$

(v^T a v vektor transzponáltja.)

Egy friss eredmény

Átlagoló Lemma (Steinberg, 2009) (október 2)

Tegyük fel, hogy P_1 és P_2 VM-ek A^*-on, $\mathrm{dom}(P_2) = A^{\leq n-1}$, és $R \subseteq Q$ állapotok egy halmaza úgy, hogy a következők teljesülnek:

1. $[R]M_{P_2}M_{P_1} = [R]$;
2. R erősen összefüggő;
3. valamely $w_0 \in A^*$-ra $Qw_0 \subseteq R$.

Akkor $d(M)$ legfeljebb

- $1 + (n-2)(n-1+L)$, ha $R = Q$;
- $\ell + (r-1)(n-1+L)$, ha $R \subsetneq Q$,

ahol $r = |R|$, L a leghosszabb $\mathrm{dom}(P_1)$-beli szó hossza, és $\ell = |w_0|$.

Ezt fogjuk vázlatosan igazolni.

Alkalmazás – euleri automaták

Tegyük fel, hogy M euleri automata. Definiáljuk a P_1 és P_2 VM-eket a következőképp:

- $P_1 = P_\varepsilon$;
- $P_2(u) = \frac{1}{n \cdot |A|^{|u|}}$, ha $0 \leq |u| < n$,

és legyen $R = Q$.

Akkor $[Q] M_{P_2} M_{P_1} = [Q]$ és alkalmazhatjuk az Átlagoló Lemmát:

$$d(M) \leq 1 + (n-2)(n-1).$$

Alkalmazás – egy-klaszteres automaták

Tegyük fel, hogy M egy-klaszteres. Legyen $a \in A$ egy olyan betű, amire a $p \mapsto pa$ transzformációnak egyetlen köre van. Legyen R ez az r-elemű kör.

Definiáljuk P_1-et és P_2-t a következőképp:

- $P_1(w) = \frac{1}{r}$, ha $w \in \{a^{n-r}, \ldots, a^{n-1}\}$;
- P_2 tetszőleges VM, amire $\mathrm{dom}(P_2) = A^{\leq n-1}$.

Akkor megint $[R]M_{P_2}M_{P_1} = [R]$ és

$$d(M) \;\leq\; 1 + 2(n-2)(n-1) = O(n^2).$$

Egy vektorteres lemma, kezdetnek

Vektorteres Lemma

Legyen $\pi : A^* \to K^{n\times n}$ homomorfizmus, K egy test, továbbá $W, V \subseteq K^n$ alterek úgy, hogy $W \subseteq V$, de $\pi(u)w \notin V$ valamely $u \in A^*$-ra és $w \in W$-re.

Akkor tetszőleges $F \subseteq W$-re, ami kifeszíti W-t, van egy $f \in F$ elem és $w \in A^*$ szó, amire $|w| \le \dim V - \dim W + 1$ és $\pi(w)f \notin V$.

Bizonyítás

Legyen W_m a $\pi(x)w$, $x \in A^{\le m}$, $w \in W$ vektorok által kifeszített altér.
Akkor $W = W_0 \subseteq W_1 \subseteq \ldots$ alterek növekvő lánca.
Amint $W_k = W_{k+1}$, a lánc stabilizálódik. A $\pi(u)w \notin V$ feltétel miatt van egy legnagyobb $m \ge 0$, amire $W_m \subseteq V$.
Tehát,

$$W_0 \subsetneq W_1 \subsetneq \cdots \subsetneq W_m \subseteq V,$$

és ezért $\dim W_0 + m \le \dim V$. Innen következik az állítás.

Az Átlagoló Lemma bizonyítása

Elég belátni, hogy tetszőleges $\emptyset \neq S \subsetneq R$-re van olyan $w \in A^*$, aminek hossza legfeljebb $n + 1 + L$ és melyre

$$|Sw^{-1} \cap R| > |S|.$$

Miért?

- Mert ha $R = Q$, akkor van egy $q \in Q$ és $a \in A$, amire $|qa^{-1}| > 1$, ezután $(n-2)$-szer meg tudjuk növelni az inverz képeket egyenként $n - 1 + L$ hosszú szavakkal és kapjuk az $1 + (n-2)(n-1+L)$ korlátot.
- Ha pedig $R \subsetneq Q$, akkor kiindulunk egy $q \in R$-ből és $(r-1)$-szer megnöveljük a halmazt egyenként $n - 1 + L$ hosszú szavakkal, így kapunk egy w szót, amire $|Rw| = 1$ és $|w| \leq (r-1)(n-1+L)$. Ekkor $w_0 w$ jó lesz.

$|Sw^{-1} \cap R| > |S|$

Legyen tehát P_1, P_2 és R a Lemma feltételeinek megfelelő és rögzítsünk egy $\emptyset \neq S \subsetneq R$ halmazt.
Jelölje P a $P_2 P_1$ VM-et.

Definálunk egy $Z_S : A^* \longrightarrow \mathbb{R}_0^+$ véletlen változót...

$$Z_S(w) \;=\; |Sw^{-1} \cap R| \;=\; [R][Sw^{-1}]^T \;=\; [R]M_{\mathbf{w}}[S]^T.$$

...aminek kiszámoljuk a várható értékét P mellett...

$$\mathbf{E}_P(Z_S) \;=\; |S|$$

Ha van olyan $v \in \mathrm{dom}(P) = \mathrm{dom}(P_2 P_1) = A^{\leq n-1}\mathrm{dom}(P_1)$, amire $Z_S(v) \neq |S|$, akkor van olyan $w \in \mathrm{dom}(P)$ is, amire $Z_S(w) = |Sw^{-1} \cap R| > |S|$ és kész vagyunk.

$|Sw^{-1} \cap R| > |S|$

Tegyük fel tehát, hogy minden $v \in \mathrm{dom}(P)$-re $Z_S(v) = |S|$.
Akkor minden $x \in \mathrm{dom}(P_1)$-re is $|Sx^{-1} \cap R| = |S|$.

γ

Jelölje γ az $[S]^T - \frac{|S|}{r}[Q]^T$ vektort.
Akkor tetszőleges $w \in A^*$-ra $M_{\mathbf{w}}\gamma = [Sw^{-1}]^T - \frac{|S|}{r}[Q]^T$, emiatt $[R]M_{\mathbf{w}}\gamma = |Sw^{-1} \cap R| - |S|$.
Ha tehát $x \in \mathrm{dom}(P_1)$, akkor $M_{\mathbf{x}}\gamma$ egy $[R]$-re merőleges nemnulla vektor.

Az utolsó lépés

Feszítsék ki az $M_{\mathbf{x}}\gamma$, $x \in \mathrm{dom}(P_1)$ vektorok a W alteret ($\mathbb{R}^n$-ben).
Akkor $0 \neq W \subseteq [R]^{\perp}$, $\dim W \geq 1$, $\dim([R]^{\perp}) = n-1$.

Kész is

Most tudjuk alkalmazni a Vektorteres Lemmát, $W = W$, $V = [R]^{\perp}$ és $\pi(u) = M_{\mathbf{u}}$ választásával.
Kijön, hogy egy $v \in \mathrm{dom}(P)$ szóra $0 \neq [R]M_{\mathbf{v}}\gamma = |Sv^{-1} \cap R| - |S|$, ezzel igazolva az állítást.

Gyengén monoton automaták

Gyengén monoton automaták

Definíció

Az $M = (Q, A, \delta)$ automata gyengén monoton, ha létezik automaták olyan $M = M_0, \ldots, M_\ell$ sorozata, $M_i = (Q_i, A, \delta_i)$, és olyan $\leq_i \subseteq Q_i \times Q_i$ relációk, $i = 0, \ldots, \ell - 1$, amikre

1. $\leq_i$ stabil részbenrendezés Q_i-n;
2. $M_{i+1} \simeq M_i / \approx_i$, ahol $\approx_i$ a $\leq_i$ által generált ekvivalencia;
3. M_ℓ triviális automata.

Stabilitás

A $\leq \subseteq Q \times Q$ reláció stabil, ha

$$p \leq q \;\Rightarrow\; pa \leq qa$$

minden $p, q \in Q$, $a \in A$ esetén.

Példák

Minden aperiodikus automata gyengén monoton.
(Mert bármely nemtriviális aperiodikus automatában van nemtriviális stabil részbenrendezés.)

Ha az M automatában pontosan egy q_0 nyelő van, vagyis amire $q_0 A = \{q_0\}$, akkor M gyengén monoton.
(egy részbenrendezés: $q_0 \leq p$ minden $p \in Q$-ra.)

Vagyis a gyengén monoton automaták osztálya valódi módon tartalmazza az aperiodikus automatákét.

Erősen összefüggőség

Észrevétel (folklór)

Ha M-ben pontosan egy nyelő van, akkor $d(M) \leq (n-1)^2$.

Észrevétel

Ha M irányítható, akkor pontosan egy $C \subseteq Q$ erősen összefüggő komponense van, mely az elérhetőségre maximális.
Ha $d(M|_C) \leq (|C|-1)^2$, akkor $d(M) \leq (n-|C|)^2 + (|C|-1)^2 \leq (n-1)^2$.
Elég tehát az erősen összefüggő automatákkal foglalkozni.

A tétel

Tétel (Volkov, 2009)

Ha M egy n-állapotú, erősen összefüggő, gyengén monoton automata, akkor irányítható és $d(M) \leq \left\lfloor \frac{n(n+1)}{6} \right\rfloor$.

Bizonyítás

Ha $n = 1$, az állítás nyilvánvaló. Legyen $M = (Q, A, \delta)$, $|Q| = n$ a feltételeknek megfelelő és haladjunk indukcióval n szerint.
Legyen $\leq$ a gyengén monotonitás definíciója szerint létező, nemtriviális stabil részbenrendezés Q-n.

Ha $S \subseteq Q$, jelölje $\min S$ ill. $\max S$ az S-ben $\leq$ szerint minimális ill. maximális elemek halmazát.

Csatolt halmazok

Állítás

Tetszőleges $S \subseteq Q$-ra és $u \in A^*$-ra

$$\min(Sv) \subseteq (\min S)v.$$

Definíció

Egy $T \subseteq Q$ állapothalmaz csatolt, ha a $(T, \leq)$ poset Hasse-diagramja összefüggő.

Észrevétel

Ha T csatolt, akkor Tv is. (Mivelhogy $\leq$ stabil.)

Észrevétel

Ha T csatolt és $|T| > 1$, akkor $\min T \cap \max T = \emptyset$. (Különben lenne izolált pont.)

A Bizonyítás Magja

Lemma

Ha $T \subseteq Q$ csatolt, $\ell = |\min T \setminus \max T|$ és $k = |\max Q|$, akkor van egy olyan w szó, amire $|Tw| = 1$ és melynek hossza legfeljebb

$$b(\ell, k) \;=\; \ell(n-k+1) - \frac{\ell(\ell+1)}{2}.$$

Bizonyítás

Ha $\ell = 0$, akkor $|T| = 1$ kell legyen és ekkor $b(\ell, k) = 0$, $w = \varepsilon$ jó lesz.
Folytatva indukcióval $\ell > 0$ szerint, ekkor $\ell = |\min T|$.
Vegyünk egy legrövidebb, $\min T$-ből $\max Q$-ba vivő u szót. (Ilyen van.)
Hossza legfeljebb $n - \ell - k + 1$ (vegyük észre: $\min T \cap \max Q = \emptyset$).
Vegyük észre, hogy

$$b(\ell - 1, k) + (n - \ell - k + 1) \;=\; b(\ell, k),$$

speciálisan $b(\ell, k) > b(\ell - 1, k)$.

Bizonyítás folytatása

Most vegyük a Tu szintén csatolt halmazt. Legyen $q' \in \min T$, $q = q'u \in \max Q$, persze $q \in Tu$.

- Ha $q \in \min Tu$, akkor $q \in \min Tu \cap \max Tu$ miatt $|T| = 1$. Tehát $w = u$ jó lesz.
- Ha $q \notin \min Tu$, akkor $\min Tu \subsetneq (\min T)u$ és alkalmazhatjuk az indukciós hipotézist.

Szummázás

Állítás

Ha $0 \leq \ell \leq k$, akkor $b(\ell, k) \leq \lfloor \frac{n(n+1)}{6} \rfloor$.
(Másodfokú egyenlőtlenség n-ben, nem-pozitív diszkriminánssal.)

A tétel állítása kijön az n szerinti indukcióval.

Nyitott probléma

Még az is lehet, hogy a gyengén monoton, erősen összefüggő automaták lineáris hosszú szóval is irányíthatók...

Tartalom

Road Coloring Problem

Kérdés

Adott egy $G = (V, E)$ d-reguláris multigráf (minden csúcs kifoka d). Mikor lehet kiszínezni az éleit az $\{1, \ldots, d\}$ színekkel úgy, hogy

- automatát kapjunk (vagyis minden (p, i), $p \in V$, $i \in \{1, \ldots, d\}$ esetén pontosan egy p-ből induló, i-vel címkézett él legyen)

  és
- ez az automata irányítható legyen?

Észrevétel

Elég erősen összefüggő multigráfokkal foglalkozni.

Egy szükséges feltétel

Ha (V, E)-nek van irányítható színezése, akkor

$$\gcd\{k : \ V\text{-ben van } k \text{ hosszú kör}\} = 1.$$

Sejtés (Weiss – Adler 1970)

Egy erősen összefüggő (V, E) d-reguláris multigráfnak pontosan akkor van irányítható színezése, ha

$$\gcd\{k : \ V\text{-ben van } k \text{ hosszú kör}\} = 1.$$

Tétel (Trahtman, 2007)

A sejtés igaz.

Összefoglalás, konklúziók

Az utóbbi évtizedben (is) komoly eredmények születtek automaták irányíthatóságával kapcsolatosan.

Jó lenne meghatározni, hogy hol vannak az Átlagoló Lemma határai, és hogy lehet-e erősíteni.

A gyengén monoton automaták esetére az a sejtés, hogy $o(n^2)$ hosszú szóval is irányíthatóak.
Jelenleg nem ismert gyengén monoton automaták olyan családja, mely $\omega(n)$ hosszon lenne irányítható.

Köszönöm a figyelmet.