

BINÁRIS KÓDOK FELBONTHATÓSÁGÁT VIZSGÁLÓ VÉGESAUTOMATA ALAPÚ

ALGORITMUSOK

Falucskai János

Nyíregyházi Főiskola, Matematika és Informatika Intézet

falu@nyf.hu

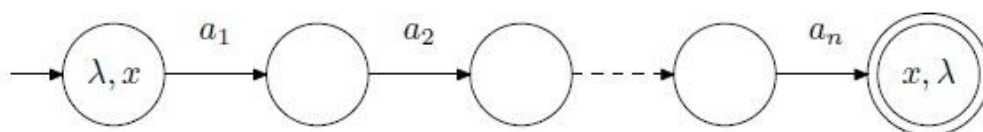
1. Bevezetés

A kódot tekinthetjük a kódszavakat tartalmazó formális nyelvnek, s véges jellege miatt ez a nyelv hármasszerű nyelvtannal leírható, így megadható véges automatával. A véges automata a hagyományos leírások (szabályhalmaz, illetve grafikai reprezentáció) mellett megadható más eszközökkel is, például kapcsolati mátrixszal vagy reguláris kifejezéssel. A célunk az volt, hogy egy adott rendszerbeli problémát egy másik rendszerben oldjunk meg, nevezetesen kódelméleti problémákat véges automatával modellezzünk. Egy ilyen probléma a kód felbonthatósága, azaz egy adott kód esetén annak eldöntése, hogy van-e két különböző sorozata a kódszavaknak, mely ugyanazon üzenetet hordozza. Ismertetünk három véges automatát, mely megoldja a fent említett problémát. A terjedelmi korlátok miatt csak áttekintést tudunk adni, nem törekedünk a teljességre.

2. A „virág” automata

Legyen X egy tetszőleges részhalmaza az ábécé tranzitívlezárt halmazának. Definiáljunk egy A automatát, ahol az automata az **1.** ábrán megadott formájú nem összefüggő élek halmazának az uniója, ahol egy-egy összefüggő „élhalmaz” tartozik minden

$x=a_1 \cdots a_n$ X -ben lévő kódszóhoz.



1. ábra Az $x=a_1 \cdots a_n$ X -ben lévő kódszóhoz tartozó automata részlet

Az X halmazhoz tartozó virág automata definíció szerint a fentebb említett módon megkonstruált automata iteráltja, melynek általában A^*_X a jelölése. Az A^*_X automatát az A automatából két lépésben nyerhetjük.

Az automata elnevezését a grafikus reprezentáció indokolja, minden kódszó esetén egy-egy „virágszirom” alakul ki, hiszen minden kódszó egy-egy egyszerű utat definiál az automatában.

Legyen $X=\{aa,ba,bb,baa,bba\}$ egy kód, határozzuk meg a hozzátartozó virág automatát. Ehhez először az A automatát kell felírunk, emiatt definiálásához elsőnek megadjuk az automata belső állapotainak Q halmazát. A felírásban egy-egy sor az egy-egy kódszóból származó állapotokat jelenti.

$$\begin{aligned} Q = & \{(\lambda, aa), (a, a), (aa, \lambda), \\ & (\lambda, ba), (b, a), (ba, \lambda), \\ & (\lambda, bb), (b, b), (bb, \lambda), \\ & (\lambda, baa), (b, aa), (ba, a), (baa, \lambda), \\ & (\lambda, bba), (b, ba), (bb, a), (bba, \lambda)\} \end{aligned}$$

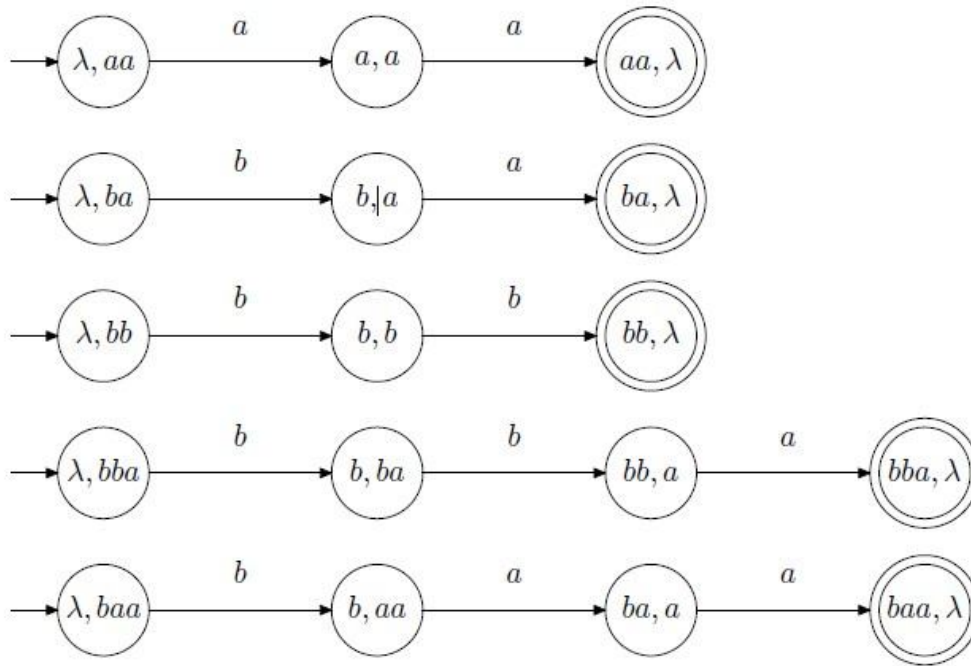
Az A automata I kezdő állapotainak halmaza az

$$I = \{(\lambda, aa), (\lambda, ba), (\lambda, bb), (\lambda, baa), (\lambda, bba)\}$$

halmaz, az elfogadó állapotok Q_F halmaza pedig a

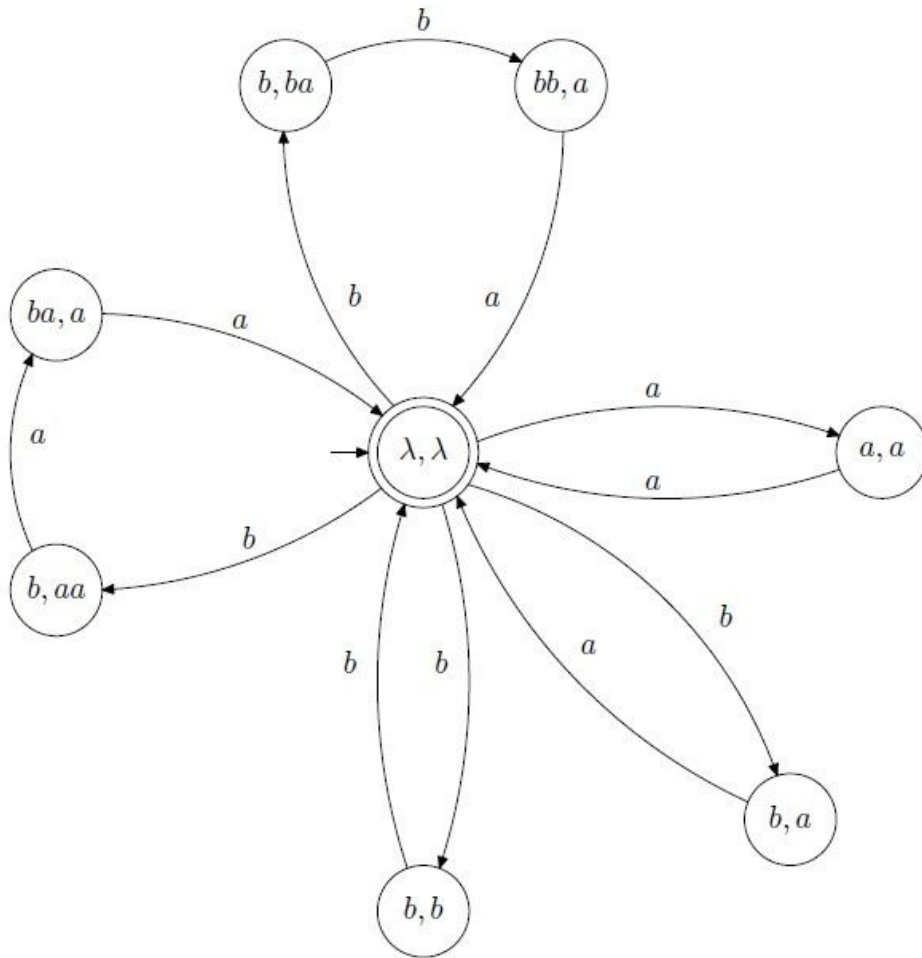
$$Q_F = \{(aa, \lambda), (ba, \lambda), (bb, \lambda), (baa, \lambda), (bba, \lambda)\}$$

halmaz. Ezekkel a jelölésekkel az A automata a 2. ábrán látható.



2. ábra: Az $X = \{aa, ba, bb, baa, bba\}$ kódhoz tartozó **A** automata

Az ω állapot bevezetése után az összefűzött és átszerkesztett automata a 3. ábrán látható.



3. ábra: Az $X = \{aa, ba, bb, baa, bba\}$ kódhoz tartozó A^* virág automata

3. A Tsuji-féle automata

Egy ábécé feletti szavakat tartalmazó véges X halmaz esetén közismert, hogy van algoritmus, mely alapján eldönthető, hogy X felbontható kódot ad-e, lsd. pl. Perrin. Definiáljuk többértelmű szóként azokat a szavakat, melyeknek több, mint két felbontása létezik, és konstruálunk egy automatát oly módon, hogy az általa elfogadott szavak halmaza egyenlő az X^* halmazban lévő összes többértelmű szó halmazával. Megmutatható, hogy az ábécé feletti szavakat tartalmazó X halmaz felbontható kód akkor, és csak akkor, ha az automata által felismert halmaz üres halmaz.

Egy ábécé feletti szavak X véges halmaza esetén legyen a $P(X)$ halmaz a következőképpen

definiálva: $P(X) = \{p \in X \mid p \text{ valódi kezdőszelete valamely } X \text{ halmazbeli szónak}\}$, azaz

$P(X) = \{p \in X \mid p \cdot q = r \in X, p \neq r, q \neq r\}$. Jelölje c_1 a $P(X)$ halmaz számosságát. Ekkor létezik egy

φ injektív leképezés, mely $P(X)$ -et a természetes számok halmazára képezi le úgy, hogy

$1 \leq \varphi(p) \leq c_1$ bármely $p \in P(X)$ esetén.

Hasonlóan az előbbiekhöz, legyen az $S(X)$ halmaz a következőképpen definiálva: $S(X) = \{s \in$

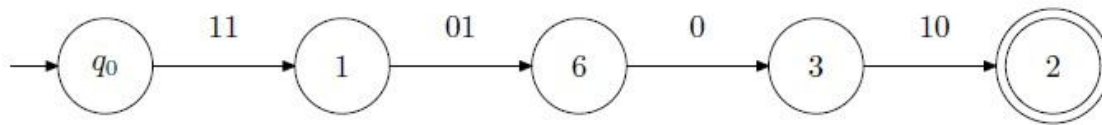
$A^+ \mid s \text{ valódi végzőszelete valamely } X \text{ halmazbeli szónak}\}$, azaz $S(X) = \{s \in A^+ \mid q \cdot s = r \in X,$

$s \neq r\}$.

Ekkor létezik egy ψ injektív leképezés, mely $S(X)$ -et a természetes számok halmazára képezi

le úgy, hogy $c_1 + 1 \leq \psi(s)$ bármely $s \in S(X)$ esetén.

Legyen adva a $K = \{010, 10, 11, 1101\}$ kód. A Tsuji-féle automata ábrája a 4. ábrán látható.

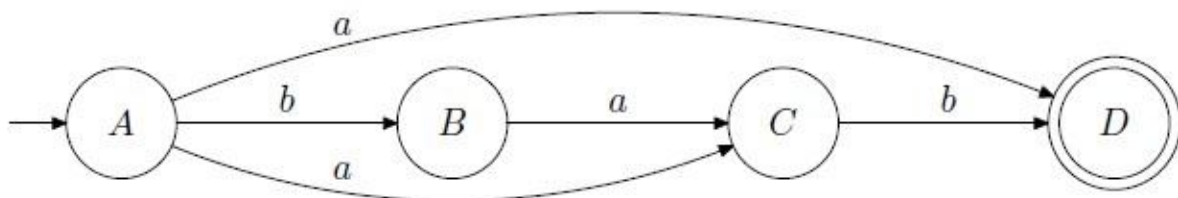


4. ábra: A $K = \{010, 10, 11, 1101\}$ kódhoz tartozó Tsuji-féle automata

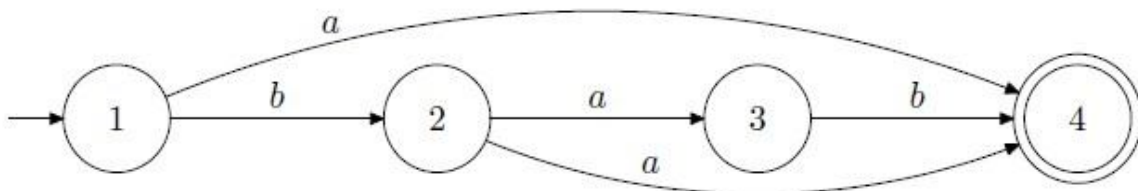
4. Automaták összefűzött szorzata

Az automatáknak egy olyan szorzatát fogjuk definiálni, amelynek segítségével eldönthető lesz egy kódról, hogy felbontható-e. Az ötlet az, hogy készítsük el a kódot elfogadó automatának az önmagával való Descartes szorzatát úgy, hogy amikor az automata elfogadó állapotba kerül, akkor egyúttal vigyük át kezdő állapotba is. Ez nemdeterminisztikus úton tehető meg. Az automata így módon elkészített, úgynevezett összefűzött szorzat automatája akkor kerül elfogadó állapotba, ha minden komponense ugyanakkor éri el az elfogadó állapotot.

A kódok felbonthatóságának vizsgálatához csak olyan összefűzött szorzat automatát fogunk vizsgálni, mely összesen két tényezőből áll. Legyenek adottak az 5. és a 6. ábrán látható automaták.

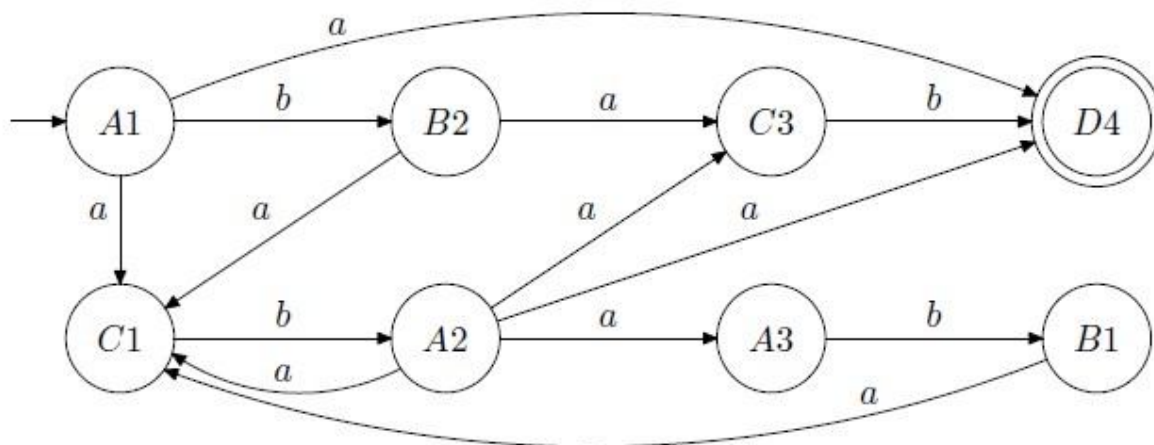


5. ábra



6. ábra

Ekkor megalkotva az összefűzött szorzatukat, a 7. ábrán látható automatát kapjuk:



7. ábra

Irodalomjegyzék:

Tsuji, Kayoko: An automaton for deciding whether a given set of words is a code. RIMS Kokyuroku 1222, 123-127, 2001.

J. Berstel and D. Perrin. Theory of codes, volume 117 of Pure and Applied Mathematics. Academic Press Inc., Orlando, FL, 1985.

R. König: Lectures on codes, Internal Reports of the IMMD I, 1994.