

Algoritmusok és adatszerkezetek II.

Sztring,-és számelméleti algoritmusok

Szegedi Tudományegyetem



$T = [t_0 t_1 \dots t_n]$ input tartalmazza-e a $P = [p_0 p_1 \dots p_m]$ mintát?
Ha igen, mely inputpozíció(k)tól/eltolási érték(ek)től kezdődően?
Tipikusan $n \gg m$



$T = [t_0 t_1 \dots t_n]$ input tartalmazza-e a $P = [p_0 p_1 \dots p_m]$ mintát?
Ha igen, mely inputpozíció(k)tól/eltolási érték(ek)től kezdődően?
Tipikusan $n \gg m$

Példa

Hányszor szerepel az 'orosz' szó a *Háború és béke* c. műben?

Nyers erőt használva legrosszabb esetben $O(mn)$ vizsgálat kell
Milyen hatékonyabb módszerek vannak?

- Mintaillesztés automatával
- Knuth-Morris-Prat
- Rabin-Karp algoritmus



Automata alatt egy $M = (Q, q_0, A, \Sigma, \delta)$ rendezett ötöst értünk, ahol

- Q a lehetséges állapotok halmaza
- q_0 a kezdőállapot
- $A \subseteq Q$ a végállapotok halmaza
- Σ egy véges ábécé
- $\delta : Q \times \Sigma \rightarrow Q$ az állapotátmenet-függvény



Mintaillesztés véges állapotú automatákkal

- Q -t válasszk $\{q_0, q_1, \dots, q_m\}$ -nak
- q_i állapot jelentése: az input aktuális pozíciójáig a minta első i karaktere illeszkedik
- q_m állapotba elérve elmondható, hogy megtaláltuk a $P = [p_0 p_1 \dots p_m]$ minta egy T -beli előfordulását

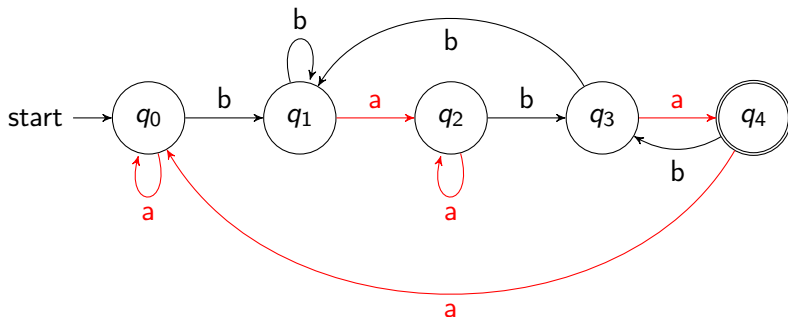


$P = baba$ minta felismerését végző véges automata

Az állapotátmenet-függvény táblázatos formában

	q_0	q_1	q_2	q_3	q_4
a	q_0	q_2	q_0	q_4	q_0
b	q_1	q_1	q_3	q_1	q_3

Kitöltése és tárolása egyaránt $O(m|\Sigma|)$ költségű



Knuth-Morris-Pratt (KMP) algoritmus

A véges automatával történő feldolgozás korlátai

Előfeldolgozás gyanánt ki kell tölteni egy $m|\Sigma|$ méretű táblázatot (és persze tárolni is kell azt)



A véges automatával történő feldolgozás korlátai

Előfeldolgozás gyanánt ki kell tölteni egy $m|\Sigma|$ méretű táblázatot (és persze tárolni is kell azt)

Észrevételek

- 1 Ha $P = aab$ minta illeszkedett az input i -edik pozíciójára, akkor az $i + 1$ pozíciótól kezdődően biztos nem beszélhetünk illeszkedésről
- 2 Ha $P = aaa$ minta nem illeszkedett az input i -edik pozíciójára, akkor az $i + 1$ pozíciótól kezdődően biztos nem beszélhetünk illeszkedésről



- P_i jelölje P -nek az i hosszúságú prefixét (kezdőszeletét), azaz pl. $P_3 = bab$, $P_1 = b$, illetve $P_0 = \epsilon$ (ϵ az üres szót jelöli)



- P_i jelölje P -nek az i hosszúságú prefixét (kezdőszeletét), azaz pl. $P_3 = bab$, $P_1 = b$, illetve $P_0 = \epsilon$ (ϵ az üres szót jelöli)
- $X \sqsubset Y$ jelölje azt, ha X sztring szuffixe Y -nak (azaz Y végződése maga X)

Példa

aaba \sqsubset cacaaaba, ugyanakkor aaba $\not\sqsubset$ cacaab**b**

Megjegyzés: Az $Y \sqsubset Y$, valamint az $\epsilon \sqsubset Y$ relációk triviálisan teljesülnek minden Y -ra.



- $\pi : \{1, 2, \dots, m\} \rightarrow \{0, 1, \dots, m-1\}$ $P = [p_1 \dots p_m]$ minta prefixfüggvénye, ha $\pi[q] = \max\{k : k < q \wedge P_k \sqsubseteq P_q\}$
- Azaz $\pi[q]$ megadja P azon leghosszabb (q -nál rövidebb) prefixének hosszát, ami valódi szuffixe $P_q = [p_0 \dots p_q]$ -nak
- Értelmezése: ha **nem sikerül továbbillesszük** a mintát az inputra, az **legalább** mely állapotig vet minket vissza



- $\pi : \{1, 2, \dots, m\} \rightarrow \{0, 1, \dots, m-1\}$ $P = [p_1 \dots p_m]$ minta prefixfüggvénye, ha $\pi[q] = \max\{k : k < q \wedge P_k \sqsubset P_q\}$
- Azaz $\pi[q]$ megadja P azon leghosszabb (q -nál rövidebb) prefixének hosszát, ami valódi szuffixe $P_q = [p_0 \dots p_q]$ -nak
- Értelmezése: ha **nem sikerül továbbilleszük** a mintát az inputra, az **legalább** mely állapotig vet minket vissza

Példa

$T = abbabababaca$ inputban keressük a $P = ababababca$ mintát

i	1	2	3	4	5	6	7	8	9	10
$P[i]$	a	b	a	b	a	b	a	b	c	a
$\pi[i]$	0	0	1	2	3	4	5	6	0	1



Az egyszerűség kedvéért a mintára és az inputra tekintsünk 10-es számrendszerbeli számokként

Alapötlet

P mintára alkalmazzunk egy $h_q(x) = x \bmod q$ hasítófüggvényt.

T -nek csak azon $S = [t_j]_{j=i}^{i+m-1}$ résztringjei egyezhetnek meg

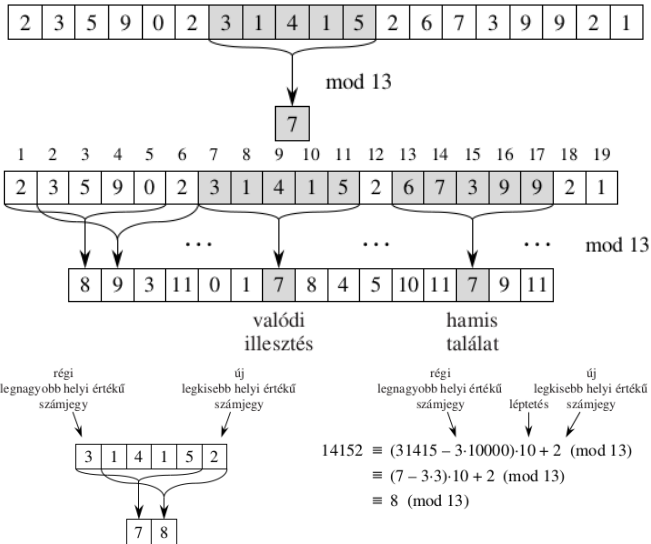
P -vel, melyekre $h_q(S) = h_q(P)$

$h_q(S) = h_q(P)$ természetesen csak szükségességi feltételt támaszt



Rabin-Karp algoritmus illusztráció (Forrás: CLRS 32.5 ábra)

$$P = 31415, h_q(x) = x \bmod 13$$



Észrevétel

h_q -nak az input minden indexén kezdődő kiszámítása költséges



Észrevétel

h_q -nak az input minden indexén kezdődő kiszámítása költséges

A hatékonyság záloga

Ahogy abc és bcd számpárral teljesül

$$bcd = 10 * (abc - 100 * a) + d$$

egyenlőség, hasonlóan igaz

$$h_q(bcd) = h_q(10 * (h_q(abc) - h_q(100) * a) + d)$$

összefüggés is.



- Probabilisztikus adatszerkezet a Keres műveletre nézve
- Implementációja: (egyenletesen szóró) h hasítófüggvény és egy (kezdetben csupa 0) bitvektor
 - x elem beszúrásakor a bitvektor $h(x)$ indexét 1-re állítjuk
 - x elem keresésnél ha a bitvektor $h(x)$ indexe 1, akkor azt mondjuk, hogy x -et tartalmazza a bloom filterünk
 - Hamis elutasítás soha nem teszünk, ugyanakkor hamis pozitív választ adhatunk
- Hatékonysága függ h hasítófüggvényről, valamint az eltárolt elemek számától (ami kihat a bitvektor kitöltöttségére)
- Linkek: [Bloom filter demo](#) és [Guava API](#)



Mintaillesztés főbb megközelítései

Algoritmus	Előfeldolgozás	Illesztés ¹
Nyers erő	0	$O(mn)$
Rabin-Karp	$\Theta(m)$	$O(mn)$
Véges automata	$O(m \Sigma)$	$\Theta(n)$
Knuth-Morris-Prat	$\Theta(m)$	$\Theta(n)$

- Rabin-Karp a nyers erő módszerének kiterjesztéseként tekinthető
- KMP pedig a véges automatákkal való illesztés egy hatékonyabb verziója

¹legrosszabb eset



A moduláris hatványozás

Alapprobléma: Mi az $a^b \bmod n$ kifejezés értéke?

Gyakorlati jelentőség: titkosító eljárások (pl. RSA) használata során szükségünk lehet ilyen számítások elvégzésére

Már viszonylag kis b -re is rengeteg bitműveletet kell elvégezzünk



A moduláris hatványozás

Alapprobléma: Mi az $a^b \bmod n$ kifejezés értéke?

Gyakorlati jelentőség: titkosító eljárások (pl. RSA) használata során szükségünk lehet ilyen számítások elvégzésére

Már viszonylag kis b -re is rengeteg bitműveletet kell elvégezzünk

Példa – Mi lesz $7^{560} \bmod 561$ értéke? Avagy

179846672920572906577258722224560336083856608137007342561
612636144396089769552955665549135995604075608096691162101
184113545972526638255004784055311390598542305958357097082
391225061077433281620117130013826448606281708665937931659
796736755253074977366471063146923373865223501532185753076
292710887401801774392779475679510556311966981952826025487
057204699261913973664257857993744045143447531121540574215
969802961003872086163860991702035506591312847029674260362
509156745965136001 mod 561=?



Moduláris hatványozás

```
MODULÁRIS-HATVÁNYOZÓ(a, b, n){
```

```
    c = 0
```

```
    d = 1
```

```
    B = [bk ... b1 b0]
```

```
    for (i=k; k >=0; --k) {
```

```
        c = 2*c
```

```
        d = (d*d) mod n
```

```
        if (B[i] == 1) {
```

```
            c = c+1
```

```
            d = (d*a) mod n
```

```
        }
```

```
    }
```

```
    return d
```

```
}
```

Megjegyzések

- 1 b -nek k bites bináris alakja B
- 2 c csak egy segédváltozó



```
MODULÁRIS-HATVÁNYOZÓ(a, b, n){
```

```
    c = 0
```

```
    d = 1
```

```
    B = [bk ... b1 b0]
```

```
    for (i=k; k >=0; --k) {
```

```
        c = 2*c
```

```
        d = (d*d) mod n
```

```
        if (B[i] == 1) {
```

```
            c = c+1
```

```
            d = (d*a) mod n
```

```
        }
```

```
    }
```

```
    return d
```

```
}
```

Megjegyzések

- 1 b -nek k bites bináris alakja B
- 2 c csak egy segédváltozó

Kérdés

- Mi lesz d és c értéke a for ciklus első végrehajtása után?



Moduláris hatványozás

```
MODULÁRIS-HATVÁNYOZÓ(a, b, n){
```

```
    c = 0
```

```
    d = 1
```

```
    B = [bk ... b1 b0]
```

```
    for (i=k; k >=0; --k) {
```

```
        c = 2*c
```

```
        d = (d*d) mod n
```

```
        if (B[i] == 1) {
```

```
            c = c+1
```

```
            d = (d*a) mod n
```

```
        }
```

```
    }
```

```
    return d
```

```
}
```

Megjegyzések

- 1 b -nek k bites bináris alakja B
- 2 c csak egy segédváltozó

Kérdés

- Mi lesz d és c értéke a for ciklus első végrehajtása után?

Műveletigény

Ha a, b és n k biten elfér, mindez $O(k)$ aritmetikai műveletet és $O(k^3)$ bitműveletet jelent



A moduláris hatványozás működése

- Az algoritmus for ciklusában minden egyes iteráció megkezdése előtt a c és d változók értékeire teljesül, hogy:
 - 1 c változó értéke megegyezik a $[b_k \dots b_{i+1}]$ bináris értékkel
 - 2 $d = a^c \bmod n$
- A fenti ciklusinvariáns teljesül, megmarad és befejeződik \rightarrow



Moduláris hatványozás példa

$$7^{560} \bmod 561 = ?$$

$$a = 7, b = 560, n = 561 \ (B = [1000110000])$$

i	9	8	7	6	5	4	3	2	1	0
b_i	1	0	0	0	1	1	0	0	0	0
c	1	2	4	8	17	35	70	140	280	560
d	7	49	157	526	160	241	298	166	67	1

