Haladvány Kiadvány 13.11.20. http://www.math.bme.hu/~hujter/halad.htm

Nagy Matematika

Szalkai István
Pannon Egyetem, Veszprém
szalkai@almos.uni-pannon.hu

A kombinatorikában egymás után írunk le rettentően nagy számokat és nem is törődünk vele, hogy mekkorák is valójában. Még meglepőbb, hogy a matematika szinte minden területén is sokszor találkozunk hasonlóan nagy méretű számokkal, számolásokkal, jelen összeállításunkban csak néhány érdekesebbet mutatunk be. A nagy számítások elméletét az *Algoritmusok bonyolultsága* tudományágban találjuk, bevezetőnek [Sz2001] III. részét és [LL1990] 3. fejezetét ajánljuk. (**Cejtin Tétel**ét azért ideírjuk: *Minden* rekurzív (*kiszámítható*) $f(n)$ *függvényhez létezik olyan algoritmikus probléma, amelynek megoldásához, n méretű adathalmazok esetén* legalább $f(n)$ *idő kell.* □ Nos, ha például $f(n) = 10^{10^{\circ\circ\circ^{10}}}$ (n magas hatvány) ???)

A feladatok megoldását a cikk második részében találjuk.

Feladatok

0) Egy n -jegyű N szám *prímtényezős felbontását* keressük. Egy tanult módszer: a páratlan számokat próbáljuk ki $\sqrt{N}$ -ig. Hány osztást kell elvégeznünk?

a) Ez mennyi idő lenne n=20, n=30, n=40 és n=50 esetén egy 5 GHz-es gépen futtatva, ha *csak* az osztásokat számítjuk egy-egy lépésnek ?

b) Mennyire csökkenne a futásidő, ha a $\sqrt{N}$ alatti prímszámokat egy táblázatban tárolnánk, és csak e prímszámokat próbálnánk ki ?

1) a) Hány szorzást kell elvégeznünk egy nxn -es mátrix *determinánsának* kiszámításához a definíció szerint?

Ez mennyi idő lenne n=15, n=20 és n=25 esetén egy 5 GHz -es gépen futtatva, ha *csak* a szorzásokat számítjuk egy-egy lépésnek ?

Becsüljük meg a kapott eredmény nagyságrendjét $n \to \infty$ esetén!

b) Ugyanekkora mátrixok *szorzásához*, illetve n -edik *hatványának* kiszámolásához hány szorzást kell elvégeznünk? Ezeket is számoljuk át *mp* –re, 5 GHz –es gépet feltételezve !

2) Legyen $f : \mathrm{R}^p \to \mathrm{R}$ egy tetszőleges p -változós, n -szer deriválható függvény.

a) Hányféle n -edik deriváltja van? (Ne feledjük Schwarz tételét!)

b) Hány tagból áll az $f(x)$ függvény N -edrendű Taylor polinomja?

c) Hány n -edik deriváltja van az olyan $g : \mathrm{R}^p \to \mathrm{R}$ függvényeknek, melyekre nem igaz Schwarz tétele (azaz $\mathrm{D}_i\, g \neq \mathrm{D}_j\, g$ ha $i \neq j$) ?

Csodáljuk meg **Faá di Bruno** formuláját is:

Ha $D_x^k u$ *jelöli az u függvény x szerinti k -adik deriváltját, akkor*

$$D_x^n w = \sum_{0 \leq j \leq n} \sum_{\substack{0 \leq k_1, k_2, \ldots, k_n \\ k_1 + k_2 \ldots + k_n = j \\ k_1 + 2k_2 + \ldots + nk_n = n}} D_u^j w \cdot \frac{n!}{k_1!(1!)^{k_1} \ldots k_n!(n!)^{k_n}} (D_x^1 u)^{k_1} \ldots (D_x^n u)^{k_n}$$

3) Tekintsünk egy n – változós f logikai függvényt.

a) Hány sorból áll igazságtáblázata? Mennyi idő alatt értékelné ki egy 5 GH**z** –es gép, ha *minden órajel alatt egy-egy sort* tudna kiértékelni ?

b) Ha feltesszük, hogy az f függvény értékeinek kb. 50% -a *igaz*, akkor hány karakterből áll az f függvény Diszjunktív Normál Forma (DNF) alakban?

Mennyi ideig nyomtatná a karaktereket egy 5 GH**z** –es gép, ha *minden órajel alatt egy-egy karaktert* nyomtatna ki?

Hány oldalon illetve hány kötetben (hány méter polcon) férne ki ez a DNF **4 pt** -os betűméretben, 152 sor, soronként 225 karakter, "biblia"-papíron 1500 lap = 4 cm? (Indexes változókat használjunk: $p_1 \dots p_n$, vagyis mindegyik változóra két-két karaktert számoljunk. A tagadás műveletét jelöljük felülvonással, vagyis ez nem külön karakter. Lehető legkevesebb zárójelet használjunk: $(\wedge \dots \wedge) \vee (\wedge \dots \wedge) \dots$ alakban.)

12345678101234567820123456783012345678401234567850123456786012345678701234567880123456789012345671001234567810123456782012345678301234567840123456785012345678601234567870123456788012345678901234567200123456781012345678201234567

c)* *Átlagosan* milyen hosszú egy DNF, ha csak a legfeljebb 50% -ban *igaz* függvényeket tekintjük ?

4) o) Hány *egyszerű* gráf van n csúcson ?

a) Két n –elemű halmaz között hány bijekció van ?

b) Ha "favágó" -módon két n –csúcsú egyszerű gráf *izomorfiáját* úgy ellenőriznénk, hogy csúcshalmazaik között az *összes* bijekció éltartóságát ellenőriznénk, akkor ez mennyi időt venne igénybe egy 5 GH**z** –es gépen, ha *minden órajel alatt egy-egy* él-ellenőrzést végezne?

5) o) Egy n –elemű és egy k –elemű halmaz között hány *tetszőleges* függvény van?

a) A "favágó" – módszer alkalmazásával mennyi idő alatt tudnánk eldönteni egy n –csúcsú gráfról, hogy 3 -*kromatikus* -e, azaz k=3 jó -e (5 GH**z**-es gép, *minden órajelben* ...) ?

b) Mi a helyzet a k=2 esetben ?

6) Hány tagból áll az $(x_1+x_2+...+x_p)^n$ kifejezés (a polinomiális tétel szerint kifejtve) ? Ez mennyi pl. n= 10 *és* p= 5 esetén?

7) Hányféleképpen lehet az x_1-x_2-…-x_n kifejezést zárójelezni? Mennyi ideig nyomtatná a végeredményt egy 5 GH**z**-es gép (*minden órajelben* ...) ?

8) Az 1,2,...,100 számok közül hányféleképpen lehet kiválasztani hármat úgy, hogy a kiválasztott számok összege osztható legyen 3 -mal ?

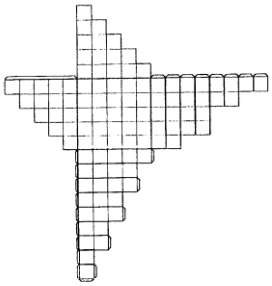
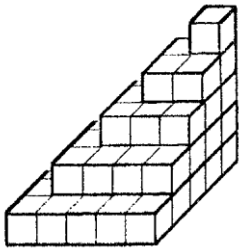
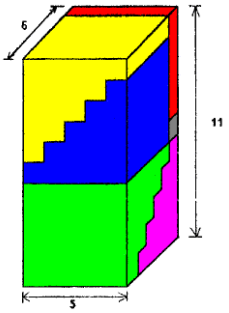
(XVII. Bátaszéki matematikaverseny, országos döntő 7.osztályos feladat, 2006.)

9) Hány tagból áll a logikai szitaformula n részhamaz esetén?

10) Tekintsük a természetes számokon a következő (végtelen) gráfot: K=(N,F), ahol az m és n csúcsokat pontosan akkor kötjük össze éllel, ha m és n relatíve prímek. Mutassuk meg, hogy ekkor tetszőleges G=(V,E) gráf pontosan akkor feszített részgráfja K -nak, ha G tetszőleges $P \in V$ csúcspontjára a $G \setminus \Gamma(P)$ gráf kromatikus száma véges (itt $\Gamma(P)$ jelöli P szomszédainak halmazát G -ben).

A feladat általánosítását lásd még [Sz1991] -ben.

11) Pihenésképpen az $1^2+2^2+...+n^2 = n(n+1)(2n+1)/6$ azonosságot szemlélteti az alábbi három ábra:

6x  => 6x  => 

.

Megoldások

0) a) Ha az N szám *n* -jegyű, akkor értéke körülbelül $N \sim 10^n$ (pontosabban $10^{n-1} \le N < 10^n$). Ekkor az osztások száma $\sqrt{N}/2$, ami

n=20 (és 5GHz) esetén $5 \cdot 10^9$ lépés = 1 mp ,

n=30 esetén $5 \cdot 10^{14}$ lépés = 10^5 mp ~ 27 óra 46 perc,

n=40 esetén $5 \cdot 10^{19}$ lépés = 10^{10} mp ~ 317 év 35 nap 18 óra,

n=50 esetén $5 \cdot 10^{24}$ lépés = 10^{15} mp ~ 31.7 millió év ... .

b) **Jelöljük** tetszőleges *x* szám esetén $\pi(x)$ -el az *x* -nél kisebb prímszámok számát! A "Nagy Prímszámtétel" (Hadamard és de la Vallée Poussin, 1896) szerint $\pi(x) \sim x/\ln(x)$. Ekkor az osztások száma $\pi(\sqrt{N}) \sim \sqrt{N}/\ln(\sqrt{N})$, ami

n=20 (és 5GHz) esetén $\sim 4.3 \cdot 10^8$ lépés < 1 mp ,

n=30 esetén $\sim 2.9 \cdot 10^{13}$ lépés ~ 5790 mp ~ 1 óra 36 perc,

n=40 esetén $\sim 2.2 \cdot 10^{18}$ lépés ~ $4.4 \cdot 10^8$ mp ~ 13 év 281 nap 13 óra,

n=50 esetén $\sim 1.4 \cdot 10^{23}$ lépés ~ $1.7 \cdot 10^{14}$ mp ~ 5.5 millió év ... .

1) A szorzások száma $n + n(n-1) + n(n-1)(n-2) + \ldots + n!$, vagy másképpen:
$n! \cdot (1 + 1/1! + 1/2! + \ldots + 1/(n-1)!)$. A Stirling -formula szerint ez aszimptotikusan:

$$\approx \frac{n^n \sqrt{2\pi n}}{e^n} \cdot \left(1 + 1/1! + 1/2! + \ldots + 1/(n-1)!\right) \sim \left(\frac{n}{e}\right)^n \cdot e \quad .$$

***n*=15** (és 5GHz) esetén ez kb.

$15^{15}\sqrt{30\pi}/e^{14}$ ~ 3 534 937 201 323 lépés = 706 986 mp ≈ **196** óra ,

***n*=20** esetén

$20^{20}\sqrt{40\pi}/e^{19}$ ~ 6 585 813 029 813 853 679 lépés

= 1 317 162 605 962 mp ≈ 365 878 501 óra ≈ **41 767 év !!!**

***n*=25** esetén

$25^{25}\sqrt{50\pi}/e^{24}$ ~ $3{,}35299 \cdot 10^{24}$ lépés ~ $6{,}70598 \cdot 10^{14}$ mp ≈ **21 264 542 év !!!**

2)a) Egy derivált $D_{k1}D_{k2} \dots D_{kp} f$ alakú, ahol a $0 \le k_1, k_2, \dots, k_p \le n$ egész számokra teljesül, hogy $k_1+k_2+\dots+k_p = n$. Az ilyen k_i számok száma ismétléses kombináció

$$C_p^{n\,(ism)} = \binom{p+n-1}{p-1} = \frac{(n+1)(n+2)\dots(n+p-1)}{(p-1)!} .$$

b) A Taylor polinom tagjainak száma

$$\sum_{n=0}^{N} \binom{p+n-1}{p-1} = \binom{p+N}{p} = \frac{(N+1)(N+2)\dots(N+p)}{p!} > \frac{N^p}{p!} .$$

c) Ha Schwarz tétele nem teljesül, akkor a deriváltak lehetséges száma ismétléses variáció:

$$V_p^{n\,(ism)} = p^n .$$

3) a) Az igazságtáblázat 2^n sorból áll.

n=10 esetén ez 2^{10} / 5GHz = 1024/5*10^9 mp = 2,048 * 10^{-7} mp,
n=20 esetén ez 2^{20} / 5GHz ≈ 2,097 * 10^{-4} mp,
n=30 esetén ez 2^{30} / 5GHz ≈ 0,215 mp,
n=40 esetén ez 2^{40} / 5GHz ≈ 219**,**902 mp ≈ 3.6 perc,
n=50 esetén ez 2^{50} / 5GHz ≈ 225 180 mp ≈ 62.5 óra ≈ 2.6 nap,
n=60 esetén ez 2^{60} / 5GHz ≈ 2,306*10^8 mp ≈ 6 405 óra ≈ 7 év 3.5 hónap,
n=70 esetén ez 2^{70} / 5GHz ≈ 2,361*10^{11} mp ≈ 6,559*10^7 óra ≈ **7 508 év !**
n=80 esetén ez 2^{80} / 5GHz ≈ 2,418*10^{14} mp ≈ **7 688 020 év !**
…

b) Minden *igaz* sorhoz egy $(p_1 \wedge \dots \wedge p_n) \vee$ jelsorozat tartozik (a tagadás műveletét nem számoljuk), ami $2+2n+n-1+1 = 3n+2$ hosszú. Mivel a DNF $2^n/2$ *igaz* sort tartalmaz, ezért a DNF hossza $\mathbf{2^n * (3n+2)/2}$ **.**

n=20 esetén ez 2^{19} *62 / 5GHz ≈ 0,006 mp,
n=30 esetén ez 2^{29} *92 / 5GHz ≈ 9,89 mp,
n=40 esetén ez 2^{39} *122/ 5GHz ≈ 13 414 mp ≈ 3 óra 43,5 perc,
n=50 esetén ez 2^{49} *152/ 5GHz ≈ 1,711*10^7 mp ≈ 6.5 hónap,
n=60 esetén ez 2^{59} *182/ 5GHz ≈ 2,098*10^{10} mp ≈ 667 év 2.5 hónap,
n=70 esetén ez 2^{69} *212/ 5GHz ≈ 2,503*10^{13} mp ≈ **795 830 év !**
n=80 esetén ez 2^{79} *242/ 5GHz ≈ 2,926*10^{16} mp ≈ **930 250 459 év !**

a karakterek száma:

n=20 esetén ez 2^{19} *62 / (152*225) ≈ 15,3 oldal,
n=30 esetén ez 2^{29} *92 / (152*225) ≈ 1 444 214 oldal ≈ 38,5 m -nyi könyv,
n=40 esetén ez 2^{39} *122/ (152*225) ≈ 1,96*10^9 oldal ≈ **52,26 km ! -nyi könyv**,
n=50 esetén ez 2^{49} *152/ (152*225) ≈ 2,5*10^{12} oldal ≈ **16 680 km ! -nyi könyv**,
n=60 esetén ez 2^{59} *182/ (152*225) ≈ 3*10^{15} oldal ≈ **81 805 736 km ! -nyi könyv**,
n=70 esetén ez 2^{69} *212/ (152*225) ≈ 3,66*10^{18} oldal ≈ **97 577 163 194 km**,
n=80 esetén ez 2^{79} *242/ (152*225) ≈ 4,28*10^{18} oldal ≈ 1,14*10^{14} km

≈ 0,012 fényév !!! -nyi könyv.

6) A 2/a) feladat alapján a kifejezés $C_p^{n\,(ism)} = \binom{n+p-1}{p-1}$ tagból áll.

7) A lehetőségek száma éppen az *n*-edik Catalan szám ([Sz2001], 137.oldal) :

$$\frac{1}{n+1}\cdot\binom{2n}{n} \approx \frac{2^{n-1}}{\sqrt{2\pi n}} \quad ,$$

a közelítés a *Stirling -formulával* történt.

n= 3 esetén ez = 2 lehetőség,
n= 5 esetén ez = 42 lehetőség,
n= 8 esetén ez = 1430 lehetőség,
n=10 esetén ez = 16 796 lehetőség,
n=20 esetén ez ≈ kb. $6{,}56*10^9$ lehetőség.

8) A felsorolt számokat 3-mal való osztási maradékaik szerint csoportosítjuk: 33 szám maradéka 0, 34 maradéka 1 és 33 maradéka 2. A kiválasztott számok összege akkor osztható 3-mal,ha három azonos maradékú, vagy egy 1-es, egy 2-es és egy 0-ás maradékú számot választottunk ki. Így a lehetőségek száma

$$2\cdot\binom{33}{3}+\binom{34}{3}+\binom{33}{1}\cdot\binom{33}{1}\cdot\binom{34}{1} = 53\,922\,.$$

9) "Csak" 2^n .

Hivatkozások

[L1990] **Lovász László**: *Algoritmusok bonyolultsága*, ELTE TTK jegyzet, Tankönyvkiadó Bp. 1990, bővített kiadás: http://www.cs.elte.hu/~kiraly/alg.pdf

[Sz1991] **Szalkai István**: *An Open Problem Concerning Spanned Subgraphs of Infinite Graphs*, VE Preprint 1991. http://math.uni-pannon.hu/~szalkai/CNo13.pdf

[Sz1997] ----- : *Diszkrét matematika feladatgyűjtemény*, Veszprémi Egyetemi Kiadó, 1997.

[Sz2001] ----- : *Diszkrét matematika és algoritmuselmélet alapjai,* Veszprémi Egyetemi Kiadó, 2001.

[SzD2011] **Szalkai István Dósa György**: *Algoritmikus számelmélet*, Typotex, 2011,

http://www.tankonyvtar.hu/hu/tartalom/tamop425/0008_szalkai_dosa_szamelmelet/adatok.html

http://tananyagfejlesztes.mik.uni-pannon.hu/index.php/elkeszuelt-tananyagok-digitalis-mellekletekkel

http://tananyagfejlesztes.mik.uni-pannon.hu/index.php/elkeszuelt-tananyagok-digitalis-mellekletekkel#Algoritmikus%20sz%C3%A1melm%C3%A9let%20%E2%80%93%20Titkos%C3%ADr%C3%A1s