TÖL403G GREINING REIKNIRITA

4. Deila-og-Drottna 2

Hjálmtýr Hafsteinsson
Vor 2022

Í þessum fyrirlestri

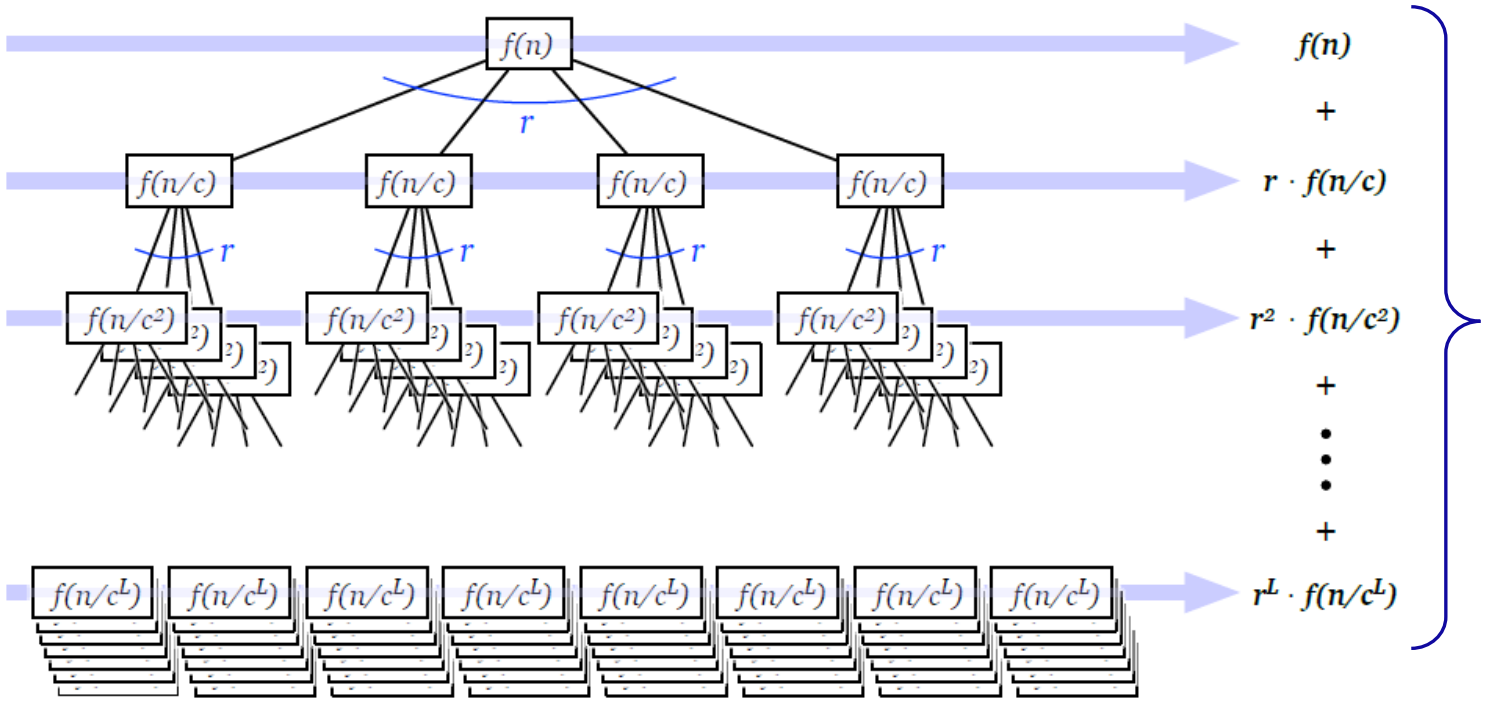
- Greining á *MoMSelect*
  - Nota rakningartré
  - Aðrar hópastærðir
- Hraðvirkari heiltölumargföldun
  - Reiknirit Karatsuba
  - Toom-Cook reikniritið
- Veldishafning (*exponentiation*)
  - Reiknirit Pingala

1.8 – 1.10

Rakningartré

- Sáum síðast:

Leysa: $T(n) = rT(n/c) + f(n)$



- Lækkandi kvótaröð:

  Lausn: $T(n) = O(f(n))$

- Jafnir liðir:

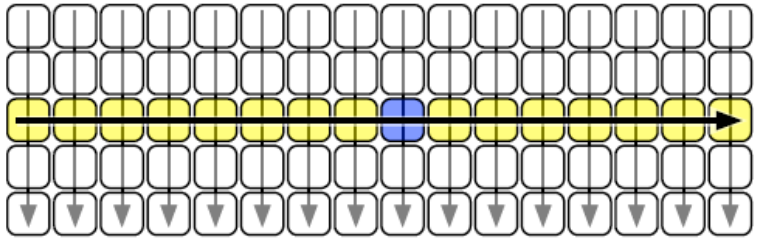
  Lausn: $T(n) = O(f(n) \cdot \log n)$

- Hækkandi kvótaröð:

  Lausn: $T(n) = O(n^{\log_c r})$

Finna miðgildi *n* staka

- Notum *QuickSelect* og veljum vendistakið sem miðgildi miðgilda í 5-staka hópum



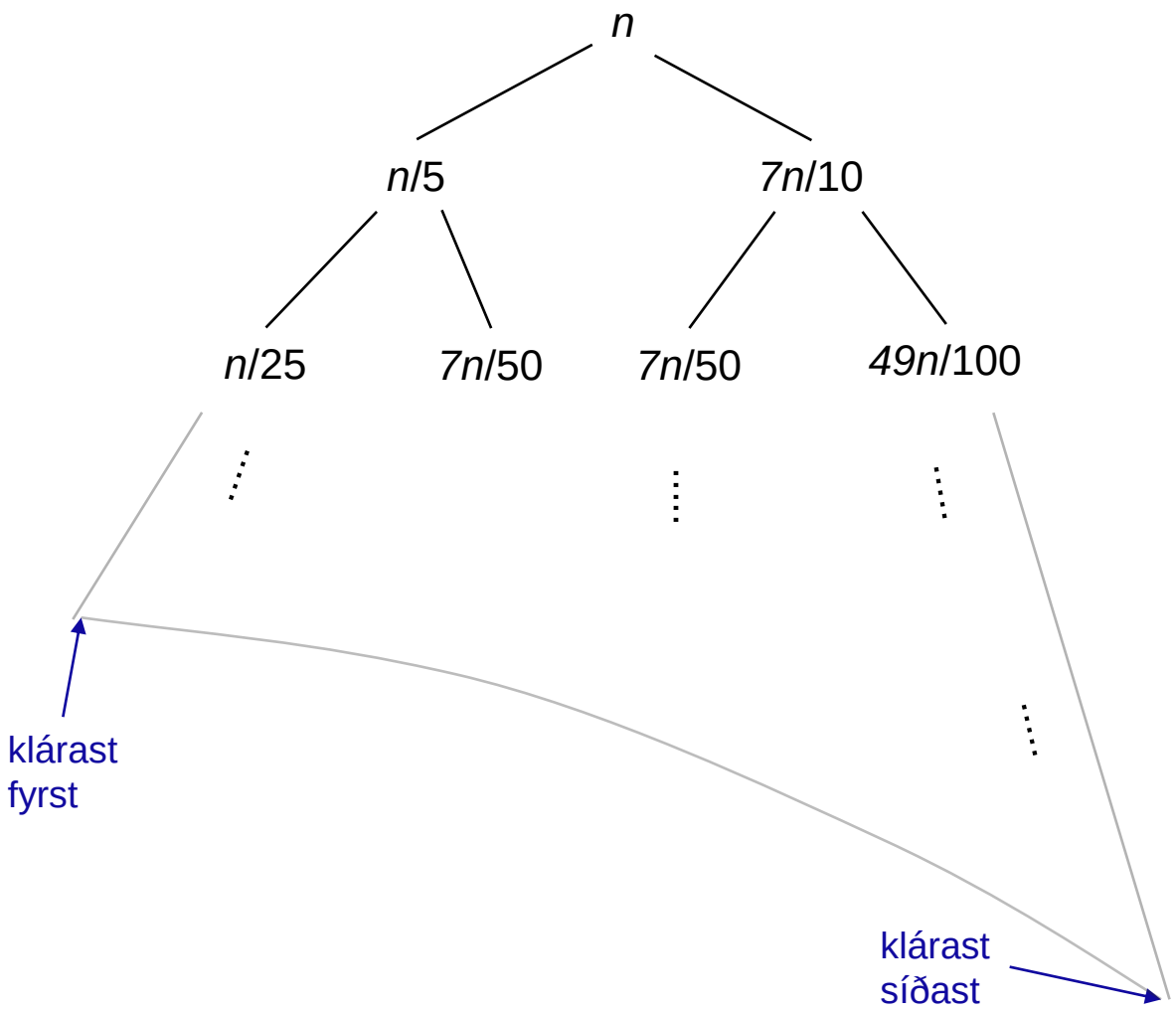
- Fáum þá rakningarvenslin

$$T(n) \leq T\left({}^{n}/_{5}\right) + T\left({}^{7n}/_{10}\right) + O(n)$$

Notum hér ≤, vegna þess að þetta er versta tilfellis skipting

Þetta er ekki alveg samkvæmt formúlunni fyrir rakningartré, en við getum samt notað þá aðferðafræði til að leysa venslin

Rakningartré fyrir venslin $T(n) = T(n/5) + T(7n/10) + O(n)$



Summa laga

n	$\leq (\frac{9}{10})^0 n$
$9n/10$	$\leq (\frac{9}{10})^1 n$
$81n/100$	$\leq (\frac{9}{10})^2 n$
⋮	

Almennt: $\leq (\frac{9}{10})^i n$

Kvótaröð því 9/10 < 1 Summa er < $\frac{1}{1-\frac{9}{10}} = 10$

Mesta hæð: $(\frac{9}{10})^i n = 1$ eða: $\log_{\frac{10}{9}} n = i$

Aðrar hópastærðir

- Er eitthvað sérstakt við töluna 5?
  - Getum við notað 3, 7, 9, ...?

- Prófum hópastærð 3:

Getum aðeins útilokað
1/3 stakanna í hvert sinn

Fáum þá rakningarvenslin: $T(n) \leq T(n/3) + T(2n/3) + O(n)$

Auðvelt að sjá að summa hvers lags er:

$$n,$$
$$\frac{n}{3} + \frac{2n}{3} = n,$$
$$\frac{n}{9} + \frac{2n}{9} + \frac{2n}{9} + \frac{4n}{9} = n,$$
$$\ldots.$$

Dýpi rakningartrésins er

$$\log_{\frac{3}{2}} n = O(\log n)$$

svo lausn rakningarvenslana er

$$T(n) \leq O(n \log n)$$

Ekki línulegur tími!

Hópastærð 7

- Stærðin 5 virkar, en stærðin 3 virkar ekki, hvað með 7?

Fáum þá rakningarvenslin: $T(n) \leq T(n/7) + T(10n/14) + O(n)$

Þá er summan á hverju lagi trésins: $\leq (\frac{6}{7})^i n$

sem er augljóslega <u>lækkandi kvótaröð</u>

Svo lausnin er $T(n) \leq O(n)$

<u>Kostir/gallar við hópastærð 7 m.v. 5</u>

- Hóparnir eru færri og því færri stök í fylkinu M. Þurfum því að finna miðgildi í *n*/7 stökum í stað *n*/5
- Á móti kemur að það er dýrara að finna miðgildi í hverjum hópi (10 samanburðir í stað 6)

Sama tímaflækja, en hærri fasti

Æfing fyrir miðgildi

- Rissið upp mynd af 77 stökum með hópastærð 7 (þá eru 11 hópar)

- Hversu mörg af þessum 77 stökum er hægt að útiloka eftir að *MoM* hefur verið fundið?

Heiltölumargföldun

- Venjuleg margföldun n-stafa heiltalna tekur $O(n^2)$ tíma

Dæmi:

```
    3141
  * 5962
---------
    6282
   18846
  28269
 15705
---------
 18726642
```

Tvöföld `for`-lykkja frá 1 til n

Grunnaðgerðir:
Eins-tölustafa aðgerðir (+ og *)

- Rússneska bændaaðferðin tekur líka $O(n^2)$ tíma

- Menn héldu lengi að það væri ekki hægt að gera betur en $O(n^2)$

Margföldun með deila-og-drottna

- Lát *X* og *Y* vera tvær *n*-stafa heiltölur
- Brjótum þær upp í tvo hluta:

$$X = a \cdot 10^{\frac{n}{2}} + b \qquad Y = c \cdot 10^{\frac{n}{2}} + d$$

Þá gildir:
$$X \cdot Y = \left(10^{\frac{n}{2}}a + b\right)\left(10^{\frac{n}{2}}c + d\right)$$
$$= 10^{n}ac + 10^{\frac{n}{2}}(bc + ad) + bd$$

Þá höfum við fjórar margfaldanir á *n*/2-stafa heiltölum
í stað tveggja margfaldanna á *n*-stafa tölum

Deild-og-drotta reiknirit

```
SplitMultiply(x, y, n):
  if n = 1
      return x · y
  else
      m ← ⌈n/2⌉
      a ← ⌊x/10^m⌋;  b ← x mod 10^m        ⟨⟨x = 10^m a + b⟩⟩
      c ← ⌊y/10^m⌋;  d ← y mod 10^m        ⟨⟨y = 10^m c + d⟩⟩
      e ← SplitMultiply(a, c, m)
      f ← SplitMultiply(b, d, m)
      g ← SplitMultiply(b, c, m)
      h ← SplitMultiply(a, d, m)
      return 10^{2m} e + 10^m (g + h) + f
```

$$X \cdot Y = 10^n ac + 10^{\frac{n}{2}}(bc + ad) + bd$$

e g h f

Rakningarvenslin eru:

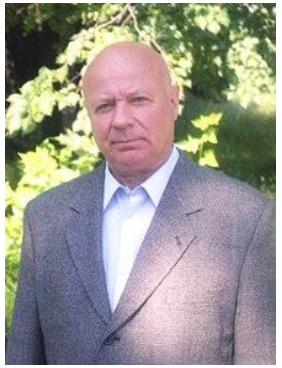
$$T(n) = 4T\left(\frac{n}{2}\right) + O(n), \qquad T(1) = 1$$

Samlagningin á liðunum

Tvær eins-stafa tölur kosta eina grunnaðgerð

Lausnin á rakningarvenslunum er $T(n) = O(n^2)$

Einföldun Karatsuba



- Árið 1960 fann Anatoly Karatsuba leið til að gera betur

Í formúlunni $10^n ac + 10^{\frac{n}{2}}(bc + ad) + bd$

þurfum við ekki að vita *bc* og *ad*, heldur bara summu þeirra!

Getum fundið gildi (*bc* + *ad*) út frá *ac*, *bd* og einni annari margföldun

$$ac + bd - (a - b)(c - d) = \cancel{ac} + \cancel{bd} - (\cancel{ac} - ad - bc + \cancel{bd}) = \underline{bc + ad}$$

Þurfum nú aðeins að framkvæma 3 margfaldanir á *n*/2-stafa tölum
ásamt 6 samlagningum (í stað 3 saml.)

Reiknirit Karatsuba

```
FastMultiply(x, y, n):
  if n = 1
      return x · y
  else
      m ← ⌈n/2⌉
      a ← ⌊x/10^m⌋;  b ← x mod 10^m        ⟨⟨x = 10^m a + b⟩⟩
      c ← ⌊y/10^m⌋;  d ← y mod 10^m        ⟨⟨y = 10^m c + d⟩⟩
      e ← FastMultiply(a, c, m)
      f ← FastMultiply(b, d, m)
      g ← FastMultiply(a − b, c − d, m)
      return 10^{2m} e + 10^m (e + f − g) + f
```

$$(bc + ad) = ac + bd - (a-b)(c-d)$$

e f g

Rakningarvensl:

$$T(n) = 3T\left(\frac{n}{2}\right) + O(n), \qquad T(1) = 1$$

Lausn fæst með rakningartré og er: $T(n) = O\left(n^{\log_2 3}\right) \approx O(n^{1.58496})$

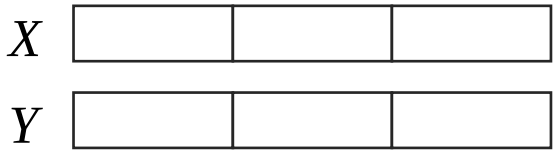
Æfing fyrir Karatsuba

- Ef X=23 og Y=45, hver eru þá gildin á a, b, c og d?
- Reiknið ($bc + ad$)
- Reiknið $ac + bd - (a - b)(c - d)$

Útvíkkun á Karatsuba

- Getum skipt tölunum *X* og *Y* upp í fleiri hluta:

Toom-3 skiptir tölunni upp í 3 hluta:



Toom-*k* skiptir tölunum upp í *k* hluta hver þeirra með *n*/*k* stafi

Toom-Cook reikniritið gerið þetta almennt.

Tími: $O(n^{1+1/(\log k)})$

Bein endurkvæmni gæfi 9 margfaldanir á n/3-stafa tölum. En Andrei Toom náði að fækka þeim niður í 5

$$T(n) = 5T\left(\frac{n}{3}\right) + O(n)$$

Lausn: $T(n) = O\left(n^{\log_3 5}\right) = O(n^{1.465\ldots})$

Með hærri fasta

Lengi vel var besta reikniritið eftir Schönhage og Strassen:

Tími: $O(n \log n \log\log n)$

Aðeins hagkvæmur fyrir tölur með fleiri en 40.000 stafi

Staðan í dag

- Árið 2019 birtu David Harvey og Joris van der Hoeven reiknirit fyrir heiltölumargföldun með tímaflækjuna $O(n \log n)$ (pdf)
  - Þetta reiknirit notar hraðavirka Fourier vörpun (*Fast Fourier Transform*, *FFT*)
  - Reiknirit Schönhage og Strassen gerir það líka

Talið að þetta sé það besta sem er mögulegt

- Aðeins fræðilega séð besta reikniritið
  - Aðeins best fyrir heiltölur með fjölda bita sem er $2^{1729^{12}}$

Þetta er tala sem hefur ~10^{38} tugastafi

Til samanburðar:
Fjöldi atóma í hinum þekkta alheimi er um 2^{270}

GMP (*The GNU Multiple Precision Arithmetic Library*) inniheldur mörg af þessum reikniritum og skiptir á milli þeirra eftir stærð heiltalnanna

Þröskuldar í GMP:
- Karatsuba um 400 tölustafir
- Schönhage-Strassen um 40.000 stafir

Veldishafning

- Gefin tala a og jákvæð heiltala n, viljum reikna a^n
- Augljósa aðferðin er að framkvæma $n-1$ margföldun með a:

```
SlowPower(a, n):
    x ← a
    for i ← 2 to n
        x ← x · a
    return x
```

Hvað er grunnaðgerðin hér?

Inntakið *a* getur verið af ýmsu tagi:

- Heiltala
- Fleytitala
- Fylki
- ...

Þar sem við vitum ekki hvers konar hluti við erum að margfalda verðum við að nota fjölda margfaldana sem grunnaðgerð

Getum svo stungið inn réttu gildi fyrir mismunandi tög

Hraðvirkari veldishafning - Pingala

- Notum deila-og-drottna aðferð:

```
PiṅgalaPower(a, n):
  if n = 1
      return a
  else
      x ← PiṅgalaPower(a, ⌊n/2⌋)
      if n is even
          return x · x
      else
          return x · x · a
```

Kennt við Acharya Pingala, indverskan stærðfræðing frá 3ju öld f.Kr.

Byggir á endurkvæmu formúlunni:

$$a^n = \begin{cases} 1 & \text{ef } n = 0 \\ (a^{n/2})^2 & \text{ef } n > 0 \text{ og } n \text{ jöfn tala} \\ (a^{\lfloor n/2 \rfloor})^2 \cdot a & \text{annars} \end{cases}$$

Hér er vinnan framkvæmd á leiðinni upp endurkvæmnina

Rakningarvenslin: $T(n) \leq T\left(\frac{n}{2}\right) + 2$ ← Geta verið 2 margfaldanir í hvert sinn

Lausn: $T(n) = O(\log n)$

Hraðvirkari veldishafning - Bændaaðferð

- Hægt að aðlaga Bændaaðferðina þannig að hún reikni veldi í stað margföldunar
  - Þá er formúlan:

$$a^n = \begin{cases} 1 & \text{ef } n = 0 \\ (a^2)^{n/2} & \text{ef } n > 0 \text{ og } n \text{ jöfn tala} \\ (a^2)^{\lfloor n/2 \rfloor} \cdot a & \text{annars} \end{cases}$$

```
PeasantPower(a, n):
  if n = 1
      return a
  else if n is even
      return PeasantPower(a^2, n/2)
  else
      return PeasantPower(a^2, ⌊n/2⌋) · a
```

Hér er vinnan að mestu framkvæmd á leiðinni niður endurkvæmnina

(þ.e. útreikningur á a^2)

Tími: $T(n) = O(\log n)$

Neðri mörk veldishafningar

- Sérhvert reiknirit til að finna a^n verður að nota $\Omega(\log n)$ margfaldanir
  - Því hver margföldun getur mest tvöfaldað núverandi gildi

- Bæði þessi reiknirit eru því með bestu mögulegu tímaflækju (*optimal*)
- Þegar *n* er heilt veldi af 2 þá framkvæma bæði reikniritin nákvæmlega $\log_2 n$ margfaldanir
- En það eru tilvik þar sem þessi reiknirit ná ekki alveg lægsta fjölda margfaldana

Fyrirlestraæfingar

1. Leysið mismunajöfnuna $T(n) = 3T(n/3) + n$ með rakningartré.
2. Reiknið 42*36 með reikniriti Karatsuba. Þá er a=4, b=2, c=3 og d=6. Það verður engin endurkvæmni í svona stuttum tölum.
3. Hvernig er hægt að beita Karatsuba reikniritinu á tölur sem hafa ekki sama fjölda tölustafa?