Stærðfræðimynstur í tölvunarfræði

Vika 7

Kafli 4: Afgangurinn af dulritun
Kafli 5: Þrepasannanir og endurkvæmni

Diffie-Hellman lyklaskipti (key exchange protocol)

- Bæði Adda (eða Alice) og Bobbi (eða Bob) og (allir aðrir) eru sammála um að nota tiltekna risastóra prímtölu p og tiltekna frumstæða rót a mátað við p
- Adda býr til risastóra leynilega slembitölu k_1 og sendir $a^{k_1}\ mod\ p$ til Bobba gegnum opinbera samskiptarás
- Bobbi býr til risastóra leynilega slembitölu k_2 og sendir $a^{k_2}\ mod\ p$ til Öddu gegnum opinbera samskiptarás
- Adda reiknar töluna $\left(a^{k_2}\ mod\ p\right)^{k_1}\ mod\ p \equiv a^{k_1 \cdot k_2}\ (mod\ p)$
- Bobbi reiknar töluna $\left(a^{k_1}\ mod\ p\right)^{k_2}\ mod\ p \equiv a^{k_1 \cdot k_2}\ (mod\ p)$
- Þetta er sama talan og Adda og Bobbi geta notað hana sem sameiginlegan dulritunarlykil fyrir samskipti gegnum opinberu samskiptarásina, en enginn annar getur á auðveldan hátt reiknað lykilinn, jafnvel þótt hann hafi hlerað öll samskipti Öddu og Bobba
- Ef einhverjum tekst að finna aðferð til að reikna stakrænan logra á hraðvirkan hátt þá verður þessi aðferð ótraust

Dreifilyklakerfi

- RSA öryggiskerfi og fleiri (DSA, ElGamal) nota tvo lykla, lyklapör
- Dreifilykill (public key) er opinber og skal vera öllum aðgengilegur
- Einkalykill (private key) er leyndarmál og hver aðili á að halda sínum einkalykli leyndum
- Dreifilykill er notaður til að dulrita skeyti til aðila sem hefur samsvarandi einkalykil
- Einkalykill er notaður til að ráða dulrituð skeyti frá hverjum sem er
- Einkalykill er notaður til að undirrita (auðkenna) skeyti frá þeim sem á þann einkalykil
- Dreifilykill er notaður til að staðfesta undirritun skeyta frá aðila með samsvarandi einkalykil

Bálkadulritunarkerfi (block cipher) og útdráttarkerfi (message digest)

- Kerfi eins og Diffie-Helman, RSA, DSA, ElGamal, eru ekki notuð beint til að dulrita heil skeyti eða undirrita heil skeyti
- Bálkadulritunarkerfi eru mun fljótari að dulrita og ráða stór skeyti, þau nota sama lykil til að dulrita og til að ráða
  - AES, DES, IDEA, RC5, og mörg mörg fleiri
  - Dæmi: Sendum móttakandanum skeyti dulritað með AES ásamt AES lykli dulrituðum með RSA dreifilykli
- Útdráttarkerfi geta á fljótvirkan hátt reiknað útdrátt úr stóru skeyti sem hefur þann eiginleika að næstum ómögulegt er að finna annað skeyti sem hefur sama útdrátt
  - SHA-1, SHA-2, SHA-3, SHA-256, MD5, MD6 og mörg fleiri
  - Dæmi: Sendum móttakandanum skeyti ásamt SHA-256 útdrætti úr skeytinu, undirrituðum með RSA einkalykli
- Allt þetta er að gerast í sífellu í samskiptum okkar yfir Internetið

Þrepasannanir (induction) og endurkvæmni (recursion)

- Þrepasönnun (induction)
- Sterk þrepasönnun (strong induction)
- Velröðun (well-ordering)
- Endurkvæmar skilgreiningar (recursive definitions)
- Endurkvæm algrím (recursive algorithms)
- Rökstuðningur endurkvæmra algríma (program correctness)

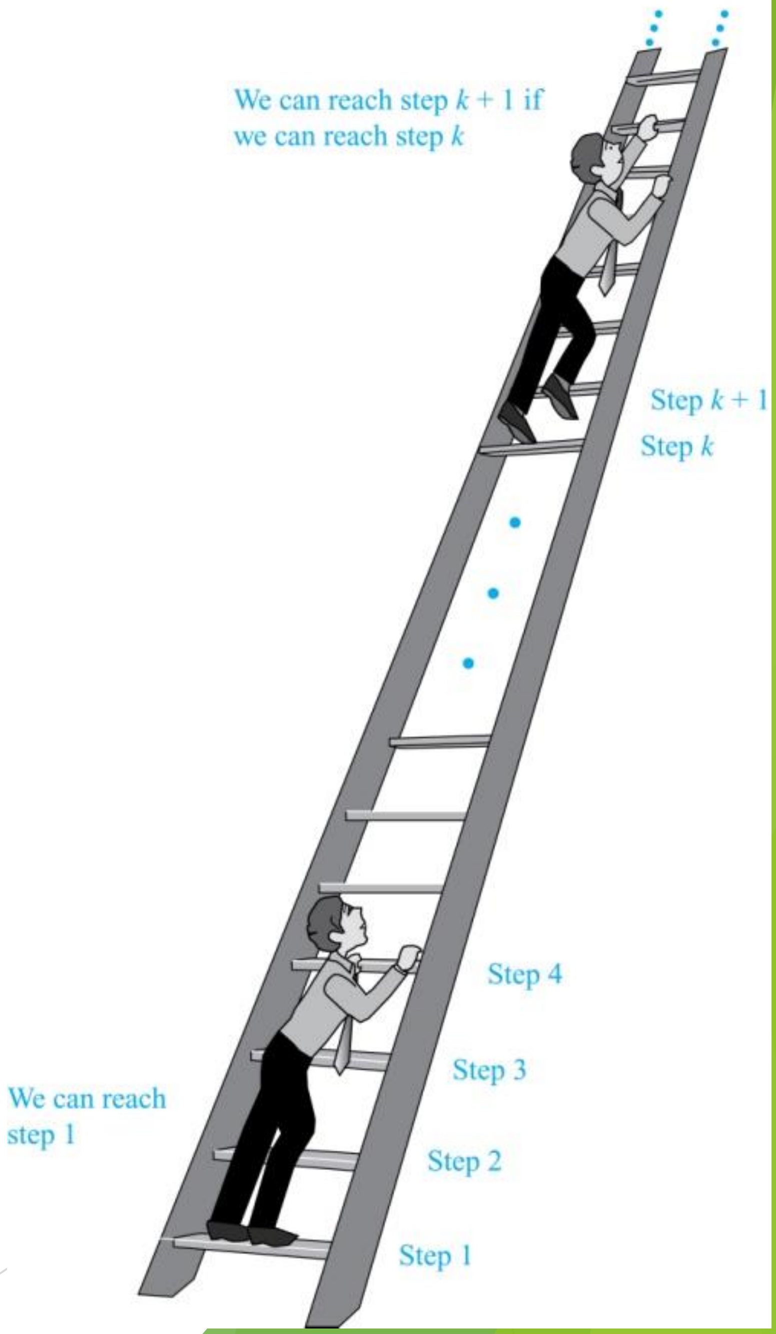
Þrepasönnun

- Skilgreining þrepasönnunar
- Dæmi um þrepasannanir
- Villur í þrepasönnnunum
- Uppsetning þrepasannana

Klifrað upp óendanlegan stiga

- Ef við höfum óendanlega háan stiga og
  1. Við komumst í fyrsta þrep stigans
  2. Ef við komumst í tiltekið þrep stigans komumst við í næsta þrep
- Þá komumst við í hvaða þrep stigans sem er

- Þetta er grunnhugmyndin í þrepasönnun



Reglan um (einfalda) þrepasönnun

- Til að sanna fyrir umsögn P að $P(n)$ gildi fyrir allar jákvæðar heiltölur dugar að sanna eftirfarandi
  - **Grunnur:** Sönnum að $P(1)$ gildi
  - **Þrepun:** Sönnum að $P(k) \to P(k+1)$ gildi fyrir allar jákvæðar heiltölur k
- Í **þrepun**inni gerum við ráð fyrir að $P(k)$ gildi (sé satt) fyrir ótiltekna heiltölu k og sönnum að $P(k+1)$ sé satt
- $P(k)$ er **þrepunarforsendan**, að sanna $P(k) \to P(k+1)$ er **þrepunarskrefið**

- Í óendanlega stiganum:
  - **Grunnur:** Við komumst í fyrsta þrep stigans, þ.e. þrep 1 í stiganum
  - **Þrepun:** Ef við komumst í þrep k í stiganum þá komumst við í þrep $k+1$
- Þar með komumst við í hvaða þrep sem er í stiganum

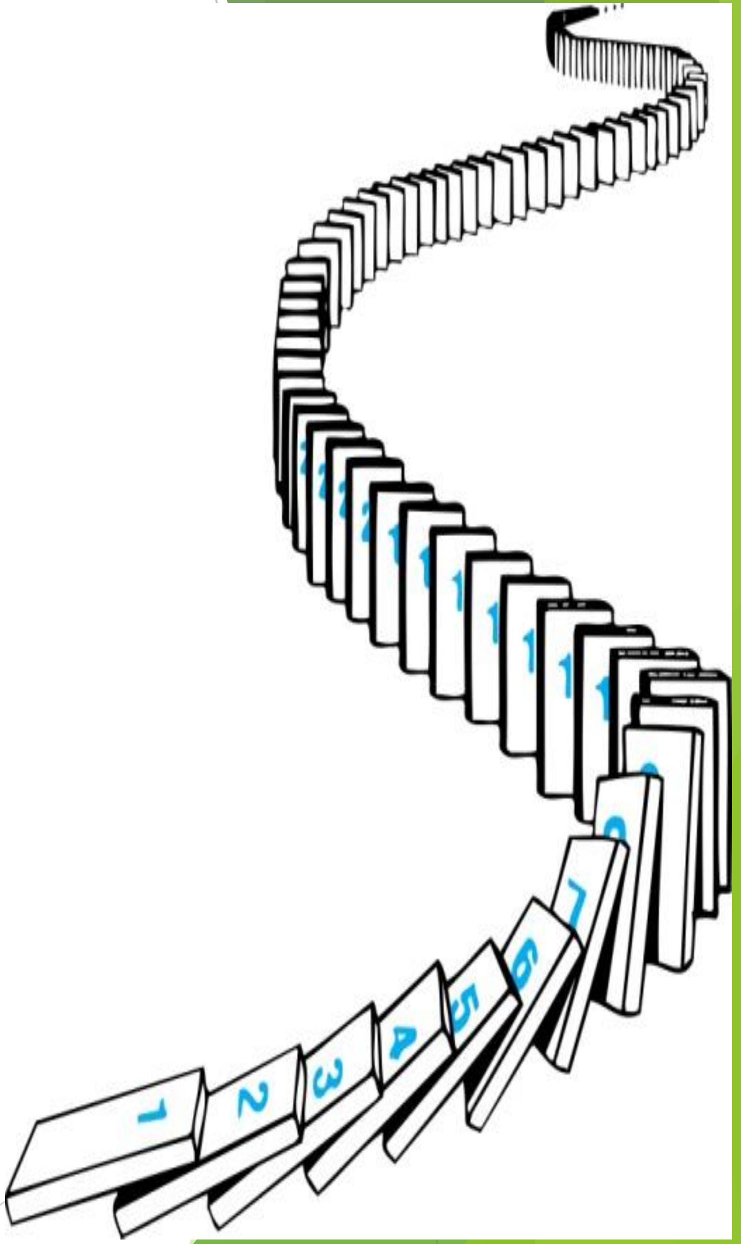
Nokkur mikilvæg atriði

- Grunnregluna um þrepun má skrifa sem röksemdareglu sem gildir fyrir allar umsagnir P:

$$\big(P(1) \land \forall k: (P(k) \to P(k+1))\big) \to \forall n: P(n)$$

þar sem óðal P er mengi jákvæðra heiltalna

- Í þrepuninni er forsendan ekki að $P(k)$ gildi fyrir allar jákvæðar heiltölur, við gerum ráð fyrir að $P(k)$ sé satt og sönnum að þá sé $P(k+1)$ satt
- Þrepunarsannanir byrja ekki alltaf á heiltölunni 1, við getum í staðinn byrjað í heiltölu b og sannað þá að eitthvað gildi fyrir allar heiltölur $\geq b$



Sönnun summuformúlu með þrepun

- **Dæmi:** Sönnum að
$$\sum_{i=1}^{n} i = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$
- **Lausn:** Skilgreinum umsögnina $P(n)$ sem jöfnuna að ofan og notum þrepunarsönnun:
  - **Grunnur:** $P(1)$ gildir vegna þess að fyrir $n = 1$ gildir $\sum_{i=1}^{n} i = \sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2} = \frac{n(n+1)}{2}$
  - **Þrepun:**
    - **Þrepunarforsenda:** Gerum ráð fyrir að $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$
    - **Þrepunarskref:** Viljum sanna að $\sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2}$.

Sönnun summuformúlu með þrepun

- Dæmi: Sönnum að

$$\sum_{i=1}^{n} i = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

- Lausn: Skilgreinum umsögnina $P(n)$ sem jöfnuna að ofan og notum þrepunarsönnun:
  - **Grunnur:** $P(1)$ gildir vegna þess að fyrir $n = 1$ gildir $\sum_{i=1}^{n} i = \sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2} = \frac{n(n+1)}{2}$
  - **Þrepun:**

Samkæmt þrepunarforsendu

- **Þrepunarforsenda:** Gerum ráð fyrir að $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$
- **Þrepunarskref:** Viljum sanna að $\sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2}$.

$\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n^2+n+2n+2}{2} = \frac{n^2+3n+2}{2} = \frac{(n+1)(n+2)}{2}$ sem er það sem sanna þurfti.

Sönnum summuformúluna með rökstuddri forritun

$\{\ n \geq 0\ \}$

Framkvæmanlegur og rökstuddur forritskafli þar sem n breytist ekki, en s fær gildi

$\{\ s = 1 + 2 + \cdots + n\ \}$
$\{\ s = n(n+1)/2\ \}$

- Hér sönnum við formúluna fyrir $n \geq 0$, ekki aðeins $n \geq 1$, en það er aukaatriði
- Jafngildir þrepasönnun **aðeins ef stöðvun forritskaflans er einnig sönnuð**
- Annars verður þetta svipað og þrepasönnun án þrepunarskrefs, sem sannar ekki formúluna

Sönnum summuformúluna með rökstuddri forritun

$\{\ n \geq 0\ \}$

Frumstilla s og k

meðan $k \neq n$

$\{\ 0 \leq k \leq n\ \}$

$\{\ s = 1 + 2 + \cdots + k\ \}$

$\{\ s = k(k+1)/2\ \}$

Viðhalda fastayrðingu lykkju

$\{\ s = 1 + 2 + \cdots + n\ \}$

$\{\ s = n(n+1)/2\ \}$

- Hér sönnum við formúluna fyrir $n \geq 0$, ekki aðeins $n \geq 1$, en það er aukaatriði
- Jafngildir þrepasönnun **aðeins ef stöðvun forritskaflans er einnig sönnuð**
- Annars verður þetta svipað og þrepasönnun án þrepunarskrefs, sem sannar ekki formúluna

Sönnum summuformúluna með rökstuddri forritun

$\{ n \geq 0 \}$
$k \coloneqq 0$
$s \coloneqq 0$
meðan $k \neq n$
    $\{ 0 \leq k \leq n \}$
    $\{ s = 1 + 2 + \cdots + k \}$
    $\{ s = k(k+1)/2 \}$
    $k \coloneqq \mathrm{k} + 1$
    $s \coloneqq s + k$
$\{ s = 1 + 2 + \cdots + n \}$
$\{ s = n(n+1)/2 \}$

- Hér sönnum við formúluna fyrir $n \geq 0$, ekki aðeins $n \geq 1$, en það er aukaatriði
- Jafngildir þrepasönnun **aðeins ef stöðvun forritskaflans er einnig sönnuð**
- Annars verður þetta svipað og þrepasönnun án þrepunarskrefs, sem sannar ekki formúluna

Sönnum summuformúluna með rökstuddri forritun

$\{\ n \geq 0\ \}$
$k := 0$
$s := 0$
meðan $k \neq n$
    $\{\ 0 \leq k \leq n\ \}$
    $\{\ s = 1 + 2 + \cdots + k\ \}$
    $\{\ s = k(k+1)/2\ \}$
    $k := \mathrm{k} + 1$
    $s := s + k$
$\{\ s = 1 + 2 + \cdots + n\ \}$
$\{\ s = n(n+1)/2\ \}$

- Hér sönnum við formúluna fyrir $n \geq 0$, ekki aðeins $n \geq 1$, en það er aukaatriði
- Jafngildir þrepasönnun **aðeins ef stöðvun forritskaflans er einnig sönnuð**
- Annars verður þetta svipað og þrepasönnun án þrepunarskrefs, sem sannar ekki formúluna
- Í þessu tilviki er stöðvun augljós: Við munum fara nákvæmlega n umferðir um lykkjuna
- Gildi formúlunnar $n - k$ er í upphafi n og minnkar í hverri umferð um 1 og getur ekki orðið minna en 0 því þá stöðvast lykkjan

Rök forritskaflans

- Munum að forritskafli:
  $\{ F \}$
  meðan C
  $\quad \{ I \}$
  $\quad$ S
  $\{ E \}$
- þarf að uppfylla eftirfarandi:

1. $F \rightarrow I$
2. $\{C \wedge I\}\mathrm{S}\{I\}$
3. $I \wedge \neg C \rightarrow E$

- Augljóst er að reglur 1 og 3 eru uppfylltar
- Regla 2 er einnig uppfyllt því ef við látum k' og s' standa fyrir gildin í breytunum k og s eftir einhverja almenna umferð lykkjunnar þá fáum við $k' = k + 1$ og við fáum

$$\begin{aligned} s' &= s + k' \\ &= 1 + 2 + \cdots + k + k' \\ &= 1 + 2 + \cdots + k + (k + 1) \\ &= 1 + 2 + \cdots + k' \end{aligned}$$

og við fáum einnig

$$\begin{aligned} s' &= s + k' \\ &= k(k + 1)/2 + k' \\ &= (k^2 + k)/2 + (k + 1) \\ &= (k^2 + 3k + 2)/2 \\ &= (k + 1)(k + 2)/2 \\ &= k'(k' + 1)/2 \end{aligned}$$

sem er það sem sanna þarf, svo fastayrðingunni sé viðhaldið (auk $0 \leq k' \leq n$, sem er augljóst)

Giskum á og sönnum summuformúlu

- Hver er formúla fyrir $1 + 3 + 5 + \cdots + (2n - 1)$?
- Svar: Við sjáum að $1 = 1,\ 1 + 3 = 4,\ 1 + 3 + 5 = 9,\ 1 + 3 + 5 + 7 = 16,\ 1 + 3 + 5 + 7 + 9 = 25$
- Giskum á að $1 + 3 + 5 + \cdots + (2n - 1) = n^2$
- Sönnum það með þrepum. Skilgreinum að umsögnin $P(n)$ hafi merkinguna
$$1 + 3 + 5 + \cdots + (2n - 1) = n^2$$
- **Setning:** $P(n)$ gildir fyrir $n = 1,2,\ldots$
- **Þrepasönnun:**
  - **Grunnur:** $P(1)$ gildir því $1 = 1^2$
  - **Þrepun:**
    - **Þrepunarforsenda:** Gerum ráð fyrir að $P(n)$ gildi
    - **Þrepunarskref:** Viljum sanna að $P(n + 1)$ gildi. Við fáum $1 + 3 + \cdots + (2(n +$

Sönnun á ójöfnum

- **Dæmi:** Notum þrepun til að sanna að $n < 2^n$ fyrir allar jákvæðar heiltölur n
- **Lausn:** Látum $P(n)$ tákna $n < 2^n$
- **Setning:** $P(n)$, þ.e. $n < 2^n$, gildir fyrir allar jákvæðar heiltölur n
- **Þrepasönnun:**
  - **Grunnur:** $P(1)$ gildir vegna þess að $1 < 2 = 2^1$
  - **Þrepun:**
    - **Þrepunarforsenda:** Gerum ráð fyrir að $P(n)$, þ.e. $n < 2^n$, gildi
    - **Þrepunarskref:** Viljum sanna að $n + 1 < 2^{n+1}$. Samkvæmt þrepunarforsendu höfum við $n < 2^n$, þar með fæst $n + 1 < 2^n + 1 \leq 2^n + 2^n = 2^{n+1}$ sem er það sem sanna þurfti

Sönnun á ójöfnum – annað dæmi

- **Dæmi:** Notum þrepun til að sanna að $2^n < n!$ fyrir allar jákvæðar heiltölur $n \geq 4$
- **Lausn:** Látum $P(n)$ tákna $2^n < n!$
- **Setning:** $P(n)$, þ.e. $2^n < n!$, gildir fyrir allar jákvæðar heiltölur $n \geq 4$
- **Þrepasönnun:**
  - **Grunnur:** $P(4)$ gildir vegna þess að $2^4 = 16 < 24 = 4!$
  - **Þrepun:**
    - **Þrepunarforsenda:** Gerum ráð fyrir að $P(n)$, þ.e. $2^n < n!$, gildi
    - **Þrepunarskref:** Viljum sanna að $2^{n+1} < (n+1)!$. Samkvæmt þrepunarforsendu höfum við $2^n < n!$, þar með fæst $2^{\mathrm{n}+1} = 2 \cdot 2^n < 2 \cdot n! < (n+1) \cdot n! = (n+1)!$ sem er það sem sanna þurfti

Takið eftir að grunnurinn er $P(4)$ því $P(0), P(1), P(2)$ og $P(3)$ eru ósannar fullyrðingar

Sönnun á deilanleika

- **Dæmi:** Notum þrepun til að sanna að $n^3 - n$ er deilanlegt með 3 fyrir sérhverja jákvæða heiltölu n
- **Þrepasönnun:** Látum $P(n)$ tákna fullyrðinguna „$n^3 - n$ er deilanlegt með 3“. Við munum sanna með þrepun að $P(n)$ gildir fyrir $n = 1,2,3,\ldots$
- **Grunnur:** Fyrir $n = 1$ fáum við $n^3 - n = 1 - 1 = 0$, sem er deilanlegt með 3
- **Þrepun:**
  - **Þrepunarforsenda:** Gerum ráð fyrir að $n^3 - n$ sé deilanlegt með 3, viljum sanna að $(n+1)^3 - (n+1)$ sé deilanlegt með 3
  - **Þrepunarskref:** Við fáum $(n+1)^3 - (n+1) = (n^3 + 3n^2 + 3n + 1) - (n+1) = (n^3 - n) + (3n^2 + 3n) = (n^3 - n) + 3 \cdot (n^2 + n)$. Samkvæmt þrepunarforsendu er fyrri liðurinn, $(n^3 - n)$, deilanlegur með 3. Seinni liðurinn er margfeldi af 3 og er því deilanlegur með 3. Því er summan deilanleg með 3, sem er það sem sanna þurfti

Fjöldi undirmengja endanlegs mengis

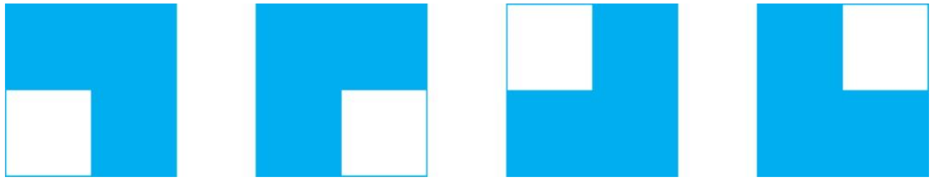
- **Setning:** Mengi S með n stök hefur 2^n mismunandi undirmengi.
- **Þrepasönnun:** Látum $P(n)$ tákna fullyrðinguna „ Mengi S með n stök hefur 2^n mismunandi undirmengi“. Við munum sanna að $P(n)$ gildir fyrir $n = 0,1,2,\ldots$
- **Grunnur:** Mengi með 0 stök er tómamengið og það hefur aðeins eitt mengi, tómamengið sjálft sem undirmengi. $P(0)$ er því satt.
- **Þrepun:**
  - **Þrepunarforsenda:** Gerum ráð fyrir að mengi með n stök hafi 2^n undirmengi. Viljum sanna að mengi með $n + 1$ stak hafi 2^{n+1} undirmengi.
  - **Þrepunarskref:** Látum T vera mengi með $n + 1$ stak. Þá má skrifa $T = S \cup \{a\}$ fyrir eitthvert stak $a \in T$, þar sem S er mengi með n stök. Sérhvert undirmengi T annaðhvort inniheldur a eða ekki. Fyrir sérhvert undirmengi U sem inniheldur a er eitt og aðeins eitt undirmengi $U - \{a\}$ sem inniheldur ekki a. Fjöldi undirmengja sem innihalda a er því sá sami og fjöldinn sem innihalda ekki a. En öll undirmengi sem innihalda ekki a eru einnig undirmengi S. Heildarfjöldi undirmengja T er því tvöfaldur fjöldi undirmengja S, þ.e. $2 \cdot 2^n = 2^{n+1}$, sem er það sem sanna þurfti

Þakning skákborða

- Eftirfarandi myndir sýna þríferning (triomino) í tveimur mismunandi stellingum

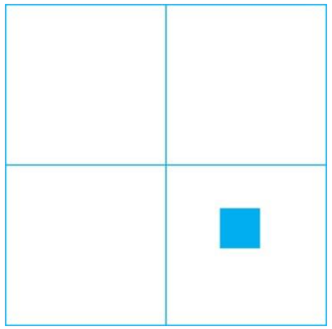
- Við gerum ráð fyrir að þríferningurinn þekji nákvæmlega þrjá reiti á skákborði

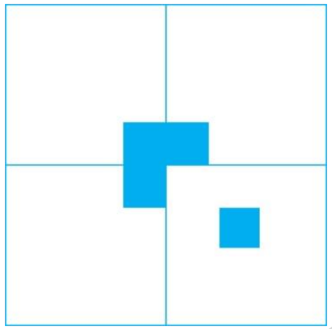
- **Setning:** Fyrir $n = 1,2,\ldots$ gildir að sérhvert skákborð af stærð $2^n \times 2^n$, þar sem búið er að fjarlægja einhvern einn reit, er hægt að þekja með þríferningum
- Við munum sanna þetta með þrepun á n
- **Grunnur:** Myndirnar að neðan sýna alla möguleika á skákborði af stærð $2^1 \times 2^1$ með einn reit fjarlægðan, ásamt samsvarandi þakningu



Þakning skákborða

- **Þrepun:**
  - **Þrepunarforsenda:** Gerum ráð fyrir að hægt sé að þekja sérhvert skákborð af stærð $2^n \times 2^n$, þar sem búið er að fjarlægja einhvern einn reit. Viljum sanna að hægt sé að þekja sérhvert skákborð af stærð $2^{n+1} \times 2^{n+1}$, þar sem búið er að fjarlægja einhvern einn reit
  - **Þrepunarskref:** Íhugum almennt skákborð af stærð $2^{n+1} \times 2^{n+1}$, þar sem búið er að fjarlægja einhvern einn reit. Það er samsett úr fjórum skákborðum af stærð $2^n \times 2^n$ og úr einu þeirra er búið að fjarlægja einn reit. Fjarlægjum einnig einn reit úr hinum þremur eins og seinni myndin sýnir. Við getum þá, samkvæmt þrepunarforsendu, þakið alla reiti sem ekki hafa verið fjarlægðir. Síðan bætum við þríferningi í miðjuna og þá er aðeins þessi eini reitur óþakinn, sem er það ástand sem við þurftum að ná fram.





Dæmi um ranga þrepasönnun

- Látum $P(n)$ tákna fullyrðinguna „sérhverjar n línur í fletinum sem engar tvær eru samsíða mætast í einum skurðpunkti
- **„Setning:“** $P(n)$ er satt fyrir $n = 2,3,\ldots$
- **Þrepasönnun:**
- **Grunnur:** $P(2)$ er satt þar eð tvær línur sem ekki eru samsíða skerast í einum punkti
- **Þrepun:**
  - **Þrepunarforsenda:** Gerum ráð fyrir að sérhverjar n línur sem ekki eru samsíða skerist í einum punkti, viljum sanna að sama gildi fyrir $n + 1$ línu
  - **Þrepunarskref:** Ef við höfum $n + 1$ línu, $L_1, L_2, \ldots, L_{n+1}$ vitum við samkvæmt þrepunarforsendu að $L_1, L_2, \ldots, L_n$ skerast í einum punkti. Við vitum líka, aftur samkvæmt þrepunarforsendu, að $L_2, L_3, \ldots, L_{n+1}$ skerast í einum punkti. Þessir tveir punktar hljóta að vera sami punkturinn því tveir punktar skilgreina eina línu og allar línurnar væru sama línan ef svo væri ekki. Því hljóta allar línurnar að skerast í einum og sama punkti.

Dæmi um ranga þrepasönnun

- Látum $P(n)$ tákna fullyrðinguna „sérhverjar n línur í fletinum sem engar tvær eru samsíða mætast í einum skurðpunkti
- **„Setning:“** $P(n)$ er satt fyrir $n = 2,3,\dots$
- **Þrepasönnun:**
- **Grunnur:** $P(2)$ er satt þar eð tvær línur sem ekki eru samsíða skerast í einum punkti
- **Þrepun:**
  - **Þrepunarforsenda:** Gerum ráð fyrir að sérhverjar n línur sem ekki eru samsíða skerist í einum punkti, viljum sanna að sama gildi fyrir $n+1$ línu
  - **Þrepunarskref:** Ef við höfum $n+1$ línu, $L_1, L_2, \dots, L_{n+1}$ vitum við samkvæmt þrepunarforsendu að $L_1, L_2, \dots, L_n$ skerast í einum punkti. Við vitum líka, aftur samkvæmt þrepunarforsendu, að $L_2, L_3, \dots, L_{n+1}$ skerast í einum punkti. Þessir tveir punktar hljóta að vera sami punkturinn því tveir punktar skilgreina eina línu og allar línurnar væru sama línan ef svo væri ekki. Því hljóta allar línurnar að skerast í einum og sama punkti.

Þessi rök virka ekki fyrir $n = 2$ því þá er aðeins ein lína fyrir $L_1, L_2, \dots, L_n$ og ein (önnur) lína fyrir $L_2, l_3, \dots, L_{n+1}$ og þess vegna er $P(2) \to P(3)$ rangt og þrepunin virkar ekki.

Allar línurnar eru sama línan fyrir $n = 2$ þar eð þá er aðeins ein lína. Það er ekki í neinni mótsögn við forsendurnar að engar tvær línur séu samsíða.

Ráðlögð uppsetning þrepasönnunar

- Notið svipað mynstur og eftirfarandi fyrir (einfalda) þrepasönnun:

  Setning: Fyrir öll $n \geq b$ gildir $P(n)$
  Þrepasönnun:
  Grunnur: $P(b)$ gildir vegna þess að …
  Þrepun:
  Þrepunarforsenda: Gerum ráð fyrir að $P(n)$ gildi fyrir eitthvert $\mathrm{n} \geq b$, viljum sanna $P(n+1)$
  Þrepunarskref: …, sem sannar að $P(n+1)$ gildir

Sterk þrepun og velröðun

- Sterk þrepun (strong induction)
- Dæmi um sterka þrepun
- Velröðun (well-ordering)

Sterk þrepun

- **Sterk þrepun:** Notum eftirfarandi skref til að sanna að $P(n)$ sé satt fyrir allar jákvæðar heiltölur n, þar sem P er umsögn um heiltölur
  - **Grunnur:** Staðfestum (sönnum) að $P(1)$ sé satt
  - **Þrepun:** Sönnum að yrðingin
    $$[P(1) \land P(2) \land \cdots \land P(n)] \rightarrow P(n+1)$$
    gildi fyrir allar jákvæðar heiltölur n

Prímþáttunarsetningin (helmingur hennar)

- **Setning:** Sérhverja heiltölu $n > 1$ má rita sem margfeldi einnar eða fleiri prímtalna
- **Þrepasönnun:**
  - **Grunnur:** Fyrir $n = 2$ gildir setningin því 2 er prímtala
  - **Þrepun:**
    - **Þrepunarforsenda:** Gerum ráð fyrir að fyrir eitthvert $n \geq 2$ sé hægt að rita sérhverja heiltölu k þannig að $1 < k \leq n$ sem margfeldi prímtalna. Viljum sanna að hægt sé að rita $n + 1$ sem margfeldi prímtalna
    - **Þrepunarskref:** Annað hvort er $n + 1$ prímtala eða ekki. Ef $n + 1$ er prímtala þá er niðurstaðan komin því $n + 1$ er þá margfeldi einnar prímtölu, þ.e. $n + 1$. Ef $n + 1$ er ekki prímtala, þá er $n + 1$ samkvæmt skilgreiningu samsett tala, þ.e. $n + 1 = a \cdot b$ þar sem a og b eru jákvæðar heiltölur, báðar > 0. Bæði a og b eru þá minni en $n + 1$. Samkvæmt þrepunarforsendu er því hægt að rita bæði a og b sem margfeldi prímtalna og því má rita $n + 1$ sem margfeldi þeirra sömu prímtalna.

Hér sjáum við að þetta er sterk þrepun

Frímerki með sterkri þrepun

- **Dæmi:** Ef við höfum nægilegan fjölda af 4 króna frímerkjum og 5 króna frímerkjum getum fengið hvaða heiltöluupphæð sem er, 12 króna eða hærri
- **Lausn:** Látum $P(n)$ þýða „við getum fengið upphæðina n sem línulegu samantektina $n = 4a + 5b$ þar sem a, b eru heiltölur, $a, b \geq 0$.
- **Setning:** Fyrir sérhverja heiltölu $n \geq 12$ gildir $P(n)$
- **Þrepasönnun:**
  - **Grunnur:** $P(12)$ er satt því $12 = 4 \cdot 3 + 5 \cdot 0$, $P(13)$ er satt því $13 = 4 \cdot 2 + 5 \cdot 1$, $P(14)$ er satt því $14 = 4 \cdot 1 + 5 \cdot 2$, $P(15)$ er satt því $15 = 4 \cdot 0 + 5 \cdot 3$.
  - **Þrepun:**
    - **Þrepunarforsenda:** Gerum ráð fyrir að $P(k)$ sé satt fyrir öll k þannig að $12 \leq k \leq n$, þar sem $n \geq 15$. Viljum sanna að $P(n+1)$ sé satt.
    - **Þrepunarskref:** Þar eð $n \geq 15$ er ljóst að $12 \leq n - 3 \leq n$, því fáum við að $P(n-3)$ er satt samkvæmt þrepunarforsendu. Þar með eru til a og b þannig að $n - 3 = 4a + 5b$. Leggjum 4 við báðu megin og fáum $n + 1 = 4(a+1) + 5b$. Við sjáum því að $n + 1$ má skrifa sem línulega samantekt eins og sanna þurfti.

Hér sjáum við að þetta er sterk þrepun

Frímerki með sterkri þrepun

- **Dæmi:** Ef við höfum nægilegan fjölda af 4 króna frímerkjum og 5 króna frímerkjum getum fengið hvaða heiltöluupphæð sem er, 12 króna eða hærri
- **Lausn:** Látum $P(n)$ þýða „við getum fengið heiltöluna (upphæðina) n sem línulegu samantektina $n = 4a + 5b$ þar sem a, b eru heiltölur, $a, b \geq 0$.
- **Setning:** Fyrir sérhverja heiltölu $n \geq 12$ gildir $P(n)$
- **Þrepasönnun:**
  - **Grunnur:** $P(12)$ er satt því $12 = 4 \cdot 3 + 5 \cdot 0$, $P(13)$ er satt því $13 = 4 \cdot 2 + 5 \cdot 1$, $P(14)$ er satt því $14 = 4 \cdot 1 + 5 \cdot 2$, $P(15)$ er satt því $15 = 4 \cdot 0 + 5 \cdot 3$.
  - **Þrepun:**
    - **Þrepunarforsenda:** Gerum ráð fyrir að $P(k)$ sé satt fyrir öll k þannig að $12 \leq k < n$, þar sem $n \geq 16$. Viljum sanna að $P(n)$ sé satt.
    - **Þrepunarskref:** Þar eð $n \geq 16$ er ljóst að $12 \leq n - 4 \leq n$, því fáum við að $P(n-4)$ er satt samkvæmt þrepunarforsendu. Þar með eru til a og b þannig að $n - 4 = 4a + 5b$. Leggjum 4 við báðu megin og fáum $n = 4(a+1) + 5b$. Við sjáum því að n má skrifa sem línulega samantekt eins og sanna þurfti.

Hér sjáum við að þetta er sterk þrepun

Frímerki með endurkvæmu stefi

{
Notkun: (a, b) := frímerki(n);
Fyrir: n er heiltala, $n \geq 12$
Eftir: $a \geq 0$ og $b \geq 0$ eru heiltölur
þannig að $4a + 5b = n$
}

stef frímerki(n: heiltala)
  ef $n = 12$ **þá skila** $(3,0)$
  ef $n = 13$ **þá skila** $(2,1)$
  ef $n = 14$ **þá skila** $(1,2)$
  ef $n = 15$ **þá skila** $(0,3)$
  (a, b) := frímerki($n - 4$)
  skila $(a + 1, b)$

Frímerki með endurkvæmu stefi

{
Notkun: (a, b) := frímerki(n);
Fyrir: n er heiltala, $n \geq 12$
Eftir: $a \geq 0$ og $b \geq 0$ eru heiltölur
þannig að $4a + 5b = n$
}

stef frímerki(n: heiltala)
ef $n = 12$ **þá skila** $(3,0)$
ef $n = 13$ **þá skila** $(2,1)$
ef $n = 14$ **þá skila** $(1,2)$
ef $n = 15$ **þá skila** $(0,3)$
(a, b) := frímerki($n - 4$)
skila $(a + 1, b)$

Grunntilvik
(grunnur)

Endurkvæmni
(þrepun)

Frímerki með endurkvæmu stefi

{
Notkun: (a,b) := frímerki(n);
Fyrir: n er heiltala, $n \geq 12$
Eftir: $a \geq 0$ og $b \geq 0$ eru heiltölur
þannig að $4a + 5b = n$
}

stef frímerki(n: heiltala)
ef $n = 12$ **þá skila** $(3,0)$
ef $n = 13$ **þá skila** $(2,1)$
ef $n = 14$ **þá skila** $(1,2)$
ef $n = 15$ **þá skila** $(0,3)$
(a,b) := frímerki($n - 4$)
skila $(a+1, b)$

Grunntilvik (grunnur)

Endurkvæmni (þrepun)

Sérhverju löglegu kalli á stefin lýkur á endanlegum tíma því viðfangið (argument) n getur ekki orðið minna en 12 og minnkar um 4 í hverju endurkvæmu kalli

Ef þessi rök sannfæra ekki (sem þau ættu að gera) þá getum við sannað með **einfaldri þrepasönnun** á gildinu $\left\lfloor\frac{n-12}{4}\right\rfloor$ að stefið **klárar útreikningana og skilar réttu gildi**, en það eru mun flóknari rök

Einfaldara er að sanna með sterkri þrepun að stefið **klárar útreikninga og skilar réttu gildi**

Frímerki með endurkvæmu stefi

{
Notkun: (a, b) := frímerki(n);
Fyrir: n er heiltala, $n \geq 12$
Eftir: $a \geq 0$ og $b \geq 0$ eru heiltölur
þannig að $4a + 5b = n$
}

stef frímerki(n: heiltala)
ef $n = 12$ **þá skila** $(3,0)$
ef $n = 13$ **þá skila** $(2,1)$
ef $n = 14$ **þá skila** $(1,2)$
ef $n = 15$ **þá skila** $(0,3)$
(a, b) := frímerki($n - 4$)
skila $(a + 1, b)$

Grunntilvik (grunnur)

Endurkvæmni (þrepun)

Takið eftir að við skiptum vandamálinu að staðfesta að stefið sé rétt í tvö aðskilin vandamál:

1. Staðfesta að ef löglegu kalli á stefið lýkur þá mun það skila réttu gildi
2. Staðfesta að sérhverju löglegu kalli á stefið lýkur, óháð því hvort gildið sem út kemur er rétt

Frímerki með endurkvæmu stefi

{
Notkun: (a, b) := frímerki(n);
Fyrir: n er heiltala, $n \geq 12$
Eftir: $a \geq 0$ og $b \geq 0$ eru heiltölur
þannig að $4a + 5b = n$
}

stef frímerki(n: heiltala)
ef $n = 12$ **þá skila** $(3{,}0)$
(a, b) := frímerki($n - 1$)
ef $a > 0$ **þá skila** $(a - 1, b + 1)$
skila $(a + 4, b - 3)$

Þessi útgáfa stefsins samsvarar frekar einfaldri þrepun heldur en sterkri þrepun því við minnkum n um einn í endurkvæma kallinu

Frímerki með endurkvæmu stefi

{
Notkun: (a, b) := frímerki(n);
Fyrir: n er heiltala, $n \geq 12$
Eftir: $a \geq 0$ og $b \geq 0$ eru heiltölur
þannig að $4a + 5b = n$
}

stef frímerki(n: heiltala)
    ef $n = 12$ **þá skila** $(3,0)$
    (a, b) := frímerki($n - 1$)
    ef $a > 0$ **þá skila** $(a - 1, b + 1)$
    { $b \geq 3$ (vegna þess að $5b = n - 1 \geq 12$) }
    skila $(a + 4, b - 3)$

Þessi útgáfa stefsins samsvarar frekar einfaldri þrepun heldur en sterkri þrepun því við minnkum n um einn í endurkvæma kallinu

Hækkum upphæðina um einn með því að skipta út einu 4 króna frímerki fyrir eitt 5 króna frímerki

Þessi athugasemd er ekki formlega nauðsynleg, en hjálpleg lesendum forritstextans

Hækkum upphæðina um einn með því að skipta út þremur 5 króna frímerkjum fyrir fjögur 4 króna frímerki

Stöðulýsingar í forritun

- **Skilgreining:** Athugasemd (comment) í forritskafla kallast **stöðulýsing** (state description) ef athugasemdin er fullyrðing um ástandið í keyrslu sem er annaðhvort sönn eða ósönn á þeim tímapunktum þegar keyrsla forritskaflans kemur að athugasemdinni
- **Mikilvæg dæmi:**
  1. Forskilyrði forritskafla er stöðulýsing sem skal vera sönn rétt áður en forritskaflinn er framkvæmdur
  2. Eftirskilyrði forritskafla er stöðulýsing sem skal vera sönn rétt eftir að forritskaflanum lýkur
  3. Fastayrðing lykkju er stöðulýsing sem skal vera sönn rétt fyrir sérhverja umferð lykkjunnar, rétt eftir sérhverja umferð lykkjunnar og bæði rétt áður en lykkjan er framkvæmd og rétt eftir að lykkjan er framkvæmd, hvort sem farin verður umferð um lykkjuna eða ekki
  4. Forskilyrði og eftirskilyrði stefs eru stöðulýsingar sem skulu vera sannar, rétt fyrir sérhvert kall á stefin (fyrir forskilyrðið) og rétt eftir sérhvert kall á stefin (fyrir eftirskilyrðið)

Naumréttir forritskaflar

- **Skilgreining: Naumréttur** (weakly correct) forritskafli er forritskafli með forskilyrði og eftirskilyrði sem hefur nægilega mikið af innri stöðulýsingum til að eftirfarandi sé uppfyllt:
  1. Unnt er að sanna með endanlegri röksemdafærslu að **sérhver runa skipana** í forritskaflanum þar sem runan hefur stöðulýsinu á undan (sem er þá forskilyrði rununnar) og stöðulýsingu á eftir (sem er þá eftirskilyrði rununnar) **uppfyllir þá lýsingu sem felast í forskilyrði og eftirskilyrði rununnar**
  2. **Allar runur skipana** með forskilyrði og eftirskilyrði sem staðfesta þarf **eru endanlegar**, til dæmis þurfa allar lykkjur að hafa fastayrðingu lykkju
- Lykkja án fastayrðingar er ekki naumrétt
- Stef án forskilyrðis og eftirskilyrðis er ekki naumrétt
- Naumréttur forritskafli hefur þann eiginleika að (sannanlegt er að, eða sannað er að) **ef og þegar honum lýkur þá er eftirskilyrði hans satt**

Rammréttir forritskaflar

- **Skilgreining:** Forritskafli er **rammréttur** (strongly correct) ef hann er naumréttur og auk þess er sannað (eða sannanlegt á auðveldan hátt) að keyrsla hans tekur ávallt enda séu forskilyrðin uppfyllt

Naumrétt? Rammrétt?

{
Notkun: x := plús(a,b)
Fyrir: a og b eru heiltölur, $b \geq 0$
Eftir: $x = a + b$
}

```
stef plús( a, b: heiltala )
    s := a; r := b
    meðan r ≠ 0
        { a + b = s + r, r ≥ 0 }
        s := s + 1
        r := r − 1
    skila s
```

Naumrétt? Rammrétt?

{
Notkun: x := plús(a,b)
Fyrir: a og b eru heiltölur, $b \geq 0$
Eftir: $x = a + b$
}

stef plús(a, b: heiltala)
    s := a; r := b
    meðan $r \neq 0$
        { $a + b = s + r$, $r \geq 0$ }
        s := $s + 1$
        r := $r - 1$
    skila s

Stef þetta er klárlega naumrétt sem glöggur lesandi getur sannreynt með einfaldri röksemdafærslu

Stefið er einnig rammrétt því r er heiltala, $r \geq 0$, sem minnkar um einn í hverri umferð og getur ekki orðið smærri en 0

Naumrétt? Rammrétt?

$\{ \; a$ og b eru heiltölur, $b \geq 0 \; \}$
s := a; r := b
meðan $r \neq 0$
    $\{ \; a + b = s + r, \; r \geq 0 \; \}$
    s := $s + 1$
    r := $r - 1$
$\{ \; s = a + b \; \}$

Stef þetta er klárlega naumrétt sem glöggur lesandi getur sannreynt með einfaldri röksemdafærslu

Stefið er einnig rammrétt því r er heiltala, $r \geq 0$, sem minnkar um einn í hverri umferð og getur ekki orðið smærri en 0

Naumrétt? Rammrétt?

{
Notkun: x := plús(a,b)
Fyrir: a og b eru rauntölur, $b \geq 0$
Eftir: $x = a + b$
}

stef plús(a, b: rauntala)
    s := a; r := b
    meðan $r \neq 0$
        { $a + b = s + r$, $r \geq 0$ }
        s := $s + r/2$
        r := $r/2$
    skila s

Naumrétt? Rammrétt?

{
Notkun: x := plús(a,b)
Fyrir: a og b eru rauntölur, $b \geq 0$
Eftir: $x = a + b$
}
stef plús(a, b: rauntala)
    s := a; r := b
    meðan $r \neq 0$
        { $a + b = s + r$, $r \geq 0$ }
        s := $s + r/2$
        r := $r/2$
    skila s

Stef þetta er klárlega naumrétt sem glöggur lesandi getur sannreynt með einfaldri röksemdafærslu

Stefið er ekki rammrétt því r er rauntala og ef $r > 0$ þá er $r/2 > 0$ og lykkjunni lýkur þá aldrei

Naumrétt? Rammrétt?

{
Notkun: x := plús(a,b)
Fyrir: a og b eru heiltölur, $b \geq 0$
Eftir: $x = a + b$
}

stef plús(a, b: heiltala)
    s := a; r := b
    meðan $r \neq 0$
        { $a + b = s + r$, $r \geq 0$ }
        s := s
    skila s

Naumrétt? Rammrétt?

{
Notkun: x := plús(a,b)
Fyrir: a og b eru heiltölur, $b \geq 0$
Eftir: $x = a + b$
}

stef plús(a, b: heiltala)
    s := a; r := b
    meðan $r \neq 0$
        { $a + b = s + r$, $r \geq 0$ }
        s := s
    skila s

Stef þetta er klárlega naumrétt sem glöggur lesandi getur sannreynt með einfaldri röksemdafærslu

Stefið er ekki rammrétt því ekkert gerist í lykkjunni og henni lýkur aldrei

Naumrétt? Rammrétt?

{
Notkun: x := reikna(n)
Fyrir: n er heiltala, $n > 0$
Eftir: $x = 1$
}

stef reikna(n: heiltala)
    meðan $n \neq 1$
        { $n > 0$ }
        ef n er oddatala **þá**
            $n := 3 \cdot n + 1$
        annars
            $n := n/2$
    skila n

Naumrétt? Rammrétt?

{
Notkun: x := reikna(n)
Fyrir: n er heiltala, $n > 0$
Eftir: $x = 1$
}

stef reikna(n: heiltala)
    meðan $n \neq 1$
        { $n > 0$ }
        ef n er oddatala **þá**
            $n := 3 \cdot n + 1$
        annars
            $n := n/2$
    skila n

Stef þetta er klárlega naumrétt sem glöggur lesandi getur sannreynt með einfaldri röksemdafærslu

Hins vegar **veit enginn** hvort sérhverju löglegu kalli á stefið lýkur og því er stefið (eins og er) ekki rammrétt

Velröðun og réttmæti þrepunar

- Þrepun er lögmæt röksemdafærsluregla vegna þess að mengi jákvæðra heiltalna er velraðað
- **Skilgreining:** Mengi S er velraðað ef sérhvert ekki-tómt hlutmengi $\mathrm{A} \subseteq S$ hefur minnsta stak sem er í A
- **Setning:** Gild þrepunarsönnun, $P(1) \wedge \forall k\colon \big(P(k) \to P(k+1)\big)$, fyrir umsögn P leiðir til þess að $P(k)$ gildir fyrir allar jákvæðar heiltölur
- **Sönnun:** Notum óbeina sönnun. Gerum ráð fyrir að
$$P(1) \wedge \forall k\colon \big(P(k) \to P(k+1)\big)$$
  sé satt, en að til sé jákvæð heiltala n þannig að $P(n)$ er ósatt.
  - Látum S vera mengi þeirra jákvæðu heiltalna n þannig að $P(n)$ er ósatt. Það mengi er þá ekki tómt.
  - Mengið S hefur þá minnsta gildi, köllum það m. Þar eð $P(1)$ er satt getur m ekki verið 1 og hlýtur því að vera stærra en 1. Þar með fæst að $m-1$ er jákvæð heiltala og $P(m-1)$ hlýtur að gilda þar eð $\mathrm{m}-1 \notin S$. En þá fáum við samkvæmt þrepunarskrefinu að $P(m)$ hlýtur að gilda vegna $P(m-1) \to P(m)$.
  - En það er í mótsögn við forsenduna að $P(m)$ sé ósatt. Því hlýtur $P(m)$ að vera satt.

Velröðunareiginleikinn (Well-Ordering)

- **Velröðunareiginleiki heiltalna:** Sérhvert ekki-tómt mengi af ekki-neikvæðum heiltölum hefur minnsta gildi.
- Fyrir jákvæðar heiltölur er velröðunareiginleikinn ein af frumsetningunum.
- Nota má velröðunareiginleikann beint í sönnunum (t.d. í stað þrepunar)
- En við getum líka skilgreint almenna útgáfu af þessum eiginleika.
- **Skilgreining:** Mengi S er velraðað ef sérhvert ekki-tómt hlutmengi hefur minnsta gildi.
  - **Dæmi:** Mengið $\mathbb{N}$ er velraðað með tilliti til $\leq$
  - **Dæmi:** Mengi endanlegra strengja yfir velraðað stafróf er velraðað með tilliti til stafrófsraðar (lexicographic ordering)
- Velröðun gefur okkur eina leið til að skilgreina almennari útgáfur þrepunar

Endurkvæmar skilgreiningar og gerðarþrepun

- Endurkvæmt skilgreind föll
- Endurkvæmt skilgreind mengi og gerðir (structures)
- Gerðarþrepun (structural induction)
- Almenn þrepun (generalized induction)

Endurkvæmt skilgreind föll

- **Skilgreining:** Endurkvæm skilgreining (eða þrepunarskilgreining – inductive definition) á falli $f\colon \mathbb{N} \to A$ samanstendur af tveimur skrefum:
  - **Grunnskref:** Skilgreining gildis fallsins í núlli eða nálægt núlli, þ.e. $f(0), f(1), \dots f(b)$, fyrir eitthvert b
  - **Þrepunarskref:** Regla til að finna fallgildið $f(n)$, fyrir $\mathrm{n} > b$ út frá fallsgildunum í $0, \dots, n-1$
- Fall $f\colon \mathbb{N} \to A$ samsvarar runu $a_0, a_1, \dots$, þar sem $a_i = f(i)$
- Við gerðum þetta áður með rakningarvensl
- Dæmi: Skilgreinum f með:
  - $f(0) = 3$
  - $f(n+1) = 2f(n) + 3$
  - Finnum $f(1), f(2), f(3)$
  - Lausn:
    - $f(1) = 2f(0) + 3 = 2 \cdot 3 + 3 = 9$
    - $f(2) = 2f(1) + 3 = 2 \cdot 9 + 3 = 21$
    - $f(3) = 2f(2) + 3 = 2 \cdot 21 + 3 = 45$

Endurkvæmt skilgreind föll

- **Dæmi:** Sýnið endurkvæma skilgreiningu á

$$\sum_{k=0}^{n} a_k$$

- **Lausn:**
  - Grunnskrefið gæti verið

$$\sum_{k=0}^{0} a_k = a_0$$

  - Þrepunarskrefið gæti verið

$$\sum_{k=0}^{n+1} a_k = \left(\sum_{k=0}^{n} a_k\right) + a_{n+1}$$

Fibonacci tölur

- Skilgreinum Fibonacci tölurnar sem endurkvæmt skilgreint fall
  - **Grunnskref:**
    - $f(0) = 0$
    - $f(1) = 1$
  - **Þrepunarskref:**
    - $f(n) = f(n-1) + f(n-2)$

- Eða, jafngilt:

$$f(n) = \begin{cases} 0 & \textbf{ef } n = 0 \\ 1 & \textbf{ef } n = 1 \\ f(n-1) + f(n-2) & \textbf{ef } n > 1 \end{cases}$$

Endurkvæmar skilgreiningar á mengjum og gerðum (structures)

- **Endurkvæmar skilgreiningar** mengja samanstanda af tveimur hlutum:
  - Grunnskref skilgreinir **upphaflegt safn staka**
  - Þrepunarskref gefur reglurnar sem nota má til að **smíða ný stök í menginu** út frá þeim sem þegar er þekkt að eru í menginu
- Stundum er líka tilgreind **útilokunarregla**, sem segir að ekkert sé í menginu nema það sem hægt er að fá með ofangreindum skrefum
- Við munum ávallt gera ráð fyrir að slík útilokunarregla sé til staðar, jafnvel þótt hún sé ekki sérstaklega nefnd
- Við munum seinna sjá afbrigði þrepunar, **gerðarþrepun** (structural induction) sem notuð er til að sanna niðurstöður um endurkvæmt skilgreind mengi

Endurkvæmt skilgreind mengi

- **Dæmi:** Undirmengi S í $\mathbb{Z}$
  - Grunnskref: $3 \in S$
  - Þrepunarskref: Ef $x \in S$ og $y \in S$ þá er $x + y \in S$
  - Upphaflega er 3 í S, síðan $3 + 3 = 6$, síðan $3 + 6 = 9$, o.s.frv.
- **Dæmi:** Náttúrlegu tölurnar $\mathbb{N}$
  - Grunnskref: $0 \in \mathbb{N}$
  - Þrepunarskref: Ef $n \in \mathbb{N}$ þá er $n + 1 \in \mathbb{N}$
  - Upphaflega er 0 í $\mathbb{N}$, síðan $0+1=1$, síðan $1+1=2$, o.s.frv.

Strengir

- **Skilgreining:** Skilgreinum mengið Σ^*, kallað mengi strengja yfir stafrófið Σ, með endurkvæmri skilgreiningu:
  - Grunnskref: $\lambda \in \Sigma^*$ (λ táknar tóma strenginn)
  - Þrepunarskref: Ef w er í Σ^* og x er í Σ þá er wx í Σ^*
- **Dæmi:** Ef $\Sigma = \{0,1\}$ þá eru strengirnir í Σ^* bitastrengirnir $\lambda, 0,1,00,01,10,11,$ o.s.frv.
- **Dæmi:** Ef $\Sigma = \{\mathrm{a}, \mathrm{b}\}$, sýnum að aab sé í Σ^*
- **Lausn:**
  - **Þar eð** $\lambda \in \Sigma^*$ **og** $a \in \Sigma$ **þá er** $a \in \Sigma^*$
  - **Þar eð** $a \in \Sigma^*$ **og** $a \in \Sigma$ **þá er** $aa \in \Sigma^*$
  - **Þar eð** $aa \in \Sigma^*$ **og** $b \in \Sigma$ **þá er** $aab \in \Sigma^*$

Samskeyting strengja

- **Skilgreining:** Setja má saman tvo strengi með **samskeytingu**. Látum Σ vera stafrófið og Σ^* vera mengi strengja yfir það stafróf. Við skilgreinum samskeytingu strengja, táknuð með samskeytingaraðgerðinni $\cdot$, endurkvæmt á eftirfarandi hátt:
  - Grunnskref: Ef $w \in \Sigma^*$ þá skilgreinum við $w \cdot \lambda = w$
  - Þrepunarskref: Ef $w_1 \in \Sigma^*$ og $w_2 \in \Sigma^*$ og $x \in \Sigma$ þá $w_1 \cdot (w_2 x) = (w_1 \cdot w_2)x$
- Oft ritum við $w_1 w_2$ í stað $w_1 \cdot w_2$
- Ef $w_1 = abra$ og $w_2 = cadabra$ þá er samskeytingin $w_1 \cdot w_2 = abracadabra$

Lengd strengs

- **Dæmi:** Sýnið endurkvæma skilgreiningu á lengd strengs
- **Lausn:** Lengd strengs má skilgreina sem fallið $l: \Sigma^* \to \mathbb{Z}$ með endurkvæmri skilgreiningu:
  - $l(\lambda) = 0$
  - $l(wx) = l(w) + 1$, fyrir $w \in \Sigma^*$ og $x \in \Sigma$

  Eða, jafngilt:

$$l(s) = \begin{cases} 0 & \textbf{ef } s = \lambda \\ l(w) + 1 & \textbf{ef } s = wx \textbf{ fyrir eitthvert } w \textbf{ og } x \end{cases}$$

Svigar í jafnvægi

- **Dæmi:** Sýnum endurkvæma skilgreiningu á menginu P sem inniheldur þá strengi yfir stafrófið $\Sigma = \{(,)\}$ með svigum í jafnvægi
- **Lausn:**
  - **Grunnskref:** $\lambda \in P$
  - **Þrepunarskref:** Ef $x \in P$ og $y \in P$ þá er $(x)y \in P$
- Sýnið að (()(())) sé í P
- Hvers vegna er))(() ekki í P?