

Lovászín lokaalilemma

- ★ Itse asiassa Paul Erdősín (1913–1996) ja László Lovászín (★1948) vuoden 1975 yhteisartikkelissa julkaistu
- ★ Olk. tapahtumat E_1, \dots, E_n tn-avaruuden epäsuotuisat tapahtumat
- ★ Tavoittemme on osoittaa, että on olemassa myös suotuisia tapahtumia tarkastelemalla ei-toivottujen tapahtumien E_1, \dots, E_n komplementtien leikkausta
- ★ Jos tapahtumat ovat riippumattomia, niin myös niiden komplementit ovat ja

$$\Pr\left(\bigcap_{i=1}^n \bar{E}_i\right) = \prod_{i=1}^n \Pr(\bar{E}_i) > 0,$$

jos $\Pr(E_i) < 1$ kaikilla i

197

- ★ Lievennetään tapahtuman E riippumattomuusoletus lokaaliksi
- ★ E on riippumaton tapahtumista E_1, \dots, E_n , jos kaikilla $I \subseteq [1, n]$

$$\Pr\left(E \mid \bigcap_{i \in I} E_i\right) = \Pr(E)$$

- ★ Paikallisten riippuvuuksien kuvaamiseen voidaan käyttää *riippuvuusverkkoa*
- ★ Tapahtumien E_1, \dots, E_n riippuvuusverkossa $G = (V, E)$ on $V = \{1, \dots, n\}$ ja E_i on riippumaton tapahtumista $\{E_j \mid (i, j) \notin E\}$
- ★ Seuraavassa esitämme symmetrisen version Lovászín lokaalilemmasta (yleinen versio kirjan luvussa 6.9)

198

Lause 6.11: Olk. E_1, \dots, E_n joukko tapahtumia, joille pätee

1. $\Pr(E_i) \leq p$ kaikilla i ;
2. tapahtumien E_1, \dots, E_n riippuvuusverkon solmujen aste on kork. d ;
3. $4dp \leq 1$.

Tällöin

$$\Pr\left(\bigcap_{i=1}^n \bar{E}_i\right) > 0.$$

- ★ Tarkastellaan sovellusta, jossa n käyttäjäparia kommunikoi keskenään käyttäen annetun verkon kaarivieraita polkuja
- ★ Kukin pari $i \in [1, n]$ valitsee polkuns m :n polun kokoelmasta F_i
- ★ Jos poluilla ei ole liikaa yhteisiä kaaria, niin Lovászín lokaalilemmalla voimme valita tarvittavat polut

199

Lause 6.12: Jos kaikilla F_i :n poluilla on yht. kaaria kork. k :n F_j :n ($i \neq j$) polun kanssa ja $8nk/m \leq 1$, niin voidaan valita n kaarivierasta polkua, jotka yhdistävät annetut n paria.

Todistus. Vetäköön kukin pari polun m :n vaihtoehtonsa joukosta riippumattomasti tasaisen jakauman mukaan. Olk. E_{ij} tapahtuma "parien i ja j valitsemilla poluilla on ainakin yksi yhteinen kaari". Koska F_i :n polulla ei ole yhteisiä kaaria kuin kork. k :n F_j :n polun kanssa, niin $p = \Pr(E_{ij}) \leq k/m$.

Olk. d riippuvuusverkon asteluku. Koska E_{ij} on riippumaton kaikista tapahtumista $E_{i'j'}, i', j' \notin \{i, j\}$, niin $d < 2n$. Koska

$$4dp < \frac{8nk}{m} \leq 1,$$

200

niin lauseen 6.11 kaikki ehdot täyttyvät ja

$$\Pr\left(\bigcap_{i \neq j} \bar{E}_{ij}\right) > 0.$$

Näin ollen n polkua voidaan valita s.e. ne ovat kaarivieraita. \square

- ★ Palataan taas lausekalkyylin kaavojen toteutuvuuteen
- ★ Tarkastellaan nyt k -SAT-kaavoja, joiden kussakin tekijässä on täsmälleen k literaalia (NP-täydellinen)
- ★ Oletetaan taas, ettei mikään tekijä sisällä sekä literaalia että sen negaatiota

Lause 6.13: Jos yksikään muuttuja ei esiinny useammassa kuin $T = 2^k/4k$ k -SAT-kaavan tekijässä, niin sillä on toteuttava arvoasetus.

201

Todistus. Vedetään muuttujien arvot riippumattomasti ja symmetrisesti. Olk. E_i tapahtuma " i s tekijä ei toteudu satunnaisella arvoasetuksella". Koska kussakin tekijässä on k literaalia, niin

$$\Pr(E_i) = 2^{-k}.$$

Tapahtuma E_i on riippumaton kaikista niihin tekijöihin liittyvistä tapahtumista, joissa ei ole samoja muuttujia kuin tekijässä i . Koska tekijän i sisältämät k muuttujaa voivat esiintyä kork. $T = 2^k/4k$:ssa muussa tekijässä, niin riippuvuusverkon astetta d rajoittaa $d \leq kT \leq 2^{k-2}$.

Tällöin $4dp \leq 4 \cdot 2^{k-2}2^{-k} \leq 1$, joten Lovászın lemman perusteella komplementtitapahtumien leikkauksen tn. on aidosti nolaa suurempi ja kaavalla on olemassa toteuttava arvoasetus. \square

202

7. Markovin ketjut ja satunnaiskulut

- ★ Stokastinen prosessi $\mathbf{X} = \{X(t) : t \in T\}$ on s -muuttujien kokoelma
- ★ Merk. myös $X(t) = X_t$
- ★ Useimmiten t vastaa aikaa ja prosessi \mathbf{X} mallintaa ajan myötä muuttuvan s -muuttujan X arvoa
- ★ $X(t)$ on prosessin *tila* ajan hetkellä t
- ★ Jos X_t :n arvoalue on numeroituva kaikilla t , niin prosessi \mathbf{X} on *diskreetti-tilainen*
- ★ Äärellisessä prosessissa X_t saa arvoja vain äärellisestä joukosta
- ★ Jos T on numeroituva, niin prosessi \mathbf{X} on *diskreettiaikainen*

203

- ★ Markovin ketjulla on muistittomuusominaisuus (l. Markov-ominaisuus)
 - ◇ X_t :n arvo riippuu tilasta X_{t-1} , muttei tiloista X_0, \dots, X_{t-2}
 - ◇ Tarkemmin

$$\begin{aligned} \Pr(X_t = a_t \mid X_{t-1} = a_{t-1}, \dots, X_0 = a_0) \\ = \Pr(X_t = a_t \mid X_{t-1} = a_{t-1}) \end{aligned}$$

- ★ Markov-ominaisuudesta ei seuraa, että X_t olisi riippumaton s -muuttujista X_0, \dots, X_{t-2}
- ★ Sen sijaan X_{t-1} :n arvo riittää ilmaisemaan X_t :n riippuvuuden historiasta
- ★ Tyydymme tarkastelemaan vain *homogeenisiä* Markovin ketjuja, joille pätee kaikilla $t, u \in T$ ja a, b

$$\begin{aligned} \Pr(X_t = a \mid X_{t-1} = b) = \\ \Pr(X_u = a \mid X_{u-1} = b) \end{aligned}$$

204

- ★ Tila-avaruus olk. \mathbb{N} tai äärellinen joukko $\{0, 1, \dots, n\}$
- ★ Tn., että prosessi siirtyy yhdessä askelella tilasta i tilaan j on *siirtymät.*

$$P_{ij} = \Pr(X_t = j \mid X_{t-1} = i)$$

- ★ Markov-ominaisuuden perusteella siirtymämatriisi \mathbf{P} määrää Markovin ketjun yksikäsitteisesti
- ★ Kukin rivi summautuu arvoon 1:

$$\sum_{j \geq 0} P_{ij} = 1$$
- ★ Merk. $p_i(t)$ on tn., että prosessi on tilassa i hetkellä t
- ★ Olk. $\vec{p}(t) = (p_0(t), p_1(t), \dots)$ vektori, joka antaa jakauman ketjun tilalle ajan hetkellä t

205

- ★ Summaamalla yli mahdollisten tilojen ajan hetkellä $t - 1$ saamme

$$p_i(t) = \sum_{j \geq 0} p_j(t-1)P_{ji}$$

- ★ Näin ollen $\vec{p}(t) = \vec{p}(t-1)\mathbf{P}$ (rivivektori)
- ★ Siirtymämatriisin avulla on siis helppo laskea Markovin ketjun tulevien tilojen jakaumia
- ★ Määr. tasan m :n askelen ($m \geq 0$) siirtymät. $P_{ij}^m = \Pr(X_{t+m} = j \mid X_t = i)$
- ★ Ensimmäisten siirtymävaihtoehtojen yli summaamalla

$$P_{ij}^m = \sum_{k \geq 0} P_{ik}P_{kj}^{m-1}$$

206

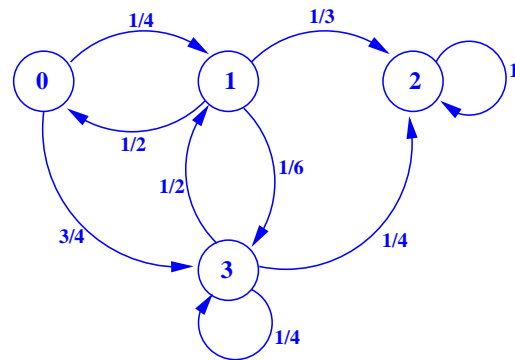
- ★ Olk. $\mathbf{P}^{(m)}$ matriisi, jonka alkiot ovat m :n askelen siirtymät. P_{ij}^m

- ★ Eo. perusteella $\mathbf{P}^{(m)} = \mathbf{P} \cdot \mathbf{P}^{(m-1)}$, josta induktiolla saadaan edelleen $\mathbf{P}^{(m)} = \mathbf{P}^m$

- ★ Täten $\vec{p}(t+m) = \vec{p}(t)\mathbf{P}^m$ kaikilla $t \geq 0$ ja $m \geq 1$

- ★ Usein Markovin ketju esitetään siirtymäverkkona, joka on painotettu suunnattu verkko $D = (V, E, w)$, missä
 - ◇ solmut V ovat ketjun tilat ja
 - ◇ kaari $(i, j) \in E$ on verkossa joss $P_{ij} > 0$ ja
 - ◇ sen paino on $w(i, j) = P_{ij}$
- ★ Tn., että prosessi seuraa tilajonoa, joka vastaa suunnattua polkua verkossa, on polun kaartten painojen tulo

207



$$\mathbf{P} = \begin{pmatrix} 0 & 1/4 & 0 & 3/4 \\ 1/2 & 0 & 1/3 & 1/6 \\ 0 & 0 & 1 & 0 \\ 0 & 1/2 & 1/4 & 1/4 \end{pmatrix}$$

$$\mathbf{P}^3 = \begin{pmatrix} 3/16 & 7/48 & 29/64 & 41/192 \\ 5/48 & 5/24 & 79/144 & 5/36 \\ 0 & 0 & 1 & 0 \\ 1/16 & 13/96 & 107/192 & 47/192 \end{pmatrix}$$

208

- ★ Ed. Markovin ketjun kolmen askelen polkuja tilasta 0 tilaan 2 on 5 kpl: $\langle 0, 1, 2, 2 \rangle$, $\langle 0, 1, 3, 2 \rangle$, $\langle 0, 3, 1, 2 \rangle$, $\langle 0, 3, 2, 2 \rangle$ ja $\langle 0, 3, 3, 2 \rangle$

- ★ Verkkoesityksestä saamme tn.:n

$$\frac{1}{4 \cdot 3} + \frac{1}{4 \cdot 6 \cdot 4} + \frac{3}{4 \cdot 2 \cdot 3} + \frac{3}{4 \cdot 4} + \frac{3}{4 \cdot 4 \cdot 4} \\ = \frac{87}{192} = \frac{29}{64} \approx 0,45$$

- ★ Sama tulos saadaan laskemalla matriisin \mathbf{P} 3-kertainen tulo itsensä kanssa \mathbf{P}^3 ja lukemalla alkio P_{02}^3
- ★ Jos lähtötila vedetään symmetrisesti kaikkien tilojen joukosta, niin kolmen askelen jälkeisen lopputilan jakauma on $(1/4, 1/4, 1/4, 1/4) \mathbf{P}^3 =$
 $(17/192, 47/384, 737/1152, 43/288)$
- ★ Joten tilaan 2 päätyminen tn. on $737/1152 \approx 0,64$

209

2-SAT

- ★ 2-SAT-kaavojen toteutuvuus on polynomisesti ratkeava ongelma toisin kuin yleinen k -SAT-kaavojen toteutuvuus
- ★ Satunnaisalgoritmi:
 1. Vedä mv. totuusarvoasetus.
 2. Toista kork. $2mn^2$ kertaa, lopettaen jos kaikki tekijät toteutuvat.
 - (a) Valitse mv. ei-toteutuva tekijä.
 - (b) Vedä symmetrisesti toinen tekijän literaaleista ja vaihda sen muuttujan arvoasetus.
 3. Jos validi totuusarvoasetus löytyi, palauta se. Muuten ilmoita, että kaava on toteutumaton.

210

- ★ Jos eo. algoritmi palauttaa toteuttavan arvoasetuksen, on se korrekki
- ★ Montako toistolauseen askelta tarvitaan, jos toteuttava arvoasetus S on olemassa?
- ★ 2-SAT-kaavassa erilaisia tekijöitä on $O(n^2)$, joten kunkin askelen vaatima aika on kork. neliöllinen
- ★ Olk. A_i n :n muuttujan arvoasetus askelen i jälkeen
- ★ Olk. edelleen X_i niiden muuttujien lkm, joilla on sama arvo nykyisessä arvoasetuksessa A_i kuin S :ssä
- ★ Kun $X_i = n$, niin toteuttava arvoasetus on löydetty, pahimmassa tapauksessa tämä on ensimmäinen löydetty arvoasetus

211

- ★ Jos $X_i = 0$, niin mistä tahansa arvon muutoksesta seuraa $X_{i+1} = 1$, eli $\Pr(X_{i+1} = 1 \mid X_i = 0) = 1$
- ★ Olk. sitten $1 \leq X_i \leq n - 1$
- ★ Koska S toteuttaa mv. valitsemamme ei-toteuttavan tekijän, niin A_i ja S poikkeavat ainakin tekijän toisen muuttujan arvoasetuksen osalta
- ★ Tn., että symmetrinen muuttujan vetäminen johtaa lisääntyneeseen yhtenevien arvojen määrään on ainakin $1/2$, eli $\Pr(X_{i+1} = j + 1 \mid X_i = j) \geq 1/2$
- ★ Jos arvot poikkeaisivat tekijän molempien muuttujien osalta, niin lisääntymistn. olisi 1
- ★ Tn., että yhtenevien arvojen määrä vähenee on kork. $1/2$:
 $\Pr(X_{i+1} = j - 1 \mid X_i = j) \leq 1/2$

212

- ★ Stokastinen prosessi X_0, X_1, X_2, \dots ei välttämättä ole Markovin ketju, koska X_i :n lisääntymistn. voi riippua siitä poikkeavatko A_i ja S valitun tekijän yhden vai kahden muuttujan osalta
- ★ Tämä puolestaan voi riippua aiemmin vedetyistä tekijöistä
- ★ Tarkast. Markovin ketjua Y_0, Y_1, Y_2, \dots :

$$\begin{aligned} Y_0 &= X_0; \\ \Pr(Y_{i+1} = 1 \mid Y_i = 0) &= 1; \\ \Pr(Y_{i+1} = j + 1 \mid Y_i = j) &= 1/2; \\ \Pr(Y_{i+1} = j - 1 \mid Y_i = j) &= 1/2 \end{aligned}$$

- ★ $Y = Y_0, Y_1, Y_2, \dots$ on pessimistinen versio stokastisesta prosessista $X = X_0, X_1, X_2, \dots$ sillä n :n saavuttamisen odotusarvo on Y :ssä suurempi

213

- ★ Markovin ketju Y kuvaa *satunnaiskulkua* (random walk) suuntaamattomassa verkossa G , jonka solmuja ovat $0, \dots, n$ ja jossa solmu i on kytketty solmuihin $i - 1$ ja $i + 1$
- ★ Olk. h_j askelten lkm:n odotusarvo n :n saavuttamiseksi kun lähtösolmu on j
- ★ $h_n = 0$ ja $h_0 = h_1 + 1$, koska solmusta 0 ei ole pääsyä muualle kuin 1:een
- ★ Olk. Z_j s-muuttuja, joka kuvaa n :n saavuttamisen edellyttämien askelten lkm:n, kun lähtösolmu on j
- ★ Solmusta j , $1 \leq j \leq n - 1$ siirrytään tn.:llä $1/2$ solmuihin $j - 1$ ja $j + 1$
- ★ Täten

$$\mathbf{E}[Z_j] = \mathbf{E}\left[\frac{1}{2}(1 + Z_{j-1}) + \frac{1}{2}(1 + Z_{j+1})\right]$$

214

- ★ Koska $\mathbf{E}[Z_j] = h_j$, niin lineaarisuuden perusteella $h_j = \frac{h_{j-1}}{2} + \frac{h_{j+1}}{2} + 1$

- ★ Ratkaistavanamme on yhtälöryhmä

$$h_j = \begin{cases} h_1 + 1, & \text{kun } j = 0 \\ \frac{h_{j-1}}{2} + \frac{h_{j+1}}{2} + 1, & \text{kun } 1 \leq j \leq n - 1 \\ 0, & \text{kun } j = n \end{cases}$$

- ★ Kaikilla $0 \leq j \leq n - 1$ pätee $h_j = h_{j+1} + 2j + 1$

◇ Väite pätee kun $j = 0$

◇ Muuten, induktiolla

$$\begin{aligned} h_{j+1} &= 2h_j - h_{j-1} - 2 \\ &= 2h_j - (h_j + 2(j - 1) + 1) - 2 \\ &= h_j - 2j - 1 \end{aligned}$$

- ★ Lopulta siis

$$\begin{aligned} h_0 &= h_1 + 1 = h_2 + 1 + 3 = \dots \\ &= \sum_{i=0}^{n-1} 2i + n = n^2 \end{aligned}$$

215

- ★ h_j on yläraja algoritmin vaatimien askelten määrän odotusarvolle ennen kuin arvoasetus on yhtäpitävä S :n kanssa kun alkutilanteessa saman arvon omaavia muuttujia on j kpl

Lemma 7.1: Olk. n :n muuttujan 2-SAT-kaavalla toteuttava arvoasetus ja annetaan algoritmin toimia siihen asti kunnes se löytää toteuttavan arvoasetuksen. Tarvittavien askelten lkm:n odotusarvo on kork. n^2 .

- ★ Algoritmin asettama askelten lkm:n rajoite huomioiden saadaan tulos

Lause 7.2: Jos annettu 2-SAT-kaava ei ole toteutuva, niin algoritmi palauttaa oikean vastauksen. Jos se puolestaan on toteutuva, niin tn.:llä $1 - 2^{-m}$ algoritmi palauttaa toteuttavan arvoasetuksen ja muuten virheellisesti väittää kaavaa ei-toteutuvaksi.

216

Todistus. Ensimmäinen väittäjä on selvä. Olk. siis kaava toteutuva. Jaetaan algoritmin toiminta m :ään $2n^2$ askelen lohkokoon. Jos toteuttavaa arvoasetusta ei löytynyt $i - 1$ ensimmäisen lohkon aikana, niin mikä on tn. ettei sellaista löydy i :nessä lohkokossakaan?

Lemman 7.1 perusteella, riippumatta alkuasemasta, toteuttava arvoasetus löytyy korkeintaan n^2 askelen kuluessa. Olk. Z askelten lkm lohkon i alusta toteuttavan arvoasetuksen löytymiseen saakka. Markovian epäyhtälön perusteella

$$\Pr(Z > 2n^2) \leq \frac{n^2}{2n^2} = \frac{1}{2}.$$

Täten yli m :n lohkon tn.:ttä, ettei algoritmi löydä toteuttavaa arvoasetusta, rajoittaa ylhäältä $(1/2)^m$. \square

217

3-SAT

- ★ 3-SAT on tunnetusti NP-täydellinen ongelma, joten (odotusarvoisesti) polynomiaikaisen ratkaisualgoritmin löytäminen satunnaistettunakaan ei ole odotettavissa
- ★ Naiivi menetelmä käy läpi kaikki 2^n mahd. arvoasetusta n :lle muuttujalle
- ★ Satunnaisalgoritmin vaatavuus on eksponentiaalinen, mutta oleellisesti naiivia lähestymistä tehokkaampi
- ★ Tarkastellaan ensin 2-SAT-algoritmin suoraviivaista muunnosta
- ★ Nyt tn., että onnistumme kasvattamaan yhtenevien arvoasetusten lukumäärää satunnaisella tekijän muuttujan arvon vaihtamisella on väh. $1/3$:
 $\Pr(X_{i+1} = j + 1 \mid X_i = j) \geq 1/3$

218

★ Vastaavasti

$$\Pr(X_{i+1} = j - 1 \mid X_i = j) \leq 2/3$$

★ Taas askelten määrää ennen kuin $X_i = n$ voidaan rajoittaa Markovian ketjulla Y_0, Y_1, Y_2, \dots

$$Y_0 = X_0;$$

$$\Pr(Y_{i+1} = 1 \mid Y_i = 0) = 1;$$

$$\Pr(Y_{i+1} = j + 1 \mid Y_i = j) = 1/3;$$

$$\Pr(Y_{i+1} = j - 1 \mid Y_i = j) = 2/3$$

- ★ Nyt ketju pienenee todennäköisemmin kuin kasvaa
- ★ Olk. h_j askelten lkm:n odotusarvo n :n saavuttamiseksi kun lähtösolmu on j
- ★ Ratkaistavanamme on yhtälöryhmä

$$h_j = \begin{cases} h_1 + 1, & \text{kun } j = 0 \\ \frac{2h_{j-1}}{3} + \frac{h_{j+1}}{3} + 1, & \text{kun } 1 \leq j \leq n - 1 \\ 0, & \text{kun } j = n \end{cases}$$

219

- ★ Esim. induktiolla voidaan osoittaa, että $h_j = h_{j+1} + 2^{j+2} - 3$, jolloin saadaan $h_j = 2^{n+2} - 2^{j+2} - 3(n - j)$
- ★ Joka tapauksessa tämän algoritmin keskimäärin vaatima askelten lkm on $\Theta(2^n)$, joka ei ole kelvallinen tulos
- ★ Havaintoja:
 - ◇ Jos alkuperäinen arvoasetus valitaan tasaisen jakauman mukaan, niin $X_0 \sim B(n, 1/2)$ ja $\mathbf{E}[X_0] = n/2$. Eksponent. pienellä, muttei merkityksettömällä tn.:llä, $X_0 \gg n/2$.
 - ◇ Algoritmi johtaa pikemmin kohti arvoa 0 kuin n . Mitä kauemmin prosessi pyörii, sitä todennäköisemmin liikahdetaan kohti 0 :aa. Parempi siis käynnistää prosessi satunn. arvoasetuksella ja ajaa sitä lyhyen aikaa, kuin ajaa pitkään samasta alkutilanteesta alkavaa prosessia.

220

★ Muutetaan algoritmia s.e. tasaisen jakauman mukaan satunnaisesti valitulla totuusarvoasetuksella suoritetaan kork. $3n$ askelta

- ◇ Jos toteuttava arvoasetus (S tai muu) löytyy, palautetaan se
- ◇ Muuten keskeytetään prosessi ja valitaan uusi satunn. alkutilanne

★ Olk. q_j alaraja tn.:lle, että algoritmi löytää toteuttavan arvoasetuksen $3n$ askelessa lähtien liikkeelle arvoasetuksesta, jossa täsmälleen j :llä muuttujalla on eri arvo kuin S :ssä

★ Alaraja sille, että algoritmi löytää toteuttavan arvoasetuksen $j + 2k \leq 3n$ askelessa on

$$q_j \geq \max_{k=0, \dots, j} \binom{j+2k}{k} \left(\frac{2}{3}\right)^k \left(\frac{1}{3}\right)^{j+k}$$

221

★ Kun $k = j$, niin

$$q_j \geq \binom{3j}{j} \left(\frac{2}{3}\right)^j \left(\frac{1}{3}\right)^{2j}$$

Lemma 7.3 (Stirlingin kaava): Arvoilla $m > 0$,

$$\sqrt{2\pi m} \left(\frac{m}{e}\right)^m \leq m! \leq 2\sqrt{2\pi m} \left(\frac{m}{e}\right)^m$$

★ Täten, kun $j > 0$,

$$\begin{aligned} \binom{3j}{j} &= \frac{(3j)!}{j!(2j)!} \\ &\geq \frac{\sqrt{2\pi(3j)}}{4\sqrt{2\pi j}\sqrt{2\pi(2j)}} \left(\frac{3j}{e}\right)^{3j} \left(\frac{e}{2j}\right)^{2j} \left(\frac{e}{j}\right)^j \\ &= \frac{\sqrt{3}}{8\sqrt{\pi j}} \left(\frac{27}{4}\right)^j = \frac{c}{\sqrt{j}} \left(\frac{27}{4}\right)^j \end{aligned}$$

vakiolla $c = \sqrt{3}/8\sqrt{\pi}$

222

★ Näin ollen, kun $j > 0$,

$$\begin{aligned} q_j &\geq \binom{3j}{j} \left(\frac{2}{3}\right)^j \left(\frac{1}{3}\right)^{2j} \\ &\geq \frac{c}{\sqrt{j}} \left(\frac{27}{4}\right)^j \left(\frac{2}{3}\right)^j \left(\frac{1}{3}\right)^{2j} \\ &\geq \frac{c}{\sqrt{j}} \frac{1}{2^j} \end{aligned}$$

★ $q_0 = 1$

★ Johdetaan nyt alaraja tn.:lle q , että prosessi saavuttaa toteuttavan arvoasetuksen $3n$ askelessa aloittaessaan satunnaisesta arvoasetuksesta

★ Olk. R_j tapahtuma "satunnainen arvoasetus poikkeaa j :n arvosta S :stä"

223

$$\begin{aligned} q &\geq \sum_{j=0}^n \Pr(R_j) \cdot q_j \\ &\geq \frac{1}{2^n} + \sum_{j=1}^n \binom{n}{j} \left(\frac{1}{2}\right)^n \frac{c}{\sqrt{j}} \frac{1}{2^j} \\ &\geq \frac{c}{\sqrt{n}} \left(\frac{1}{2}\right)^n \sum_{j=0}^n \binom{n}{j} \left(\frac{1}{2}\right)^j 1^{n-j} \\ &\stackrel{(*)}{=} \frac{c}{\sqrt{n}} \left(\frac{1}{2}\right)^n \left(\frac{3}{2}\right)^n \\ &= \frac{c}{\sqrt{n}} \left(\frac{3}{4}\right)^n, \end{aligned}$$

sillä $(*) \sum_{j=0}^n \binom{n}{j} x^j y^{n-j} = (x+y)^n$

★ Jos toteuttava arvoasetus on olemassa, niin prosessin kokeilemien satunnaisien arvoasetusten lkm on geom. jakautunut parametrilla q

224

- ★ Kokeiltujen arvoasetusten lkm:n odotusarvo on $1/q$ ja kutakin kohden algoritmi käyttää $3n$ askelta
- ★ Täten tarvittavien askelten lkm:n odotusarvoa rajoittaa

$$\frac{3n\sqrt{n}}{c(3/4)^n} = O\left(n^{3/2}(4/3)^n\right)$$

- ★ Saadaan siis Monte Carlo -algoritmi kuten 2-SAT-ongelmallekin, joskin nyt askelten lkm:n odotusarvo on eksponentiaalinen n :n suhteen
- ★ Sopivalla parametrin valinnalla saadaan epäonnistumisen tn. painettua matalaksi