

Keerukusteooria alused

Ahto Buldas

Arvutatavus

Funktsiooni $A \xrightarrow{f} B$ **arvutatavus**: hulkade A ja B elemendid on sobivalt kodeeritud ja leidub arvutiprogramm (lõplik käskude jada), mis iga elemendi $a \in A$ koodist $\text{Code}(a)$ arvutab lõpliku aja jooksul välja elemendi $f(a) = b \in B$ koodi $\text{Code}(b)$.

Koodideks võetakse kõigi lõplike 0, 1-jadade hulk $\{0, 1\}^*$.

Kõigi k -elemendiliste 0, 1-jadade hulka tähistame $\{0, 1\}^k$. Arvestame ka 0 pikkusega jada, mida tähistame tavaliselt ϵ . Seega

$$\{0, 1\}^* = \bigcup_{k \in \mathbb{N}} \{0, 1\}^k,$$

kus $\mathbb{N} = \{0, 1, 2, \dots\}$ on kõigi naturaalarvude hulk.

Mittearvutatavad Funktsioonid

Kaugeltki mitte kõik funktsioonid $\mathbb{N} \xrightarrow{f} \mathbb{N}$ ei ole arvutatavad.

See tuleneb juba ainuüksi faktist, et kõigi selliste funktsioonide hulk $\mathbb{N}^{\mathbb{N}}$ on mitteloenduv, samal ajal kui lõplikke programme on ainult loenduv hulk.

Cantori diagonaalne tõestus hulgateooriast näitab, et kõigi funktsioonide $\mathbb{N} \rightarrow \{0, 1\}$ hulka ei ole võimalik nummerdada naturaalarvudega.

On konkreetseid (ja vajalikke) funktsioone, mis ei ole arvutatavad. Näiteks programmi peatumise probleemi lahendav funktsioon.

Turingi Masin

Arvuti enimkasutatav matemaatiline mudel on nn *Turingi masin*—teatud liiki lõplik automaat M koos lõpmatu järjestikmäliga (nn. *lint*), millele ligipääs on võimalik “kursori” (või ka “pea”) kaudu.

- Lint — jada $L = (\ell_0, \ell_1, \ell_2, \dots)$, mille iga element $\ell_i \in \{0, 1, \epsilon\}$. Igal arvutussammul võib muuta ainult seda pesa, millel on kursor, st pesa ℓ_k .
- Kursor k on naturaalarv, mis näitab, millise pesaga masin parasjagu tegeleb. Igal arvutussammul saab kursorit nihutada paremale (st $k := k + 1$), vasakule $k := k - 1$ või jätta paigale (k jääb muutumatuks). Arvutuse esimesel sammul $k = 0$.
- Igal sammul on masin mingis olekus $s \in S$, kus S on mingi lõplik hulk. Algolekut tähistame s_0 ja lõppolekut h .

Turingi Masina Programm

Järgmise sammu olek s' , lindi seis l'_k ja kursori asend k' arvutatakse funktsioonidega

$$s' := \delta_s(s, l_k) \in S$$

$$l'_k := \delta_l(s, l_k) \in \{0, 1, \epsilon\}$$

$$k' := k + \delta_k(s, l_k) \in \{k - 1, k, k + 1\}, \text{ st. } \delta_k(s, l_k) \in \{-1, 0, +1\}.$$

Lindi algseisu loetakse masina sisendiks ja lõppseisu väljundiks. Näiteks funktsiooni $\mathbb{N} \xrightarrow{f} \mathbb{N}$ arvutatavus tähendab seda, et leidub Turingi masin M , mis teisendab lindile L salvestatud arvu $x \in \mathbb{N}$ koodi arvu $y = f(x)$ koodiks, mis on lindil sel hetkel, kui masin jõuab olekusse h .

Nullfunktsiooni Arvutatavus

Näiteks nullfunktsioon $f(x) = 0, \forall x \in \mathbb{N}$ on arvutatav, sest leidub teda arvutatav kahe-olekuline Turingi masin:

s	ℓ_k	s'	ℓ'_k	$(k' - k)$
s_0	0	s_1	0	+1
	1	s_1	0	+1
	ϵ	h	0	0
s_1	0	s_1	ϵ	+1
	1	s_1	ϵ	+1
	ϵ	h	ϵ	0

Siin on eeldatud, et lindil L on esialgu arvu x kood, mis lõpeb tühja pesaga. Lindi lõpupoole võib olla veel mittetühje pesasid, kuid need ei tule kodeerimise/dekodeerimise juures arvesse.

Kaks Harjutust

Harjutus 1: Leida Turingi masin, mis arvutab funktsiooni $y = 2x + 1$, eeldades, et arv $x = b_0 2^0 + b_1 2^1 + \dots + b_n 2^n$ (kus $b_i \in \{0, 1\}$) kodeeritakse lindi seisuga $L = (b_n, b_{n-1}, \dots, b_1, b_0, \epsilon, \epsilon, \dots)$.

Harjutus 2: Sama, mis eelmises ülesandes, kasutades kodeeringut vastupidises bittide järjestuses, et $L = (b_0, b_1, \dots, b_{n-1}, b_n, \epsilon, \epsilon, \dots)$.

Turingi Tees

Ehkki Turingi masin võib näida ülilihtsa arvutusseadmena, usutakse, et tema abil saab arvutada absoluutselt kõike, mis on kuidagi arvutatav.

Sellist uskumust nimetatakse *Turingi teesiks*.

Et see tees ise ei ole matemaatiline lause (“kuidagi arvutatav” ei ole defineeritud), siis ei saa ka seda teesi matemaatiliselt tõestada.

Edaspidi me lihtsalt usume seda teesi ja enamikul juhtudest ei süvene Turingi masinate “siseellu”.

Pseudokood

Programmide kirjeldamiseks kasutame programmeerimiskeelt meenutavat pseudokoodi. Näiteks võiks nullfunktsiooni arvutavat Turingi masinat esitada järgmise pseudokoodina:

$k := 0$

s0: **IF** $L[k] = \epsilon$ **THEN** $L[k] := 0$, **HALT**

ELSE $k := k + 1$, **GOTO** s1

s1: **IF** $L[k] = \epsilon$ **THEN** **HALT**

ELSE $L[k] := \epsilon$, $k := k + 1$, **GOTO** s1

Keeled ja Ülesanded

Olgu $L \subseteq \{0, 1\}^*$ mingi keel, st suvaline 0, 1-jadade hulk. Ütleme, et Turingi masin M *tuvastab keele* L , kui iga $x \in \{0, 1\}^*$ korral

$$M(x) = 1 \Leftrightarrow x \in L,$$

kus tähise $M(x)$ all mõeldakse Turingi masina M väljundit, eeldades, et sisend on x . Eeldame, sisendi ja väljundi lõpuks loetakse esimest (minimaalse indeksiga) tühja pesa. Esimesele tühikule järgnev lindi sisu ei ole oluline.

Kombinatorikaülesannete lahendamist saab enamasti formuleerida keele tuvastamise ülesandena. Selleks tuleb eelnevalt kokku leppida, kuidas kodeeritakse kombinatorikaülesanne keele sõneks.

Arvutusaeg ja keerukus

Olgu M Turingi masin ja x mingi sisend. Turingi masina M arvutusajaks $T(M(x))$ kohal x nimetatakse masina M poolt sooritatud arvutussammude arvu, kuni masina peatumiseni (jõudmiseni olekusse h).

Turingi masina M asümptootiliseks (ajaliseks) keerukuseks nimetatakse funktsiooni $\mathbb{N} \xrightarrow{T} \mathbb{N}$, nii et iga $n \in \mathbb{N}$ korral

$$T_M(n) = \max\{T(M(x)) : x \in \{0, 1\}^n\}.$$

Sel viisil defineeritud keerukust nimetatakse ka *halvima juhu* keerukuseks (*worst case complexity*), sest iga n korral läheb siin arvesse raskeim juht. Alternatiivne lähenemine on nn. *keskmise keerukus* (*average case complexity*).

O -tähistused ja klass P

Olgu $f(n)$ ja $g(n)$ mingid funktsioonid tüüpi $\mathbb{N} \rightarrow \mathbb{N}$. Võtame kasutusele järgmised tähistused:

$$f(n) = O(g(n)) \equiv \exists c, n_0 \in \mathbb{N}: \forall n \geq n_0: f(n) \leq c \cdot g(n)$$

$$f(n) = \Omega(g(n)) \equiv g(n) = O(f(n))$$

$$f(n) = \Theta(g(n)) \equiv f(n) = O(g(n)) = \Omega(g(n))$$

$$f(n) = \omega(g(n)) \equiv \lim_{n \rightarrow \infty} \frac{g(n)}{f(n)} = 0 .$$

Klass P : Keel $L \subseteq \{0, 1\}^*$ loetakse kuuluvaks klassi P , kui leidub keelt L tuvastav Turingi masin M asümptootilise keerukusega $T_M(n) = n^{O(1)}$.

Mittedeterministlik Turingi Masin

Matemaatiline mudel, mis esitab teatud ebarealistlikult võimasat arvutit, millel on piiramatu võime “kahestuda” ja jätkata arvutusi paralleelselt kahes erinevas harus (mis omakorda võivad ise hiljem “kahestuda”).

Järgmist olekut arvutav funktsioon δ annab järgmise oleku asemel vastuseks *olekute paari*, mis langevad kokku, kui hargnemist ei toimu.

Turingi masin siirdub mõlemasse uude olekusse samaaegselt ja jätkab sõltumatult tööd mõlemas olekus, st kui valida hargnemisel alati ainult üks haru, siis muutub masina olek ja lindi seis täpselt nii nagu teisi harusid ei olekski olemas.

Mittedeterministlik Turingi masin *tuvastab keelt* L , kui $x \in L$ parajasti siis, kui kõik harud lõpetavad töö ja leidub haru, milles lõpuks väljastatakse 1.

Nullkoha Leidmine Mittedeterministliku Masinaga

Mittedeterministlik programm funktsiooni $\{0, 1\}^* \xrightarrow{f} \{0, 1\}$ nullkoha $x \in \{0, 1\}^n$ olemasolu kindlakstegemiseks:

$x := \epsilon$

L2: IF $n > 0$ **GOTO** L0, L1

ELSE GOTO L3

L0: $x := x||'0'$ $n := n - 1$

GOTO L2

L1: $x := x||'1'$ $n := n - 1$

GOTO L2

L3: IF $f(x) = 0$ **RETURN** 1

HALT

Mittedeterministliku Masina Tööaeg

Mittedeterministliku Turingi masina N tööajaks $T(N(x))$ kohal x nimetatakse maksimaalse arvutussammudega haru pikkust, eeldusel et sisendiks on x . Turingi masina N asümptootiliseks ajaliseks keerukuseks (või ka lihtsalt *tööajaks*) $T_N(n)$ nimetatakse funktsiooni $\mathbb{N} \xrightarrow{T} \mathbb{N}$, nii et iga $n \in \mathbb{N}$ korral

$$T_N(n) = \max\{T(N(x)) : x \in \{0, 1\}^n\}.$$

Klass NP

Klass NP: Keel L loetakse kuuluvaks klassi NP, kui leidub keelt L tuvas-tav mittedeterministlik Turingi masin N tööajaga $T_N(n) = n^{\mathcal{O}(1)}$.

Tegelikult saab klassi NP defineerida ka mittedeterministliku Turingi masina mõistet kasutamata.

Paneme tähele, et kui masin N teeb pikimas harus ℓ sammu, siis saab iga haru kodeerida jadaga $a \in \{0, 1\}^\ell$.

Kui iga n korral $T_N(n) \leq p(n)$, kus $p(n)$ on mingi funktsioon, siis mis tahes sisendi $x \in \{0, 1\}^n$ korral saab iga haru esitada jadaga $a \in \{0, 1\}^{p(n)}$.

Jada a mingi bitt ütleb kumba haru kahest võimalikust harust tuleb valida.

Mittedeterministliku Masina Haru Simuleerimine

Teoreem: Iga polünoomiaalses ajas töötava mittedeterministliku Turingi masina N korral leidub (tavaline) polünoomiaalses ajas töötav Turingi masin M ja polünoom $p(n)$, nii et iga $n \in \mathbb{N}$, iga $a \in \{0, 1\}^a$ ja iga $x \in \{0, 1\}^n$ korral: $M(x, a) = 1$ parajasti siis kui $N(x)$ haru koodiga a aktsepteerib x .

Tõestus: Masin M konstrueeritakse masinast N järgmiselt. Iga hargnemiskäsu (järjekorranumbriga i) asemel valitakse vaid üks haru — see, millele osutab bitt $a[i] \in \{0, 1\}$, kus a on masina M teine sisendväärtus. Et masina N tööaeg on polünoomiaalne, siis leidub seda tööaega ülalt tõkestav polünoom $p(n)$. Iga N käsu simuleerimiseks kulub lisaaeg, mis on vajalik $a[i]$ järgmise biti lugemiseks. Seega on M tööaeg polünoomiaalne.

Mittedeterministliku Masina Dekompositsioon

"Aadressi" a fikseerimine muudab masina tavaliseks Turingi masinaks M .

Seda kõike võib ette kujutada ka nii, et iga mittedeterministliku Turingi masina programm on kaheosaline:

- Esimeses (mittedeterministlikus) osas genereeritakse kõikvõimalikud $a \in \{0, 1\}^{p(n)}$ väärtused. Seda saab teha analoogilise programmijupi abil, mida kasutasime funktsiooni nullkoha otsimisel.
- Teises (determineeritud) osas arvutatakse tavalise Turingi masina M (mis ei sisalda hargnevat GOTO käsku) abil välja $y = M(a, x)$.

Klassi NP alternatiivne definitsioon: I

Klass NP: $L \in \text{NP}$ parajasti siis kui leidub (tavaline) Turingi masin M tööajaga $T_M(n) = n^{O(1)}$ ja polünoom $p(n)$, nii et iga $x \in \{0, 1\}^n$ korral:

$$x \in L \Leftrightarrow \exists a \in \{0, 1\}^{p(n)} : M(x, a) = 1 .$$

Ekvivalentsus esialgse definitsiooniga: Kui $L \in \text{NP}$, siis leidub polünomiaalses ajas töötav mittedeterministlik Turingi masin N , nii et $x \in L$ parajasti siis, kui $N(x)$ aktsepteerib x . Järelikult leidub polünoom $p(n)$ ja tavaline polünomiaalses ajas töötav Turingi masin M , nii et $M(x, a)$ väljund langeb kokku $N(x)$ selle haru väljundiga, mille kood on a .

Kui aga leidub M (uue definitsiooni järgi), siis koostame mittedeterministliku masina N nii, et N esmalt kahestub seni, kuni harudes on olemas kõikvõimalikud a väärtused ja seejärel arvutab $M(x, a)$ kasutades M koodi (tabelit).

Klassi NP alternatiivne definitsioon: II

Klass NP: $L \in \text{NP}$ parajasti siis kui leidub (tavaline) Turingi masin V (verifitseerija) tööajaga $T_M(n) = n^{\mathcal{O}(1)}$, polünoom $p(n)$, ja piiramatu tööajaga Turingi masin P (tõestaja), nii et nii et iga $x \in \{0, 1\}^n$ korral:

$$x \in L \Leftrightarrow V(x, P(x)) = 1 .$$

kus bitijada $a = P(x) \in \{0, 1\}^{p(n)}$ nimetatakse **sertifikaadiks**.

Põhjendus: Kui $L \in \text{NP}$ vanas mõttes, siis leidub polünoomiaalne M , nii et $x \in L$ parajasti siis kui $M(x, a) = 1$ mingi $a \in \{0, 1\}^{p(n)}$ korral. Võtame $V \equiv M$ ja P olgu algoritm, mis vaatab läbi kõikvõimalikud a -d ja võimaluse korral väljastab "õige" a .

Kui aga $L \in \text{NP}$ uues mõttes, siis piisab tähelepanekust, et P -d saab simuleerida mittedeterministliku Turingi masinaga.

P versus NP

Tänapäevani ei teata, kas klassid P ja NP on võrdsed või mitte.

Et paremini mõista lauset $P = NP$, esitame selle lause kaks versiooni, mis tegelikult on ekvivalentsed:

- **Otsustusversioon:** Igale polünomiaalsele Turingi masinale F , mis arvutab funktsioonide peret $f_n: \{0, 1\}^n \times \{0, 1\}^{p(n)} \rightarrow \{0, 1\}$ leidub polünomiaalne Turingi masin D , nii et iga $x \in \{0, 1\}^n$ korral

$$D(x) = 1 \Leftrightarrow \exists a \in \{0, 1\}^{p(n)} : F(x, a) = 1 .$$

- **Otsinguversioon.** Igale polünomiaalsele Turingi masinale F , mis arvutab funktsioonide peret $f_n: \{0, 1\}^n \times \{0, 1\}^{p(n)} \rightarrow \{0, 1\}$ leidub polünomiaalne Turingi masin S , nii et iga $x \in \{0, 1\}^n$ korral

$$F(x, S(x)) = 1 \Leftrightarrow \exists a \in \{0, 1\}^{p(n)} : F(x, a) = 1 .$$

Kaks ülesannet

Ülesanne 1: Tõesta, et $P = NP$ otsustus- ja otsinguversioonid on sama-väärsed laused, st üks järeldub teisest.

Ülesanne 2: Tõesta, et kui $P = NP$, kui F on polünoomiaalne Turingi masin, mis arvutab funktsioonide peret $\{0, 1\}^n \xrightarrow{f_n} \{0, 1\}^{p(n)}$, siis leidub polünoomiaalne Turingi masin G , nii et iga $x \in \{0, 1\}^n$ korral

$$F(x) = F(G(F(x))) .$$

See tulemus tähendab sisuliselt seda, et kui $P = NP$, siis on iga efektiivselt arvutatav funktsioon ka kergesti pööratav ja tänapäeva krüptograafia jaoks nii olulisi ühesuunalisi funktsioone ei oleks olemas.

Stohhastiline Turingi masin

Stohhastiline Turingi masin on abstraktne arvutusseade, mis on lähedane mittedetermineeritud Turingi masinale, kuid kus kaheks hargnemise tähendus on erinev — selle asemel et paralleelselt täita mõlemat haru, valib masin juhuslikult ühe harudest (tõenäosusega $\frac{1}{2}$).

Pea igas reaalses tänapäeva arvutis ja programmeerimiskeeles on võimalik kasutada juhuarve.

Nii nagu mittedeterministlikku Turingi masinat, saab ka stohhastilist Turingi masinat defineerida tavalise Turingi masina abil.

Kui vastava mittedetermineeritud masina tööaeg on $p(n)$, siis saab stohhastiline Turingi masin teha ülimalt $p(n)$ mündiviset, st masina väljund on üheselt määratud, kui me teame sisendit x ja mündivisete tulemusi kodeerivat 0, 1-jada $a \in \{0, 1\}^{p(n)}$.

Polünomiaalne stohhastiline Turingi masin

Stohhastiline Turingi masin N tööajaga $t(n)$ on "arvutusseade", mis saades sisendiks $x \in \{0, 1\}^n$, valib juhuslikult ja ühtlase jaotusega $a \in \{0, 1\}^{t(n)}$, arvutab väljundi $N(x) = M(a, x)$, mis üldiselt sõltub nii sisendist x kui ka suurusest a .

Seega, $y \leftarrow N(x)$ ei ole funktsioon, vaid pigem juhuslik katse, mis võib sisendile x vastavusse seada erinevaid väljundväärtusi. Tõenäosus $P(y|x)$ et $N(x) = y$ avaldub seega järgmiselt:

$$P(y|x) = \Pr[y \leftarrow N(x)] = \Pr_a[M(a, x) = y] ,$$

kus tõenäosus arvutatakse üle kõikvõimalike $a \in \{0, 1\}^{t(n)}$.

Kui $t(n) = n^{\mathcal{O}(1)}$, siis masinat N nimetatakse *polünomiaalseks stohhastiliseks Turingi masinaks*.

Klass RP

Def: Keel $L \subseteq \{0, 1\}^*$ kuulub klassi **RP** kui leidub polünoomiaalne stohhastiline Turingi masin N , nii et iga $x \in \{0, 1\}^*$ korral:

- $x \in L \Rightarrow \Pr[1 \leftarrow N(x)] > \frac{1}{2}$
- $x \notin L \Rightarrow \Pr[1 \leftarrow N(x)] = 0$.

Sellise omadusega Turingi masinat nimetatakse ka *Monte Carlo* masinaks.

Monte Carlo algoritmi iseärasus seisneb selles, et kui saame vastuseks $1 \leftarrow N(x)$, siis on kindlalt teada, et $x \in L$. Kui aga $0 \leftarrow N(x)$, siis on mingi tõenäosusega teada, et $x \notin L$.

Kasutades algoritmi k korda (iga kord sõltumatute juhuarvudega), siis vea tõenäosus on $(1 - \epsilon)^k$, kus $\epsilon < 0.5$ on tõenäosus, et $x \in L$ ja $0 \leftarrow N(x)$.

Klassid coRP ja ZPP

Def: Keele $L \subseteq \{0, 1\}^*$ kuulub klassi coRP kui leidub polünoomiaalne stohhastiline Turingi masin N , nii et iga $x \in \{0, 1\}^*$ korral:

- $x \in L \Rightarrow \Pr[1 \leftarrow N(x)] = 1$;
- $x \notin L \Rightarrow \Pr[1 \leftarrow N(x)] < \frac{1}{2}$.

Def: Keele $L \subseteq \{0, 1\}^*$ täiendiks \bar{L} nimetatakse kõigi selliste lõplike $0, 1$ -jadage hulka, mis ei ole L elemendid.

$L \in \text{coRP}$ parajasti siis kui $\bar{L} \in \text{RP}$.

Def: $\text{ZPP} = \text{RP} \cap \text{coRP}$. Kui leiduvad Monte Carlo masinad N_1 keele L jaoks ja N_0 keele \bar{L} jaoks, siis rakendades neid (näiteks vaheldumisi) k korda sisendile x . Saame algoritmi, mis tõenäosusega $1 - 2^{-k}$ annab kindla vastuse ühele lauseist $x \in L$ ja $x \notin L$. Sellist algoritmi nimetatakse **Las Vegase algoritmiks**.

Klass PP

Def: Keel $L \subseteq \{0, 1\}^*$ kuulub klassi **PP** kui leidub polünoomiaalne stohhastiline Turingi masin N , nii et:

$$x \in L \Leftrightarrow \Pr[1 \leftarrow N(x)] > \frac{1}{2}.$$

Kui klassid **RP**, **coRP** ja **ZPP** esitasid ka praktikas hästi töötavaid stohhastilisi algoritme, siis klassi **PP** definitsioon ei anna praktikas töötavat algoritmi. Aktsepteerimise ja mitteaktsepteerimise tõenäosuste vahe võib olla väga väike. Statistika ei tööta!

NB! $L \in \mathbf{NP}$ parajasti siis, kui leidub polünoomiaalne stohhastiline Turingi masin N , nii et iga $x \in \{0, 1\}^n$ korral $x \in L \Leftrightarrow \Pr[1 \leftarrow N(x)] > 0$.

Ülesanne: Tõesta, et $\mathbf{NP} \subseteq \mathbf{PP}$.

Klass BPP

Klasside **RP** ja **coRP** definitsioonis esinev stohhastiline algoritm N on nn. *ühepoolse veaga*:

- **RP** definitsioonis töötab $N(x)$ alati korrektselt juhul kui $x \notin L$;
- **coRP** definitsioonis töötab $N(x)$ korrektselt kui $x \in L$.

Järgnevalt kirjeldatav keerukusklass **BPP** on aga defineeritud stohhastilise Turingi masina N abil, mis mõlemal juhul ($x \in L$ ja $x \notin L$) töötab korrektselt tõenäosusega $\frac{3}{4}$.

Def: Keel $L \subseteq \{0, 1\}^*$ kuulub klassi **BPP** kui leidub polünoomiaalne stohhastiline Turingi masin N , nii et iga $x \in \{0, 1\}^n$ korral:

- $x \in L \Rightarrow \Pr[1 \leftarrow N(x)] > \frac{3}{4}$;
- $x \notin L \Rightarrow \Pr[1 \leftarrow N(x)] < \frac{1}{4}$.

Hääletusalgoritm

Olgu $L \in \text{BPP}$ ja N vastav polünoomiaalne stohhastiline Turingi masin, st iga $x \in \{0, 1\}^n$ korral, tõenäosusega vähemalt $\frac{3}{4}$ on $N(x)$ korrektne vastus küsimusele kas $x \in L$.

Algoritmi korrektsust saab parandada järgmise, nn. *hääletusalgoritmi* abil:

- arvutame $N(x)$ paaritu arv m korda ja salvestame tulemused:

$$b_1 \leftarrow N(x), b_2 \leftarrow N(x), \dots, b_m \leftarrow N(x) .$$

- Kui üle poolte b_i -dest on 1-d, st kui $\sum_{i=1}^m b_i > \frac{m}{2}$ siis väljastame 1;
- Vastasel korral väljastame 0.

Küsimus: Kui suur tuleb valida m , et saavutada etteantud usaldusväärsust?

Hääletusalgoritmi analüüs

Teoreem (Tšernovi tõke) (Chernoff bound) Olgu x_1, \dots, x_m sõltumatud juhuslikud suurused, mille väärtus on kas 1 või 0 vastavalt tõenäosusega p ja $1 - p$. Siis iga $0 \leq \Theta \leq 1$ korral

$$\Pr \left[\sum_{i=1}^m x_i \geq (1 + \Theta)pm \right] \leq e^{-\frac{\Theta^2}{3}pm} .$$

Hääletusalgoritmi analüüs: Olgu $x_i \in \{0, 1\}$ juhuslik suurus, mis = 1 parajasti siis kui i -ndal katsel $N(x)$ vastab küsimusele "Kas $x \in L$?" valesti, st kui $N(x) \neq [x \in L]$. Vastavalt BPP def-ile $p = \Pr[x_i = 1] < \frac{1}{4}$. Võttes $\Theta = 1$, saame

$$\Pr \left[\sum_{i=1}^m x_i \geq \frac{m}{2} \right] \leq e^{-\frac{m}{12}} .$$

Seega eksib hääletusalgoritmi tõenäosusega $< e^{-\frac{m}{12}}$.

Klass BPP_ϵ

Olgu $\epsilon: \mathbb{N} \rightarrow [0 \dots 1]$ mingi funktsioon.

Def: Keel $L \subseteq \{0, 1\}^*$ kuulub klassi BPP_ϵ kui leidub polünoomiaalne stohastiline Turingi masin N , nii et iga $x \in \{0, 1\}^n$ korral:

- $x \in L \Rightarrow \Pr[N(x) = 1] > 1 - \epsilon(|x|)$;
- $x \notin L \Rightarrow \Pr[N(x) = 1] < \epsilon(|x|)$.

Ülesanne: Tõesta järgmised laused:

- Kui $\epsilon(n) = 2^{-n^{O(1)}}$, siis $\text{BPP}_\epsilon = \text{BPP}$.
- Kui $\epsilon(n) = n^{-O(1)}$, siis $\text{BPP}_{\frac{1}{2}-\epsilon} = \text{BPP}$.

Arvutused nõuannetega

Keel $L \subseteq \{0, 1\}^*$ loetakse kuuluvat klassi \mathbf{P}/\mathbf{Poly} , kui leidub polünomiaalne Turingi masin M , polünoom $p(n)$ ja jada $a = (a_1, a_2, \dots, a_n, \dots)$, kus $a_n \in \{0, 1\}^{p(n)}$, nii et iga $x \in \{0, 1\}^n$ korral:

$$x \in L \Leftrightarrow M(x, a_n) = 1.$$

Jada a elemente nimetatakse nõuanneteks (ingl. *advice*).

NB! Klass \mathbf{P}/\mathbf{Poly} sisaldab keeli, mis ei ole äratuntavad tavalise Turingi masinaga.

Olgu L mingi keel, mis ei ole tuvastatav Turingi masinaga. Olgu $\text{Code}: \mathbb{N} \rightarrow \{0, 1\}^*$ mingi kodeerimisviis, nii et $\text{Code}(\mathbb{N}) = \{0, 1\}^*$.

Defineerime jada (a_0, a_1, \dots) , nii et $a_n \in \{0, 1\}$ ja $a_n = 1$ parajasti siis, kui $\text{Code}(n) \in L$. On selge, et U ei ole äratuntav ühegi tavalise Turingi masinaga, sest see tähendaks ka keele L äratuntavust, mille me aga välistasime.

Teiselt poolt, on lihtne koostada algoritmi M , mis sisendi (x, a) korral kontrollib, kas $x = 1^n$ mingi n korral ja väljastab 1, kui $a = 1$. Kõigil muudel juhtudel $M(a, x) = 0$.

BPP \subseteq P/Poly

Teoreem: BPP \subseteq P/Poly.

Tõestus: Olgu $L \in \text{BPP}$. Et $\text{BPP} = \text{BPP}_{2^{-n}}$, siis leidub polünoomiaalne turingi masin M tööajaga $t(n)$, nii et iga $x \in \{0, 1\}^n$ korral on vea tõenäosus:

$$\Pr_a [M(x, a) \neq [x \in L]] < 2^{-n} .$$

Seega,

$$\Pr_a [\exists x \in \{0, 1\}^n : M(x, a) \neq [x \in L]] < \sum_{x \in \{0, 1\}^n} 2^{-n} = 1 .$$

Järelikult leidub $a_n \in \{0, 1\}^{t(n)}$, nii et iga $x \in \{0, 1\}^n$ korral

$$M(x, a_n) = [x \in L] .$$

Seega, masin M nõuannete jadaga $a = (a_0, a_1, \dots)$ tuvastab keele L ja seetõttu $L \in \text{P/Poly}$.

Tõenäosusteooria: Markovi võrratus

Markovi võrratus: Olgu X positiivsete reaalarvuliste väärtustega juhuslik suurus, mille erinevate väärtuste hulk on loenduv. Siis iga $k > 0$ korral

$$\Pr[X \geq k \cdot \mathbf{E}(x)] \leq \frac{1}{k} ,$$

Tõestus:

$$\begin{aligned} \mathbf{E}(x) &= \sum_x x \cdot \Pr[x] = \sum_{x < k \cdot \mathbf{E}(x)} x \cdot \Pr[x] + \sum_{x \geq k \cdot \mathbf{E}(x)} x \cdot \Pr[x] \geq \\ &\geq k \cdot \mathbf{E}(x) \cdot \Pr[X \geq k \cdot \mathbf{E}(x)] . \end{aligned}$$

Järeldus: Olgu $X \geq 0$ mingi mittenegatiivne lõpliku keskväärtusega $\mathbf{E}[X]$ juhuslik suurus. Siis iga $\alpha > 0$ korral

$$\Pr[X \geq \alpha] \leq \frac{1}{\alpha} \mathbf{E}[X] .$$

Tõenäosusteooria: Kaks abivõrratust

Lemma 1: Iga $0 \leq \Theta \leq 1$ korral: $-\frac{\Theta^2}{2} \leq \Theta - (1 + \Theta) \ln(1 + \Theta) \leq -\frac{\Theta^2}{3}$.

Tõestus: Kõigepealt paneme tähele, et:

$$\begin{aligned} \Theta - (1 + \Theta) \ln(1 + \Theta) &= \Theta - (1 + \Theta) \cdot \left(\frac{\Theta}{1} - \frac{\Theta^2}{2} + \frac{\Theta^3}{3} - \frac{\Theta^4}{4} + \dots \right) \\ &= -\frac{\Theta^2}{1 \cdot 2} + \frac{\Theta^3}{2 \cdot 3} - \frac{\Theta^4}{3 \cdot 4} + \frac{\Theta^5}{4 \cdot 5} \dots \\ &= \sum_{n=2}^{\infty} (-1)^{n-1} \frac{\Theta^n}{n(n-1)}. \end{aligned}$$

Et rida $r = \frac{\Theta^3}{2 \cdot 3} - \frac{\Theta^4}{3 \cdot 4} + \frac{\Theta^5}{4 \cdot 5} \dots$ on vahelduvate märkidega ja tema liikmete absoluutväärtused on kahanevad, * siis järelikult on selle rea summa

*Võrratus $\frac{\Theta^n}{(n-1)n} \geq \frac{\Theta^{n+1}}{n(n+1)}$ tuleneb otseselt võrratusest $\frac{n-1}{n+1}\Theta \leq 1$.

positiivne, sest tema esimene liige on positiivne. Järelikult:

$$\Theta - (1 + \Theta) \ln(1 + \Theta) = -\frac{\Theta^2}{2} + r \geq -\frac{\Theta^2}{2}.$$

Samal põhjusel võib väita, et rea $s = \frac{\Theta^4}{3 \cdot 4} - \frac{\Theta^5}{4 \cdot 5} + \frac{\Theta^6}{4 \cdot 5} - \dots$ summa on positiivne, mistõttu:

$$\begin{aligned} \Theta - (1 + \Theta) \ln(1 + \Theta) &= -\frac{\Theta^2}{2} + \frac{\Theta^3}{3} - s \leq -\frac{\Theta^2}{2} + \frac{\Theta^3}{3} \\ &\leq -\frac{\Theta^2}{2} + \frac{\Theta^2}{3} = -\frac{\Theta^2}{6}. \end{aligned}$$

Lemma 2: Iga $0 \leq \Theta \leq 1$ korral: $\Theta - (1 - \Theta) \ln(1 - \Theta) \geq \frac{\Theta^2}{2}$.

Tõestus Võrratus järeldub vahetult järgmisest tähelepanekust:

$$\Theta - (1 - \Theta) \ln(1 - \Theta) = \frac{\Theta^2}{2 \cdot 1} + \frac{\Theta^3}{3 \cdot 2} + \frac{\Theta^4}{4 \cdot 3} + \dots = \sum_{n=2}^{\infty} \frac{\Theta^n}{n(n-1)}.$$

Tõenäosusteooria: Tšernovi tõkked

Teoreem: Olgu x_1, \dots, x_m sõltumatud juhuslikud suurused, mille väärtus on kas 1 või 0 vastavalt tõenäosustega p ja $1 - p$. Olgu $X = \sum_{i=1}^m x_i$. Siis iga $0 \leq \Theta \leq 1$ korral kehtivad võrratused:

$$\Pr[X \geq (1 + \Theta)pm] \leq e^{-\frac{\Theta^2}{3}pm} \quad (1)$$

$$\Pr[X \leq (1 - \Theta)pm] \leq e^{-\frac{\Theta^2}{2}pm} . \quad (2)$$

Tõestus: (1): Kui $t \in \mathbb{R}^+$, siis $\Pr[X \geq (1 + \Theta)pm] = \Pr[e^{tX} \geq e^{t(1+\Theta)pm}]$. Markovi võrratusest saame, et $\Pr[e^{tX} \geq k \cdot \mathbf{E}(e^{tX})] \leq 1/k$ iga $k > 0$ korral. Võtame $k = e^{t(1+\Theta)pm} (\mathbf{E}(e^{tX}))^{-1}$. Siis

$$\Pr[X \geq (1 + \Theta)pm] \leq e^{-t(1+\Theta)pm} \mathbf{E}(e^{tX}) .$$

Et $\mathbf{E}(e^{tX}) = (\mathbf{E}(e^{tx_1}))^m = (1 + p(e^t - 1))^m$, siis tehes asenduse, saame

$$\begin{aligned} \Pr[X \geq (1 + \Theta)pm] &\leq e^{-t(1+\Theta)pm} (1 + p(e^t - 1))^m \\ &\leq e^{-t(1+\Theta)pm} \cdot e^{pm(e^t - 1)}. \end{aligned}$$

Siin kasutatakse asjaolu, et $(1 + a)^m \leq e^{am}$ iga $a > 0$ korral. Lõpuks võttes $t = \ln(1 + \Theta)$, saame **Lemma 1** põhjal, et

$$\Pr[X \geq (1 + \Theta)pm] \leq e^{pm[\Theta - (1+\Theta)\ln(1+\Theta)]} \leq e^{-\frac{\Theta^2}{3}pm}.$$

(2): Kui $t \in \mathbb{R}^+$, siis $\Pr[X \leq (1 - \Theta)pm] = \Pr[pm - X \geq \Theta pm] = \Pr[e^{t(pm-X)} \geq e^{t\Theta pm}]$. Markovi võrratusest saame, et

$$\Pr[e^{t(pm-X)} \geq k \cdot \mathbf{E}(e^{t(pm-X)})] \leq 1/k$$

iga $k > 0$ korral. Võttes $k = e^{t\Theta pm} (\mathbf{E}(e^{t(pm-X)}))^{-1}$ saame

$$\Pr[X \leq (1 - \Theta)pm] \leq e^{-t\Theta pm} \cdot \mathbf{E}(e^{t(pm-X)}) = e^{t(1-\Theta)pm} \cdot \mathbf{E}(e^{-tX}).$$

Et $\mathbf{E}(e^{-tX}) = (\mathbf{E}(e^{-tx_1}))^m = (1 - p(1 - e^{-t}))^m$, siis tehes asenduse, saame

$$\begin{aligned} \Pr[X \leq (1 - \Theta)pm] &\leq e^{-t(1-\Theta)pm} (1 - p(1 - e^{-t}))^m \\ &\leq e^{-t(1-\Theta)pm} \cdot e^{-pm(1-e^{-t})} \\ &= e^{-pm[t(1-\Theta)+1-e^{-t}]} . \end{aligned}$$

Lõpuks võttes $t = -\ln(1 - \Theta)$, saame **Lemma 2** põhjal, et

$$\Pr[X \leq (1 - \Theta)pm] \leq e^{-pm[\Theta - (1-\Theta)\ln(1-\Theta)]} \leq e^{-\frac{\Theta^2}{2}pm} .$$

