Kommunikaatiokompleksisuus

Nuutti Lindroos

LuK-tutkielma
Helmikuu 2024

Tarkastaja:
Dos. Ville Salo

MATEMATIIKAN JA TILASTOTIETEEN LAITOS

Turun yliopiston laatujärjestelmän mukaisesti tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck-järjestelmällä

Sisällys

Johdanto

Tässä Luk-tutkielmassa tutustutaan kommunikaatiokompleksisuuteen. Kommunikaatio tarkoittaa kaikkea mahdollista viestintää eri tahojen välillä kuten vaikkapa puhetta ihmiseltä toiselle tai sähköpostien lähettämistä internetissä. Kompleksisuus on puolestaan varsin uusi mielenkiinnon kohde matematiikassa. Kompleksisuus tarkoittaa sitä, että ongelman ratkaisemisen sijaan tarkastellaan sitä, että kuinka vaikeaa kyseinen ongelma on ratkaista. Tässä tutkielmassa erityisen kiinnostuksen kohteina ovat ylä- ja alarajat viestinnän määrälle, eli kuinka monta bittiä pitää lähettää, että jokin ongelma saadaan ratkaistua ja toisaalta, missä kohtaa menetelmämme muuttuu huonoksi. Yksinkertaisuuden vuoksi tässä tutkielmassa keskitytään kahden viestittäjän, Alisan ja Börjen, väliseen kommunikaatioon. Lisäksi oletetaan, että heillä kummallakin on ääretön määrä laskentatehoa käytössään. Tällöin heidän toisilleen lähettämät viestit siirtyvät tarkastelun keskiöön.

Luvussa 1 tutustutaan tarkemmin tähän kommunikaatiomalliin, jonka esitteli alun perin Andrew Chi-Chih Yao vuonna 1979. Samoin luvussa tu-

tustutaan erilaisiin alarajatekniikoihin ja esitetään yläraja kaikille protokollille.

Luvussa 2 tutustutaan epädeterministiseen kommunikaatiokompleksisuuteen ja esitetään avoin ongelma kommunikaatiokompleksisuuteen liittyen.

Oma päälähteeni on ollut Eyal Kushilevitzin ja Noam Nisanin Communication Complexity (1997), erityisesti sen 2 ensimmäistä lukua [1].

Käsitteitä

Määritelmää 0.1 tarvitaan luvun 2 tuloksien ymmärtämiseen. Kyseessä on siis asymptoottisen suuruusluokan yleinen määrittely, joka saattaa olla lukijalle tuttu algoritmien aikavaativuuksien tarkastelusta. Kommunikaatiokompleksisuuden tapauksessa tutkitaan kuitenkin viestien lähettämiseen käytettävien bittien määrän kasvua algoritmin suoritusajan kasvamisen sijaan.

Määritelmä 0.1. Olkoot f ja $g : \mathbb{R} \to \mathbb{R}$ funktioita. Tällöin voidaan merkitä, että:

1. $f(n) = O(g(n))$, jos on olemassa jokin vakio $c \in \mathbb{R}$, siten että $f(n) \leq c \cdot g(n)$, kun $n \to \infty$.

2. $f(n) = \Theta(g(n))$, jos on olemassa jotkin vakiot $c_1, c_2 \in \mathbb{R}$, siten, että $c_1 \cdot g(n) \leq f(n) \leq c_2 \cdot g(n)$, kun $n \to \infty$.

1 Kommunikaatiomalli ja alarajat

Tässä luvussa kerrotaan, mitä protokollat ovat ja mitä kompleksisuus niiden kohdalla tarkoittaa. Viimeiset kaksi lukua on omistettu kahden erilaisen alarajatekniikan esittelylle.

1.1 Protokollat

Aloitetaan kommunikaatiomallin tarkastelu aivan sen perusteista. Olkoon X, Y ja Z äärellisiä joukkoja ja olkoon $f : X \times Y \to Z$ kuvaus joukoista

X ja Y joukkoon Z. Malli olettaa, että kaksi eri tahoa Alisa ja Börje haluavat laskea funktion f arvon jollakin syötteellä $f(x, y)$, missä $x \in X$ ja $y \in Y$. Ongelmana on se, että Alisa tietää ainoastaan arvon x ja Börje tietää ainoastaan arvon y. Täten laskeakseen funktion f arvon heidän on kommunikoitava keskenään. Kommunikaatio seuraa jotakin ennalta määrättyä protokollaa $\mathcal{P}$, joka on riippuvainen vain ja ainoastaan funktiosta f. Protokolla $\mathcal{P}$ koostuu Alisan ja Börjen toisilleen lähettämistä tiedoista, joiden avulla funktion arvo $f(x, y)$ lopulta määritetään.

Hyvä protokolla määrittää jokaisessa vaiheessa onko laskenta päättynyt. Jos laskenta on päättynyt, niin protokollan täytyy määrittää laskemansa arvo ja jos protokolla ei ole päättynyt, niin sen täytyy kertoa mitä tietoa täytyy lähettää ja mistä kyseinen tieto täytyy lähettää ja minne.

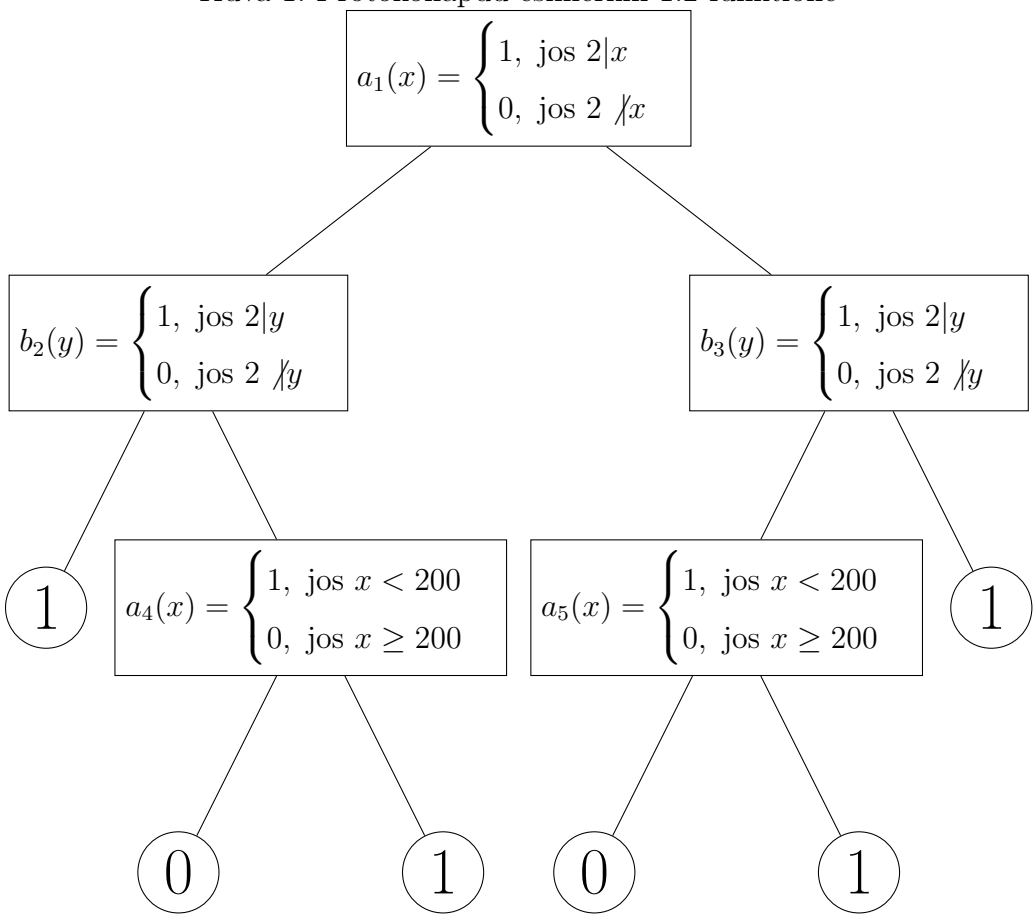
Mallissa haluamme tutkia Alisan ja Börjen toisilleen lähettämien viestien määrää emmekä niinkään sitä, että miten yksittäinen lasku etenee. Tästä syystä oletammekin, että sekä Alisalla että Börjellä on käytettävissään ääretön määrä laskentatehoa eli ainoa laskun etenemistä hidastava tekijä on tiedon puute. Protokollan $\mathcal{P}$ käyttämien bittien määrää syötteelle (x, y) kutsutaan protokollan bittivaativuudeksi. Protokollan $\mathcal{P}$ vaativuus on sen suurin bittivaativuus yli kaikkien syötteiden (x, y). Funktion f kompleksisuus on vaativuudeltaan pienin protokolla, joka laskee funktion f. Intuitiivinen ajatus mallista voidaan formalisoida binääripuiden avulla:

Määritelmä 1.1. Protokolla $\mathcal{P}$ yli määrittelyjoukon $X \times Y$ maalijoukkoon Z on binääripuu, jonka jokainen haara sisältää joko funktion $a_v : X \to \{0, 1\}$ tai funktion $b_v : Y \to \{0, 1\}$ ja jonka jokainen lehti sisältää jonkin alkion $z \in Z$.

Protokollan $\mathcal{P}$ arvo syötteelle (x, y), missä $x \in X$ ja $y \in Y$ on puun lehti, joka määritetään kulkemalla puun haarasta vasemmalle, jos $a_v(x) = 0$ ja oikealle jos $a_v(x) = 1$ sekä vastaavasti kulkemalla vasemmalle, jos $b_v(x) = 0$ ja oikealle jos $b_v(x) = 1$. Protokollan $\mathcal{P}$ bittivaativuus on reitin pituus juurisolmusta lehteen syötteellä (x, y). Protokollan $\mathcal{P}$ vaativuus $D(\mathcal{P})$ on sitä vastaavan binääripuun korkeus.

Lisäksi sanotaan, että protokolla $\mathcal{P}$ laskee funktion $f : X \times Y \to Z$, jos kaikille syöttepareille $x \in X$ ja $y \in Y$ seuraamalla protokollaa $\mathcal{P}$ päästään

Kuva 1: Protokollapuu esimerkin 1.2 funktiolle



johonkin maalijoukon arvoon $z \in Z$, siten että $f(x, y) = z$ ja sekä Alisa että Börje tietävät kyseisen arvon.

Esimerkki 1.2. Alisalle ja Börjelle arvotaan kokonaisluku suljetulta väliltä $[1, 1000]$ ja heidän pitää laskea seuraavan funktion arvo

$$f(x, y) = \begin{cases} 1, \text{ jos x ja y ovat molemmat joko parillisia tai parittomia} \\ 1, \text{ jos } x < 200 \text{ ja eri pariteettia kuin y} \\ 0, \text{ muulloin.} \end{cases}$$

Kuvassa 1 on eräs mahdollinen protokollapuu ongelman ratkaisemiseksi.

Määritelmä 1.3. Funktion $f : X \times Y \to Z$ kompleksisuus on pienin vaativuus yli protokollien, jotka laskevat funktion f. Funktion f kompleksisuutta merkitään $D(f)$. Eli $D(f) = \min\{D(\mathcal{P}) \mid \mathcal{P} \text{ laskee funktion } f\}$.

Helpoin tapa funktion f arvon määrittämiseksi jollekin syötteelle on se, että Alisa lähettää saamansa alkion $x \in X$ Börjelle, minkä jälkeen Börje ratkaisee tehtävän ja lähettää vastauksen Alisalle. Täten voidaan määritellä seuraava yläraja.

Seuraus 1.4. Kaikille funktioille $f : X \times Y \to Z$

$$D(f) \leq \log_2 |X| + \log_2 |Z| .$$

Todistus. Alisa tarvitsee korkeintaan $\log_2 |X|$ bittiä syötteen $x \in X$ lähettämiseen Börjelle, joka ratkaisee tehtävän. Tämän jälkeen Börje lähettää laskemansa vastauksen Alisalle, mikä vaatii $\log_2 |Z|$ bittiä. □

Mallin selkeyttämiseksi tästä eteenpäin ellei toisin todeta oletetaan lisäksi, että funktion f arvo on joko 0 tai 1, eli $f : X \times Y \to \{0, 1\}$. Tämä tulkinta on riittävä sillä funktiolle g, joka ei ole tätä tyyppiä voidaan määritellä apufunktio $g_i(x, y)$, joka laskee luvusta $g(x, y)$ indeksistä i löytyvän bitin arvon.

Seuraus 1.4 esittää ylärajan kaikille funktioille. Luvussa 1.2 lähdetään etsimään alarajaa eri funktioille, eli sitä että kuinka monta bittiä pitää vähintään lähettää ongelman ratkaisemiseksi.

1.2 Suorakulmiot

Tiukkojen alarajojen löytäminen eri protokollille edellyttää kombinatorista lähestymistapaa. Ajatuksena on jakaa lähtöjoukon $X \times Y$ syöteparit x, y joukkoihin siten, että yhdessä joukossa ovat kaikki ne syöteparit, joita laskettaessa protokolla viestittää saman tiedon. Binääripuiden kontekstissa tämä tarkoittaa sitä, että samassa joukossa ovat ne syöteparit, joista protokolla siirtyy samaan lehtisolmuun. Kun lähtöjoukko $X \times Y$ jaetaan tällä tavalla ja otetaan huomioon, että vain Alisa näkee joukon X ja vain Börje näkee joukon Y muodostuu lähtöjoukon ositus, joka koostuu suorakulmioista. Näitä

suorakulmoita kutsutaan kombinatorisiksi suorakulmioiksi. Esitellään aluksi kombinatoriset suorakulmiot yleisesti.

Määritelmä 1.5. Olkoon $\mathcal{P}$ protokolla ja v protokollan $\mathcal{P}$ binääripuun haarasolmu. Tällöin R_v on syötteiden (x, y) joukko, joka saavuttaa haarasolmun v.

Määritelmästä 1.5 voidaan johtaa lause 1.6.

Lause 1.6. Olkoon L protokollan $\mathcal{P}$ lehtisolmujen joukko. Tällöin $\{R_l\}_{l \in L}$ on avaruuden $X \times Y$ ositus.

Kombinatoriset suorakulmiot voidaan määritellä määritelmän 1.5 ja lauseen 1.6 avulla.

Määritelmä 1.7. Kombinatorinen suorakulmio joukossa $X \times Y$ on osajoukko $R \subseteq X \times Y$, jolle $R = A \times B$ joillekin $A \subseteq X$ ja $B \subseteq Y$.

Kombinatorisille suorakulmioille on myös vaihtoehtoinen esitys kuten lause 1.8 osoittaa.

Lause 1.8. $R \subseteq X \times Y$ on kombinatorinen suorakulmio, jos ja vain jos

$$(x_1, y_1) \in R \text{ ja } (x_2, y_2) \in R \Rightarrow (x_1, y_2) \in R.$$

Todistus. Todistetaan molempiin suuntiin. Olkoon R suorakulmio eli $R = A \times B$. Jos on olemassa syötepari $(x_1, y_1) \in R$, niin väistämättä $x_1 \in A$ ja vastaavasti jos $(x_2, y_2) \in R$, niin $y_2 \in B$. Tästä seuraa, että $(x_1, y_2) \in A \times B = R$. Todistetaan vielä toiseen suuntaan. Olkoon

$$A = \{x| \text{ on olemassa } y \text{ siten, että } (x, y) \in R\}$$

ja

$$B = \{y| \text{ on olemassa } x \text{ siten, että } (x, y) \in R\}.$$

Todistetaan, että $R = A \times B$. Joukkojen A ja B määrittelyn perusteella on selvää, että $R \subseteq A \times B$. Todistetaan vielä, että $A \times B \subseteq R$. Olkoon $(x, y) \in A \times B$, koska $x \in A$ on olemassa y' siten, että $(x, y') \in R$. Vastaavasti koska $y \in B$ on olemassa x' siten, että $(x', y) \in R$. Täten oletuksen nojalla $(x, y) \in R$. □

Jatkossa selkeyden nimissä kutsun kombinatorista suorakulmiota vain suorakulmioksi.

Lause 1.9 esittää kommunikaatiokompleksisuuden ja suorakulmioitten välisen yhteyden.

Lause 1.9. Kaikille protokollille $\mathcal{P}$ ja niiden lehtisolmuille l, R_l on suorakulmio.

Todistus. Todistetaan lause käyttämällä induktiota. Juurisolmulle pätee ilmiselvästi, että $R_{juuri} = X \times Y$ on suorakulmio. Olkoon solmu w solmun v äitisolmu ja olkoon solmu v solmun w vasemman puoleinen lapsisolmu sekä lisäksi oletetaan, että solmussa w on Alisan vuoro viestittää, eli solmussa w on funktio $a_w : X \to \{0, 1\}$. Tällöin

$$R_v = R_w \cap \{(x, y) | a_w(x) = 0\}$$

Induktio-oletus on, että $R_w = A_w \times B_w$ ja täten

$$R_v = (A_w \cap \{x | a_w(x) = 0\}) \times B_w,$$

joka on suorakulmio. □

On hyvä huomata, että lauseen 1.9 täsmällinen tulos on se, että kaikki joukot R_v ovat suorakulmioita eivät ainoastaan ne, jotka vastaavat binääripuun lehtisolmuja. Esitetään vielä toinen todistus lauseelle 1.9 käyttäen lausetta 1.8

Todistus. Oletetaan, että $(x_1, y_1) \in R_l$ ja $(x_2, y_2) \in R_l$. Osoitetaan, että oletuksesta seuraa, että $(x_1, y_2) \in R_l$. Toisin sanoen on osoitettava, että protokolla käyttäytyy kaikille edellä luetelluille syötepareille samalla tavalla eli syötepari (x_1, y_2) saavuttaa lehtisolmun l. Jos protokolla on haarasolmussa v ja on Alisan vuoro puhua, niin hän laskee syötteen (x_1, y_1) samalla tavalla kuin hän laskee syötteen (x_1, y_2). Molemmissa tapauksissa Alisa siis laskee funktion $a_v(x_1)$ arvon. Täten Alisan haarasolmuissa protokolla etenee kohti lehtisolmua l. Vastaavasti jos protokolla saavuttaa haarasolmun v, jossa on Börjen vuoro puhua, niin hän laskee syötteen (x_2, y_2) samalla tavalla kuin hän laskee syötteen (x_1, y_2). Molemmissa tapauksissa Börje laskee funktion $b_v(y_2)$

arvon.Täten myös Börjen haarasolmuissa protokolla etenee kohti lehtisolmua l. Täten lauseen 1.8 nojalla R_v on suorakulmio. □

Näiden tuloksien avulla voidaan esittää seuraava määritelmän.

Määritelmä 1.10. Osajoukkoa $R \subseteq X \times Y$ kutsutaan f-monokromaattiseksi tai monokromaattiseksi jos funktio f on vakio joukossa R.

Tämä siis tarkoittaa sitä, että jos protokolla $\mathcal{P}$ laskee funktion f, niin kaikilla protokollan $\mathcal{P}$ lehtisolmuilla l kaikki syöteparit $(x, y) \in R_l$ tuottavat funktiolle f saman arvon, joka on lehtisolmussa l.

Määritelmän 1.10 avulla voidaan aiemmat tulokset tiivistää.

Lemma 1.11. Mikä tahansa protokolla $\mathcal{P}$, joka laskee funktion f, määrittää lähtöavaruuden $X \times Y$ osituksen f-monokromaattisiin suorakulmioihin. Suorakulmioita on yhtä monta kuin protokollan $\mathcal{P}$ binääripuussa on lehtisolmuja.

Seuraus 1.12. Jos avaruuden $X \times Y$ osittamiseen f-monokromaattisiin suorakulmioihin käytetään t kappaletta suorakulmioita, niin $D(f) \geq \log_2 t$.

Todistus. Lemman 1.11 nojalla funktion f laskevan protokollan $\mathcal{P}$ binääripuun lehtisolmut virittävät avaruuden $X \times Y$ osituksen f-monokromaattisiin suorakulmioihin. Täten oletuksen nojalla protokollan $\mathcal{P}$ binääripuussa on oltava t kappaletta lehtisolmuja eli binääripuun korkeus on $\log_2 t$. □

Seuraus 1.12 esittää tavan löytää jonkin alarajan funktion f kommunikaatiokompleksisuudelle: pitää vain löytää jokin alaraja avaruuden $X \times Y$ osituksessa olevien f-monokromaattisten suorakulmioiden määrälle. Seuraavat kappaleet esittävät kaksi erilaista tekniikka monokromaattisten suorakulmioiden määrän arvioimiseksi.

1.3 Huijarijoukot ja suorakulmion koko

Huijarijoukot ovat yksi tekniikka monokromaattisten suorakulmioiden määrän alarajan löytämiseksi. Aiemmat tulokset osoittavat, että jos syöteparit (x_1, y_1) ja (x_2, y_2) kuuluvat samaan monokromaattiseen suorakulmioon, niin

myös (x_1, y_2) ja (x_2, y_1) kuuluvat samaan suorakulmioon. Täten on kääntäen tosi, että jos $f(x_1, y_2) \neq f(x_2, y_1)$, niin (x_1, y_1) ja (x_2, y_2) eivät kuulu samaan suorakulmioon.

Määritelmä 1.13. Olkoon $f : X \times Y \to \{0, 1\}$. Joukkoa $S \subset X \times Y$ kutsutaan huijarijoukoksi, jos on olemassa $z \in \{0, 1\}$, jolle

- Jokaiselle syöteparille $(x, y) \in S$, $f(x, y) = z$
- Jokaiselle erilliselle parille (x_1, y_1) ja (x_2, y_2) joukossa S joko $f(x_1, y_2) \neq z$ tai $f(x_2, y_1) \neq z$.

Lemma 1.14. Jos funktiolla f on huijarijoukko S, jonka koko on t, niin $D(f) \geq \log_2 t$.

Todistus. Riittää osoittaa, että jokainen monokromaattinen suorakulmio sisältää vain yhden alkion joukosta S. Oletetaan, että monokromaattinen suorakulmio R sisältää kaksi erillistä syöteparia (x_1, y_1) ja (x_2, y_2), jotka molemmat kuuluvat joukkoon S. Lauseen 1.8 nojalla suorakulmio R sisältää täten myös syöteparit (x_1, y_2) ja (x_2, y_1). Koska joukko S on huijarijoukko ja $f(x_1, y_1) = f(x_2, y_2) = z$, niin joko $f(x_1, y_1) \neq z$ tai $f(x_2, y_2) \neq z$. Täten suorakulmio R ei voi olla monokromaattinen. Täten joukon S peittäminen vaatii vähintään t kappaletta suorakulmioita ja seurauksen 1.12 nojalla $D(f) \geq \log_2 t$. □

Alarajan löytäminen huijarijoukkotekniikalla on erityistapaus yleisemmästä tavasta alarajan etsimiselle. Ideana on osoittaa, että jokaisen monokromaattisen suorakulmion koko on hyvin pieni ja täten joukon $X \times Y$ositus edellyttää paljon monokromaattisia suorakulmioita. Suorakulmion koon kykenee usein valitsemaan edullisella tavalla ja yleisesti voidaankin käyttää todennäköisyysjakaumaa suorakulmion koon mittana.

Lause 1.15. Olkoon μ joukon $X \times Y$ todennäköisyysjakauma. Jos jokin f-monokromaattinen suorakulmio R on kooltaan $\mu(R) \leq \delta$, niin $D(f) \geq \log_2 1/\delta$.

Todistus. Koska $\mu(X \times Y) = 1$, niin joukon $X \times Y$ ositus f-monokromaattisiin suorakulmioihin edellyttää vähintään $1/\delta$ kappaletta suorakulmioita. Täten seurauksen 1.12 nojalla $D(f) \geq \log_2 1/\delta$. □

Huijarijoukot ovat lauseen 1.15 todennäköisyysjakaumien erikoistapaus. Huijarijoukolle S, jonka koko on t voidaan muodostaa todennäköisyysjakauma μ siten, että $\mu(x, y) = 0$, jos $(x, y) \notin S$ ja $\mu(x, y) = 1/t$, jos $(x, y) \in S$. Lemman 1.14 todistuksen mukaan jokainen monokromaattinen suorakulmio R voi sisältää korkeintaan yhden alkion joukosta S ja täten suorakulmion R koko on sama $\mu(R) = 1/t$.

1.4 Matriisit ja alarajat

Tässä luvussa esitellään toinen tekniikka jonkin funktion f kommunikaatiokompleksisuuden selvittämiseksi. Kuten edellä jälleen etsitään jotain alarajaa monokromaattisten suorakulmioiden määrälle, mutta tällä kertaa lähestymistapa pohjautuu algebraan. Tekniikassa jokaiselle funktiolle $f : X \times Y \to \{0, 1\}$ muodostetaan matriisi M_f. Matriisi M_f on $|X| \times |Y|$ matriisi ja matriisin vaakarivit on indeksoitu joukon X alkioilla ja sen pystyrivit joukon Y alkioilla. Alkiota (x_i, y_j) siis vastaa matriisin M_f solu $a_{i,j} = f(x_i, y_j)$. Näin voidaan määritellä seuraava ominaisuus funktioille.

Määritelmä 1.16. $\mathsf{rank}(f)$ on matriisin M_f aste.

Lemma 1.17. Funktiolle $f : X \times Y \to \{0, 1\}$,

$$D(f) \geq \log_2 \mathsf{rank}(f).$$

Todistus. Olkoon $\mathcal{P}$ protokolla, joka laskee funktion f ja olkoon L_1 niiden lehtisolmujen joukko protokollalle $\mathcal{P}$, missä $(x, y) = 1$. Jokaiselle lehtisolmulle $l \in L_1$ määritetään matriisi M_l siten, että $M_l(x, y) = 1$, jos $(x, y) \in R_l$ ja $M_l(x, y) = 0$ jos $(x, y) \notin R_l$. R_l on siis suorakulmio syötteitä, jotka saavuttavat lehtisolmun l. Näin määriteltynä kaikki syöteparit (x, y), joille $f(x, y) = 0$ ovat nolla kaikissa matriiseissa M_l. Puolestaan kaikki syöteparit (x, y), joille $f(x, y) = 1$ saavat arvon 1 vain yhdessä matriisissa. Toisin sanoen

$$M_f = \sum_{l \in L_1} M_l.$$

Matriisin asteen ominaisuuksien perusteella voidaan siis määrittää yläraja

$$\mathsf{rank}(M_f) \leq \sum_{l \in L_1} \mathsf{rank}(M_l).$$

Lopulta nähdään, että $\mathsf{rank}(M_l) = 1$ eli $\mathsf{rank}(M_f) \leq |L|_1 \leq |L|$. Erityisesti protokollan $\mathcal{P}$ binääripuun täytyy sisältää vähintään $\mathsf{rank}(f)$ lehtisolmua ja täten seurauksen 1.12 nojalla väittämä on tosi. □

Lemma 1.17 antaa alarajan 1-suorakulmioille. Voidaan määritellä funktio $ei(f)$, joka laskee vataavasti 0-suorakulmioiden määrälle alarajan. Matriisien M_f ja $M_{ei(f)}$ asteiden erotus on korkeintaan 1 sillä $M_{ei(f)} = J - M_f$, missä J on 1-matriisi, jonka aste on 1. Täten lemman 1.17 nojalla

$$D(f) \geq \log_2(2\ \mathsf{rank}(f) - 1).$$

2 Epädeterministiset protokollat

Aiemmin esitellyt protokollat ovat olleet deterministisiä, eli protokolla kulkee jokaiselle syötteelle samat askeleet. Epädeterministisessä tapauksessa Alisalla ja Börjellä on jotain ulkopuolista lähtötietoa, joka salli heidän siirtyä suoraan lopputulokseen tai ainakin jättää joitakin protokollan vaiheita suorittamatta. Tässä luvussa tutustutaan epädeterministiseen kommunikaatiokompleksisuuteen ja sen suhteeseen deterministisen kommunikaatiokompleksisuuden kanssa.

2.1 Peitteet

Vaikka jokainen protokolla osittaa joukon $X \times Y$ f-monokromaattisiin suorakulmioihin, niin jokainen joukon $X \times Y$ ositus monokromaattisiin suorakulmioihin ei vastaa mitään protokollaa. Olisikin siis helpompaa, jos monokromaattisten suorakulmioiden sijaan voitaisiin käyttää peitteitä. Peitteet ovat kombinatoriikan kannalta helpommin käsiteltäviä ja niitä tarvitaan epädeterministen protokollien kompleksisuuden laskemiseen.

Määritelmä 2.1 esittelee luvun 2.2 tuloksiin tarvittavat merkinnät.

Määritelmä 2.1. Olkoon $f : X \times Y \to \{0,1\}$ funktio.

1. Merkintä $C^P(f)$ tarkoittaa pienintä määrää lehtisolmuja funktion f laskevassa binääripuussa.

2. Merkintä $C^D(f)$ on pienin määrä erillisiä monokromaattisia suorakulmioita, jotka tarvitaan joukon $X \times Y$ peittämiseen.

3. Merkintä $C(f)$ tarkoittaa pienintä määrää monokromaattisia suorakulmioita, jotka tarvitaan peittämään joukko $X \times Y$ (peitteet voivat olla päällekkäisiä).

4. Alkiolle $z \in \{0,1\}$, merkintä $C^z(f)$ tarkoittaa z-syötteiden peittämiseen vaadittavien monokromaattisten suorakulmioiden määrää (peitteet voivat olla päällekäisiä).

Määritelmästä 2.1 seuraa:

Lause 2.2. Kaikille $f : X \times Y \to \{0,1\}$

1. $C(f) \leq C^D(f) \leq C^P(f) \leq 2^{D(f)}$.

2. $C(f) = C^0(f) + C^1(f)$.

Lauseen 2.2 tulokset ovat suoria seurauksia määritelmästä 2.1 ja määritelmästä 1.3.

2.2 Epädeterministinen kommunikaatiokompleksisuus

Luvulla $C^z(f)$ on luonnollinen tulkinta funktion f epädeterministisenä kommunikaatio kompleksisuutena. Avataan hieman tarkemmin, mitä tällä tarkoitetaan. Lähde [2] on ollut suureksi avuksi seuraava esitystä koottaessa.

Oletetaan, että on olemassa kaikkinäkevä matemaatikko, joka yrittää todistaa Alisalle ja Börjelle, että heille annetut bittijonot x ja y ovat keskenään erisuuret. Tällöin hän voi yksinkertaisesti lähettää indeksin i, jolle $x_i \neq y_i$. Kun Alisa ja Börje ovat vastaanottaneet indeksin i he voivat yksinkertaisesti vain vaihtaa kyseiset bitit keskenään ja todeta, että ne ovat erisuuret. Tässä

tapauksessa heidän ei siis tarvitse käydä koko bittijonoa läpi, koska heillä on ulkopuolista alkutietoa, joka kerrotaan heille.

Jos bittijonot ovat identtiset, niin tällöin ei ole olemassa yhtäkään indeksiä i, joka vakuuttaisi Alisan ja Börjen siitä, että bittijonot ovat erisuuret.

Yleisemmin voidaan siis ajatella, että jos $f(x, y) = 1$ ja kaikkinäkevä matemaatikko yrittää vakutta Alisalle ja Börjelle että funktion arvo on 1, niin on olemassa jokin todistus a, siten että käyttämällä tätä todistusta Alisa ja Börje laskevat funktion f arvoksi 1. Vastaavasti jos $f(x, y) = 0$, niin mikään todistus a ei vakuuta Alisaa ja Börjeä siitä, että funktion f arvo olisi 1, vaan he laskevat sen aina oikein. Protokollaa, jossa matemaatikko lähettää Alisalle ja Börjelle todistuksen a kutsutaan epädeterministiseksi protokollaksi. Tässä esimerkissä Alisa ja Börje laskevat funktiota, jonka arvolle 1 on olemassa todistus ja arvolle 0 ei. Tällöin epädeterminististä kommunikaatiokompleksisuutta merkitään $N^1(f)$. Tällöin $N^1(f) = \log_2 C^1(f)$.

Käänteistä tapausta, jossa Alisa ja Börje laskevat funktiota, jonka arvolle 0 on olemassa todistus, mutta arvolle 1 ei, kutsutaan rinnakaiseksi epädeterministiseksi kommunikaatiokompleksisuudeksi (yksinkertaisimmillaan voidaan vain ajatella aiemman esimerkin funktiosta riippuvaista funktiota g, jolle $g = 1 - f$). Rinnakkaista epädeterminististä kommunikaatiokompleksisuutta merkitään $N^0(f)$ ja $N^0(f) = \log_2 C^0(f)$.

Tapausta, jossa Alisa ja Börje ovat kiinnostuneet molemmista arvoista 1 ja 0 merkitään $N(f)$ ja $N(f) = \log_2 C(f)$.

Perustellaan vielä, että mistä arvo $N^1(f) = \log_2 C^1(f)$ tulee. Vastaava päättely toimii arvon $N^0(f)$ kohdalla. Mikä tahansa maalijoukon Z arvojen z peite muodostaa todistusjärjestelmän, jossa todistus funktion f arvolle on suorakulmion $S \times T$ nimi. Funktion f arvo syötteelle (x, y) on tässä kyseisessä suorakulmiossa. Suorakulmion nimen kertominen edellyttää $\log_2(\textit{suorakulmioiden määrä})$ bittiä.

Määritelmä 2.3. Epädeterministinen kompleksisuus funktiolle $f : X \times Y \to \{0, 1\}$ on $N^1(f) = \log_2 C^1(f)$. Rinnakkainen epädeterministinen kompleksisuus funktiolle f on $N^0(f) = \log_2 C^0(f)$, lisäksi $N(f) = \log_2 C(f)$.

Jotkin protokollat voivat virittää vain pienen määrän suorakulmioita,

mutta protokollan osapuolien täytyy viestittää toisilleen suuria määriä bittejä. Toisin sanoen protokollapuu on syvä, mutta siinä on vain vähän lehtisolmuja. Lemma 2.4 osoittaa, että tällöin $D(f) = \Theta(\log C^p(f))$.

Lemma 2.4. $\log_2 C^p(f) \leq D(f) \leq 2 \log_{3/2} C^p(f)$.

Todistus. Alaraja seuraa suoraan Lauseesta 2.2. Todistetaan vielä yläraja. Todistuksen ideana on se, että protokollapuun, jolla on tietty määrä lehtisolmuja voi muuttaa "tasapainotetuksi"protokollapuuksi, jonka syvyys riippuu lehtisolmujen logaritmista.

Olkoon $\mathcal{P}$ protokolla, joka laskee funktion f ja protokollan $\mathcal{P}$ protokollapuussa on t kappaletta lehtisolmuja. Täten on olemassa haarasolmu v, jolle t_v, eli haarasolmusta v alkava alipuulle, pätee, että $t/3 < t_v < 2t/3$. Tämä haarasolmu on löydettävissä kulkemalla protokollapuun juurisolmusta kohti lehtiä, siten että aina edetään haarasolmuun u, jolla on yli $2t/3$ lehtisolmua sen alipuussa. Kun tällaista solmua ei enää ole reitillä, niin tällöin viimeisenä löydetyn solmun o lapsisolmu täyttää asetetun ehdon. Olkoon R_v suorakulmio, niille syötteille, joilla protokolla saavuttaa haarasolmun v. Täten voidaan määritellä uusi protokolla funktiolle f seuraavasti:

1. Alisa ja Börje määrittävät, että onko $(x, y) \in R_v$. Tämä edellyttää kahden bitin verran kommunikaatiota.

2. Jos $(x, y) \in R_v$, niin Alisa ja Börje laskevat funktion f rekursiivisesti suorakulmiossa R_v, jolle heillä on jo protokolla, jossa on t_v kappaletta lehtisolmuja.

3. Jos $(x, y) \notin R_v$, niin Alisa ja Börje laskevat funktion f' rekursiivisesti joukossa $X \times Y$, missä $f' = f$ suorakulmion R_v ulkopuolella ja $f' = 0$ suorakulmiossa R_v. Käyttämällä alkuperäisen funktion f laskevaa protokollaa ja korvaamalla alipuun alkaen haarasolmusta v, muodostuu uusi protokolla funktiolle f', jolla on $t - t_v + 1$ lehtisolmua.

Täydellisyyden vuoksi osoitetaan vielä, että kolmannessa askeleessa laskettava f' ei muuta tulosta, sillä syötteet $(x, y) \in R_v$ eivät saavuta askelta kolme. Johtuen haarasolmun v valinnasta uudella protokollalla on korkeintaan $2t/3$

lehtisolmua. Täten arvolle $D(t)$, aloittaen protokollapuusta, jolla on t kappaletta lehtiä, voidaan muodostaa rekursiivinen yhtälö $D(t) \leq 2 + D(2t/3)$. Lisäksi on ilmeistä, että $D(1) = 0$, joten ratkaisemalla rekursioyhtälö saadaan yläraja $D(t) \leq 2 \log_{3/2} t$. Määritelmän 2.1 nojalla voidaan vielä tehdä sijoitus $t = C^p(f)$.

Ylärajan kannan voi myös vaihtaa:

$$\log_{3/2}(C^p(f)) = \frac{\log_2 C^p(f)}{\log_2(3/2)}.$$

Ero ylä- ja alarajan välillä on siis vain vakiokertoimen suuruinen. □

Lemman 2.4 nojalla $D(f) = \Theta(\log C^p(f))$. Toisaalta $D(f)$ saattaa olla eksponentiaalisesti suurempi kuin $\log C^1(f)$. On siis epäselvää, että mikä on lukujen $D(f), C(f)$ ja $C^D(f)$ suhde. Lauseen 2.2 mukaan $D(f) \geq \log C^D(f)$, mutta ei ole varmaa kuinka tiukka tämä raja on.

Avoin ongelma 2.5. Onko $D(f) = O(\log C^D(f))$?

Lauseen 2.6 mukaan lukujen $D(f)$ ja $\log C^D(f)$ välinen etäisyys ei ole kovinkaan suuri. Edes lukujen $D(f)$ ja $N(f)$ väli ei ole iso.

Lause 2.6. Kaikille funktioille $f : X \times Y \to \{0, 1\}$,

$$D(f) = O(N^0(f)N^1(f)). \tag{1}$$

Todistus. Todistetaan ensin eräs suorakulmioiden ominaisuus, jota tarvitaan myöhemmin todistuksessa: Olkoon $R = S \times T$ 0-monokromaattinen suorakulmio ja $R' = S' \times T'$ 1-monokromaattinen suorakulmio. Tällöin R ja R' eivät risteä joko riveissä ($S \cap S' = \emptyset$) tai sarakeissa ($T \cap T' = \emptyset$). Jos ne risteäisivät molemmissa, niin olisi olemassa $x \in S \cap S'$ ja $y \in T \cap T'$, siten että (x, y) kuuluisi molempiin joukkoihin R ja R', mikä on ristiriita.

Olkoon $L(k, l)$ suurin $C^P(g)$ yli kaikkien Boolen funktioiden g ja $C^1(g) \leq k$ ja $C^0(g) \leq l$. Tutkitaan optimaalista peitettä funktiolle f. Olkoon $R = S \times T$ 0-monokromaattinen suorakulmio kyseisessä peitteessä. Todistuksen alussa todistetun ominaisuuden nojalla voidaan olettaa, että vähintään puolet 1-monokromaattisista suorakulmioista $R' = S' \times T'$ eivät leikkaa suorakulmiota

R, eli $S \cap S' = \emptyset$. Jos näin ei ole, niin Alisan voi korvata Börjellä ja rivin S jonolla T ja todistus etenee sen jälkeen samoin.

Funktiolle f voidaan määrittää protokolla seuraavasti: Ensin Alisa kertoo Börjelle, kuuluuko $x \in S$. Jos $x \in S$, niin Alisa ja Börje laskevat funktion f rekursiivisesti yli joukon $S \times Y$. Tässä joukossa funktiolla f on 1-peite, jossa on enintään $k/2$ suorakulmiota (Ne suorakulmiot R', joille $S \cap S' = \emptyset$). Jos $x \notin S$, niin Alisa ja Börje ratkaisevat funktion f yli joukon $\bar{S} \times Y$. Tässä joukossa funktiolla f on 0-peite, jossa on korkeintaan $l-1$ suorakulmiota (alkuperäinen peite ilman suorakulmiota R). Täten voimme muodostaa rekursioyhtälön $L(k,l) \leq L(k/2,l)+L(k,l-1)$. Täten $C^P(f) \leq (C^0(f)+1)^{\log C^1(f)}$. Väite seuraa, sillä lemman 2.4 mukaan $D(f) = O(\log C^P(f))$. □

Viitteet

[1] E. Kushilevitz N. Nisan: *Communication complexity.* 1997.

[2] Shachar Lovett: CSE 291: *Communication complexity, Winter 2019, Nondeterministic protocols* February 4, 2019