Többszereplős kommunikációs komplexitás

SZAKDOLGOZAT

Készítette: Róka Dániel
Témavezetők: Tardos Gábor
Katona Gyula

Absztrakt:

A Yao által definiált két szereplős kommunikációs modell lehetőséget kínál a szereplők száma szerinti általánosításra. Ennek rengeteg különböző módja lehet, melyek közül többet is megpróbálunk áttekinteni. Egy ilyen lehetőség a lineáris hálózat, melyet P. Tiwari vetett fel egy 1987-es cikkében, majd erdeményei 1996-97-ben lettek pontosítva. A „homlokra ragasztott szám" modell az előbbitől igen eltér. Ebben is ismert több eredmény. Mind alsó, mind felső becslések akadnak szép számmal bizonyos függvények kommunikációs komplexitására, melyek azonban nem teljesen kielégítőek, hiszen minden eddig ismert alsó becslés a szereplők számának növekedésével exponenciálisan csökken. E két modell részletes vizsgálatán kívül felvetünk egy új kommunikációs modellt: a csillag modellt, melyet a jelen szakdolgozat vizsgál először.

Tartalom:

1. Többszereplős kommunikációs komplexitás

A Yao féle kétszereplős kommunikáció

A Yao féle kommunikációs modellben két játékos, A és B mindegyike rendelkezik egy-egy saját inputtal. A számára $x \in X$, B számára pedig $y \in Y$ ismert, ahol X, illetve Y a játékosok számára lehetséges inputok halmazai. Egy $f : X \times Y \longrightarrow \{0,1\}$ függvény mellett szeretnék $f(x,y)$-t kiszámítani, mégpedig úgy, hogy a lehető legkevesebb bitet kelljen egymásnak elküldeni. A játékosok tetszőleges mennyiségű számítást végezhetnek, csak az egymásnak elküldött információért kell „fizetni". Egy ún. kommunikációs protokoll meghatározza, hogy egy adott pillanatban véget ért-e már a kommunikációs folyamat, ha igen, akkor mi a keresett függvényérték, ha nem, akkor pedig melyik játékos mondjon egy bitet, és az milyen bit legyen. Hogy mikor ki beszéljen az csak az addig elhangzott bitektől függhet azért, hogy ne legyen egyszerre beszélésre lehetőség. Végetérés esetén a végeredményt szintén csak az elhangzott bitektől tehetjük függővé, hiszen ez mindkét játékos számára ugyanaz kell legyen. Végül az, hogy ki mit mond az elhangzott bitek, és a szólásra következő játékos inputjának függvénye. Egy $\mathcal{P}$ protokoll hossza a leghosszabb bitsorozat hossza, amely az adott protokoll mellet elhangozhat a két játékos között, azaz ha $\mathcal{P}(x,y)$ jelöli a két játékos között elhangzott bitsorozatot a $\mathcal{P}$ protokoll és x, y inputok mellett, akkor $|\mathcal{P}| = \max_{x\in X, y\in Y} |\mathcal{P}(x,y)|$. Az f függvény kommunikációs komlexitása pedig a legrövidebb f-et számoló protokoll hossza, tehát $C(f) = \min |\mathcal{P}|$, ahol a minimalizálás az f-et helyesen kiszámoló protokollokra történik.

$C(f)$ lehetséges kiszámításával, illetve becslésével részletesen most nem foglalkozunk, csak néhány alapvető tényt jegyezzünk meg:

1.1 TÉTEL: Amennyiben az inputok n bitesek, akkor $C(f) \leq n+1$

Bizonyítás: A triviális protokollal pl. A egyszerűen elküldheti az egész x-et B-nek, aki így kiszámíthatja $f(x,y)$-t és egyetlen bittel A-t is tájékoztathatja az eredményről. $\diamond$

1.2 DEFINÍCIÓ: Az $f : X \times Y \longrightarrow \{0,1\}$ függvény kommunikációs mátrixa az az M_f mátrix, melynek sorait X, oszlopait Y elemeivel azonosítjuk, és $x \in X, y \in Y$ esetén $(M_f)_{xy} = f(x,y)$

1.3 DEFINÍCIÓ: Az M_f mátrix egy részmátrixa monokromatikus, ha a részmátrix minden eleme azonos. Ekkor a részmátrixnak megfelelő $X^* \times Y^* \subseteq X \times Y$ halmazt is (az f-re nézve) monokromatikusnak mondjuk.

1.4 TÉTEL: Ha az f függvény M_f mátrixának monokromatikus részmátrixokkal való lefedéséhez szükség van legalább t monokromatikus részmátrixra, akkor $C(f) \geq \lceil \log t \rceil$.

(Itt is, és továbbiakban is mindenhol a logaritmus kettes alapú.)

Bizonyítás: Minden kommunikációs protokollhoz rendelhetünk egy bináris fát, az ún. protokoll fát, melynek csúcsait megjelöljük az A és B betűk valamelyikével aszerint, hogy az adott pillanatban az A vagy a B játékos következik szólásra. A csúcsból kiinduló két élre nullát illetve egyet írunk, és attól függően, hogy a szólásra következő játékos milyen bitet mond, a megfelelő irányba megyünk tovább. A protokoll fa leveleiben a protokoll véget ér, tehát a játékosok tudják a végeredményt. Azon (x,y) inputpárokra, melyekre egy rögzített

ℓ levélben kötünk ki, az $f(x,y)$ ezért ugyananazt az értéket adja, jelöljük ezen inputpárok halmazát a továbbiakban R_ℓ-lel. Az R_ℓ egy részmátrixa M_f-nek ugyanis amikor az A (illetve B) játékos elküld egy bitet, ezzel az M_f-ből bizonyos sorokat (illetve oszlopokat) kizár, a számára lehetséges inputpok halmaza pedig a maradékra korlátozódik. Az M_f ilyen függőleges és vizszintes szabdalásával valóban egy részmátrix keletkezik. Vagyis R_ℓ az M_f mátrixban egy monokromatikus részmátrixot ad, így a protokoll fa levelei az M_f-et monokromatikus részmátrixokra partícionálják. Ha a tétel feltétele teljesül, akkor a protokoll fának legalább t levele kell legyen, ami egy bináris fa esetén csak úgy lehetséges, ha a mélysége legalább $\lceil \log t \rceil$. $\diamond$

1.5 DEFINÍCIÓ: Az $f : X \times Y \longrightarrow \{0,1\}$ függvényre egy
$T = \{(x_i, y_i) : i \in \{1, \dots t\}\} \subseteq X \times Y$ ún. t méretű becsapós halmaz, amennyiben
(1) $f(x_i, y_i) = z \ \forall i \in \{1, \dots, t\}$, ahol $z \in \{0,1\}$ rögzített, továbbá
(2) ha $(x_i, y_i), (x_j, y_j) \in T$, és $i \neq j$,akkor $f(x_i, y_j) = \bar{z}$ és $f(x_j, y_i) = \bar{z}$ közül legalább az egyik igaz, ahol $\bar{z} = 1 - z$ a z negáltja.

1.6 TÉTEL: Ha az f függvény M_f mátrixa tartalmaz t méretű becsapós halmazt, akkor $C(f) \geq \lceil \log t \rceil$.

Bizonyítás: Vegyük észre, hogy egy becsapós halmaz semely két eleme nem lehet az f függvény M_f mátrixának ugyanabban a monokromatikus részmátrixában. Ebből az 1.4 Tétel felhasználásával könnyen adódik a tétel. $\diamond$

1.7 TÉTEL: Ha az f függvény mátrixa M_f, akkor $C(f) \geq \log rang M_f$.

Bizonyítás: Ha az M_f mátrixot t darab monokromatikus részmátrixra partícionáljuk, akkor az M_f előáll $M_f = \sum_{i=1}^{t} M_i$ alakban, ahol M_i az i-edik monokromatikus részmátrixa M_f-nek, kibővítve nullákkal a részmátrixon kívül. Azaz

$$(M_i)_{xy} = \begin{cases} (M_f)_{xy} & \text{ha } (x,y) \text{ az } i\text{-edik monokromatikus részmátrixban van} \\ 0 & \text{egyébként.} \end{cases}$$

Kihasználva, hogy $rang(M_i) \leq 1$ és $rang(A+B) \leq rang(A) + rang(B)$, azt kapjuk, hogy $rang(M_f) = rang(\sum_{i=1}^{t}(M_i)) \leq \sum_{i=1}^{t} rang(M_i) \leq t$. Amiből az 1.4 Tétellel következik a kívánt eredmény. $\diamond$

Az általánosítás lehetőségei

Amennyiben a Yao féle kommunikációt szeretnénk több szereplőre kiterjeszteni, több lehetőség is kínálkozik az általánosításra. Nézzünk most végig egy párat ezen alternatívák közül.

Amikor a kommunikációban több játékossal dolgozunk, a legfontosabb, amit el kell döntenünk, hogy a szereplők között miként zajlik a kommunikáció. Beszélhetünk személyes kommunikációról, amikor mindig csak két szereplő beszélhet egymással. Ekkor arról is kell nyilatkoznunk, hogy mely játékos-párok között engedünk meg információáramlást. Ez azt jelenti, hogy mondjuk k darab játékos esetén a $\binom{k}{2}$ játékos-pár mindegyikéről el kell dönteni, hogy létesítünk-e közöttük kapcsolatot. Ezekkel a döntésekkel tulajdonképpen egy gráfot definiálunk a k szereplőn, mint csúcsokon úgy, hogy a gráf élein engedjük meg a kommunikációt. Ekkor megőrizzük a Yao féle kétszereplős modellnek azt a tulajdonságát, hogy a kommunikáció két játékos között zajlik. Ha viszont a kétszereplős modellből inkább azt szeretnénk átvinni a többszereplős modellbe, hogy egy elküldött bitről minden játékosnak tudomása van (ami nyilván teljesül a kétszereplős modellben) , akkor egy ún. táblás kommunikációt kapunk, amelyben a szólásra következő játékos mindig egy bitet ír fel egy olyan képzeletbeli táblára, melynek tartalmát az összes játékos láthatja. Az előbbi modellben egy bit elküldésének árán csak egy, míg utóbbiban az összes játékos hozzájut a bitben megtestesülő információhoz, így nyilvánvaló, hogy ugyanazon függvény kiszámítása az utóbbi modellben jóval könnyebb, azaz kevesebb (vagy legalábbis nem több) bit elküldését teszi szükségessé. A két lehetőség akár keverhető is egymással, így lehetnek egyszerre két szereplő közötti kapcsolatok és a játékosok bizonyos részhalmazaihoz rendelt táblák is a modellben, ami tulajdonképpen azt jelenti, hogy a gráf, amellyel meghatározzuk a szereplők közötti kapcsolatokat egy hipergráf, ahol a 2-nél több csúcsot tartalmazó élek a megfelelő táblák. Ez utóbbi eset viszont annyira bonyolult, hogy nem fogunk vele részletesebben foglalkozni.

Hasonlóan az előbbihez arról is döntenünk kell, hogy a kétszereplős modellből azt a tényt vigyük át, hogy az összes szereplő rendelkezik saját inputtal, vagy azt, hogy pontosan két szereplő rendelkezik inputtal. Utóbbi esetben az új játékosoknak nem adunk inputot, ők egy kezdeti, üres állapotból indulnak. Szintén többféle lehetőség kínálkozik az általánosításra aszerint, hogy egy-egy inputrészt hány játékos számára teszünk hozzáférhetővé. Ez a kérdés természetesen a kétszereplős modellben fel sem vetődött, azonban ha 2-nél több szereplő rendelkezik inputtal, akkor egy inputot nem feltétlenül csak egy játékosnak adhatunk ki. Meghatározhatjuk minden egyes inputrészhez, hogy a játékosok mely csoportjának adunk ehhez hozzáférési jogot. Ennek egy igen szélsőséges esetével fogunk találkozni a 3. fejezetben, ahol egy-egy játékosnak majdnem az összes inputrészhez lesz hozzáférési lehetősége.

Vegyük észre, hogy nem sok értelme lenne a táblás kommunikációt azzal az esettel kombinálni, amikor csak két szereplő rendelkezik inputtal, hiszen ez a jól ismert kétszereplős kommunikációs modellt adná vissza, néhány új játékossal kiegészítve, akiknek viszont semmi beleszólása nem lenne az eseményekbe.

A Yao féle kommunikáció lényeges tulajdonsága, hogy nem az időt tekinti lényegesnek, hanem csak az elküldött bitek számát, ugyanis korlátlan számítási lehetőséget biztosít a két játékosnak. Ezt szeretnénk átvinni mindenképpen a többszereplős modellekre is. Éppen ezért a személyes kommunikáción belül csak az úgynevezett aszinkron modellekkel fogunk foglalkozni, melyekben az idő semmilyen szerephez nem jut. Lehetőség lenne ugyanis szinkron modelleket is vizsgálni, ahol ugyan a korlátlan számítási lehetőséget meghagynánk, de a sok kapcsolaton elhangzó bitek között valamilyen egyidejűséget, és egymásutániságot néznénk. A célunk tehát az időfogalom teljes kiküszöbölése, mint azt a lineáris hálózat modelljének pontos definícióján keresztül jól fogjuk majd látni.

Az aszinkronitás biztosítása azonban még nem teszi egyértelművé, hogy milyen feltételeket szabjunk a megengedett protokolloknak. Az egyszerre beszélést, és egyéb zavarokat a legegyszerűbben úgy küszöbölhetjük ki, ha az, hogy mikor ki következik szólásra csak a kapcsolatokon addig elhangzott bitek függvénye. Ez meg is felelne a kétszereplős modellben használt protokollfogalomnak. Viszont ha egy többszereplős modellben egy x inputhoz több játékosnak is van hozzáférése, akkor az, hogy közülük ki lesz a következő bitküldő függhet akár az x inputtól is anélkül, hogy ez zavarokat okozna.

Látható tehát, hogy számtalan fajta többszereplős modellt lehet definiálni. A következőkben két igen eltérő modellt fogunk részletesen megvizsgálni. A 2. fejezetbeli lineáris hálózat személyes kommunikáción alapul, és csak két szereplő rendelkezik saját inputtal, míg a 3. fejezetbeli „homlokra ragasztott szám" modellben a kommunikáció táblás, és inputja minden játékosnak van méghozzá úgy, hogy a hozzáférés is elég különös, ugyanis egy játékos majdnem minden inputot lát. Ezek után pedig megnézünk egy új lehetőséget, a csillag modellt, ami mindkét előbb említett modellel tartalmaz néhány közös vonást, és jelen szakdolgozat új kutatási témáját képezi.

2. A lineáris hálózat

A modell

Egyik lehetséges módja a többszereplős kommunikációs modell definiálásának, ha a Yao féle kétszereplős modellt bővítjük ki további szereplőkkel, akiknek azonban nem adunk inputrészt. Tehát továbbra is csak két kitűntetett játékos rendelkezik az $x \in X$, illetve $y \in Y$ inputtal, és egy kétváltozós $f : X \times Y \longrightarrow \{0,1\}$ függvényt szándékoznak kiszámítani. Viszont több új szereplő is bekapcsolódik a játékba úgy, hogy a szereplőkre, mint pontokra illesztett G gráffal meghatározzuk, hogy ki kivel beszélgethet. Egy kommonikációs folyamat hosszát az egyes kapcsolatokon (gráféleken) elhangzott bitek számainak összegével definiálhatjuk. Egy f-re adott protokoll hossza természetesen a leghosszabb előforduló kommunikáció hossz a lehetséges (x, y) inputok mellett, és az f kommunikációs kompexitása a G gráf által meghatározott kommunikációs modellben így $C_G(f) = \min_{\mathcal{P}} |\mathcal{P}|$, ahol $\mathcal{P}$ megengedett protokoll f számolására a G gráffal adott többszerelős modellben.

Amennyiben a G gráfot egy k hosszú útnak választjuk a két kitűntetett játékos között, akkor a P. Tiwari által felvetett lineáris hálózathoz jutunk. E modellben tehát $k+1$ játékos $(P_0, P_1, \ldots, P_k)$ vesz részt. P_0 x-et, P_k y-t ismeri, a többi játékosnak nincsen semmilyen információja. A játékosok egy utat alkotnak, tehát kapcsolata P_i-nek csak P_{i-1}-gyel és P_{i+1}-gyel van. (A kitüntetett P_0-nak és P_k-nak persze csak egy beszélgetőpartnere van.) Az $f(x, y)$-t kommunikációs komplexitását e modellben jelölje $C_k(f)$.

1.abra

Vegyük észre, hogy akármilyennek is választanánk a G gráfot ekvivalens problémát kapnánk a lineáris hálózat modellel, hiszen a két inputtal rendelkező játékosnak az aszinkron modellünkben kizárólag a köztük lévő legrövidebb út mentén lesz célszerű kommunikálni.

Yao már korábban felvetette e modell valamivel egyszerűbb változatát, amelyben a kommunikáció csak az egyik irányban zajlik, tehát a kisebb indexű játékostól a nagyobb indexű felé. E modellben az idő kizárása egyáltalán nem jelent gondot, nem úgy, mint a Tiwari féle kétirányú modellben. Nagyon fontos ezért, hogy utóbbit pontosan definiáljuk. A Yao féle egyirányú hálózatot is meg fogjuk vizsgálni, de most nézzük meg hogyan kell a kétirányú modellt jól, tehát aszinkron módon definiálni:

Tekintsük úgy az x, y inputokat, mintha azok a virtuális nulladik illetve $(k+1)$-edik kapcsolaton hangzanának el rögtön a kommunikáció kezdetekor. Egy adott pillanatban s_i-vel jelöljük az i-edik kapcsolaton addig elhangzott bitek sorozatát. Egy a lineáris hálózatra adott protokoll több részből áll. Tartalmaz minden kapcsolathoz egy-egy protokoll fát, mely, akár a kétszereplős modellben meghatározza a két szereplő közötti kommunikáció lefolyását. Azaz megadja, hogy mikor melyik játékos következik szólásra az adott kapcsolaton, illetve ha a kommunikáció már véget ért az adott kapcsolaton, akkor mi az eredmény. Mindezeket persze az adott kapcsolaton addig elhangzott bitek függvényében mondja meg. Tartalmaz továbba minden $1 \le i \le k$ -hoz (azaz minden kapcsolathoz) két függvényt, ezek

$$\Phi_i^+, \Phi_i^- : \{0,1\}^* \times \{0,1\}^* \longrightarrow \{0,1,\perp\}$$

$$\Phi_i^+ : \quad (s_{i-1}, s_i) \longmapsto \Phi_i^+(s_{i-1}, s_i) \ ,$$
$$\Phi_i^- : \quad (s_i, s_{i+1}) \longmapsto \Phi_i^-(s_i, s_{i+1}) \ .$$

Ezek a függvények megmondják, hogy az i-edik kapcsolaton balról, illetve jobbról milyen bitet küldjön P_{i-1} illetve P_i játékos. A $\perp$ azt jelenti, hogy most nem küldhet bitet. Ez lehet azért, mert ezen a kapcsolaton nem ő következik szólásra, vagy akár azért, mert még további biteket vár a másik oldalról, mielőtt eldönti, hogy milyen bitet küldjön erre az oldalra. Amennyiben például $\Phi_i^+(s_{i-1}, s_i) = 1$, akkor a P_{i-1} ezt az egyes bitet elküldheti P_i-nek most, vagy akármikor a későbbiekben. Ha megfelelő feltételeket szabunk egy protokollnak, akkor ezek biztosítani fogják, hogy ez értelmes legyen, ne tudjon megállni, és valóban aszinkron legyen. Ezek a feltételek a következők:

(1) Konzisztencia a protokoll fákkal: Ha az i-edik kapcsolathoz rendelt protokoll fa adott pillanatban egy P_i-vel megjelölt csúcsban, vagy egy levélben van, akkor e pillanatban a $\Phi_i^+(s_{i-1}, s_i) = \perp$ (azaz P_{i-1} nem szólhat), hasonlóan fordítva.

(2) Nincs szándékos blokkolás: (a) Ha az i-edik, és $(i+1)$-edik kapcsolaton $(1 \leq i < k)$ egyaránt P_i következik szólasra, akkor $\Phi_i^-(s_i, s_{i+1})$, és $\Phi_{i+1}^+(s_i, s_{i+1})$ közül legalább az egyik nem $\perp$.

(b) Ha az i-edik $(0 \leq i < k)$kapcsolaton a kommunikáció befejeződött, és az $i+1$-edik kapcsolaton P_i következik szólásra, akkor $\Phi_{i+1}^+(s_i, s_{i+1}) \neq \perp$. Hasonlóan a másik oldalra.

(3) Senki sem gondolhatja meg magát: Ha $\Phi_i^+(s_{i-1}, s_i) \neq \perp$ $(1 \leq i \leq k)$, továbbá az $s_{i-1}^* = s_{i-1}t_{i-1}$ az s_{i-1} meghosszabítása, akkor $\Phi_i^+(s_{i-1}^*, s_i) = \Phi_i^+(s_{i-1}, s_i)$.

(4) Egyhangúság: Ha a protokoll befejeződött, akkor a k kapcsolathoz tartozó protokoll fák azonos eredményt jelentő levélben kötöttek ki. Ez a protokoll által kiszámolt eredmény.

Ha a modellt a fenti feltételekkel definiáljuk, akkor egyszerűen igazolható a most következő lemma, ami minden további eredményhez nélkülözhetetlen.

2.1 LEMMA: Adott protokoll egy adott (x, y) input mellet midig lefuttatható, és minden lefuttatása esetén ugyanazokat a kommunikációkat eredményezi minden egyes kapcsolaton.

A későbbiekben gyakran szükségünk lesz a következő lemmára, ami a 2.1 Lemma teljesülése miatt nem kíván bizonyítást.

2.2 LEMMA: Amennyiben rögzítünk egy kapcsolatot, pl. az l-ediket $(1 \leq l \leq k)$, úgy a hálózatnak megfeleltethetünk egy kétszereplős kommunikációs modellt, melyben az A játékos szimulálja a $\{P_0, P_1, \ldots, P_{l-1}\}$, a B pedig a $\{P_l, P_{l+1}, \ldots, P_k\}$ játékosok tevékenységét. Ekkor az l-edik kapcsolaton elhangzott bitsorozat a hálózatban, és a kétszereplős modell kommunikációs bitsorozata megegyezik.

Az 1. fejezetben a kétszereplős kommunikációs modell definiálásakor már tisztáztuk, hogy az, hogy mikor ki beszél az csak az addig elhangzott bitektől függ. Ennek következménye, hogy azon bitsorozatok, melyek elhangozhatnak a két szereplő közötti kommunikáció során egy ún. prefix-mentes halmazt alkotnak, azaz a halmaznak nem lehet két olyan eleme, hogy az egyik a másik prefixe (kezdőszelete). Ugyanis ha lenne két ilyen bitsorozat, akkor a rövidebbik elhangzása után nem lenne egyértelmű mindkét játékos számára, hogy véget ért a kommunikáció, vagy esetleg egyikük még szólásra következik.

Ha ezt a gondolatmenetet a lineáris hálózat kétszereplős szimulációjával együtt használjuk, az alábbi fontos lemmát kapjuk:

2.3 LEMMA: A lineáris hálózat tetszőleges kapcsolatát rögzítve, a különböző inputok mellett az ezen kapcsolaton elhangzó bitsorozatok egy prefix-mentes halmazt alkotnak.

Egy ilyen halmazról a következőt tudjuk:

2.4 LEMMA: Ha $S = \{s_1, s_2, \ldots, s_t\}$ egy prefix-mentes részhalmaza $\{0,1\}^*$-nak, akkor $\sum_{j=1}^{t} |s_j| \geq t \cdot \log t$.

Bizonyítás: Minimalizáljuk adott t mellett a $\sum_{j=1}^{t} |s_j|$ (összhossz) értéket, amikor $S = \{s_1, s_2, \ldots, s_t\}$ prefix-mentes halmaz. Amennyiben léteznek $i, j \in \{1, 2, \ldots, t\}$ indexek, hogy s_j legalább 2 bittel hosszabb s_i-nél, akkor s_i, s_j elhagyásával, és helyettük s_i0 valamint s_i1 bitsorozatok S-be bevételével az összhossz nem nő, viszont a hosszak négyzetösszege csökken. Ezért az összhossz a minimumát biztosan felveszi olyan S halmaz mellett, amelyre az s_i-k hosszai közötti eltérések maximuma 1. Legyen tehát most S ilyen.

Ebben az esetben a legrövidebb bitsorozathosszúságok, amik előlfordulhatnak azok $\lfloor \log t \rfloor$ és $\lfloor \log t \rfloor + 1$, ennél rővidebb elemekből ugyanis biztosan nem lehet egy t elemű prefix-menets halmazt összeállítani. Jelölje c, hogy hány $\lfloor \log t \rfloor$ hosszú szó van, ekkor persze a $\lfloor \log t \rfloor + 1$ hosszú szavak száma $t - c$. Az összhossz minimalizálása most már csak a c maximalizálását jelenti.

Egyrészt nyilván $c \leq 2^{\lfloor \log t \rfloor}$, másrészt viszont egy $\lfloor \log t \rfloor$ hosszú szó kizárja két $\lfloor \log t \rfloor + 1$ hosszú szó S-be kerülésének lehetőségét (azt a kettőt, amelyeknek ő prefixe), így kapunk egy másik feltételt is c-re, méghozzá azt, hogy legalább annyi szóbajöhető $\lfloor \log t \rfloor + 1$ hosszú szó marad, amennyi kell, azaz $t - c \leq 2^{\lfloor \log t \rfloor + 1} - 2c$. Ez átalakítva $c \leq 2^{\lfloor \log t \rfloor + 1} - t$. Viszont könnyen látszik, hogy a második feltétel mindig erősebb ($2^{\lfloor \log t \rfloor} \geq 2^{\lfloor \log t \rfloor + 1} - t$). Az optimum tehát $c = 2^{\lfloor \log t \rfloor + 1} - t$. Ebből az optimális összhossz

$$c\lfloor \log t \rfloor + (t - c)(\lfloor \log t \rfloor + 1) = (2^{\lfloor \log t \rfloor + 1} - t)\lfloor \log t \rfloor - 2^{\lfloor \log t \rfloor + 1}(\lfloor \log t \rfloor + 1) =$$

$$= t\lfloor \log t \rfloor + 2(t - 2^{\lfloor \log t \rfloor})$$

Ez tehát a $\sum_{j=1}^{t} |s_j|$ minimális értéke. Hogy ez nagyobb $t \cdot \log t$ -nél az pedig abból látszik, hogy amennyiben t egy 2-hatvány, akkor láthatóan egyenlőség áll fenn. Két szomszédos 2-hatvány között viszont $\lfloor \log t \rfloor$ állandó, így a minimális érték e darabon lineáris függvény, mely mivel a $t \cdot \log t$ függvény konvex (második deriváltja pozitív), ezért a $t \cdot \log t$ függvénygörbéje felett halad.$\diamond$

Yao egyirányú hálózata

Az egyszerűség kedvéért nézzük először a Yao által vizsgált speciális esetét a lineáris hálózatnak, amikor a játékosok közötti kapcsolatok csak egyirányúak, tehát amikor P_i a P_{i+1}-nek tud küldeni információt, de fordítva nem. Ekkor természetesen csak azt kívánjuk meg egy protokollról, hogy a végére P_k tisztában legyen az $f(x, y)$ értékkel. Ebben az esteben a következő pontos eredményt tudjuk, ha $C_k^{\rightarrow}(f)$-val jelöljük e modellben a kommunikációs komplexitást:

2.5 TÉTEL: Ha M_f-nek pontosan t különböző sora van, akkor

$$\lceil k \log t \rceil \leq C_k^{\rightarrow}(f) \leq k \lceil \log t \rceil.$$

Bizonyítás: A felső becslés triviális, hisz P_0-nak csak az inputnak megfelelő sor számát kell végigküldenie a hálózaton. Nézzük tehát az alsó becslést: Legyen $x_1, x_2, \ldots, x_t$ olyan t input, melyekhez tartozó M_f-beli sorok páronként különbözőek. Jelölje $s_l(i)$ azt a bitsorozatot, amely az l-edik kapcsolaton (P_{l-1} és P_l között) hangzik el, ha P_0 inputja x_i. Az egyirányú adagyovábbítás következtében ez tényleg csak a P_0-nál lévő inputtól függ. Az, hogy x_i és x_j sora különbözik M_f-ben azt jelenti, hogy létezik olyan $y \in Y$, melyre $f(x_i, y) \neq f(x_j, y)$. Ha $s_l(i) = s_l(j)$ lenne valamely l, i, j értékekre, akkor $f(x_i, y) = f(x_j, y)$ állna $\forall y \in Y$ mellett, ami viszont ellentmondás. Ezért $s_l(i) \neq s_l(j)$ kell legyen minden l, i, j esetén, azaz egy rögzített kapcsolaton áthaladó bitsorozat minden különböző x_i inputra más és más. Az $\{s_l(i) : 1 \leq i \leq t\}$ halmaz így t különböző bitsorozatból áll, és azt is tudjuk (2.3 Lemma), hogy prefix-mentes halmaz, ebből a 2.4 Lemma alkalmazásával adódik, hogy

$$\sum_{j=1}^{t} \sum_{l=1}^{k} |s_l(j)| = \sum_{l=1}^{k} \sum_{j=1}^{t} |s_l(j)| \geq \sum_{l=1}^{k} t \log t = k \cdot t \cdot \log t.$$

Ahol $\sum_{l=1}^{k} |s_l(j)|$ éppen a teljes kommunikáció hossza az x_j input mellett, így a bal oldalon álló kifejezés nem más, mint a kommunikációk hosszainak összege a különböző x_j inputok mellett. Ezért az erre kapott alsó becslésünkből skatulya-elvvel következik, hogy létezik olyan j, melyre a kommunikáció hossza $\geq \lceil k \log t \rceil$. $\diamond$

Tiwari sejtése

Térjünk most vissza a Tiwari féle hálózati modellhez, ahol mindkét irányban zajlik a kommunikáció.

Amennyiben a lineáris hálózatban a közbülső, tehát inputtal nem rendelkező játékosoknak csak azt a feladatot adjuk, hogy továbbítsák az információt a két kitüntetett játékos között, akkor az így kapott protokoll tulajdonképpen egy kétszereplős kommunikáció azzal a különbséggel, hogy egy bit elküldése helyett ugyanezt k-szor kell megtenni. Ebből az adódik, hogy $C_k(f) \leq k \cdot C(f)$, ahol $C(f)$ az f hagyományos (kétszereplős) kommunikációs komplexitása. Segíthetnek-e a közbülső játékosok ennél hatékonyabban egy függvény kiszámításában, azaz szigorú-e az egyenlőtlenség, amit az előbb felírtunk? Vagy talán egyenlőség áll, és semmilyen más protokoll nem jobb az egyszerű adattovábbításnál?

E fejezetben be fogjuk bizonyítani a következő, Tiwaritól származó (ld. [2]) tételt:

2.6 TÉTEL: Majdnem minden f függvényre teljesül, hogy $C_k(f) \geq k(C(f) - 1)$.

A majdnem minden szót úgy kell érteni, hogy egy véletlenszerűen választott $f : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}$ függvényre 1-hez tartó valószínűséggel igaz a tétel ($n \to \infty$).

Ebből Tiwari azt sejtette, hogy a 2.6 Tétel minden f függvényre fennáll. Hogy a sejtés nem igaz, azt később látni fogjuk, most azonban igazoljuk a 2.6 Tételt. A továbbiakban az egyszerűség kedvéért az X, Y inputalaphalmazok a $\{0,1\}^n$ legyenek.

Mint azt az 1.6 Tételben láttuk, az f függvény kommunikációs mátrixában egy becsapós halmaz jelenléte lehetőséget adott $C(f)$ alsó becslésére. Hasonlót állíthatunk a lineáris hálózaton:

2.7 TÉTEL: Ha az f függvény M_f mátrixa tartalmaz t méretű becsapós halmazt, akkor $C(f) \geq \lceil k \cdot \log t \rceil$.

Bizonyítás: Legyen $T = \{(x_i, y_i) : 1 \leq i \leq t\}$ egy t méretű becsapós halmaz M_f-ben, és jelölje $s_l(i)$ az l-edik kapcsolaton elhangzott bitsorozatot az (x_i, y_i) input mellett. Az l-edik kapcsolat mentén vehetjük a kétszereplős szimulációját a hálózatnak (2.2 Lemma). Ebből ha $s_l(i) = s_l(j)$ állna fenn valamilyen $i, j \in \{1, \dots, t\}$ mellett, akkor $f(x_i, y_i) = f(x_i, y_j) = f(x_j, y_i) = f(x_j, y_j)$ lenne, ami ellentmond annak, hogy T egy becsapós halmaz. Itt tulajdonképpen egy a későbbiekben kimondandó lemma (2.10 Kicserélési lemma) speciális esetét alkalmaztuk. Ebből rögzített l-re az $s_l(i)$ bitsorozatok minden i-re különbözőek, innen pedig a bizonyítás vége egy az egyben a 2.5 Tétel bizonyításának végével egyezik meg. $\diamond$

Ez azt jelenti, hogy egy kellően nagy becsapós halmaz jelenléte M_f-ben azt eredményezi, hogy $C(f)$ n-hez, $C_k(f)$ pedig kn-hez lesz közeli, ebből következően Tiwari sejtése igaz, ha megfelelően nagy (2^n-hez közeli) méretű becsapós halmaz létezik M_f-ben. Mivel azonban egy általános f-re leggtöbbször nem mutatható ki egy ilyen nagy becsapós halmaz jelenléte, így a log-rang módszer irányába fogunk továbbmenni, előbb azonban egy kis előkészítésre lesz szükség.

2.8 DEFINÍCIÓ: Legyen $\mathcal{P}$ egy protokoll az $f(x, y)$ függvény kiszámítására a lineáris hálózaton. A $\mathcal{P}$ kommunikációs gráfja az a $G_{\mathcal{P}}$ gráf, melyet a következőképpen kapunk:

Jelölje S_l bitsorozatok azon halmazát, melyek valamilyen (x, y) input mellett elhangozhatnak az l-edik kapcsolaton. Tekintsük úgy, hogy az x illetve y inputok a P_0 illetve P_k játékosok számára a képzeletbeli nulladik illetve $(k+1)$-edik kapcsolaton hangzanak el. Ekkor $G_{\mathcal{P}}$ pontjai $k+2$ halmaz elemei. E halmazok: $X = S_0, S_1, S_2, \dots, S_k, S_{k+1} = Y$. $G_{\mathcal{P}}$ egy szintezett gráf az S_l halmazokkal ($0 \leq l \leq k+1$), mint szintekkel, élek csak a szomszédos szintek, tehát S_l és S_{l+1} között vezetnek. Az S_l és S_{l+1} közötti élek halmaza, E_l a következőképpen van definiálva ($l \in \{0, 1, \dots, k\}$) :

$E_l = \{(s_l, s_{l+1})$: Létezik $(x, y) \in X \times Y$, hogy $f(x, y) = 1$ és s_l, s_{l+1} megjelennek, mint kommunikáció az l-edik illetve $(l+1)$-edik kapcsolatokon az $f(x, y)$ számítása közben$\}$

2.abra

2.9 DEFINÍCIÓ: A $G_{\mathcal{P}}$ gráfban „hosszú út”-nak nevezünk egy $k+1$ élű utat, mely az $X = S_0$ halmaz egy x elemét köti össze az $Y = S_{k+1}$ halmaz egy y elemével, és minden S_l halmazból pontosan egy elemet érint.

Világos, hogy amennyiben $f(x, y) = 1$, úgy (x, y) input mellett a protokoll futtatása után a kapcsolatokon megjelenő bitsorokkal mint köztes pontokkal egy „hosszú út” van

$G_{\mathcal{P}}$-ben x és y között. Ennek viszont a megfordítása is igaz, mint azt a 2.11 Tételben látni fogjuk. Előbb azonban következzék egy nagyon fontos lemma:

2.10 LEMMA (KICSERÉLÉSI LEMMA): Ha az (x,y) és (x^*,y^*) inputpárok esetén a $\mathcal{P}$ protokoll mellett a kapcsolatokon rendre az $(s_1,s_2,\ldots,s_k)$ illetve a $(s_1^*,s_2^*,\ldots,s_k^*)$ bitsorozatok jelennek meg a kommunikáció során, és az l-edik kapcsolaton ugyanaz az $s_l = s_l^*$ jön létre, akkor az (x,y^*) inputpár mellett az $(s_1,s_2,\ldots,s_{l-1},s_l,s_{l+1}^*,\ldots,s_k^*)$ fog a kapcsolatokon létrejönni.

Bizonyítás: A lemma állítása egyszerűen következik abból, hogy az l-edik kapcsolattól balra lezajló kommunikációk csak az l-edik kapcsolaton elhangzó bitektől, és a P_0 játékosnál lévő inputtól függenek. Mivel a lemma feltételei mellett mindkettő azonos az (x,y) és (x,y^*) inputpárok esetén, így az első $l-1$ kapcsolaton ugyanaz a bitsorozat kell elhangozzon a két inputpár mellett. Ugyanígy az l-edik kapcsolattól jobbra lévő kapcsolatokon az (x,y^*) és az (x^*,y^*) inputpárok eredményezik ugyanazt a kommunikációt.

Hasonló gondolatmenettel igazolható, hogy az (x^*,y) inputpár pedig az $(s_1^*,s_2^*,\ldots,s_{l-1}^*,s_l,s_{l+1},\ldots,s_k)$ bitsorozatokat eredményezi a kapcsolatokon. $\diamond$

2.11 TÉTEL: $G_{\mathcal{P}}$-ben létezik egy „hosszú út” $x \in X$ és $y \in Y$ között $\{s_l : l = 1,\ldots,k\}$ köztes pontokkal $\Longleftrightarrow$ $f(x,y) = 1$ és $f(x,y)$ kiszámítása során az l-edik kapcsolaton s_l a kommunikációs bitsorozat.

Bizonyítás: A $\Longleftarrow$ irányt már láttuk, így már csak a $\Longrightarrow$ irányt kell megmutatnunk. Az, hogy létezik egy „hosszú út” x és y között $\{s_l : l = 1,\ldots,k\}$ köztes pontokkal definíció szerint azt jelenti, hogy léteznek (x_i,y_i) párok $(i = 0,1,2,\ldots,k)$, hogy $f(x_i,y_i) = 1$, $x_0 = x$, $y_k = y$ és $f(x_i,y_i)$ számítása mellett s_i és s_{i+1} lesz a kommunikáció az i-edik illetve $(i+1)$-edik kapcsolaton. Teljes indukcióval megmutatjuk, hogy minden j-re (j=0, 1, 2, …, k) igaz, hogy $f(x,y_j)$ számolásánál az l-edik kapcsolaton s_l a kommunikáció minden $1 \le l \le (j+1)$ esetén. Az indukciós állítás y_0 választása miatt igaz $j=0$-ra. Ha igaz $(j-1)$-re, akkor $f(x,y_{j-1})$ számításánál az első j kapcsolaton a kívánt kommunikáció hangzik el, míg $f(x_j,y_j)$ számításánál azt tudjuk, hogy a j-edik és $(j+1)$-edik kapcsolaton s_j illetve s_{j+1} a bitsorozat. Ebből a kicserélési (2.10) Lemmával következik, hogy $f(x,y_j)$-re már az első $(j+1)$ kapcsolaton az s_l-ek hangzanak el. A $j=k$ esteben (amely éppen igazolja a tételt) a bizonyitás csak annyiban különbözik , hogy nincs $(k+1)$-edik kapcsolat. $\diamond$

2.12 KÖVETKEZMÉNY: Legfeljebb egy „hosszú út” vezethet $G_{\mathcal{P}}$ bármely két pontja között.

Bizonyítás: A 2.11 Tétel és a 2.1 Lemma közös következménye. $\diamond$

Jelölje A^i a $G_{\mathcal{P}}$ gráf $S_i \cup S_{i+1}$-re való megszorításával létrejövő páros gráf adjacencia mátrixát. Akkor:

2.13 LEMMA: $M_f = A^0 A^1 \ldots A^k$.

Bizonyítás: Jelölje $B := A^0 A^1 \ldots A^k$, akkor

$$B_{xy} = \sum_{s_1,s_2,\ldots,s_k} A^0_{xs_1} A^1_{s_1 s_2} \ldots A^k_{s_k y}.$$

Az összegben egy nem-nulla elem egy „hosszú út”-nak felel meg x és y között, így a 2.11 Tétellel és 2.12 Következménnyel $B_{xy} = (M_f)_{xy}$. $\diamond$

2.14 LEMMA: Legyen $A_{m\times m}$ a G páros gráf adjacencia mátrixa . Ha A nem szinguláris a valós test felett, akkor G-ben van teljes párosítás.

Bizonyítás: Az A valós test feletti permanense, $per(A)$ megadja a G-ben lévő teljes párosítások számát. Az A nem szinguláris , azaz $det(A) \neq 0$, így az A 0/1 mátrix volta miatt ez azt jelenti, hogy $per(A) > 0$, ebből pedig G-ben létezik legalább egy teljes párosítás. $\diamond$

2.15 TÉTEL (BINET-CAUCHY): Legyen $A_{m\times m} = B_{m\times k} \cdot C_{k\times m}$ és legyen $k \geq m$. Akkor

$$det(A) = \sum_{S\subseteq\{1,2,\ldots,k\},|S|=m} det(B(S))det(C(S))$$

ahol $B(S)$ (ill. $C(S)$) a B (ill. C) azon részmátrixa, melyet az S által megjelölt oszlopok (ill. sorok) kiválasztásával nyerünk.

Bizonyítás: Megtalálható pl. [11]-ben. $\diamond$

2.16 KÖVETKEZMÉNY: Ha $A = BC$ nem szinguláris, akkor van egy $S \subseteq \{1, 2, \ldots, k\}$ és $|S| = m$, hogy $B(S)$ és $C(S)$ is nem szinguláris.

Jelölje G_i $(i = 0, 1, 2, \ldots, k)$ azt a páros gráfot, melyet a $G_{\mathcal{P}}$ gráf $S_i \cup S_{i+1}$ halmazra való megszorításával nyerünk. Ennek adjacencia mátrixa A^i, mint már említettük. Jelölje $B^j := A^0A^1 \ldots A^j$. Mint láttuk a 2.13 Lemmában : $B^k = M_f$. Most $X = Y = \{0, 1\}^n$ legyen, ekkor $|X| = |Y| = 2^n$.

2.17 TÉTEL: Amennyiben M_f nem szinguláris, akkor $G_{\mathcal{P}}$-ben létezik 2^n darab pontdiszjunkt „hosszú út”, melyek mindegyike különböző X-beli pontból indul, és különböző Y-beli pontba érkezik.

Bizonyítás: Az állítást k-ra (a hálózat hosszára) vonatkozó indukcióval bizonyítjuk. A $k = 0$ eset ugyan valójában nem létezik, mégis ez lesz az indukció kiindulópontja. Ekkor a képzeletbeli $G_{\mathcal{P}}$-nek két szintje lenne X és Y, azaz páros gráf lenne. Ekkor ha $B^0 = A^0$ nem szinguláris, akkor a 2.14 Lemma szerint a páros gráfban létezik teljes (2^n méretű) párosítás. Tegyük fel, hogy k-ra igaz, hogy a $k+2$ szinttel rendelkező szintezett $G_{\mathcal{P}}$ gráfra ha a B^k nem szinguláris, akkor létezik 2^n darab pontdiszjunk „hosszú út” a két szélső szint között. Ekkor $(k+1)$-re $B^{k+1} = B^k \cdot A^{k+1}$, ahol B^k egy $2^n \times |S_{k+1}|$ méretű, A^{k+1} pedig egy $|S_{k+1}| \times 2^n$ méretű mátrix. Ha B^{k+1} nem szinguláris, akkor a 2.15 Tétel értelmében létezik $S \subseteq S_{k+1}$, ahol $|S| = 2^n$ és $B^k(S)$ valamint $A^{k+1}(S)$ nem szinguláris $2^n \times 2^n$-es mátrixok. Az indukciós feltevés szerint létezik 2^n darab pontdiszjunkt út $S_0 = X$ és $S \subseteq S_{k+1}$ között. A 2.16 Következmény értelmében pedig az S és $S_{k+2} = Y$ halmazok között létezik teljes párosítás. Az előbbi utakat a párosításbali élekkel meghosszabbítva megkapjuk a kívánt 2^n darab pontdiszjunkt utat X és Y között. $\diamond$

2.18 TÉTEL: Ha M_f nem szinguláris, akkor $C_k(f) \geq kn$.

Bizonyítás: Mivel M_f nem szinguláris, így a 2.17 Tétel biztosítja, hogy létezik 2^n pontdiszjunk „hosszú út” $G_{\mathcal{P}}$-ben. Ha az i-edik út végpontjai x_i, y_i , akkor a $T =$

$\{(x_1, y_1), \ldots, (x_{2^n}, y_{2^n})\}$ halmaz 2^n olyan inputpárból áll, hogy semely kettőnek nem egyezik meg a kommunikációs bitsorozata egyik kapcsolaton sem. A 2.5 Tételbeli skatulya-elvvel azonos módon mutatható meg, hogy ekkor létezik egy j, hogy (x_j, y_j) mellett az öszes kommunikáció legalább kn bit. $\diamond$

2.19 KÖVETKEZMÉNY: Ha M_f az f függvény mátrixa, akkor

$$C_k(f) \geq k \cdot \log(rang(M_f)).$$

Bizonyítás: Ha M_f nem nem szinguláris, akkor a 2.18 Tételt alkalmazhatjuk a legnagyobb nem szinguláris részmátrixára, amelynek mérete $rang(M_f)$. $\diamond$

Már csak annyit kell megmutatnunk, hogy egy általános f függvény mátrixának nagy a rangja:

2.20 TÉTEL: Majdnem minden $n \times n$-es 0/1 mátrix rangja $\geq n - f(n)$ $GF(2)$ felett tetszőleges olyan f függvényre, mely ∞-hez tart $n \to \infty$ esetén.

Bizonyítás: Becsüljük alulról a legalább r rangú 0/1 mátrixok számát, m_r-et, méghozzá azon mátrixok számával, melyek első r sora független $GF(2)$ felett: Az első r sor megválasztására $\prod_{i=0}^{r-1}(2^n - 2^i)$ lehetőség van, míg ezek után a mátrixot $2^{n(n-r)}$ -féleképpen lehet befejezni. Ezért

$$m_r \geq 2^{n(n-r)} \cdot \prod_{i=0}^{r-1}(2^n - 2^i).$$

Az $n \times n$-es 0/1 mátrixokból összesen $2^{n^2} =: m$ van. Így a legalább r rangú mátrixok aránya az összes mátrixok között:

$$\frac{m_r}{m} \geq \frac{\prod_{i=0}^{r-1}(2^n - 2^i)}{2^{nr}} = \prod_{i=0}^{r-1}(1 - \frac{1}{2^{n-i}}) \geq 1 - \sum_{i=0}^{r-1} \frac{1}{2^{n-i}} \geq 1 - \frac{1}{2^{n-r}}$$

Ez pedig $r = n - f(n)$ esetén 1-hez tart. $\diamond$

A valós test feletti rang ennél már csak nagyobb lehet. Arra jutottunk tehát, hogy a függvények túlnyomó részére a log-rang becslés nagyon jól becsli $C(f)$-et és $C_k(f)$-et egyaránt, ezekre a függvényekre ezáltal igaz Tiwari sejtése.

A sejtés cáfolata

Mivel Tiwarinak sikerült bizonyítania, hogy majdnem minden f függvényre teljesül, hogy $C_k(f) \geq k(C(f) - 1)$, így azt sejtette, hogy ez tetszőleges f függvényre fennáll. A sejtés cáfolatához olyan függvényt kell konstruálni, melynek kiszámításához a közbülső játékosok intelligensebb módon is hozzájárulhatnak, mint ha csak biteket továbbítanak a két kitűntetett játékos között. Egy ilyen f függvényre $C_k(f)$-et felülről, $C(f)$-et pedig alulról kell becsülni ahhoz, hogy a sejtést megcáfoljuk. E. Kushilevitz, N. Nisan és R. Ostrovsky [3]-ban olyan végtelen sok függvényből álló osztályt mutattak, melyre

$$C_k(f) \leq (\frac{3}{4} + o(1)) \cdot k \cdot C(f). \qquad (*)$$

ahol k tetszőleges páros szám, az $o(1)$ hibatag pedig $n \to \infty$ mellett értendő.

Legyen $g : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}$ egyelőre tetszőleges függvény. Hogy milyen feltételeknek kell eleget tegyen az később fog majd kiderülni. E g segítségével konstruáljunk egy f_g-vel vagy egyszerűen csak f-fel jelölt függvényt a következőképpen:

2.21 DEFINÍCIÓ: Legyen $f : \{0,1\}^{2n} \times \{0,1\}^{2n} \longrightarrow \{0,1\}$ az a függvény, amelyre $x_1, x_2, y_1, y_2 \in \{0,1\}^n$ esetén

$$f([x_1, x_2], [y_1, y_2]) := \begin{cases} g(x_1, y_2) & \text{ha } g(x_1, y_1) = 1 \\ g(x_2, y_1) & \text{ha } g(x_1, y_1) = 0 \end{cases}$$

Azt állítjuk, hogy a lehetséges g függvények túlnyomó részére az így definiált f-re fennáll (*), ezt a 2.25 Tétel fogja kimondani. Ehhez $C_k(f)$-et felülről, $C(f)$-et pedig alulról kell megbecsülni.

2.22 TÉTEL: A fenti f-re $C_k(f) \leq \frac{3}{2}k \cdot n + 2k$, ha k páros.

Bizonyítás: Adunk egy megfelelő protokollt a k hosszú lineáris hálózaton, amennyiben k páros. Kezdetben P_0 számára $[x_1, x_2]$, P_k számára $[y_1, y_2]$ ismert. Küldje el P_0 az x_1-et, P_k pedig az y_1-et a $P_{k/2}$ „középső" játékosnak a $\{P_i : i = 1, 2, \cdots, \frac{k}{2} - 1\}$ illetve a $\{P_i : i = \frac{k}{2} + 1, \frac{k}{2} + 2, \cdots, k - 1\}$ játékosok továbbításával. Ehhez eddig $2 \cdot \frac{k}{2} \cdot n$ bit kommunikációra van szükség. Ezután $P_{k/2}$ számítsa ki x_1 és y_1 ismeretében $g(x_1, y_1)$ értékét. Amennyiben $g(x_1, y_1) = 1$, akkor $P_{k/2}$ küldje el x_1-et P_k-nak, így ő tudja számolni $g(x_1, y_2)$ (tehát az f) értékét. Ehhez újabb $\frac{k}{2} \cdot n$ bit szükséges majd a végeredményről P_k minden további játékost tájékoztathat k bit kommunikációval. Hasonlóan ha $g(x_1, y_1) = 0$, akkor $P_{k/2}$ küldje el P_0-nak az y_1-et, aki így számolhatja $g(x_2, y_1)$-et (tehát f-et), stb. Azonban még mielőtt $P_{k/2}$ elküldi például x_1-et a P_k-nak küldenie kell egy-egy bitet P_0 és P_k játékosok felé, ezzel tájékoztatva őket, hogy inputrészt várjanak, vagy csak a végeredményt. Mondjuk az 1-es azt jelenti, hogy az inputrész következik, a 0 pedig, hogy neki már nincs más dolga, mint megvárni az eredménybitet. Ez még további $2 \cdot \frac{k}{2}$, azaz k bit kommunikációt jelent. Az összes kommunikáció $\frac{3}{2}kn + 2k$, ami igazolja a tételt.$\diamond$

Páratlan k esetén a $\frac{3k}{2}$ helyett mindenhol $\frac{3k+1}{2}$ lenne irandó a bizonyításban, ami egy újab k-tól függő hibatagot eredményezne.

Míg a 2.22 Tétel a g választásától függetlenül igaz, addig $C(f)$ alulról történő becslése nem lehetséges akármilyen g mellett, azonban mint nemsokára kiderül a függvények legtöbbje megfelelő lesz. Válasszuk egyelőre véletszerűen a g függvényt.

Jelölje $N := 2^n$. Legyenek $0 \leq \alpha \leq 1$ és $\beta \geq 1$ később meghatározandó konstansok. Jelölje továbbá $L := \beta n$. Álljon R_1 az M_g (a g $N \times N$-es mátrixának) sorainak L darab diszjunkt párjából, és ugyanígy R_2 az M_g oszlopainak L diszjunkt párjából. Ekkor az $R_1 \times R_2$ tartalmaz L^2 darab 2×2-es részmátrixot M_g-ből. Az $R_1 \times R_2$-t nevezzük α-kiegyensúlyozottnak, ha a lehetséges $2^4 = 16$ lehetséges 2×2-es részmátrix mindegyike legalább αL^2-szer előfordul $R_1 \times R_2$-ben.

Definiáljuk a következő feltételt:

(F1) Az $\alpha = 1/32$ érték mellett az M_g mátrix minden $2L \times 2L$ részmátrixa α-kiegyensúlyozott.

2.23 TÉTEL: Majdnem minden g függvényre teljesül az (F1) feltétel.

Bizonyítás: Itt most elhagyjuk az egyébként egyszerű számolást igénylő bizonyítást.$\diamond$

Az alsó becslés folyamatosan használja, hogy g kielégíti az (F1) feltételt, és annak az alábbi közvetlen következményeit.

(F2) Az M_g nem tartalmaz $L \times L$ méretű monokromatikus részmátrixot.

(F3) Az M_g minden $2L \times L$ méretű részmtrixában a lehetséges 4 darab 2×1-es részmátrix mindegyike legalább αL^2-szer előfordul. Hasonlón az M_g minden $L \times 2L$ méretű részmtrixában a lehetséges 4 darab 1×2-es részmátrix mindegyike legalább αL^2-szer előfordul.

Az M_g egy $A \times B$ részmátrixának $x \in A$ sorát B-re nézve α-kiegyensúlyozottnak mondunk, ha a részmátrixon belül az x sorban a nullák aránya 8α és $1 - 8\alpha$ között van.

(F4) Ha $A \times B$ az M_g részmátrixa, és $|B| \geq L$, akkor A-ban legfeljebb $2L$ sor nem kiegyensúlyozott B-re nézve ($\alpha = 1/32$). Ugyanígy ha $|A| \geq L$, akkor pedig B-nek lehet csak legfeljebb $2L$ A-ra nézve kiegyensúlyozatlan oszlopa.

2.24 TÉTEL: Ha g eleget tesz az (F1) feltételnek, akkor a belőle nyert $f = f_g$ függvényre $C(f) \geq (2 - o(1)) \cdot n$.

Bizonyítás (vázlat): $C(f)$ alulról történő becsléséhez nem használhatjuk az eddig ismert, és alkalmazott technikákat, hiszen olyan f függvényekre, melyek kommunikációs komplexitását a „log-rang" illetve a „becsapós halmaz" technikával jól lehet alulról becsülni, azokra Tiwari bizonyította a sejtését, így reménytelen, hogy bármelyik módszer működjön a sejtést cáfoló f-ekre. Tehát mindenképpen egy új becslési technikára van szükség. Az új technika lényege, hogy a függvényre adott tetszőleges protokoll fájában olyan csúcs létezését igazoljuk, melyhez vezető út kellően hosszú, és a csúcsból szintén megfelelően hosszú út található a fa egyik leveléhez. A sok számolást igénylő bizonyítást itt most elhagyjuk, megtalálható [3]-ban.$\diamond$

2.25 TÉTEL: Ha k és n páros, akkor létezik végtelen sok olyan $f : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}$ függvény, amelyre

$$C_k(f) \leq (\frac{3}{4} + o(1)) \cdot k \cdot C(f).$$

Bizonyítás: Minden $g : \{0,1\}^{n/2} \times \{0,1\}^{n/2} \longrightarrow \{0,1\}$ függvényre $C_k(f_g) \leq \frac{3}{4}k \cdot n$ a 2.22 Tétel értelmében. A 2.24 Tétel pedig biztosítja, hogy majdnem minden g-re $C(f_g) \geq (1 - o(1)) \cdot n$. E kettőből pedig majdnem minden g-ből kapott f_g-re igaz a tétel.$\diamond$

A legjobb, minden f-re igaz eredmény

Láttuk, hogy $C_k(f)$ lehet kisebb $kC(f)$-nél, akár egy 3/4-es szorzóval. Jó lenne viszont azt is tudni, hogy legfeljebb mennyivel lehet kisebb.

Sokáig a legjobb ismert alsó becslés $C_k(f)$-re az alábbi volt:

2.26 TÉTEL: $C_k(f) = \Omega(k \cdot (\sqrt{C(f)} - \log k))$.

Bizonyítás: Megmutatjuk, hogy $R_0(f) \leq \frac{C_k(f)}{k} + \log k$, ahol $R_0(f)$ az f randomizált, 0-hibás kommunikációs komplexitása a kétszereplős modellben. Azaz $R_0(f)$ az a kommunikációs komplexitás, amit akkor kapunk, ha protokollnak egy a hagyományos módon értelmezett, és az adott függvényt jól kiszámoló protokolokon vett véletlen eloszlást tekintünk, és az így kapott protokoll hosszán a véletlenszerűen választott hagyományos protokoll hosszának a várható értékét értjük. Mivel ismert (ld. pl. [12]), hogy $R_0(f) = \Omega(\sqrt{C(f)})$, így az állítás már következik.

Adott protokollhoz a k hosszú lineáris hálózaton, mely $C_k(f)$ kommunikációt használ konstruálunk egy kétszereplős randomizált, 0-hibás protokollt a következőképpen: Az A játékos véletlenszerűen, egyenlő valószínűséggel választ egyet a k kapcsolat közül, mondjuk az l-ediket, és elküldi l-et B-nek ($\log k$ bit). Ezek után lefolytatják a hálózat kétszereplős szimulációját az l-edik kapcsolat mentén (2.2 Lemma). E protokoll mellett a kommunikáció várható értéke $\frac{C_k(f)}{k}$. Tehát valóban $R_0(f) \leq \frac{C_k(f)}{k} + \log k$. $\diamond$

Azonban ennél sokkal jobb becslést sikerült adnia M. Dietzfelbingernek [4]-ben. Igazolta, hogy létezik γ konstans, hogy $C_k(f) \geq \gamma \cdot k \cdot C(f)$. A probléma viszont csak akkor lesz teljesen megoldott, ha sikerül a legnagyobb ilyen γ-t meghatározni, a legjobb eddig ismert érték γ-ra: $0,275$. Nézzünk azonban előbb néhány nagyon fontos lemmát. Szükség lesz a kicserélési lemma (2.10) egy egyszerű, de alapvető fontosságú következményére.

2.27 LEMMA (KÖZREFOGÁSI LEMMA): Ha az (x,y) és (x^*,y^*) inputpárok esetén a $\mathcal{P}$ protokoll mellett a kapcsolatokon rendre az $(s_1, s_2, \ldots, s_k)$ illetve a $(s_1^*, s_2^*, \ldots, s_k^*)$ bitsorozatok jelennek meg a kommunikáció során, és az i-edik és j-edik kapcsolaton ($1 \leq i \leq j \leq k$) egyaránt ugyanaz az $s_i = s_i^*$ illetve $s_j = s_j^*$ jön létre, akkor miden köztes kapcsolaton is megegyezik a kommunikáció, azaz $s_l = s_l^*$ $\forall i \leq l \leq j$.

Bizonyítás: A 2.10 Lemmát először az i-edik kapcsolatra alkalmazva azt kapjuk, hogy (x, y^*) inputra a kapcsolatokon $(s_1, s_2, \ldots, s_i^*, s_{i+1}^*, \ldots, s_k^*)$ lesz. Alkalmazva ismét a 2.10 Lemmát, ezúttal a j-edik kapcsolatra, és az (x, y^*), (x, y) inputokra pedig azt adja, hogy az (x, y) esetén meglelenő bitsorozatok: $(s_1, \ldots, s_{i-1}, s_i^*, \ldots, s_j^*, s_{j+1}, \ldots, s_k)$, amiből az egyértelműség miatt (2.1 Lemma) következik a kívánt állítás. $\diamond$

A most következő lemma kulcsszerepet játszik az alsó becslésben:

2.28 LEMMA: Ha $\mathcal{P}$ egy protokoll az f kiszámítására a k hosszú lineáris hálózaton, akkor f-re van kétszereplős protokoll, mely nem több, mint $2^{|\mathcal{P}|/\lceil k/2 \rceil}$ különböző bitsorozatot használ.

Bizonyítás: Legyen k páros az egyszerűség kedvéért. A $\mathcal{P}$ indukál egy kétszereplős protokollt (2.2 Lemma) a $(k/2)$-edik kapcsolat mentén. Tegyük fel, hogy e kétszereplős kommunikáció során t különböző bitsorozat hangozhat el. (Azaz a hálózat $k/2$-edik kapcsolatán a $\mathcal{P}$ protokoll mellett t bitsorozat hangozhat el.) Megmutatjuk, hogy $|\mathcal{P}| \geq (k/2) \cdot \log t$, ami páros k-ra igazolja az állítást. Legyenek $(x_1, y_1), (x_2, y_2), \ldots, (x_t, y_t)$ olyan inputpárok, melyekre a $(k/2)$-edik kapcsolaton elhangzó bitsorozatok - azaz $s_{k/2}(x_1, y_1)$, $s_{k/2}(x_2, y_2)$, $\ldots$, $s_{k/2}(x_t, y_t)$ - mind különbözőek. Nyilvánvaló, hogy $|\mathcal{P}| \geq \frac{1}{t} \cdot \sum_{j=1}^{t} |s(x_j, y_j)|$, ahol $s(x_j, y_j) = s_1(x_j, y_j) s_2(x_j, y_j) \cdots s_k(x_j, y_j)$, azaz az összes elhangzott kommunikáció konkatenációja az (x_j, y_j) input mellett. Ebből

$$|\mathcal{P}| \geq \frac{1}{t} \cdot \sum_{j=1}^{t} |s_{k/2}(x_j, y_j)| + \sum_{l=1}^{(k/2)-1} \frac{1}{t} \sum_{j=1}^{t} |s_l(x_j, y_j) s_{k-l+1}(x_j, y_j)|.$$

Az $s_{k/2}(x_j, y_j)$ bitsorozatok egy prefix-mentes halmazt alkotnak, mint azt a 2.3 Lemmában láttuk. Viszont a közrefogási (2.27) lemma miatt az $s_l(x_j, y_j)s_{k-l+1}(x_j, y_j)$ bitsorozatok is mind különböznek, így ezek is egy prefix-mentes halmazt alkotnak. Ezért a 2.4 Lemma mind a $k/2$ darab átlagértékre alkalmazható, amiből

$$|\mathcal{P}| \geq \log t + \sum_{j=1}^{(k/2)-1} \log t = (k/2) \cdot \log t.$$

Ha k páratlan, akkor $k/2$ helyett mindenhol $\lceil k/2 \rceil$ irandó. $\diamond$

2.29 TÉTEL: Ha f-re létezik kétszereplős protokoll t lehetséges kommunikációs bitsorozattal, akkor $C(f) \leq 2 \log_{\frac{3}{2}} t$.

Bizonyítás: A feltétel azt jelenti, hogy létezik f-re kétszereplős protokoll, melyhez tartozó protokoll fának t levele van. Elképzelhető azonban, hogy e protokoll fának nagy a mélysége. A $C(f)$ felső becsléséhez e fából egy kiegyensúlyozottabb fával rendelkező protokollt konstruálunk, melynek mélysége legfeljebb $2 \log_{\frac{3}{2}} t$, ami biztosítja tétel állítását. Egy t levelű bináris fában létezik olyan v pont, hogy t_v -a v gyökerű részfa leveinek számateljesíti a $t/3 < t_v \leq 2t/3$ feltételt. Ilyet találhatunk, ha elindulunk a gyökérből, és mindig abba az irányba megyünk, amelyik gyerekhez tartozó részfának több, mint $2t/3$ levele van. Amikor ezt már nem tudjuk megtenni, akkor egy olyan pontban vagyunk, melynek egyik gyereke megfelel v-nek. Jelölje R_v azon (x, y) inputpárok halmazát $X \times Y$-ból, melyek eljutnak a v pontba. Tekintsük a következő új protokollt f-re:

Elsőként A és B játékosok eldöntik, hogy a kapott (x, y) inputpár R_v-ben ven-e. Ehhez 2 bit kommunikációra van szükség.

(1.) Amennyiben $(x, y) \in R_v$, akkor az eredeti protokollt a v pontból folytatják azaz az R_v-re megszorított f-re, melyre tehát egy t_v levelű protokoll fa áll rendelkezésre.

(2.) Ha $(x, y) \notin R_v$, akkor akkor az eredeti protokollt használják az $f^* : X \times Y \longrightarrow \{0, 1\}$ függvényre, ahol $f^* = f$ az R_v-n kívül, és $f^* = 0$ az R_v-n. Az f-re vonatkozó protokoll fájában a v gyökerű részfát egy 0-val helyettesítve egy $t - t_v + 1$ levelű protokoll fát kapunk f^*-ra. Nem okoz gondot, hogy a 2. esetben f helyett f^*-ot számolják a játékosok, ugyanis ha $(x, y) \in R_v$, akkor nem is ezt az estet alkalmazzuk.

A v megválasztása miatt mindkét esetre kaptunk egy-egy protokollt nem több, mint $2t/3$ levéllel. Ha $D(t)$-vel jelöljük, hogy egy t levelű protokollból ezen algoritmus ismételgetésével mekkora mélységű protokollhoz lehet biztosan eljutni, akkor $D(t) \leq 2 + D(2t/3)$ kell teljesüljön. Mivel $D(1) = 0$, így a rekurzív képletből $D(t) \leq 2 \log_{\frac{3}{2}} t$ következik. $\diamond$

Most már készen állunk, hogy kimondjuk a kívánt tételt:

2.30 TÉTEL: Létezik γ konstans, hogy minden f, k mellett fennáll

$$C_k(f) \geq \gamma \cdot k \cdot C(f).$$

Bizonyítás: A 2.28 Lemmából f-re létezik kétszereplős protokoll, melyhez tartozó protokoll fának legfeljebb $2^{C_k(f)/\lceil k/2\rceil}$ levele van. Alkalmazva a 2.29 Tételt a $C(f) \leq 2\log_{3/2}(2^{C_k(f)/\lceil k/2\rceil})$ eredményre jutunk, amit átalakítva kapjuk, hogy

$$C_k(f) \geq \frac{1}{2}\log\frac{3}{2} \cdot \lceil k/2\rceil \cdot C(f) > \gamma \cdot k \cdot C(f)\ ,$$

ahol $\gamma > 0,146$. $\diamond$

2.31 MEGJEGYZÉS: E. Kushilevitz rámutatott, hogy a 2.29 Tételbeli becslés javításával akár $C(f) \leq 1,813\ldots \cdot \log t$ is elérhető, amiből egy erősebb, $C_k(f) \geq 0,275 \cdot k \cdot C(f)$ becslést kapunk.

3. A „homlokra ragasztott szám" modell

A modell

Ebben a modellben, melyet [1] részletesen tárgyal k játékos vesz részt. Mindegyikük saját inputtal rendelkezik, a kommunikáció pedig táblás, azaz egy elhangzott bitről minden játékos tudomást szerez. Van még egy igen speciális tulajdonsága is ennek a modellnek, mégpedig az, hogy a szereplők inputjai között nagy (sőt a lehető legnagyobb) az átfedés. A legjobban úgy fogalmazhatunk, hogy a szereplők mindegyike nem egy-egy inputtal rendelkezik, hanem éppenhogy egy-egy inputtal nem rendelkezik. Azaz minden szereplő birtokában van a k darab inputrészből $(k-1)$, és persze mindegyiküktől másik inputrész hiányzik. A modell az elnevezését is e speciális tulajdonságáról kapta, hiszen úgy képzelhetjük el a játékosokat, mintha egy asztal körül ülve mindegyiküknek egy-egy szám lenne ragasztva a homlokára, így valamennyi játékos látná az összes számot, kivéve a saját homlokán lévőt.

Pontosabban megfogalmazva tehát a $P_1, P_2, \dots P_k$ szereplők kívánják egy adott $f : (\{0,1\}^n)^k \longrightarrow \{0,1\}$ függvény $f(x_1, x_2, \dots, x_k)$ értékét kiszámítani úgy, hogy a P_i játékos inputja $(x_1, x_2, \dots, x_{i-1}, x_{i+1}, \dots x_k)$, ahol tehát az x_j-k n hosszú 0/1-sorozatok, azaz $x_j \in \{0,1\}^n : j = 1, 2, \dots, k$.

Ehhez rendelkeznek egy $\mathcal{P}$ protokollal, mely megmondja hogy adott pillanatban véget ért-e a kommunikációs folyamat (ez esetben mi az eredmény), és ha nem, akkor melyik játékos következik szólásra, ez (az egyszerre beszélés kizárása érdekében) csak a tábla addigi tartalmától függ. Megmondja továbbá, hogy a soron következő játékos saját inputjának, és a tábla addigi tartalmának függvényében milyen bitet írjon fel a táblára. A kommunikáció hossza a táblára felírt bitek száma. Szokásos módon a protokoll hossza, a különböző inputok mellett a leghosszabb előforduló kommunikáció hossza, és egy függvény kommunikációs komplexitása - melyet e modellben jelöljön $C^k(f)$ - pedig a függvényt számoló lehető legrövidebb protokoll hossza.

Cilinder metszetek

E modell legnagyobb előnye, hogy a protokoll fa nagyon hasonlóan viselkedik, mint a kétszereplős esetben. Emlékezzünk vissza, hogy ott egy olyan bináris fáról volt szó, melynek csúcsait A és B betükkel jelöltük meg, aszerint, hogy ki következett szólásra, és a csúcsokból az elküldött bit alapján haladtunk tovább a két lehetséges gyerek valamelyikébe. A különbség itt csak az, hogy a protokoll fa csúcsainak k lehetséges megjelölése lehet, hisz k játékos következhet szólásra. Ebben a "homlokra ragasztott szám" modellben egy, az 1.4 Tétellel teljesen analóg tétel igaz, azzal a különbséggel, hogy az ottani részmátrixoknak itt cilinder-metszetek felelnek meg.

3.1 DEFINÍCIÓ: Az $S_i \subseteq X_1 \times X_2 \times \dots \times X_k$ halmaz cilinder halmaz az i-edik dimenzióban, ha az S_i-beliség, mint tulajdonság nem függ az i-edik koordinátától, azaz

$$(x_1, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_k) \in S_i \Longleftrightarrow (x_1, \dots, x_{i-1}, x_i^*, x_{i+1}, \dots, x_k) \in S_i$$

$$\forall x_j \in X_j (j = 1, \dots, k) \ , \ \forall x_i^* \in X_i$$

3.2 DEFINÍCIÓ: Az $S \subseteq X_1 \times X_2 \times \cdots \times X_k$ halmaz cilinder-metszet, ha előáll $S = \bigcap_{i=1}^k S_i$ alakban, ahol S_i halmaz rendre cilinder az i-edik dimenzióban.

A jobb szemléltetés érdekében is hasznos megadni a cilinder-metszetek egy másik, ekvivalens definícióját, amit a szemléltetésen túl sok helyen tudunk majd kíválóan alkalmazni.

3.3 DEFINÍCIÓ: Egy pont k-ast csillagnak nevezünk $X_1 \times X_2 \times \cdots \times X_k$-ban, ha a következő alakú:

$$(x_1^*, x_2, \ldots, x_k)\ ,\ (x_1, x_2^*, \ldots, x_k)\ , \ldots ,\ (x_1, x_2, \ldots, x_k^*)$$

ahol $x_i, x_i^* \in X_i$, és $x_i \neq x_i^*$ $\forall i \in \{1, \ldots, k\}$.
A fenti csillag középpontja $(x_1, x_2, \ldots, x_k)$

3.4 TÉTEL: S cilinder-metszet $\Longleftrightarrow$ minden $C \subseteq S$ csillag középpontja is S-ben van.

Bizonyítás: ($\Longrightarrow$) Tegyük fel, hogy S cilinder-metszet az $S = \bigcap_{i=1}^k S_i$ előállítással, és $C = \{(x_1^*, x_2, \ldots, x_k)\ ,\ (x_1, x_2^*, \ldots, x_k)\ , \ldots ,\ (x_1, x_2, \ldots, x_k^*)\}$ egy csillag S-ben. Akkor minden i mellett teljesül $(x_1, \ldots, x_i^*, \ldots, x_k) \in S \subseteq S_i \Longrightarrow (x_1, \ldots, x_i, \ldots, x_k) \in S_i$, hiszen S_i cilinder az i-edik dimenzióban. Mivel $(x_1, \ldots, x_i, \ldots, x_k) \in S_i$ $\forall i = 1, 2, \ldots, k$ ebből $(x_1, \ldots, x_i, \ldots, x_k) \in S$, tehát a csillag középpontja is S-ben van.

($\Longleftarrow$) Legyen az S olyan, hogy minden S-beli csillag középpontja is S-ben van. Az $S_i := \{(x_1, \ldots, x_i, \ldots, x_k) \in X_1 \times X_2 \times \cdots \times X_k \mid \exists x_i^* \in X_i : (x_1, \ldots, x_i^*, \ldots, x_k) \in S\}$ jelölés mellett $(i = 1, 2, \ldots, k)$ nyilvánvaló, hogy S_i halmaz cilinder az i-edik dimenzióban. Meg kell még mutatnunk, hogy $S = \bigcap_{i=1}^k S_i$. Az S_i-k definíciójából világos, hogy $S \subseteq S_i$ $\forall i \Longrightarrow S \subseteq \bigcap_{i=1}^k S_i$. Az $S \supseteq \bigcap_{i=1}^k S_i$ irányú tartalmazás pedig abból következik, hogy amennyiben $(x_1, \ldots, x_i, \ldots, x_k) \in \bigcap_{i=1}^k S_i$, akkor $\forall i$-re $\exists x_i^*$, hogy $(x_1, \ldots, x_i^*, \ldots, x_k) \in S$. Ezek az S-beli elemek egy csillagot alkotnak, melynek középpontja, azaz $(x_1, \ldots, x_i, \ldots, x_k)$ a feltétel szerint ugyancsak S-ben kell legyen. $\diamond$

Jelöljük R_ℓ-lel azon inputok halmazát az $X_1 \times X_2 \times \cdots \times X_k$-ból, melyek mellett az ℓ levélbe jutunk a protokoll fában.

3.5 TÉTEL: A protokoll fa mindel ℓ levelére az R_ℓ halmaz egy monokromatikus cilinder-metszet.

Bizonyítás: Hogy R_ℓ monokromatikus, az nyilvánvaló. Az 1.4 Tétel bizonyításához hasonlóan teljes indukcióval megmutatható, hogy a protokoll fa minden v pontjára az inputok azon R_v halmaza, melyek elérik a v pontot cilinder-metszetet alkotnak. Azonban a 3.4 Tétel által adott ekvivalens definíciót használva a cilinder-metszetre egy mégegyszerűbb bizonyítást adhatunk:

Megmutatjuk, hogy minden R_ℓ-beli csillag középpontja is ott van. Ez igaz hiszen ha $(x_1^*, x_2, \ldots, x_k)\ ,\ (x_1, x_2^*, \ldots, x_k)\ , \ldots ,\ (x_1, x_2, \ldots, x_k^*) \in R_\ell$, akkor ezen inputok mind az ℓ levélbe vezetnek. Viszont amikor P_i játékos $(i = 1, 2, \ldots, k)$ mond egy bitet, akkor ő nem tud különbséget tenni az $(x_1, \ldots, x_i^*, \ldots, x_k)$ és $(x_1, \ldots, x_i, \ldots, x_k)$ inputok között, így a kommunikáció az $(x_1, \ldots, x_i, \ldots, x_k)$ input esetén is az ℓ levélbe jut. $\diamond$

3.6 KÖVETKEZMÉNY: Egy t bit hosszúságú protokoll az $X_1 \times X_2 \times \cdots \times X_k$ inputhalmazt legfeljebb 2^t darab monokromatikus cilinder-metszetre osztja.

Becslések diszkrepanciával

Általában a kétszereplős kommunikációs komplexitásra vonatkozó alsó becslések nem működnek a többszereplős modellben. Az egyetlen módszer, amely egy az egyben átvihető az a diszkrepancia módszer. E módszer jól használható a kétszereplős modellben az ε-hibás kommunikációs komplexitás, és ezáltal a kommunikációs komplexitás alsó becslésére is.

3.7 DEFINÍCIÓ: Azt mondjuk, hogy egy $\mathcal{P}$ protokoll ε hibával kiszámolja az f függvényt a kétszereplős modellben ($0 \leq \varepsilon \leq 1/2$), ha $Pr(P(x,y) = f(x,y)) \geq 1 - \varepsilon$, ahol $P(x,y)$-nal azt az eredményt jelöljük, amit a $\mathcal{P}$ protokoll számol az (x,y) inputra. A valószínűséget itt úgy kell érteni, hogy a lehetséges $(x,y) \in X \times Y$ inputok egyenlő valószínűséggel léphetnek fel. Tehát a protokoll egy 1/2-nél nagyobb, de nem feltétlenül 1 valószínűséggel adja a helyes eredményt egy (x,y) véletlenszerűen választott inputon. Jelöljük $C_\varepsilon(f)$-fel a legrövidebb, f-et ε hibával számoló protokoll hosszát. Megjegyzendő, hogy eredetileg ezt a jelölést olyan esetben alkalmazzák, amikor a protokoll véletlent (pl. pénzfeldobásokat) is használhat. A tételek, melyeket igazolunk erre az esetre is igazak, de nincs szükség e fejezetben a véletlen használatára, így a definíciót e nélkül mondtuk ki.

Ha M az M_f mátrix egy részmátrixa, akkor

$$Disc(f,M) := |Pr[f(x,y) = 0, (x,y) \in M] - [Pr[f(x,y) = 1, (x,y) \in M]|,$$

ahol a valószínűséget az inputok egyenletes eloszlása mellett kell érteni. A diszkrepanciát a kétszereplős modellben egy adott f függvényre a következőképpen definiáljuk:

$$Disc(f) := \max_M Disc(f,M),$$

ahol M végigfut az M_f összes részmátrixán.

A diszkrepanciát természetesen nem csak egyenletes inputeloszlás mellett lehet értelmezni, de itt nekünk csak arra lesz szükségünk.

3.8 TÉTEL: Minden $f : X \times Y \longrightarrow \{0,1\}$ függvény, és $0 \leq \varepsilon \leq 1/2$ mellett igaz, hogy $C_{\frac{1}{2}-\varepsilon}(f) \geq \log \frac{2\varepsilon}{Disc(f)}$.

Bizonyítás: Amennyiben $\mathcal{P}$ egy t bitet használó protokoll az f-re, amely legalább $\frac{1}{2} + \varepsilon$ valószínűséggel ad helyes eredményt, akkor

$$\begin{aligned}2\varepsilon &\leq Pr[P(x,y) = f(x,y)] - Pr[P(x,y) \neq f(x,y)] = \\ &= \sum_\ell (Pr[P(x,y) = f(x,y) \text{ és } (x,y) \in R_\ell] - Pr[P(x,y) \neq f(x,y) \text{ és } (x,y) \in R_\ell])\end{aligned}$$

ahol a szummázás a protokoll fa összes levelére történik. Mivel az R_ℓ halmazok P-re nézve monokromatikusak, így a kifejezés tovább becsülhető felülről azzal, hogy:

$$\sum_\ell |Pr[f(x,y) = 0 \text{ és } (x,y) \in R_\ell] - Pr[f(x,y) = 1 \text{ és } (x,y) \in R_\ell]| \,.$$

Mivel minden R_ℓ egy-egy részmátrixa M_f-nek, így a szumma minden egyes tagját felülről becsli a $Disc(f)$. A szummának pedig legfeljebb 2^t tagja lehet, hiszen legfeljebb ennyi levéllel rendelkezhet egy t mélységű bináris fa. Tehát azt kaptuk, hogy $2\varepsilon \leq 2^t Disc(f)$, amiből átrendezéssel a kívánt $t \geq \log\left(\frac{2\varepsilon}{Disc(f)}\right)$ egyenlőtlenség adódik. $\diamond$

3.9 KÖVETKEZMÉNY: $C(f) \geq \log \frac{1}{Disc(f)}$

Nézzük hogyan vihető át ez a tétel a „homlokra ragasztott szám" modellre. Ebben a többszereplős modellben a diszkrepanciát a következőképpen definiálhatjuk:

3.10 DEFINÍCIÓ: Ha $f : X_1 \times X_2 \times \cdots \times X_k \longrightarrow \{0,1\}$ függvény, S pedig egy cilinder-metszet $X_1 \times X_2 \times \cdots \times X_k$-ben, akkor

$$Disc(f,S) := |Pr[f(x_1,x_2,\ldots,x_k) = 0,(x,y) \in S] - [Pr[f(x_1,x_2,\ldots,x_k) = 1,(x,y) \in S]|$$

$$Disc(f) := \max_S Disc(f,S) \ ,$$

ahol a maximumot az összes cilinder-metszet felett vesszük.

A kétszereplős esettel analóg módon definálható k szereplő esetén az ε-hibás kommunikációs komplexitás (C^k_ε), melyre akárcsak ott is igaz a következő tétel.

3.11 TÉTEL: $C^k_{\frac{1}{2}-\varepsilon}(f) \geq \log \frac{2\varepsilon}{Disc(f)}$.

Bizonyítás: A 3.8 Tétel bizonyítása egy az egyben átvihető a többszereplős esetre.$\diamond$

3.12 KÖVETKEZMÉNY: $C^k(f) \geq \log \frac{1}{Disc(f)}$

E következmény felhasználásával a diszkrepancia felső becslésével a kommunikációs komplexitást alulról tudjuk becsülni. Nézzük ezt meg az általánosított belső szorzat (a GIP) függvény esetében.

3.13 DEFINÍCIÓ: Ha $x_1, x_2, \ldots, x_k \in \{0,1\}^n$, akkor az általánosított belső szorzat függvényt úgy definiáljuk, hogy $GIP^k_n(x_1,x_2,\ldots,x_k) = 1$ pontosan akkor, ha páratlan azon $1 \leq j \leq n$ indexek száma, melyekre valamennyi x_i j-edik bitje 1.

E függvény kommunikációs komplexitására először Babai, Nisan és Szegedy adott alsó becslést [5]-ben:

3.14 TÉTEL: $C^k(GIP^k_n) = \Omega(\frac{n}{4^k})$

Bizonyítás: A 3.12 Következmény értelmében elég megmutatnunk, hogy

$$Disc(GIP^k_n) \leq e^{-(\frac{n}{4^k})}.$$

Az egyszerűbb algebrai kezelhetőség érdekében vezessük be a következő f függvényt:

$$f(x_1,\ldots,x_k) := \begin{cases} +1 & \text{ha } GIP^k_n(x_1,\ldots,x_k) = 0 \\ -1 & \text{ha } GIP^k_n(x_1,\ldots,x_k) = 1 \end{cases}$$

Jelölje

$$\Delta_k(n) = \max_{\phi_1,\ldots,\phi_k} |\mathbf{E}_{x_1,\ldots,x_k}[f(x_1,\ldots,x_k)\cdot\phi_1(x_1,\ldots,x_k)\cdots\phi_k(x_1,\ldots,x_k)]| \ ,$$

ahol a maximumot az összes olyan $\phi_1, \ldots, \phi_k$ függvénysorozat felett vesszük, ahol $\phi_i : (\{0,1\}^n)^k \longrightarrow \{0,1\}$ függvény nem függ az x_i változótól, az $\mathbf{E}_{x_1,\ldots,x_k}$ pedig várható értéket jelöl az inputok egyenlő valószínéggel történő választása mellett. Vegyük észre, hogy $Disc(GIP_n^k) = \Delta_k(n)$, ugyanis azon pontok halmaza az $X_1 \times \cdots \times X_k$ inputtérből, melyekre $\phi_1(x_1, \ldots, x_k) \cdots \phi_k(x_1, \ldots, x_k)$ érték 1-et ad egy cilinder metszetet alkot, és minden cilinder-metszet felírható egy ilyen szorzattal. Továbbá mivel áttértünk a $\{-1, +1\}$ értékekre, ezért itt a várható érték megegyezik a valószínűségek különbségével a diszkrepancia definíciójában.

Definiáljuk rekurzív módon a következő számsorozatot: $\beta_1 := 0$, és $\beta_j := \sqrt{\frac{1+\beta_{j-1}}{2}}$. Indukcióval könnyen kijön, hogy $\beta_k \leq 1 - 4^{1-k} < e^{-4^{1-k}}$, ezért azt kell igazolnunk, hogy

$$\Delta_k(n) \leq (\beta_k)^n \ .$$

Ezt k-ra vonatkozó teljes indukcióval fogjuk megtenni. Nyilván $\Delta_1(n) = 0 = \beta_1$, hiszen ekkor ϕ_1 konstans, ezáltal $\Delta_1(n) = \mathbf{E}_{x_1}[f(x_1)] = 0$. Tegyük fel, hogy $k \geq 2$, és k-nál kisebb értékekre tudjuk, hogy igaz az állítás. Legyenek $\phi_1, \ldots, \phi_k$ olyan függvények, melyek mellet $\Delta_k(n)$ felveszi az értékét. Mivel ϕ_k függvény nem függ az x_k változótól, és abszolút értékét felülről becsülhetjük 1-gyel, így

$$\Delta_k(n) \leq \mathbf{E}_{x_1,\ldots,x_{k-1}}[|\mathbf{E}_{x_k}[f(x_1, \ldots, x_k) \cdot \phi_1(x_1, \ldots, x_k) \cdots \phi_{k-1}(x_1, \ldots, x_k)]|] \ .$$

Felhasználva a Cauchy-Schwartz egyenlőtlenség egy speciáciális esetét, azaz, hogy egy z valószínűségi változóra $(E[z])^2 \leq E[z^2]$ azt kapjuk, hogy

$$\Delta_k(n) \leq (\mathbf{E}_{x_1,\ldots,x_{k-1}}[\mathbf{E}_{x_k}[f(x_1, \ldots, x_k) \cdot \phi_1(x_1, \ldots, x_k) \cdots \phi_{k-1}(x_1, \ldots, x_k)]]^2)^{1/2} =$$

$$= (\mathbf{E}_{u,v,x_1,\ldots,x_{k-1}}[f(x_1, \ldots, x_{k-1}, u) \cdot f(x_1, \ldots, x_{k-1}, v) \cdot \phi_1^u \cdot \phi_1^v \cdots \phi_{k-1}^u \cdot \phi_{k-1}^v])^{1/2} \ ,$$

ahol $\phi_i^u = \phi_i(x_1, \ldots, x_{k-1}, u)$ és $\phi_i^v = \phi_i(x_1, \ldots, x_{k-1}, v)$.

Az $x_i \in \{0,1\}^n$ vektorokat tekinthetjük egy n elemű X halmaz egy-egy részhalmazának a karakterisztikus vektorának, azaz az x_i vektort azonosíthatjuk a neki megfelelő részhalmazzal. Vegyük észre, hogy ekkor $f(x_1, \ldots, x_k) = (-1)^{|\bigcap_{i=1}^k x_i|}$, ahol a jobb oldalon lévő x_i-k már mint halmazok értendők. Ebből $u \triangle v$-vel jelölve az u és v halmazok szimmetrikus differenciáját az adódik, hogy

$$f(x_1, \ldots, x_{k-1}, u) \cdot f(x_1, \ldots, x_{k-1}, v) = (-1)^{|u \cap \bigcap_{i=1}^{k-1} x_i| + |v \cap \bigcap_{i=1}^{k-1} x_i|} =$$
$$= (-1)^{|(u \triangle v) \cap \bigcap_{i=1}^{k-1} x_i|} = (-1)^{\bigcap z_i} = f(z_1, \ldots, z_{k-1})$$

ahol $z_i = x_i \cap (u \triangle v)$, azaz minden x_i vektor két részre, y_i-re és z_i-re osztható, ahol z_i az x_i azon j-edik koordinátáiból áll, amelyekre $u_j \neq v_j$. Itt kihasználtuk, hogy azon elemek, melyek u-ban és v-ben (mint részhalmazban) egyaránt benne vannak, illetve amelyek egyikben sincsenek benne, azok a (-1) kitevőjében páros sokszor szerepelnek, így nyugodtan elhagyhatók. Akkor tehát

$$\Delta_k(n) \leq (\mathbf{E}_{u,v,y_1,\ldots,y_{k-1}}[\mathbf{E}_{z_1,\ldots z_{k-1}}[f(z_1, \ldots, z_{k-1}) \cdot \phi_1^u \phi_1^v \cdots \phi_{k-1}^u \phi_{k-1}^v]])^{1/2} \ .$$

A z_i-k, mint láttuk $|u\triangle v|$ hosszú vektorok, a $\phi_i^u \cdot \phi_i^v$ szorzatfüggvény pedig tekinthető a $(z_1, z_2, \ldots, z_{k-1})$ változókon értelmezett függvénynek, amely viszont nem függ a z_i változótól, így az indukciós feltevés miatt

$$\mathbf{E}_{z_1,\ldots z_{k-1}}[f(z_1,\ldots,z_{k-1})\cdot\phi_1^u\phi_1^v\cdots\phi_{k-1}^u\phi_{k-1}^v] \leq \Delta_{k-1}(|u\triangle v|) \leq (\beta_{k-1})^{|u\triangle v|} .$$

Tehát azt kaptuk, hogy

$$\Delta_k(n) \leq (\mathbf{E}_{u,v,y_1,\ldots,y_{k-1}}[\beta_{k-1}^{|u\triangle v|}])^{1/2} = (\mathbf{E}_{u,v}[\beta_{k-1}^{|u\triangle v|}])^{1/2} .$$

Amennyiben u és v uniform módon választott véletlen vektorok a $\{0,1\}^n$-ből, akkor az $u \triangle v$ vektor (illetve halmaz) eloszlása is egyenletes, tehát $Pr(|u\triangle v| = m) = \binom{n}{m}2^{-n}$. Ezért a becslés így folytatható tovább:

$$\Delta_k(n) \leq [\sum_{m=0}^{n}\binom{n}{m}2^{-n}\beta_{k-1}^m]^{1/2} = [2^{-n}(1+\beta_{k-1})^n]^{1/2} = (\beta_k)^n \ .\diamond$$

3.15 MEGJEGYZÉS: Ez a becslés tovább javítható, ugyanis, mint azt Chung és Tetali [8]-ban megmutatta $GIP_n^k = \Omega(\frac{n}{2^k})$. Bizonyításuk a kvázi-random gráfok elméletén alapul.

Ebben a modellben valamennyi ismert alsó becslés, akárcsak ez is a k növelésével exponenciálisan csökken. Jó lenne olyan függvényt találni, melyre k-tól legalább nem exponenciálisan függő, például $\frac{n}{k^c}$ típusú alsó becslés adható. Az előbb látott GIP függvény biztosan nem ilyen, ugyanis Grolmusz Vince [10]-ben igazolta, hogy az $\frac{n}{2^k}$ alsó becslés már éles.

3.16 TÉTEL: $GIP_n^k = O(k\frac{n}{2^k})$

Bizonyítás: Célszerű az inputokat egy $k\times n$-es A mátrixként tekinteni, melynek tehát i-edik sora az x_i inputrész. A GIP_n^k függvény az A mátrix csupa 1-esekből álló oszlopai számának paritását adja meg. Tekintsük a következő protokollt ennek kiszámítására.

Bontsuk fel az A mátrixot $2^{k-1}-1$ oszlopból álló blokkokra, persze az utolsó blokkba a maradék oszlopok kerülnek, melyek száma lehet ennél kisebb. Vegyük észre, hogy ha a GIP_n^k értékét ezekre a blokkokra kiszámítjuk , akkor ezeket az értékeket már csak összegezni kell modulo 2. Nézzük, hogyan számolhatjuk ki egy adott blokkra a GIP_n^k értékét nem több, mint $2k$ bit kommunikációval:

Először P_1, az első játékos kijelent egy olyan α vektort, amely nem szerepel az adott blokk oszlopai között. Ugyan nem ismeri az első sort, mégis tud ilyet mondani, hiszen a legfeljebb $2^{k-1}-1$ oszlop mindegyikének csak az első koordinátáját nem ismeri, így azok helyére mindkét lehetséges bitet beírva is csak 2^k-2 oszlop jöhet számításba, viszont összesen 2^k féle oszlopvektor létezik.

Amennyiben $\alpha = (1,1,\ldots,1)$, akkor e blokkra a GIP_n^k értéke biztosan 0, és nincs is szükség további kommunikációra. Ha nem, akkor az α vektornak létezik 0 koordinátája. Feltehetjük, hogy $\alpha = (0,\ldots,0,1,\ldots,1)$ alakú, ahol l darab 0 után $k-l$ darab 1-es következik, ugyanis ellenkező esetben a játékosok átpermutálhatók úgy, hogy ilyen alakúvá váljon. Jelölje y_i $(i = 0, 1, 2, \ldots, k)$ a blokkban szereplő $(0, \ldots, 0, 1, \ldots, 1)$ alakú oszlopok számát mod 2, ahol i darab 0 után jön $k - i$ darab 1-es, z_i pedig $(i = 1, 2, \ldots, k)$ a blokkban szereplő $(0, \ldots, 0, *, 1, \ldots, 1)$ alakú oszlopok számát mod 2, ahol $i - 1$ darab 0-t egy tetszőleges bit követ az i-edik pozícióban, majd $n - i$ darab 1-es következik. Most minden i-re P_i bejelenti a z_i értékét, amit nyilván meg tud állapítani a saját inputjából. Mivel $z_i = y_i + y_{i-1}$, és $y_l = 0$ ismert, mert α nem fordul elő az oszlopok között, így a z_i-kből kiszámítható y_0, ami nem más, mint a GIP_n^k-nak erre a blokkra megszorított értéke. Méghozzá

$$y_0 = y_0 + y_l = \bigoplus_{i=1}^{l} z_i \ .$$

(A $\oplus$ mod 2 összeadást jelent.)

Az α bejelentése k bitet igényel, míg a z_i-k közlése további k bit. Mivel a blokkok száma $O(\frac{n}{2^k})$, és minden blokkra elég $2k$ bit kommunikáció, így e protokoll valóban $O(k\frac{n}{2^k})$ kommunikációval számolja GIP_n^k értékét. $\diamond$

A kocka-módszer

Ez a módszer valójában még a diszkrepanciát használó alsó becslési módszerek közé tartozik. Ran Raz [9] felfedezett egy olyan, függvényekhez rendelhető mennyiséget, amely a diszkrepanciát felülről becsli, viszont kiszámítása sokkal egyszerűbb. Tulajdonképpen a 3.14 Tétel bizonyításának egy általánosításáról van szó, melyet ha elvégzünk, akkor sok függvényre a számolás jelentősen csökkenthető.

3.17 DEFINÍCIÓ: Az $\bar{X} = X_1 \times X_2 \times \cdots \times X_k$ inputtérben kockának nevezünk egy $D = \{a_1, b_1\} \times \{a_2, b_2\} \times \cdots \times \{a_k, b_k\}$ alakú részhalmazt, ahol $\forall i:\ a_i, b_i \in X_i$ (nem feltétlenül különbözőek). Jelölje $\mathcal{D}$ az összes kockák halmazát.

3.18 DEFINÍCIÓ: Egy $D \in \mathcal{D}$ kocka (f-re vonatkozó) előjele legyen

$$S_f(D) := \prod_{d_1 \in \{a_1, b_1\}} \prod_{d_2 \in \{a_2, b_2\}} \cdots \prod_{d_k \in \{a_k, b_k\}} f(d_1, \ldots, d_k),$$

ahol az f a $\{-1, +1\}$-be képező függvény. A $\{0, 1\}$-be képező Boole-függvényeket ezért előbb át kell alakítani ilyenné, mint azt a 3.14 Tétel bizonyításában is tettük. Látható, hogy az $S_f : \mathcal{D} \longrightarrow \{-1, +1\}$ függvény pontosan akkor ad $+1$ értéket, amennyiben a D kockán az f páros sok helyen vesz fel -1-et (és ekkor 1-et is).

3.19 DEFINÍCIÓ: Jelölje $\mathcal{E}(f) := \mathbf{E}_D[S_f(D)]$, ahol a várható értéket a D uniform megválasztása mellet tekitjük (ez persze ekvivalens azzal, hogy az a_i, b_i elemeket uniform módon választjuk az X_i-ből minden $i = 1, 2, \ldots, k$ mellett).

Ennek az $\mathcal{E}(f)$-nek az $\frac{1}{2^k}$-adik hatványa lesz az a mennyiség, ami felülről becsli a diszkrepanciát. Ezt majd a 3.22 Tételben fogjuk látni.

3.20 LEMMA: Jelölje egy $h : \bar{X} \longrightarrow \{-1, +1\}$ függvényre $\Delta(h) := \mathbf{E}_{\bar{x} \in \bar{X}}[h(\bar{x})]$, ahol a várható értéket az egyenletes eloszlás szerint vesszük. Akkor

$$\mathcal{E}(h) \geq |\Delta(h)|^{2^k}.$$

Bizonyítás:

$$\mathcal{E}(h) = \mathbf{E}_D[S_h(D)] = \mathbf{E}_{a_1,b_1\in X_1}\cdots\mathbf{E}_{a_k,b_k\in X_k}\prod_{d_1\in\{a_1,b_1\}}\cdots\prod_{d_k\in\{a_k,b_k\}} h(d_1,\ldots,d_k).$$

Tetszőleges X_k-n értelmezett g függvényre fennáll

$$\mathbf{E}_{a_k,b_k\in X_k}[g(a_k)g(b_k)] = (\mathbf{E}_{x_k\in X_k}[g(x_k)])^2.$$

Rögzített $a_1, b_1, \ldots, a_{k-1}, b_{k-1}$ mellett legyen most

$$g(x_k) = \prod_{d_1\in\{a_1,b_1\}}\cdots\prod_{d_{k-1}\in\{a_{k-1},b_{k-1}\}} h(d_1,\ldots,d_{k-1},x_k).$$

Ezáltal

$$\mathcal{E}(h) = \mathbf{E}_{a_1,b_1\in X_1}\cdots\mathbf{E}_{a_{k-1},b_{k-1}\in X_{k-1}}\Big(\mathbf{E}_{x_k}\prod_{d_1\in\{a_1,b_1\}}\cdots\prod_{d_{k-1}\in\{a_{k-1},b_{k-1}\}} h(d_1,\ldots,d_{k-1},x_k)\Big)^2.$$

Alkalmazva a Cauchy-Schwartz egyenlőtlenséget, mely szerint egy z valószínűségi változóra $E[z^2] \ge (E[z])^2$, az következik, hogy

$$\mathcal{E}(h) \ge (\mathbf{E}_{a_1,b_1\in X_1}\cdots\mathbf{E}_{a_{k-1},b_{k-1}\in X_{k-1}}\mathbf{E}_{x_k}\prod_{d_1\in\{a_1,b_1\}}\cdots\prod_{d_{k-1}\in\{a_{k-1},b_{k-1}\}} h(d_1,\ldots,d_{k-1},x_k))^2$$

$$= \Big(\mathbf{E}_{x_k}\mathbf{E}_{a_1,b_1\in X_1}\cdots\mathbf{E}_{a_{k-1},b_{k-1}\in X_{k-1}}\prod_{d_1\in\{a_1,b_1\}}\cdots\prod_{d_{k-1}\in\{a_{k-1},b_{k-1}\}} h(d_1,\ldots,d_{k-1},x_k)\Big)^2.$$

Ezt k-szor ismételve pedig azt kapjuk, hogy

$$\mathcal{E}(h) \ge (\mathbf{E}_{x_k\in X_k}\cdots\mathbf{E}_{x_1\in X_1}h(x_1,\ldots,x_k))^{2^k} = |\Delta(h)|^{2^k}.\diamond$$

3.21 LEMMA: Tetszőleges $f : \bar{X} \longrightarrow \{-1,+1\}$ függvényhez létezik egy olyan $h : \bar{X} \longrightarrow \{-1,+1\}$ függvény, amelyre $\mathcal{E}(h) = \mathcal{E}(f)$, és $|\Delta(h)| \ge Disc(f)$.

Bizonyítás: Azt fogjuk használni, hogy amennyiben tetszőleges $i \in \{1,2,\ldots,k\}$ mellett g nem függ az i-edik változójától, akkor $\mathcal{E}(fg) = \mathcal{E}(f)$ (itt $fg(x) = f(x)g(x)$ a szorzatfüggvényt jelöli). Ez $\forall\ f,g$ mellett igaz, hiszen nyilván minden D kockára a definíció szerint $S_{fg}(D) = S_f(D)S_g(D)$, és ha g nem függ például az x_k változótól, akkor $g(d_1,\ldots,d_{k-1},a_k) = g(d_1,\ldots,d_{k-1},b_k)$ $\forall d_1,\ldots,d_k,a_k,b_k$ mellett, így a g függvény páros sok D-beli elemen ad 1-et, tehát $S_g(D) = 1$. Ebből az is következik, hogy ha g_i nem függ az i-edik változójától, akkor

$$\mathcal{E}(fg_1g_2\cdots g_k) = \mathcal{E}(f).$$

Jelöljön most $T = \bigcap_{i=1}^k T_i$ egy olyan cilinder-metszetet, melyre $Disc(f,T) = Disc(f)$. Legyen $i \in \{1,2,\ldots,k\}$ esetén $g_i : \bar{X} \longrightarrow \{-1,+1\}$ a következő függvény (valószínűségi változó): $g_i(\bar{x}) = 1$ (1 valószínűséggel) ha $\bar{x} \in T_i$, ellenkező esetben pedig $\frac{1}{2}$ valószínűséggel $g_i(\bar{x}) = 1$ illetve $\frac{1}{2}$ valószínűséggel $g_i(\bar{x}) = -1$. A g_i-k legyenek persze függetlenek. Jelölje továbbá $g := g_1 g_2 \cdots g_k$. Akkor az előbb említettek miatt teljesül

$$\mathcal{E}(fg) = \mathcal{E}(f).$$

Vegyük észre, hogy amennyiben $\bar{x} \in T$, akkor (1 valószínűséggel) $g(\bar{x}) = 1$, különben pedig $\frac{1}{2}$ valószínűséggel $g(\bar{x}) = 1$, és $\frac{1}{2}$ valószínűséggel $g(\bar{x}) = -1$. Ezért ha $\bar{x} \in T$, akkor $\mathbf{E}_g[g(\bar{x})] = 1$ ha pedig $\bar{x} \notin T$, akkor $\mathbf{E}_g[g(\bar{x})] = 0$. Azaz $\mathbf{E}_g$ éppen a T halmaz karakterisztikus függvénye. Ezáltal

$$|\mathbf{E}_g \Delta(fg)| = |\mathbf{E}_g \mathbf{E}_{\bar{x}}[f(\bar{x})g(\bar{x})]| = |\mathbf{E}_{\bar{x}} \mathbf{E}_g[f(\bar{x})g(\bar{x})]| = |\mathbf{E}_{\bar{x}}[f(\bar{x})\mathbf{E}_g[g(\bar{x})]]| =$$

$$= ||\{\bar{x} : \bar{x} \in T, f(\bar{x}) = 1\}| - |\{\bar{x} : \bar{x} \in T, f(\bar{x} = -1)\}|| = Disc(f, T).$$

A konvexitás miatt pedig

$$\mathbf{E}_g|\Delta(fg)| \geq |\mathbf{E}_g \Delta(fg)| = Disc(f, T) = Disc(f).$$

Tehát létezik olyan g, hogy a $h = fg$ választás mellett teljesülnek a kívánt feltételek.$\diamond$

3.22 TÉTEL: $\forall f : \bar{X} \longrightarrow \{-1, +1\}$ függvényre $\mathcal{E}(f) \geq Disc(f)^{2^k}$.

Bizonyítás: A 3.21 Lemmából nyert h-ra alkalmazva a 3.20 Lemmát

$$\mathcal{E}(f) = \mathcal{E}(h) \geq |\Delta(h)|^{2^k} \geq Disc(f)^{2^k}.\diamond$$

3.23 KÖVETKEZMÉNY: $C^k(f) \geq 2^{-k} \log \frac{1}{\mathcal{E}(f)}$.

Bizonyítás: A 3.12 Következmény és a 3.22 Tétel következménye.$\diamond$

Hogy eddig eljussunk sokat kellett számolnunk, de megérte, ugyanis sok f-re az $\mathcal{E}(f)$ pontos értéke könnyen, kombinatorikai eszközökkel számolható. Nézzük meg például a GIP függvényhez tartozó $\mathcal{E}$ értéket.

3.24 ÁLLÍTÁS: $\mathcal{E}(f) = (1 - \frac{1}{2^{k-1}})^n$, ahol f a GIP_n^k függvény $\{-1, +1\}$ értékkészletű változata.

Bizonyítás: Legyen $D = \{a_1, b_1\} \times \{a_2, b_2\} \times \cdots \times \{a_k, b_k\}$ egy tetszőleges kocka $(\{0,1\}^n)^k$-ban. Mint azt a 3.14 Tétel bizonyításában már láttuk, ez a függvény tulajdonképpen egy n elemű alaphalmaz részhalmazaira megadja a metszet paritását. Jelöljük ezért a kisbetűs 0/1 sorozatoknak megfeleltethető részhalmazt a megfelelő nagybetűvel. Akkor

$$S_f(D) = \prod_{\substack{d_i \in \{a_i, b_i\} \\ i \in \{1,2,\ldots,k\}}} f(d_1, \ldots, d_k) = \prod_{\substack{D_i \in \{A_i, B_i\} \\ i \in \{1,2,\ldots,k\}}} (-1)^{|\bigcap_{i=1}^k D_i|} = (-1)^{\sum_{\substack{D_i \in \{A_i, B_i\} \\ i \in \{1,2,\ldots,k\}}} |\bigcap_{i=1}^k D_i|}.$$

Ebből pedig

$$S_f(D) = (-1)^{|\bigcap_{i=1}^k A_i \triangle B_i|},$$

hiszen azon elemek, melyek nem $A_i \triangle B_i$-ben vannak biztosan páros sokszor adódnak össze a (-1) kitevőjében.

A D kocka véletlen megválasztása ekvivalens az A_i, B_i halmazok uniform módon történő megválasztásával. Ekkor pedig az $A_i \triangle B_i$ halmaz is az egyenletes eloszlás szerint választódik ki, azaz minden alaphalmazbeli elem $1/2$ valószínűséggel van $A_i \triangle B_i$-ben. Ebből

$$\mathcal{E}(f) = \mathbf{E}_D[S_f(D)] = \sum_{j=1}^{n} (-1)^j \cdot p_j,$$

ahol p_j annak a valószínűsége, hogy az n elemű alaphalmaz k darab véletlenszerűen választott részhalmazának metszete j elemű. Tehát

$$p_j = \binom{n}{j} \left(\frac{1}{2^k}\right)^j \left(1 - \frac{1}{2^k}\right)^{n-j}$$

És így

$$\mathcal{E}(f) = \sum_{j=1}^{n} (-1)^j \binom{n}{j} \left(\frac{1}{2^k}\right)^j \left(1 - \frac{1}{2^k}\right)^{n-j} = \left(\left(1 - \frac{1}{2^k}\right) - \frac{1}{2^k}\right)^n = \left(1 - \frac{1}{2^{k-1}}\right)^n. \ \diamond$$

Ebből pedig a 3.23 Következménnyel ismét adódik a 3.14 Tétel.

Nézzünk meg a kocka módszert egy másik függvény esetén is. Jelölje $X = \{0,1\}^{n \times n}$ az $n \times n$-es $0/1$ mátrixok halmazát. Ha $x_1, x_2, \ldots, x_k \in X$, akkor az F, mátrix szorzás függvényt a következőképpen értelmezzük:

$$F(x_1, x_2, \ldots, x_k) = (x_1 \cdot x_2 \cdots x_k)_{1,1}.$$

Tehát $F(x_1, x_2, \ldots, x_k)$ az $x_1, x_2, \ldots, x_k$ mátrixok ($GF(2)$ felett tekintett) szorzatának bal felső sarkában lévő eleme. Térjünk át ismét $\{-1, +1\}$ értékkészletre, azaz legyen $f(x_1, x_2, \ldots, x_k) := (-1)^{F(x_1, x_2, \ldots, x_k)}$.

3.25 ÁLLÍTÁS: Erre az f-re $\mathcal{E}(f) \leq \frac{k-1}{2^n}$.

Bizonyítás: Legyen $D = \{a_1, b_1\} \times \{a_2, b_2\} \times \cdots \times \{a_k, b_k\}$ egy tetszőleges kocka X^k-ban. Akkor

$$S_f(D) = \prod_{\substack{d_i \in \{a_i, b_i\} \\ i \in \{1,2,\ldots,k\}}} f(d_1, \ldots, d_k) = \prod_{\substack{d_i \in \{a_i, b_i\} \\ i \in \{1,2,\ldots,k\}}} (-1)^{F(d_1, d_2, \ldots, d_k)} = (-1)^{\sum_{\substack{d_i \in \{a_i, b_i\} \\ i \in \{1,2,\ldots,k\}}} F(d_1, d_2, \ldots, d_k)}$$

Az utóbbi összegzés nyilván elég, ha $GF(2)$ felett történik. Mivel F minden változójában lineáris, így ha $\oplus$ jelöli a $GF(2)$ feletti összeadást, akkor

$$S_f(D) = (-1)^{F(a_1 \oplus b_1, a_2 \oplus b_2, \ldots, a_k \oplus b_k)}$$

Ha a D kocka uniform módon választott, akkor $(a_1 \oplus b_1, a_2 \oplus b_2, \ldots, a_k \oplus b_k)$ is egyenletes eloszlással van választva X^k-ból, ezért

$$\mathcal{E}(f) = \mathbf{E}_D[S_f(D)] = \mathbf{E}_D[(-1)^{F(a_1\oplus b_1, a_2\oplus b_2, \ldots, a_k\oplus b_k)}] =$$

$$= \mathbf{E}_{\vec{x}}[(-1)^{F(x_1,x_2,\ldots,x_k)}] = \mathbf{E}_{\vec{x}}[f(x_1, x_2, \ldots, x_k)] =: \Delta(f)$$

A $\Delta(f)$ becsléséhez legyen $(x_1, x_2, \ldots, x_k)$ véletlen vektor egyenletes eloszlással véve az X^k-ból. Jelölje E_d ($1 \le d \le k$ esetén) azt az eseményt, hogy az $x_1 \cdot x_2 \cdots x_d$ mátrix első sorának minden eleme 0. Legyen ezek után $p_d := Pr(E_d)$. Akkor $p_1 = Pr(E_1) = \frac{1}{2^n}$, valamint $Pr(E_{d+1}|E_d) = 1$, és mivel x_{d+1} is egyenletes eloszlású, így $Pr(E_{d+1}|\neg E_d) = \frac{1}{2^n}$. Ebből ha $1 \le d < k$, úgy

$$p_{d+1} = p_d + (1 - p_d)\frac{1}{2^n} \le p_d + \frac{1}{2^n},$$

ami d-re vonatkozó indukcióval adja, hogy

$$p_d \le d\frac{1}{2^n}.$$

Amennyiben E_{k-1} fennáll, úgy $f(x_1, x_2, \ldots, x_k)$ biztosan 1, ellenkező esetben pedig mivel x_k is egyenletes eloszlású, ezért $f(x_1, x_2, \ldots, x_k)$ ekkor egyenlő valószínűséggel lehet $+1$ illetve -1, azaz

$$\mathcal{E}(f) = \Delta(f) = p_{k-1} \le (k-1)\frac{1}{2^n} \quad \diamond$$

Ezzel az állítással a 3.23 Következmény segítségével megkaptuk, hogy a mátrix szorzás függvényére a „homlokra ragasztott szám" modellben $C^k(f) = \Omega(\frac{n}{2^k})$.

Raz egyébként azt sejti, hogy ez az alsó becslés egyáltalán nem éles, így a mátrixszorzás függvénye egyike azon függvényeknek, melyekre várható, hogy egy k-ban nem exponenciálisan csökkenő alsó becslést lehet igazolni.

Ramsey típusú becslések

Időnként Ramsey típusú számokkal is lehet becsülni e modellben a kommunikációs komplexitást. A most következő függvényre mindkét irányú becslést e módszerrel adjuk meg.

3.26 DEFINÍCIÓ: Jelölje $E_N^k : \{1, \ldots, N\}^k \longrightarrow \{0, 1\}$ azt a függvényt, amelyre $E_N^k(x_1, \ldots, x_k) = 1 \Leftrightarrow \sum_{i=1}^k x_i = N$. Ez az ún. „pontosan N" függvény.

3.27 DEFINÍCIÓ: Definiáljuk a $\xi_k(N)$ Ramsey számot a következőképpen:

$\xi_k(N)$ az a legkisebb természetes szám, melyre $\xi_k(N)$ színnel ki lehet színezni az $\{1, 2, \ldots, N\}^{k-1}$ halmazt úgy, hogy minden $(x_1, \ldots, x_{k-1})$ és minden $\lambda \ne 0$ mellet ha

$$\begin{gathered}(x_1 + \lambda, x_2, \ldots, x_{k-1})\\ (x_1, x_2 + \lambda, \ldots, x_{k-1})\\ \vdots\\ (x_1, x_2, \ldots, x_{k-1} + \lambda)\\ (x_1, x_2, \ldots, x_{k-1})\end{gathered}$$

vektorok mind $\{1,2,\ldots,N\}^{k-1}$-ből valók, akkor nem mind egyforma színnel van színezve. Egy ilyen színezést a továbbiakban legálisnak mondunk.

3.28 TÉTEL: $C^k(E_N^k) = O(k + \log \xi_k(N))$.

Bizonyítás: Színezzük ki $\{1,2,\ldots,N\}^{k-1}$-et $\xi_k(N)$ színnel legálisan, és tekintsük a következő protokollt E_N^k kiszámítására:

Minden $i \le k-1$ -re a P_i játékos számolja ki az $x_i^* := N - \sum_{j \ne i} x_j$ értéket. Megteheti, hisz x_i kivételével minden inputot ismer. Az x_i^* az az érték, amennyinek az x_i-nek kell lennie, hogy az E_N^k függvény 1-et adjon. Amennyiben $\exists i :\ x_i^* \le 0$, akkor biztos, hogy a szumma nagyobb N-nél, így P_i már tudja is, hogy a végeredmény 0. Egyébként az előbbi P_i-k számolják ki az $(x_1,\ldots,x_i^*,\ldots,x_{k-1})$ színét. A P_k játékos számolja az $(x_1,\ldots,x_k)$ színét. Ezek után a játékosok ellenőrzik, hogy valamennyi szín megegyezik-e. Ha igen, az eredmény 1, ha nem, az eredmény 0. Vegyük észre, hogy ehhez elég az első játékosnak felírnia a számolt színt ($\log \xi_k(N)$ bit), a többieknek pedig csak egy-egy bitet kell küldeni aszerint, hogy az ő színük megegyezik-e azzal.

Az így számolt eredmény azért helyes, mert amennyiben $\sum_{j=1}^k x_j = N$, akkor minden i-re $x_i = x_i^*$, így ekkor mindenki az $(x_1,\ldots,x_k)$ színét számolja, míg ha $\sum_{j=1}^k x_j \ne N$, akkor $\sum_{j=1}^k x_j = N - \lambda$, így ekkor a játékosok által számolt színek az

$$\begin{gathered}(x_1+\lambda, x_2, \ldots, x_{k-1})\\ (x_1, x_2+\lambda, \ldots, x_{k-1})\\ \vdots\\ (x_1, x_2, \ldots, x_{k-1}+\lambda)\\ (x_1, x_2, \ldots, x_{k-1})\end{gathered}$$

vektorok színei. Mivel legális színezést vettük, ezért ezek a színek nem mind egyformák. $\diamond$

3.29 TÉTEL: $C^k(E_N^k) \ge \log \xi_k(\lfloor \frac{N-1}{k-1} \rfloor)$.

Bizonyítás: Tehát azt kell belátnunk, hogy $2^{C^k(E_N^k)} \ge \xi_k(\lfloor \frac{N-1}{k-1} \rfloor)$. Tekintsünk egy optimális protokollt E_N^k-ra, akkor az ehhez tartozó protokoll fa mélysége $C^k(E_N^k)$, ezért leveleinek száma legfeljebb $2^{C^k(E_N^k)}$. Azonosítsuk a különböző leveleket egy-egy különböző színnel, így azt kell megmutatni, hogy ezekkel a színekkel meg lehet az $\{1,\ldots,\lfloor \frac{N-1}{k-1} \rfloor\}^{k-1}$ elemeit legálisan színezni.

A színezést úgy végezzük, hogy az $(x_1,\ldots,x_{k-1})$ vektor azt a levelet kapja színéül, amelybe az $(x_1,\ldots,x_{k-1}, N - \sum_{i=1}^{k-1} x_i)$ input mellett a protokoll fa visz. Mivel az x_i-k $\{1,\ldots,\lfloor \frac{N-1}{k-1} \rfloor\}$-ből vannak, így ez értelmes, azaz a k-adik komponens is $1,\ldots,N$-be esik. Az így megadott színezés legális, ugyanis ha van k egyszínű vektor az $\{1,\ldots,\lfloor \frac{N-1}{k-1} \rfloor\}$-ből a következő alakban:

$$\begin{gathered}(x_1+\lambda, x_2, \ldots, x_{k-1})\\ (x_1, x_2+\lambda, \ldots, x_{k-1})\\ \vdots\\ (x_1, x_2, \ldots, x_{k-1}+\lambda)\\ (x_1, x_2, \ldots, x_{k-1})\end{gathered}$$

akkor az alábbi k input azonos levélbe vezet:

$$\begin{gathered}(x_1+\lambda, x_2, \ldots, x_{k-1}, N-\sum_{i=1}^{k-1} x_i-\lambda)\\ (x_1, x_2+\lambda, \ldots, x_{k-1}, N-\sum_{i=1}^{k-1} x_i-\lambda)\\ \vdots\\ (x_1, x_2, \ldots, x_{k-1}+\lambda, N-\sum_{i=1}^{k-1} x_i-\lambda)\\ (x_1, x_2, \ldots, x_{k-1}, N-\sum_{i=1}^{k-1} x_i)\end{gathered}$$

Ez a 3.5 Tétel miatt azt jelenti, hogy ez a k input egyazon 1-monokromatikus cilinder metszetben van. Mivel a fenti inputok láthatóan egy csillagot alkotnak, így a 3.4 Tétel értelmében a csillag középpontja, $(x_1, x_2, \ldots, x_{k-1}, N-\sum_{i=1}^{k-1} x_i-\lambda)$ is ebben az 1-monokromatikus cilinder-metszetben van. Ami nyilvánvalóan ellentmondás, hiszen ezen inputra a tagok összege $N-\lambda$, így a protokoll 0 eredményt kell adjon. $\diamond$

3.30 MEGJEGYZÉS: Könnyen belátható, hogy $\xi_k(N) \leq k \cdot \xi_k(\frac{N}{k})$, ebből az előző tétel úgy fogalmazható, hogy $C^k(E_N^k) = \Omega(\log \xi_k(N))$. Azaz utóbbi két tételünk a E_k^N függvény pontos nagyságrendjét adják a $\xi_k(N)$ függvényében, viszont sajnos a $\xi_k(N)$ értéke nem ismert. Egyedül $k = 3$ mellett ismert egy jó becslés, ui. tudjuk, hogy $\xi_3(N) \leq exp(\sqrt{\log N} \log\log N)$.

Más alternatíva a protokoll definiálására

E fejezet végén felhívnánk a figyelmet arra, hogy a protokoll fogalmának definiálása sem egyértelmű a többszereplős kommunikáció esetén. A protokollt eddig a kétszereplős modell mintájára úgy definiáltuk a „homlokra ragasztott szám" modellben is, hogy olyan függvény, mely kijelöli azt, hogy mikor ki szól, illetve végetérés esetén a végeredményt az elhangzott bitek függvényében. Illetve megmondja, hogy a szólásra következő játékos milyen bitet mondjon a játékos inputja, és az elhangzott bitek függvényében. Azért definiáltuk így a protokoll fogalmát minden esetben, hogy biztosítsuk, hogy a játékosok számára mindig egyértelmű legyen, hogy ki következik szólásra, illetve a protokoll végén minden játékos ugyanarra a végeredményre gondoljon. Viszont egyszerűen úgy is definiálhatjuk a protokoll fogalmát, hogy utóbbi tulajdonságait feltételként szabjuk meg neki. A szakdolgozat szerzőjének tudomása szerint a most következő protokoll definícióval még nem vizsgálta senki a „homlokra ragasztott szám" modellt.

3.31 DEFINÍCIÓ: Személyre szóló protokollnak nevezünk egy tetszőleges kommunikációs modellben egy olyan függvénycsoportot, melyben minden szereplőhoz tartozik egy függvény, ami egy adott pillanathoz megmondja, hogy ez a szereplő következik-e szólásra, és ha igen milyen bitet mondjon, illetve ha véget ért a kommunikáció, akkor mi a végeredmény. Mindezt a játékos inputja, és az elhangzott bitek függvényében teszi. E mellet teljesül, hogy:

Minden pillanatban pontosan egy játékos gondolja, hogy ő következik szólásra, kivéve, ha véget ért a kommunikáció (ilyenkor persze egy sem), ekkor pedig minden szereplő ugyanarra a végeredményre gondol.

Látható, hogy a különbség a szólásra következő játékos kijelölésében, és a végeredmény meghatározásában rejlik. Míg a hagyományos protokoll minden játékos számára elérhető adatokból, és ezért minden játékos számára egyértelműen közölte, hogy ki következik szólásra, addig a személyre szóló protokoll esetén a játékosok nem tudják, hogy ki a szólásra következő, csak annyit tudnak, hogy éppen ők jönnek, vagy sem. E mellet feltételként szabtuk meg, hogy egyértelmű legyen, ki küldjön éppen bitet. Ezen túl személyre szóló protokollnál azt is megengedjük, hogy a játékos által gondolt végeredmény is függjön a játékos inputjától, szintén feltételként megszabva, hogy ez minden játékosnál ugyanaz legyen. Könnyen látszik, hogy:

3.32 ÁLLÍTÁS: A Yao-féle kétszereplős kommunkációs modellben a hagyományos és a személyre szóló protokoll fogalma megegyezik.

Bizonyítás: Egy hagyományos protokoll olyan függvényekből áll, melyek az A és B játékosok közötti kommunikáció függvényében határozzák meg a következő játékost, illetve végetérés esetén a végeredményt. Az elküldendő bit meghatározása megegyezik a két esetben. Így egy hagyományos protokoll megfelel egy személyre szóló protokollnak, az ugyanis még ennél több dolog függvényében határozza meg az előbbieket. Pontosabban a szólásra következő játékost, és végeredményt kijelölő függvényből mindkét játékosnak adva egy-egy példányt egy személyre szóló protokollt kapunk. Azt kell még megmutatni, hogy a kétszereplős modellben a személyre szóló protokollnál a játékos szólásra következése, és a végeredmény ténylegesen nem függhet a játékos inputjától. Ez pedig azért igaz, mert különben létezne olyan $x, x^* \in X$, $y \in Y$, és s bitsorozat, hogy az s elhangzása után, ha B-nél y input van, és A-nál x, akkor A azt hiszi, hogy ő jön szólásra, viszont ha A-nál x^* van, akkor azt hiszi, hogy B következik. Ez biztosan nem lehet, ugyanis B is gondol valamelyikükre, így az egyik esetben egyszerre próbálnának beszélni.$\diamond$

Sőt a k szereplős táblás kommunikációs modellben is egybeesik a két fogalom, ha az inputok között nincs átfedés (mindenki csak egy inputot lát), a fenti bizonyítás ekkor is működik.

Viszont a „homlokra ragasztott szám" modellben a hagyományos, és személyre szóló protokollok eltérnek. Látható például, hogy egy személyre szóló protokoll megengedi azt, hogy a $P_2, P_3, \ldots, P_k$ játékosok közül a mindannyiuk számára elérhető x_1 input alapján dőljön el, hogy ki következik szólásra.

Ez azt eredményezi, hogy a kommunikációs komplexitása is különböző lehet egy függvénynek a két protokollfogalom mellett. Nézzünk meg erre egy egyszerű példát:

Legyen $k = 3$, és f az a függvény, amelyre $f(x_1, x_2, x_3)$ érték az x_2 első bitjével egyezik meg ha x_1 első bitje 0, és x_3 első bitjével egyezik meg, ha x_1 első bitje 1.

3.33 ÁLLÍTÁS: Erre az f-re $C_S^3(f) < C^3(f)$, ahol az S az indexben a személyre szóló protokollokra utal.

Bizonyítás: Személyre szóló protokollt tudunk adni 1 bit kommunikációval, hiszen azt mondjuk, hogy x_2 következzék szólásra, ha x_1 első bitje 1, és x_3 következik szólásra, ha x_1 első bitje 0. Ekkor a szólásra következő játékos látja a végeredményt, és így fel tudja írni a táblára. Viszont hagyományos protokoll legalább 2 bit kommunikációt igényel, ugyanis egy 1 bites kommunikációban a bitet felíró játékost mindentől függetlenül kell kijelölni, és bárkit is jelölünk ki, könnyen adható olyan input, melyre az a játékos nem tudja az eredményt felírni.$\diamond$

Az a kérdés, hogy a két kommunikációs komplexitás között mekkora eltérés lehet. Mint láttuk a személyre szóló definíció általánosabb a hagyományosnál, így $C_S^k(f) \leq C^k(f)$ mindig teljesül, de mennyivel lehet $C_S^k(f)$ kisebb. Erre egy felső korlátot tudunk adni.

3.34 TÉTEL: $(k+1)C_S^k(f) + 1 \geq C^k(f)$ minden f-re.

Bizonyítás: Egy személyre szóló protokollból mindig tudunk készíteni egy hagyományosat a következőképpen. Amikor a személyre szóló protokoll szerint egy játékos felír egy bitet a táblára, akkor még ez előtt minden játékos írjon fel egy-egy bitet indexük szerinti sorrendben, méghozzá 1-est pontosan az a játékos írjon, aki szólásra következik. Ezzel a módosítással már egy hagyományos protokollhoz jutottunk, hiszen a táblán lévő bitekből mindig megmondható, hogy ki következik szólásra. Esetleg szükség lehet még egy bitre, az eredmény felírására, hisz elképzelhető, hogy ez nem történt meg, és a játékosok még inputjuktól is függően gondolnak valamilyen végeredményre. Ebből következik a tétel.$\diamond$

Sejthető esetleg, hogy ez már majdnem éles, és adható olyan f függvény, amelyre körülbelül egy $(k-1)$ szorzóval nagyobb a hagyományos értelemben vett kommunikációs komplexitás. Ennek bizonyításához azonban mindenképpen valami új technikára lenne szükség. Ugyanis könnyen látszik, hogy a protokoll fa adott levelébe érkező inputok halmaza az altarnatív protokoll definíció mellett is cilinder metszetet alkot. Ezáltal az alsó becslési technikák mind működnek ekkor is, így ha eltérést szeretnénk bizonyítani, úgy a hagyományos komplexitásra más módszerrel kell adnunk egy jobb alsó becslést.

4. A csillag modell

A csillag modellben, melyet e szakdolgozatban elsőként vizsgálunk k játékos, $P_1, P_2, \ldots, P_k$ vesz részt, egy-egy inputtal a $\{0,1\}^n$-ből. Mindegyikük kapcsolatban áll egy $k+1$-edik, központi P_0 játékossal, aki azonban nem rendelkezik inputrésszel. Így kell a szereplőknek egy $f : (\{0,1\}^n)^k \longrightarrow \{0,1\}$ függvény értékét kiszámolják minimális kommunikáció felhasználásával, ahol a kommunikáció a k kapcsolaton elhangzott kommunikációk összege. Tehát az 1. fejezetben ismertetett kategorizálással ez a modell személyes kommunikáción alapuló modell, ahol a kommunikációs gráf egy k ágú csillag, és inputrésszel a központi játékoson kívül mindenki rendelkezik.

3.abra

Ez a modell a 2. fejezetben tárgyalt lineáris hálózatra annyiban hasonlít, hogy az inputtal rendelkező játékosok input nélküli közbülső szereplőkön keresztül kénytelenek kommunikálni. A 3. fejezetbeli modellel pedig az a közös vonás, hogy sok szereplő rendelkezik inputtal.

Nézzük meg, hogyan kell e modellben a megengedett protokollt definiálni ahhoz, hogy akár a 2. fejezetben egy olyan aszinkron modellt kapjunk, melyben egy protokoll mindig lefuttatható, és minden lefutása ugyanazon bitsorozatokat eredményezi valamennyi kapcsolaton: Minden kapcsolathoz rendeljünk itt is egy protokoll fát, mely azon a kapcsolaton addig elhangzott bitek függvényében meghatározza, hogy a két játékos közül melyik következik szólásra, illetve ha már egyikük sem, akkor számukra mi a végeredmény. Ha egy kapcsolaton az inputtal rendelkező játékos következik szólásra, akkor a protokoll megadja, hogy a játékos az inputja, és a kapcsolaton addig elhangzott bitek függvényében milyen bitet küldjön a központnak. Az aszinkronitás miatt ezt a bitet bármikor elküldheti, de a szándékos blokkolás kiküszöbölése érdekében véges időn belül ezt meg is kell tennie. A protokollhoz tartozik még k függvény, $\Phi_1, \Phi_2, \ldots, \Phi_k$, ahol Φ_i függvény azt adja meg, hogy ha az i-edik kapcsolaton a P_0 következik szólásra, akkor az összes kapcsolaton addig elhangzott bitek függvényében a központ milyen bitet küldjön a P_i-nek. A Φ_i értékkészlete $\{0,1,\perp\}$, és $\perp$ az érték pontosan akkor, ha az i-edik kapcsolaton nem a központ következik szólásra, vagy a központ még biteket vár más játékosoktól ahhoz, hogy eldöntse, milyen bitet küldjön P_i-nek. A szükséges feltételek hasonlóak a lineáris hálózatra tettekkel:

(1) Konzisztencia a protokoll fákkal: Ha az i-edik kapcsolaton adott pillanatban P_i következik szólásra, akkor e pillanatban a Φ_i értéke $\perp$ (azaz a központ nem szólhat).

(2) Nincs szándékos blokkolás: Ha egyik kapcsolaton sem az inputtal rendelkező játékos következik szólásra (azaz minden kapcsolaton vagy P_0 jön, vagy már nincs további kommunikáció), és a protokoll még nem fejeződött be, akkor létezik olyan i, hogy a Φ_i értéke nem $\perp$.

(3) A központ nem gondolhatja meg magát: Ha Φ_i értéke nem $\perp$, akkor ez az érték már nem változhat meg további kommunikáció hatására.

(4) Egyhangúság: Ha a protokoll befejeződött, akkor a k kapcsolathoz tartozó protokoll fák azonos eredményt jelentő levélben kötöttek ki. Ez a végeredmény.

A lineáris hálózatnál azt vizsgáltuk meg, hogy az ottani kommunikációs komplexitás hogyan viszonyul a hagyományos kétszereplős modellbelihez. Itt a csillag modellben viszont a szereplők egy k-változós függvényt számítanak ki, ezért kapcsolatot csak olyan modellbeli kommunikációs komplexitással kereshetünk, ahol ugyanez áll fenn. A modell, amelyhez viszonyítunk az a modell lesz, amelyben k szereplő - mindegyike saját inputtal a $\{0,1\}^n$-ből - szeretné kiszámítani egy $f : (\{0,1\}^n)^k \longrightarrow \{0,1\}$ k-változós függvény értékét táblás kommunikácikóval (ld. 1. fejezet). Ezt a modellt a továbbiakban táblás modellnek hívjuk majd.

Jelölje a továbbiakban egy k-változós f függvény kommunikációs komlexitását a táblás modellben $C_k^T(f)$, a csillag modellben pedig $C_k^*(f)$. Mind alsó, mind felső becslést fogunk adni a $C_k^*(f)$-re a $C_k(f)$ függvényében.

4.1 TÉTEL: $C_k^*(f) \leq k \cdot C_k^T(f)$

Bizonyítás: Tekintsünk egy optimális, azaz $C_k^T(f)$ bitet használó protokollt az f kiszámítására a táblás modellben. Amikor az i-edik játékos e protokoll szerint felír a táblára egy bitet, akkor a csillag modellben a P_i játékos küldje el a bitet a központnak, aki pedig továbbítsa az összes többi $k-1$ játékosnak. Így a csillag modellben szimuláljuk a táblás kommunikációt, hiszen valóban minden bitről minden játékos tudomást szerez. A táblás modellbeli minden bithez k darab bit elküldése szükséges e szimulációhoz, tehát a tételbeli felső becslés valóban fennáll.$\diamond$

4.2 TÉTEL: Ha f nem konstans, akkor $C_k^*(f) \geq C_k^T(f) + (k-1)$.

Bizonyítás: Tekintsünk egy optimális, azaz $C_k^*(f)$ bitet használó protokollt az f kiszámítására a csillag modellben. Adunk egy protokollt a táblás modellre, mely legfeljebb $C_k^*(f)$ kommunikációt használ. Amikor az i-edik játékos ($i \neq 0$) egy bitet küld a központnak a csillag modellben, akkor a táblás modellben az i-edik játékos írja fel ezt a bitet a táblára. Amennyiben egyszerre több inputtal rendelkező játékos is szólásra következik, akkor köztük valamilyen előre meghatározott sorrend (például indexük) döntse el, hogy kit szimulálunk először. Ezek után amikor a központ küld egy bitet például a j-edik játékosnak a csillag modellben, akkor a táblás modellben ne történjék semmi. Nem is kell, hiszen a központ az elküldött bitet a hozzá addig beérkezett bitekből számolta ki, ezek viszont mind a táblán vannak, így a j-edik játékos ezt maga is kiszámolhatja. Így a táblás modellre adott protokoll annyival kevesebb bitet használ a csillag modellbelinél, ahány bit a központból továbbítódott valamely inputtal rendelkező játékos felé. Ebből persze $C_k^*(f) \geq C_k^T(f)$ azonnal következik, méghozzá az f-re tett feltétel nélkül is. Azt hogy a tétel is igaz azt a következőkben igazoljuk.

Ha f nem konstans, akkor a csillag modellben minden kapcsolaton el kell legalább egy bitnek hangzania valamilyen irányban, hiszen ha mondjuk az i-edik kapcsolaton nincs kommunikáció, ez azt jelentené, hogy P_i számára a végeredmény semmitől sem függ, tehát f konstans. Ha a csillag modellbeli kommunikáció során minden inputtal rendelkező játékoshoz érkezik bit a központból, akkor legalább k bitet megspórolunk a táblás modellben a fenti szimulációval. Akkor van csak gond, ha valamely inputtal rendelkező játékos, mondjuk P_i nem kap bitet a központból. Ez azt jelenti, hogy ő az inputjából már biztosan tudja a végeredményt, azaz nála egy a függvény értékét rögzítő input van. Ha egyetlen játékosnál van csak rögzítő input, akkor $(k-1)$ bitet még mindig megspórolunk. Tegyük fel, hogy több játékosnál is lehet rögzítő input. Vegyük észre, hogy ekkor ezek csak ugyanazt a függvényértéket rögzíthetik, külñben ellentmondás lenne, ha az egyik játékos egy nullát, másik pedig egy 1-et rögzítő inputot kapna. Legyen P_i a legkisebb indexű játékos, aki rögzítő inputot kapott.

Az i-edik kapcsolaton ez esetben is kell kommunikációnak történnie, amely tehát kizárólag P_i-től a központ felé irányul. Tehát valamilyen bitsorozattal P_i tájékoztatja a központot, hogy ő már tudja a végeredményt. Módosítsuk ekkor a fenti táblás szimulációnkat úgy, hogy amennyiben P_i ezt a jelsorozatot írja fel a táblára, akkor a játékosok azonnal tudják a végeredményt, ezáltal nincs is szükség további kommunikációra. Igazából a játékosok csak azt tudják meg, hogy P_i-nél rögzítő input van, de mint láttuk ez csak egyféle függvényértéket rögzíthet, így a végeredményt is tudják. Ekkor az i-nél nagyobb sorszámú kapcsolatokon még nem hangzott el bit, és mivel láttuk, hogy legalább egy bit el fog hangzani, így ezeket mind megspóroltuk. Az i-nél kisebb sorszámú kapcsolatokon pedig szintén megspóroltunk legalább egy-egy bitet, hisz azokon küldött, vagy küldeni fog a központ kifelé bitet. Összefoglalva tehát bárhogy is zajlik a csillag modellben a kommunikáció, a táblás modelllben $(k-1)$ bitet megspórolva szimulálhatjuk azt, ebből pedig adódik a tétel.$\diamond$

A továbbiakban azt vizsgáljuk, hogy a 4.1 és 4.2 Tételek által adott becslések mennyire élesek. A most következő tétel azt mondja, hogy a 4.1 Tétel becslése éles.

4.3 TÉTEL: Létezik olyan f függvény, melyre $C_k^*(f) \geq k \cdot C_k^T(f) - k^2$.

Bizonyítás: Legyen az f a k-változós egyenlőség függvény, vagyis az az $f : (\{0,1\}^n)^k \longrightarrow \{0,1\}$ függvény, melyre $f(x_1, x_2, \ldots, x_k) = 1$ pontosan akkor, ha $x_1 = x_2 = \cdots = x_k$ áll fenn. Akkor $C_k^T(f) \leq n + (k-1)$, hiszen elég ha P_1 felírja a táblára a teljes inputját, majd ezek után a többi $(k-1)$ játékos egy-egy bitet küld, amely 1-es ha az ő inputja megegyezik a felírttal, és 0, ha nem. Ekkor az f értéke pontosan akkor 1, ha a $(k-1)$ utoljára felírt bit mind 1-es.

Megmutatjuk, hogy az egyenlőség függvényre a csillag modellben $C_k^*(f) \geq kn$. Ebből $C_k^*(f) \geq kn \geq k(C_k^T(f)-(k-1)) = k \cdot C_k^T(f) - k(k-1)$, ami igazolja a tételt. Vegyünk ennek érdekében egy jó protokollt a csillag modellben az egyenlőség függvény kiszámítására. Legyen $x, y \in \{0,1\}^n$, ekkor azt állítjuk, hogy az $(x, x, \ldots, x)$ és az $(y, y, \ldots, y)$ input k-as mellett egy adott (tetszőleges) kapcsolaton más bitsorozatok hangzanak el. Ugyanis ha például az i-edik kapcsolaton ugyanaz a kommunikáció hangzana el az $(x, x, \ldots, x)$ és az $(y, y, \ldots, y)$ input k-asok mellett, akkor ugyanez a bitsorozat hangzana el az i-edik kapcsolaton akkor is ha P_i játékos y-t, az összes többi pedig x-et kapna inputjául. Hiszen a $\{P_j : j \neq i\}$ játékoscsoport nem tudja, hogy P_i-nél milyen input van, így köztük ugyanaz történik ha P_i-nél az x illetve az y van, amennyiben persze ő is ugyanazokat a biteket küldi. Ugyanígy P_i sem tudja, hogy a többi inputtal rendelkező játékosnál csupa x, vagy csupa y input van. Viszont ez ellentmondás, hiszen ha az i-edik kapcsolaton a kommunikáció ugyanaz ha P_i-nél y van, a többieknél pedig x, illetve ha mindenkinél x van, akkor P_i a kommunikáció végén ugyanarra a végeredményre is gondol, viszont az eredmény az első esetben 0, az utóbbiban pedig 1. Ebből persze az is következik, hogy minden kapcsolat esetén a rajta elhangzó bitsorozatok halmaza prefix-mentes halmazt alkot, midőn az input végigfut az $\{(x, x, \ldots, x) : x \in \{0,1\}^n\}$ halmazon. Jelölje $s_l(x)$ az l-edik kapcsolaton elhangzott bitsorozatot az $(x, x, \ldots, x)$ input mellett. Akkor alkalmazva a prefix-mentes halmazokra vonatkozó 2.4 Lemmát azt kapjuk, hogy

$$\sum_{x\in\{0,1\}^n}\sum_{l=1}^{k}|s_l(x)| = \sum_{l=1}^{k}\sum_{x\in\{0,1\}^n}|s_l(x)| \geq k\cdot 2^n\log 2^n = 2^n\cdot kn$$

Ebből viszont következik, hogy létezik olyan $x\in\{0,1\}^n$, hogy az $(x,x,\ldots,x)$ input mellet az összes kommunikáció legalább kn.$\diamond$

A 4.2 Tételben szereplő $(k-1)$-es különbség a két kommunikációs komplexitás között biztosan nem javítható k-nál nagyobbra, ugyanis ha az egyenlőségtesztet nézzük az inputok első bitjeire, akkor ennek a függvénynek a kommunikációs komplexitása könnyen igazolható, hogy a táblás modellben k (mindenki felírja az első bitet a táblára), a csillag modellben pedig $2k$ (mindenki beküldi az első bitjét a központba, az pedig mindenkit értesít az eredményről). Ilyen értelemben tehát éles a 4.2 Tétel becslése. Igazából viszont az az érdekes kérdés, hogy teljesül-e valamilyen k-tól függő $c\geq 1$-re, hogy $C_k^*(f)\geq c\cdot C_k^T(f)+F(k)$, ahol $F(k)$ valamilyen k-tól függő hibatag. Ezt nem tudjuk, így a 4.2 Tétel nem tekinthető élesnek, viszont tudjuk, hogy a c-t az $(1+\frac{1}{k-1})$ érték alatt érdemes csak keresni, hiszen:

4.4 TÉTEL: Majdnem minden $f:(\{0,1\}^n)^k\longrightarrow\{0,1\}$ függvényre ($n\to\infty$ esetén) $C_k^*(f)\leq(1+\frac{1}{k-1})\cdot C_k^T(f)+k$.

Bizonyítás: Azt tudjuk, hogy $C_k^*(f)\leq kn+k$, hiszen a csillag modellben minden függvényre alkalmazható a triviális protokoll, mely során valamennyi szereplő beküldi az inputját a központba (kn bit), majd a központ az f értékének kiszámítása után az eredményről minden játékost tájékoztat (további k bit). Elég ha megmutatjuk, hogy $C_k^T(f)\geq(k-1)n$ teljesül majdnem minden f függvényre, ugyanis ebből

$$C_k^*(f)\leq kn+k=\frac{k}{k-1}(k-1)n+k\leq\frac{k}{k-1}C_k^T(f)+k$$

ami a bizonyítandó állítás.

A bizonyítás leszámlálással történik.

Az $f:(\{0,1\}^n)^k\longrightarrow\{0,1\}$ függvények száma $f_{n,k}=2^{2^{nk}}$, hiszen $(\{0,1\}^n)^k$-nak 2^{nk} eleme van, és egy függvény e halmaz minden eleméhez kétféle értéket rendelhet.

A táblás modellben a legfeljebb t bitet használó protokollok száma (amit p_t jelöl) becsülhető felülről a $(2k)^{2^t}\cdot 2^{2^n\cdot 2^t}$ értékkel, hiszen egy protokoll a táblás modellben két függvényből áll. Az egyik az addig táblára került bitek függvényében megadja, hogy ki következik szólásra, amennyiben persze még nem ért véget a protokoll. Mivel ekkor a táblán lévő bitek száma legfeljebb $(t-1)$, így ezt legfeljebb $k^{\sum_{i=0}^{t-1}2^i}$-féleképpen teheti meg. Ha pedig már véget ért (ekkor legfeljebb t bit van a táblán), akkor a protokoll meghatározza a tábla függvényében a végeredményt, erre tehát legfeljebb 2^{2^t} lehetőség van. Kihasználva, hogy $\sum_{i=0}^{t-1}2^i\leq 2^t$ azt kapjuk, hogy az eddigiek meghatározására legfeljeb $(2k)^{2^t}$ lehetőség van. A protokoll másik függvénye az ily módon kijelölt játékos inputjának, és a tábla addigi tartalmának függvényében adja meg, hogy a kijelölt játékos milyen bitet írjon a táblára. Ennek viszont legfeljebb $2^{2^n \cdot 2^t}$ módja lehet. Vagyis azt kaptuk, hogy $p_t \leq (2k)^{2^t} \cdot 2^{2^n \cdot 2^t} = 2^{2^t(2^n + \log k + 1)}$.

Amennyiben $t = (k-1)n - 1$, és $\log k + 1 \leq 2^{n-1}$ (ez utóbbi feltehető, hisz $n \to \infty$ esetet nézzük), akkor

$$2^t(2^n + \log k + 1) \leq \frac{3}{4} \cdot 2^{nk}.$$

Ebből

$$\frac{p_t}{f_{n,k}} \leq \frac{2^{2^t(2^n+\log k+1)}}{2^{2^{nk}}} \leq 2^{-\frac{1}{4}2^{nk}}$$

ami nullához tart $n \to \infty$ esetén. Viszont p_t a legfeljebb t bitet használó protokollok száma, tehát felülről becsli a legfeljebb t kommunikációs komplexitású függvények számát, így ezen függvények aránya az összes függvények között 0-hoz tart. Ez pedig azt jelenti, hogy majdnem minden függvény kommunikációs komplexitása a táblás modellben legalább $(k-1)n$.$\diamond$

Mivel ez a legjobb alsó határ, amit $C_k^*(f)$-fel el tudtunk érni, így sejthetnénk azt is, hogy minden f-re $C_k^*(f) \geq (1 + \frac{1}{k-1})C_k^T(f)$ teljesül. Azonban ez biztosan nem igaz. Erre éppen a 2. fejezetben láthattunk egy ellenpéldát. Vegyük ugyanis észre, hogy $k = 2$ mellett a Tiwari féle lineáris hálózat modell megegyezik a csillag modellel.A sejtés $k = 2$ mellett, azt állítaná, hogy $C_2^*(f) \geq 2 \cdot C_2^T(f)$, ami éppen Tiawri sejtése a 2 hosszú lineáris hálózatra, amiről megmutattuk, hogy nem igaz. Tiwari sejtésére az ellenpélda egy olyan f függvény volt, melyre ottani jelöléssel élve $C_k(f) \leq (\frac{3}{4} + o(1)) \cdot k \cdot C(f)$ teljesült. Viszont $k = 2$ mellett az ottani $C_2(f)$, mint említettük azonos az e fejezetben definiált $C_2^*(f)$-fel, és az ottani $C(f)$, azaz a hagyományos kétszereplős kommunikációs komplexitás pedig természetesen megegyezik a kétszereplős táblás modellbeli komplexitással, amit pedig e fejezetben $C_2^T(f)$-fel jelölünk. Áttérve tehát az e fejezetben használt jelölésekre olyan f-et ismerünk a 2. fejezetből, amelyre $C_2^*(f) \leq (\frac{3}{4} + o(1)) \cdot 2 \cdot C_2^T(f) = (\frac{3}{2} + o(1)) \cdot C_2^T(f)$.

Ha azonban a protokolokra mind a táblás, mind a csillag modellben egy igen erős megkötést teszünk, akkor ez az eddig rossz sejtés igazzá, és ezáltal a 4.4 Tétel élessé válik. Ez az erős megkötés pedig a „nemtörődöm” tulajdonság.

Azt mondjuk egy protokollra, hogy nemtörődöm protokoll, ha az, hogy mikor ki szóljon a játékosok közül az nem függ az addig elhangzott bitektől, és ezáltal az inputoktól sem. A protokoll tehát előre megmondja, hogy mikor, ki, kinek küld egy bitet.

4.5 TÉTEL: Ha a táblás modellben, és a csillag modellben egyaránt csak nemtörődöm protokollokat engedünk meg, és az új komplexitásokat kalappal különböztetjük meg az eddigiektől, akkor minden f függvényre teljesül, hogy $\hat{C}_k^*(f) \geq (1 + \frac{1}{k-1}) \cdot \hat{C}_k^T(f)$

Bizonyítás: Tekintsünk egy optimális, azaz $\hat{C}_k^*(f)$ bitet használó nemtörődöm protokollt az f kiszámítására a csillag modellben. Konstruálunk egy nemtörődöm protokollt a táblás modellre, amely legfeljebb $(1-\frac{1}{k}) \cdot \hat{C}_k^*(f)$ bitet használ, ebből $\hat{C}_k^T(f) \leq (1-\frac{1}{k}) \cdot \hat{C}_k^*(f)$, amiből a tétel átrendezéssel következik.

Legyen P_l az a játékos, aki az adott nemtörődöm protokoll esetén a legkevesebb bitet kommunikálja a központtal. Ez tehát ebben az esetben nem függ az inputoktól. Tekintsük a táblás modellben a következő protokollt:

Amikor a csillag modellben P_i játékos beküld egy bitet a központba ($i \neq l$), akkor a táblás modellben a P_i játékos felírja ezt a bitet a táblára, ha viszont a csillag modellben P_l küld bitet a központnak, akkor a táblás modellben nem történik semmi. Szintén nem történik semmi, ha a központ küld bitet P_l-nek. Végezetül ha a központ küld a csillag modellben egy bitet a P_i ($i \neq l$) játékosnak, akkor ezt a bitet a táblás modellben a P_l játékos fogja felírni a táblára. Ezt azért tudja megtenni, mert a központ az alapján dönti el, hogy milyen bitet küld a P_i-nek, hogy milyen biteket kapott eddig a játékosoktól. Amiket a P_j ($j \neq l$) játékosoktól kapott, azok fenn vannak a táblán, így P_l birtokában van az összes kommunikációnak, hogy szimulálja a központ tevékenységet.

A táblás modellre így egy olyan protokollt adtunk, amelyben a csillag modellhez képest megspóroltuk azt a kommunikációt, amely a központ és P_l között zajlott. Ez legalább $\frac{1}{k}\hat{C}_k^*(f)$ bit megtakarítást jelent, hiszen a P_l a legtöbbet, és így legalább a kommunikáció k-ad részét kommunikálta a központtal.

4.6 MEGJEGYZÉS: Ha nem tesszük fel a nemtörődöm tulajdonságot a megengedett protokollokról, hanem a szokványos módon értelmezzük azokat (tehát az, hogy mikor ki következik, az az addig elhangzott bitektöl is függ), akkor ezzel a módszerrel is csak annyit tudunk bizonyítani, hogy $C_k^*(f) \geq C_k^T(f)$. Hiszen azt, hogy melyik kapcsolaton fogjuk megspórolni a kommunikációt az inputoktól függetlenül kellett megadnunk, és előfordulhat olyan input, melyre ezen a kapcsolaton csak minimális az elhangzó kommunikáció.

4.7 MEGJEGYZÉS: Ha csak a nemtörődöm protokollokkal foglalkozunk, attól még a 4.4 Tétel igaz marad, ugyanis a csillag modellben a triviális protokoll is egy nemtörődöm protokoll, és a leszámlálás is ugyanúgy működik, mint a hagyományos protokoll értelmezéssel. Azzal a különbséggel, hogy annak kijelölésére, hogy mikor ki beszél nem csak hogy legfeljebb k^{2^t} lehetőség van, hanem ennél kevesebb: k^t, de ettől még a k^{2^t} felső becslés csak még inkább igaz. Ebből az látszik, hogy a nemtörődöm protokollokra a $\hat{C}_k^*(f) \geq (1+\frac{1}{k-1}) \cdot \hat{C}_k^T(f)$ egy éles alsó becslés.

Azonban a nemtörődöm tulajdonság egy igen erős megkötés a protokollokra, amit például az is mutat, hogy Tiwari sejtése nemtörődöm protokollokra szorítkozva azonnal igazzá válna. Rádásul rendkívül egyszerűen igazolható is: Tekintsük a lineáris hálózat kétszereplős szimulációját bármely kapcsolat mentén. Akkor léteznek olyan x, y inputok, melyek mellett ezen a kapcsolaton $\hat{C}(f)$ bit hangzik el. Mivel egy nemtörődöm protokoll az inputoktól függetlenül adja meg, hogy mikor ki beszél, így minden kapcsolatra kénytelen $\hat{C}(f)$ bit kommunikációt kijelölni. Ebből azonnal következik a $\hat{C}_k(f) \geq k \cdot \hat{C}(f)$ állítás.

Összefoglalva tehát eddigi eredményeinket arra jutottunk, hogy nemtörődöm protokollok esetén $(1+\frac{1}{k-1}) \cdot \hat{C}_k^T(f) \leq \hat{C}_k^*(f) \leq k \cdot \hat{C}_k^T(f)$, ahol ráadásul a becslés mindkét oldalról éles. A hagyományos módon értelmezett protokollok esetén viszont azt tudjuk, hogy $C_k^T(f) + (k-1) \leq C_k^*(f) \leq k \cdot C_k^T(f)$, és az alsó irányból nem tudjuk, hogy éles-e a becslés.

Felhasznált irodalom:

[1] E. KUSHILEVITZ, N. NISAN, Communication Complexity, Cambridge University Press, Cambridge, 1997

[2] P. TIWARI, Lower Bounds on Communication Complexity in Distributed Computer Networks, J. Assoc. Comput. Mach. **34**, 921-938, 1987

[3] E. KUSHILEVITZ, N. LINIAL, R. OSTROVSKY, The Linear-Array Conjecturec in Communication Complexity is False, In Proc. of the 28th Annual ACM Symposium on Theory of Computing, 1-10, 1996

[4] M. DIETZFELBINGER, The Linear-Array Problem in Communication Complexity Resolved, In Proc. of the 29th Annual ACM Symposium on Theory of Computing, 373-382, 1997

[5] L. BABAI, N. NISAN, M. SZEGEDY, Multiparty Protocols and Logspace-hard Pseudorandom Sequences, In Proc. of the 21st Annual ACM Symposium on Theory of Computing, 1-11, 1989

[6] A. K. CHANDRA, M. L. FURST, R. J. LIPTON, Multi-party Protocols, In Proc. of the 15th Annual ACM Symposium on Theory of Computing, 94-99, 1983

[7] F. R. K. CHUNG, Quasi-random Classes of Hypergraphs, Random Structures and Algorithms, Vol 1, No 4, 363-382, 1990

[8] F. R. K. CHUNG, P. TETALI, Communication Complexity and Quasi Randomness, SIAM J. Discrete Math. , Vol 6, No 1, 110-123, 1993

[9] R. RAZ, The BNS-Chung Criterion for Multi-party Communication Complexity, manuscript

[10] V. GROLMUSZ, The BNS Lower Bound for Multi-party Protocols is Nearly Optimal, Information and Computation, **112**(1), 51-54, 1994

[11] M. MARCUS, H. MINC, A survey of Matrix Theory and Matrix Inequalities. Allyn and Bacon, Boston, Mass. , 1964

[12] A. AHO, J. ULLMAN, M. YANNAKAKIS, On Notions of Information Transfer in VLSI Circuits, In Proc. of the 15th Annual ACM Symposium on Theory of Computing, 133-139, 1983