Obsah

Úvod

Nájsť efektívny algoritmus na výpočet určitej funkcie je obvykle ťažká úloha. Ešte ťažšie je často nájsť dolný odhad zložitosti danej funkcie, teda dokázať, že všetky algoritmy pre túto funkciu majú väčšiu zložitosť. Jednou z techník vyvinutých na dokazovanie dolných odhadov v rôznych modeloch je komunikačná zložitosť.

Základný model komunikačnej zložitosti bol zavedený v roku 1979 v článku [17]. V tomto modeli máme dvoch hráčov a každý z nich pozná jeden vstupný údaj. Hráči môžu spolu komunikovať (vymieňať si správy) a ich úlohou je vypočítať hodnotu určitej funkcie pre danú dvojicu vstupov. Snaha je nájsť taký spôsob výpočtu (algoritmus, protokol), pri ktorom si vymenia čo najmenej bitov.

Tento výpočtový model je veľmi jednoduchý a existujú pre neho kombinatorické charakterizácie zložitosti a jednoduché techniky hľadania dolných odhadov zložitosti funkcií. Navyše boli nájdené aj redukcie, ktoré umožňujú previesť dolné odhady komunikačnej zložitosti funkcií na dolné odhady v iných modeloch. Komunikačná zložitosť bola takto aplikovaná ako nástroj na hľadanie dolných odhadov pre VLSI obvody, booleovské obvody, rozhodovacie stromy, ale aj napríklad Turingove stroje a dátové štruktúry. Takéto aplikácie si často vyžadovali použiť určitú obmenu základného modelu komunikačnej zložitosti, preto dnes existuje mnoho rôznych variantov.

Aplikácia dolných odhadov do iných modelov však nie je jediným významom komunikačnej zložitosti. Jednoduchosť tohto výpočtového modelu umožňuje lepšie skúmať jeho vlastnosti a účinok, aký majú zmeny základného modelu na zložitosť funkcií.

Táto práca sa zaoberá otázkami súvisiacimi s dvoma otvorenými problémami v oblasti komunikačnej zložitosti. Prvým z nich je amortizovaná komunikačná zložitosť, druhým simultánna komunikačná zložitosť. V obidvoch častiach práca podáva vlastné čiastkové výsledky, ako aj prehľad už známych výsledkov.

Amortizovaná komunikačná zložitosť je komunikačná zložitosť výpočtu funkcie na viacerých vstupoch naraz. Situácia je teda takáto: nezávisle od seba zvolíme dve dvojice vstupov a obe dvojice rozdelíme hráčom. Hráči majú pre každú dvojicu vypočítať výsledok. Samozrejme, môžu počítať tak, že najprv vypočítajú výsledok pre prvú dvojicu vstupných hodnôt, potom pre druhú dvojicu. To znamená, že komunikačná zložitosť takéhoto výpočtu bude dvojnásobkom zložitosti výpočtu pre jednu dvojicu vstupov. Otázkou zostáva, či to je najlepší spôsob, t.j. či hráči nemôžu nejako využiť skutočnosť, že poznajú dva vstupy súčasne a ušetriť tak časť komunikácie.

Túto otázku môžeme skúmať v rôznych obmenách základného modelu. Ak sa skúma komunikačná zložitosť relácií, problém amortizovanej zložitosti má aj určité aplikácie do zložitosti booleovských obvodov. Pre čiastočné funkcie sa zas objavil príklad, kde je naozaj možné výpočtom pre viac vstupov naraz ušetriť časť komunikácie. My sa budeme zaoberať prípadom úplných funkcií, kde problém nemá aplikáciu pre iné modely, je však stále zaujímavý z teoretického hľadiska. Problém amortizovanej komunikačnej zložitosti je jednou zo základných otázok, ktoré si môžeme o určitom výpočtovom modeli položiť, pri zložitejších výpočtových modeloch je však zložité ju skúmať.

V tejto práci podávame stručný prehľad známych výsledkov a dôkaz, že pre väčšinu funkcií sa nedá ušetriť viac ako 4 bity komunikácie. Takisto uvádzame definíciu komunikačnej zložitosti, prehľad metód dolných odhadov a ich súvislosť s problémom amortizovanej komunikačnej zložitosti.

Simultánna komunikačná zložitosť používa značne odlišný model komunikácie. Vychádza z mnohoúčastníckej zložitosti, čo je zovšeobecnenie základného modelu pre viac účastníkov. V mnohoúčastníckej komunikačnej zložitosti máme n hráčov a počítame funkciu n vstupov. Hráč i pritom pozná všetky vstupy okrem i-teho. Informácia poskytnutá jednotlivým hráčom sa teda do značnej miery prekrýva.

V modeli simultánnej zložitosti, na rozdiel od mnohoúčastníckej komunikačnej zložitosti, máme ešte jedného hráča navyše ("rozhodcu"), ktorý nepozná žiaden vstup. Ostatní hráči nemôžu navzájom komunikovať a každý z nich pošle rozhodcovi iba jednu správu zostavenú na základe vlastných vstupov. Rozhodca po prijatí všetkých správ musí vedieť vypočítať výsledok. My sa budeme zaoberať týmto modelom pre troch hráčov (a jedného rozhodcu).

Otvoreným problémom v oblasti simultánnej komunikačnej zložitosti troch hráčov je pre nejakú konkrétnu funkciu ukázať, že má veľkú komunikačnú zložitosť. Zaujímajú nás však iba také funkcie, ktoré možno vypočítať polynomiálne na nedeterministickom Turingovom stroji a pre ktoré je dĺžka jedného zo vstupov exponenciálne väčšia ako dĺžky druhých dvoch vstupov. Ak by sa takýto dolný odhad podarilo nájsť, znamenalo by to vyriešenie dlho otvoreného problému pre booleovské obvody.[1]

Model simultánnej zložitosti je pomerne nový (zavedený v článku [13]), takže o ňom nebolo publikovaných veľa prác. Na rozdiel od základného modelu simultánnej zložitosti pre tento model nie sú známe žiadne metódy dolných odhadov. V práci podávame prehľad známych výsledkov — jednak spomínanú aplikáciu do booleovských obvodov a tiež známe dolné a horné odhady pre niektoré skúmané funkcie. Vlastné výsledky sa týkajú dvoch oblastí: charakterizácie simultánnej komunikačnej zložitosti pomocou základných parametrov a kombinatoricko-grafovej charakterizácie.

V prvej oblasti sa snažíme charakterizovať zložitosť funkcie pomocou jej základných parametrov, ktoré možno pre danú funkciu pomerne jednoducho zistiť. Pomocou týchto parametrov určujeme horný odhad a kde sa dá aj dolný odhad simultánnej zložitosti funkcie. Nakoľko sú skúmané parametre veľmi jednoduché, získané dolné a horné odhady sú od seba veľmi vzdialené. Poskytujú však základnú orientáciu vo vlastnostiach uvedeného modelu. K nájdeným dolným a horným odhadom uvádzame dôkaz ich optimálnosti. Špeciálne dôkaz optimálnosti horného odhadu vlastne zna-

[1] Týmto problémom je pre nejakú konkrétnu funkciu (počítateľnú polynomiálne na nedeterministickom Turingovom stroji) dokázať, že sa nedá počítať booleovským obvodom s hĺbkou $O(\log n)$ a veľkosťou $O(n)$.

mená dokázať, že existuje funkcia s veľkou komunikačnou zložitosťou. Náš dôkaz však žiaľ nie je konštruktívny, takže neprispieva k riešeniu uvedeného otvoreného problému.

V oblasti kombinatoricko-grafovej charakterizácie podávame charakterizácie dvoch miernych obmien simultánneho modelu pomocou bipartitných grafov a matíc. Simultánna komunikačná zložitosť je zavedená pomocou pojmov ako protokol, dĺžka správy a podobne. Uvedené charakterizácie presne charakterizujú komunikačnú zložitosť funkcie pomocou pojmov z oblasti kombinatoriky a teórie grafov. Ako príklad uvedieme poslednú z týchto charakterizácií – k funkcii priradíme množinu matíc a hľadáme čo najmenšiu maticu, ktorej budú všetky matice z tejto množiny podmaticami. Veľkosť výslednej matice určuje simultánnu komunikačnú zložitosť funkcie. Aj keď naše charakterizácie neumožňujú priamo jednoducho nájsť dolné odhady komunikačnej zložitosti, umožňujú použiť na ich hľadanie prostriedky z kombinatoriky, či teórie grafov.

V dôkazoch uvedených tvrdení používame predovšetkým informačno-teoretické a kombinatorické metódy (odhadovanie počtu objektov určitého typu). Časť dôkazov má konštrukčný charakter, kde priamo konštruujeme objekt požadovaných vlastností.

Práca je členená do dvoch kapitol, každá kapitola sa venuje jednej zo spomenutých oblastí. Na začiatku kapitoly je vždy uvedená definícia uvažovaného komunikačného modelu a prehľad známych výsledkov. Potom nasledujú vlastné výsledky.

Pojmy a označenia

V tejto časti zavedieme niektoré pojmy a označenia používané v práci. Ďalšie označenia sú zavedené priamo v texte.

Definičné obory, reťazce, matice

V oblasti komunikačnej zložitosti sa obvykle skúmajú funkcie, ktorých definičným oborom sú konečné množiny. Zvyčajne sa uvažujú n-bitové binárne reťazce, t.j. množina $\{0,1\}^n$. Vo všeobecnosti budeme pre slovo v nad nejakou abecedou označovať $|v|$ jeho dĺžku a prázdne slovo budeme označovať ε. Zreťazenie slov u a v budeme označovať $u \cdot v$ alebo len uv. Znaky v reťazcoch budeme **číslovať od nuly** a i-ty znak reťazca u budeme označovať $u(i)$. Teda podľa tohoto označenia máme, že $u = u(0) \cdot u(1) \cdots u(|u|-1)$.

V kapitole o simultánnej komunikačnej zložitosti budeme uvažovať funkcie definované nad množinou $\{0,1,2,\ldots,n-1\}$, ktorú budeme označovať Z_n. Túto množinu budeme zvyčajne chápať ako podmnožinu prirodzených čísel a prípadné aritmetické operácie vykonávané s jej prvkami sú myslené ako operácie v množine prirodzených čísel. Ak budeme uvažovať sčítanie v konečnej cyklickej grupe Z_n, budeme ho zapisovať ako $(x+y) \bmod n$.

Ďalším často používaným objektom budú matice, spravidla binárne. Ich riadky a stĺpce budeme opäť číslovať od nuly a prvok matice A nachádzajúci sa v riadku i a stĺpci j budeme označovať $A(i,j)$. Jednotlivé riadky a stĺpce matice budeme často považovať za binárne reťazce.

Informačno-teoretické pojmy

O množine slov X na nejakou abecedou budeme hovoriť, že je **bezprefixová**, ak neobsahuje navzájom rôzne slová x a y také, že x je prefixom y.

Často budeme používať nasledujúcu vlastnosť bezprefixových množín. Majme bezprefixovú množinu slov X nad abecedou $\{0, 1\}$. Potom ak najdlhšie slovo v X má dĺžku n, tak množina X obsahuje najviac 2^n slov. Naopak, ak X obsahuje n slov, tak aspoň jedno z nich má dĺžku aspoň $\lceil \log n \rceil$. Pri tejto príležitosti poznamenajme, že označenie $\log n$ používame pre **dvojkový logaritmus**.

Booleovské obvody

Booleovským obvodom budeme rozumieť orientovaný acyklický graf, v ktorom do každého vrcholu vchádzajú nanajvýš 2 hrany. Vrcholy, do ktorých nevchádza žiadna hrana, budeme nazývať vstupnými vrcholmi a vrcholy, z ktorých žiadna hrana nevychádza budú výstupmi obvodu. Každý vrchol okrem vstupných vrcholov je označený symbolom *AND*, *OR* alebo *NOT*, pričom prvé dva symboly označujú iba vrcholy, do ktorých vchádzajú 2 hrany a *NOT* označuje iba vrcholy, do ktorých vchádza jedna hrana. Výpočet takéhoto obvodu sa definuje prirodzeným spôsobom – na začiatku sa na vstupné vrcholy umiestnia vstupné bity. Ostatné vrcholy zodpovedajú hradlám, ktoré počítajú z jednej alebo dvoch vstupných hodnôt príslušný výsledok podľa typu hradla.

Na booleovských obvodoch budeme skúmať dve zložitostné miery: hĺbku a veľkosť. Hĺbkou obvodu budeme rozumieť počet vrcholov na najdlhšej orientovanej ceste v príslušnom grafe, veľkosťou obvodu budeme rozumieť počet hradiel obvodu.

Kapitola 1

Amortizovaná komunikačná zložitosť

V tejto kapitole sa budeme zaoberať problémom amortizovanej komunikačnej zložitosti. Najprv v prvých podkapitolách zavedieme základný model komunikačnej zložitosti a uvedieme tiež definíciu problému amortizovanej komunikačnej zložitosti.

Ďalej práca obsahuje prehľad používaných techník dolných odhadov pre deterministickú i nedeterministickú komunikačnú zložitosť.

V nasledujúcej podkapitole uvádzame prehľad známych výsledkov pre amortizovanú komunikačnú zložitosť. Uvádzame jednak vlastnosti dolných odhadov v kontexte amortizovaných výpočtov, jednak známe dolné a horné odhady amortizovanej zložitosti. Táto podkapitola tiež obsahuje pôvodný príklad funkcie, ktorej amortizovaná zložitosť sa rovná presne komunikačnej zložitosti.

Posledná podkapitola uvádza tvrdenie, že väčšina funkcií má veľkú amortizovanú zložitosť, ktoré je vlastným výsledkom.

1.1 Komunikačná zložitosť

V tejto časti zadefinujeme základný model komunikačnej zložitosti. Budeme vychádzať z definície uvedenej v [10].

Zaoberajme sa nasledujúcou komunikačnou hrou: máme daných dvoch hráčov 1 a 2, ktorí chcú vypočítať hodnotu funkcie $f(x, y)$, pričom ale hráč 1 pozná iba vstup x a hráč 2 pozná iba vstup y. Hráči si navzájom posielajú správy podľa daného protokolu, pričom na konci výpočtu obaja poznajú odpoveď. Úlohou je nájsť pre danú funkciu protokol, pri ktorom si hráči vymenia čo najmenej bitov. Uvažujú sa rôzne druhy komunikačných protokolov – deterministické, nedeterministické i pravdepodobnostné. My budeme uvažovať predovšetkým deterministické protokoly, uvedieme však aj definíciu nedeterministických protokolov.

1.1.1 Deterministické protokoly

Deterministický protokol je predpis, ktorý v každom bode výpočtu určuje len na základe dovtedy prebehnutej komunikácie, či už je koniec výpočtu. Ak áno, tak protokol ďalej určuje výsledok výpočtu. Ak ešte nie je koniec, tak určuje, ktorý hráč má poslať ďalší bit. Pre hráča, ktorý má poslať bit, určuje protokol tento bit na základe jeho vstupu a dovtedy prebehnutej komunikácie. Formálnejšie môžeme definovať protokol ako strom:

Definícia 1.1 *Nech D_1, D_2 a H sú konečné množiny.* **Deterministický protokol** *z $D_1 \times D_2$ do H je binárny strom, pre ktorý platí:*

- *každý list je označený prvkom z množiny H,*
- *každému vnútornému vrcholu je priradená dvojica (i, f), kde i je 1 alebo 2 a f je ľubovoľná funkcia $f : D_i \to \{0, 1\}$,*
- *hrany v strome sú označené číslami 0 a 1, pričom z dvojice hrán vychádzajúcich z vnútorného vrcholu k jeho synom je vždy jedna označená nulou a jedna jednotkou.*

Intuitívne teda výpočet podľa protokolu zodpovedá niektorej ceste z koreňa do listu. Hodnota v liste určuje výsledok protokolu. Hodnota vo vnútornom vrchole určuje hráča, ktorý je ďalší na ťahu a pre neho určuje, aký bit má poslať. Z vrcholu vždy pokračujeme po tej hrane, ktorá je označená práve poslaným bitom. Ak by sme teda uvažovali pozorovateľa, ktorý nepozná vstupy, iba vidí jednotlivé posielané bity, tak takýto pozorovateľ vie, v ktorom vrchole protokolu sa výpočet práve nachádza. Vie teda určiť, kto je na ťahu, prípadne aký je výsledok výpočtu. Ak vie výsledok určiť pozorovateľ bez znalosti vstupu, tak ho isto vedia určiť aj hráči 1 a 2.

Definícia 1.2 *Nech D_1, D_2 a H sú konečné množiny a P nech je deterministický protokol z $D_1 \times D_2$ do H. Ďalej nech $(x_1, x_2) \in D_1 \times D_2$.* **Výpočtom** *protokolu P pre vstup (x_1, x_2) budeme nazývať cestu v strome protokolu, pre ktorú platí:*

- *Začína v koreni stromu.*
- *Končí v niektorom liste stromu.*
- *Ak cesta prechádza cez vnútorný vrchol u označený dvojicou (i, f), tak pokračuje do toho syna vrcholu u, ku ktorému vedie hrana označená hodnotou $f(x_i)$.*

Komunikácia *protokolu P pre vstup (x_1, x_2) je zreťazenie všetkých označení hrán na ceste zodpovedajúcej výpočtu.*

Výsledok *protokolu P pre vstup (x_1, x_2) je označenie listu, v ktorom končí cesta zodpovedajúca výpočtu.*

Protokol P **počíta funkciu** *$f : D_1 \times D_2 \to H$, ak pre každé $(x_1, x_2) \in D_1 \times D_2$ je výsledkom protokolu P pre vstup (x_1, x_2) hodnota $f(x_1, x_2)$.*

Teraz už môžeme pristúpiť k samotnej definícii deterministickej komunikačnej zložitosti. Komunikačnou zložitosťou deterministického protokolu budeme rozumieť dĺžku komunikácie pre jeden vstup v najhoršom prípade. Deterministickou komunikačnou zložitosťou[1] funkcie budeme nazývať komunikačnú zložitosť "najlepšieho" protokolu, ktorý túto funkciu počíta.

Definícia 1.3 *Nech P je deterministický protokol z $D_1 \times D_2$ do H.* **Komunikačná zložitosť protokolu** *P (budeme označovať $\mathrm{C}_D(P)$) je definovaná ako hĺbka stromu zodpovedajúceho protokolu P (t.j. počet hrán na najdlhšej ceste od koreňa k listu).*

Deterministickú komunikačnú zložitosť funkcie *$f : D_1 \times D_2 \to H$ (označujeme $\mathrm{C}_D(f)$) definujeme takto:*

$$\mathrm{C}_D(f) = \min\{\mathrm{C}_D(P) \mid P \text{ je deterministický protokol počítajúci } f\}.$$

Nakoniec uveďme prvú lemu, ktorá poskytuje dolný odhad komunikačnej zložitosti konkrétneho protokolu v závislosti od počtu listov jeho stromu. Je to veľmi triviálny odhad, je však základom všetkých uvádzaných odhadov komunikačnej zložitosti funkcií, ktoré sa snažia odhadnúť, koľko aspoň musí byť listov v každom protokole pre danú funkciu.

Lema 1.4 *Nech P je deterministický protokol z $D_1 \times D_2$ do H, ktorého strom má L listov. Potom platí $\mathrm{C}_D(P) \geq \log L$.*

Dôkaz: Pre daný protokol P je zostrojme pre každú cestu z koreňa do listu príslušný vykomunikovaný reťazec. Množina X všetkých týchto reťazcov je bezprefixová množina, lebo žiadna cesta nie je začiatkom inej (každá cesta končí v liste).

Najdlhší reťazec z X má dĺžku $\mathrm{C}_D(P)$, množina X teda obsahuje najviac $2^{\mathrm{C}_D(P)}$ prvkov. Súčasne má množina X presne L prvkov, lebo do každého listu vedie práve jedna cesta z koreňa, ktorej zodpovedá práve jeden reťazec. Teda platí $L \leq 2^{\mathrm{C}_D(P)}$.□

Na náš protokol sa môžeme pozerať aj tak, že hráči si striedavo vymieňajú správy (dĺžky aj väčšej ako 1), pre každú situáciu v priebehu protokolu je však množina správ, ktoré môže poslať niektorý z hráčov, bezprefixová. V strome táto množina správ zodpovedá všetkým cestám z aktuálneho vrcholu, ktoré prechádzajú iba cez vrcholy označené tým istým hráčom.

1.1.2 Nedeterministické protokoly

Nedeterministické protokoly sú miernou obmenou deterministických protokolov. Líšia sa tým, že hráči môžu mať v jednotlivých bodoch výpočtu na výber z viacerých správ, pričom "hádajú", ktorá možnosť vedie k výsledku. Pre jeden vstup takto môže existovať viacero možných výpočtov, pričom niektoré z nich môžu skončiť neúspechom. Požaduje sa však, aby pre každý vstup existoval aspoň jeden úspešný výpočet a aby všetky úspešné výpočty pre jeden vstup dávali rovnaký výsledok.

[1] Slovo deterministický budeme občas vynechávať.

Definícia 1.5 *Nech D_1, D_2 a H sú konečné množiny.* **Nedeterministický protokol** *z $D_1 \times D_2$ do H je binárny strom, pre ktorý platí:*

- *každý list je označený prvkom z množiny $H \cup \{\texttt{fail}\}$,*
- *každému vnútornému vrcholu je priradená dvojica (i, f), kde i je 1 alebo 2 a f je ľubovoľná funkcia $f : D_i \to \{\{0\}, \{1\}, \{0, 1\}\}$,*
- *hrany v strome sú označené číslami 0 a 1, pričom z dvojice hrán vychádzajúcich z vnútorného vrcholu k jeho synom je vždy jedna označená nulou a jedna jednotkou.*

Jediný rozdiel medzi definíciu deterministického a nedeterministického protokolu je teda v tom, že v nedeterministickom protokole môžu byť listy označené aj špeciálnym znakom `fail` a vo vnútorných vrcholoch môže mať hráč, ktorý je práve na ťahu, pre daný vstup neprázdnu množinu možných bitov. Analogicky ako v prípade deterministických protokolov zadefinujeme aj výpočet a funkciu počítanú protokolom. Všimnite si, že nie každý nedeterministický protokol počíta nejakú funkciu.

Definícia 1.6 *Nech P je nedeterministický protokol z $D_1 \times D_2$ do H. Ďalej nech $(x_1, x_2) \in D_1 \times D_2$.* **Výpočtom** *protokolu P pre vstup (x_1, x_2) budeme nazývať ľubovoľnú cestu v strome protokolu, pre ktorú platí:*

- *Začína v koreni stromu.*
- *Končí v niektorom liste stromu.*
- *Ak cesta prechádza cez vnútorný vrchol u označený dvojicou (i, f), tak pokračuje do niektorého zo synov vrcholu u, ku ktorému vedie hrana označená hodnotou z množiny $f(x_i)$.*

Výpočet sa nazýva **neúspešný**, *ak končí v liste označenom* `fail`. *Výpočet sa nazýva* **úspešný**, *ak končí v liste označenom prvkom $h \in H$. Pre úspešný výpočet sa* **výsledkom** *výpočtu nazýva táto hodnota h.*

Protokol P **počíta funkciu** *$f : D_1 \times D_2 \to H$, ak pre každé $(x_1, x_2) \in D_1 \times D_2$ existuje aspoň jeden úspešný výpočet a výsledkom každého úspešného výpočtu pre vstup (x_1, x_2) je hodnota $f(x_1, x_2)$.*

Nakoniec zadefinujeme nedeterministickú komunikačnú zložitosť funkcie a protokolu, opäť podobne ako pri deterministických protokoloch.

Definícia 1.7 *Nech P je nedeterministický protokol z $D_1 \times D_2$ do H.* **Komunikačná zložitosť protokolu** *P — $\mathrm{C}_N(P)$ je hĺbka stromu zodpovedajúceho protokolu P.*

Nedeterministická komunikačná zložitosť funkcie *$f : D_1 \times D_2 \to H$ — $\mathrm{C}_N(f)$ je definovaná takto:*

$$\mathrm{C}_N(f) = \min\{\mathrm{C}_N(P) \mid P \text{ je nedeterministický protokol počítajúci } f\}.$$

Poznámka: V literatúre sa zvyknú nedeterministické protokoly definovať trochu odlišne. Uvažujú sa len funkcie, ktorých oborom hodnôt H je množina $\{0, 1\}$. Protokol potom nemá listy označené symbolom `fail`, ale iba symbolmi 0 a 1, pričom výsledkom protokolu pre daný vstup je 1 práve vtedy, ak existuje výpočet s výsledkom 1. Je to teda podobná definícia nedeterminizmu ako v prípade konečných automatov, Turingových strojov a podobne.

V tejto práci používame definíciu z [5], ktorá sa dá použiť aj pre viacprvkové množiny H, aké sa vyskytujú pri skúmaní amortizovanej komunikačnej zložitosti.

Na záver uvedieme obmenu lemy 1.4 pre nedeterministické protokoly:

Lema 1.8 *Nech P je nedeterministický protokol z $D_1 \times D_2$ do H, ktorého strom má L listov. Potom platí $\mathrm{C}_N(P) \geq \log L$.*

Dôkaz: Podobne ako v leme 1.4 môžeme aj tu pre každý list zostrojiť vykomunikovaný reťazec, pričom najdlhší vykomunikovaný reťazec má dĺžku $\mathrm{C}_N(P)$ a množina všetkých vykomunikovaných reťazcov je bezprefixová. preto môže obsahovať najviac $2^{\mathrm{C}_N(P)}$ rôznych reťazcov a teda máme $L \leq 2^{\mathrm{C}_N(P)}$. □

1.2 Amortizovaná komunikačná zložitosť

Vezmime ľubovoľný výpočtový model a zaoberajme sa nasledujúcim problémom: máme dve funkcie a pre každú z nich príslušný vstup, pričom vstupy sú navzájom nezávislé. Otázka je, či výpočtová zložitosť výpočtu funkčných hodnôt pre obidve funkcie naraz môže byť menšia, ako keby sme počítali najskôr jednu a potom druhú funkciu. Model komunikačnej zložitosti je dostatočne jednoduchý a sú v ňom známe niektoré nástroje na získavanie dolných odhadov zložitosti funkcií, takže je možné sa v ňom pokúsiť túto otázku riešiť. Ukazuje sa, že v niektorých prípadoch je možné trochu komunikácie ušetriť, ak počítame dve funkcie naraz. Väčšina problémov v tejto oblasti však naďalej zostáva otvorených.

Prvotný impulz k skúmaniu amortizovanej komunikačnej zložitosti bol v článku [9]. Autori sa zaoberajú separáciou tried NC^1 a NC^2. Navrhujú postup, akým by sa možno dalo dokázať, že existuje funkcia, ktorú je možné počítať booleovským obvodom hĺbky $O(\log^2 n)$, ale nie obvodom hĺbky $O(\log n)$. Jedným z krokov ich postupu je dokázať, že amortizovaná komunikačná zložitosť relácie sa nelíši príliš od komunikačnej zložitosti tejto relácie. Amortizovaná komunikačná zložitosť sa ďalej skúmala v [5, 8, 7].

My sa budeme zaoberať iba amortizovanou komunikačnou zložitosťou funkcií, nie relácií. Amortizovaná zložitosť funkcií síce nemá (zatiaľ) takéto využitie pre booleovské obvody, je však stále zaujímavá z hľadiska lepšieho pochopenia vlastností výpočtového modelu komunikačnej zložitosti. Najprv presne sformulujeme otázku amortizovanej komunikačnej zložitosti.

Označenie 1.9 *Majme funkcie $f : D_1 \times D_2 \to H$ a $f' : D_1' \times D_2' \to H'$. Potom označme $f \otimes f'$ funkciu $f \otimes f' : (D_1 \times D_1') \times (D_2 \times D_2') \to (H \times H')$, pre ktorú platí*

$$(f \otimes f')((x, x'), (y, y')) = (f(x, y), f'(x', y')).$$

Samozrejme funkcie, ktoré spájame operáciou $\otimes$ nemusia byť navzájom rôzne. Môžeme definovať aj funkciu $f^{(l)}$, ktorá je vlastne l inštanciami funkcie f.

Označenie 1.10 *Nech f je funkcia $f : D_1 \times D_2 \to H$. Potom definujeme $f^{(l)}$ nasledovne:*

$$f^{(l)} = \begin{cases} f & \text{pre } l = 1 \\ f \otimes f^{(l-1)} & \text{pre } l > 1 \end{cases}$$

Našim cieľom bude skúmať vzťah medzi medzi $\mathrm{C}_D(f \otimes f')$ a $\mathrm{C}_D(f) + \mathrm{C}_D(f')$. Takisto nás pre danú funkciu f bude zaujímať súvislosť medzi $\mathrm{C}_D(f)$ a $\frac{1}{l}\mathrm{C}_D(f^{(l)})$. Napokon zavedieme ešte jeden súvisiaci pojem — amortizovanú komunikačnú zložitosť.

Definícia 1.11 *Nech f je funkcia $f : D_1 \times D_2 \to H$.* **Amortizovaná komunikačná zložitosť** *funkcie f je*

$$\overline{\mathrm{C}_D}(f) = \limsup_{l \to \infty} \left(\frac{1}{l} \mathrm{C}_D(f^{(l)}) \right).$$

Amortizovaná komunikačná zložitosť funkcie teda vyjadruje, koľko komunikácie treba na výpočet jednej dvojice vstupov, ak počet naraz spracovávaných dvojíc ide do nekonečna.

Priamo z definície triviálnou úvahou dostávame nasledujúcu lemu:

Lema 1.12

$$\mathrm{C}_D(f \otimes f') \leq \mathrm{C}_D(f) + \mathrm{C}_D(f')$$
$$\mathrm{C}_D(f^{(l)}) \leq l \cdot \mathrm{C}_D(f)$$
$$\overline{\mathrm{C}_D}(f) \leq \mathrm{C}_D(f)$$

Táto lema nám napríklad pre mieru $\mathrm{C}_D(f^{(l)})$ dáva horný odhad pomocou $\mathrm{C}_D(f)$. Avšak stále sme však neuviedli

1. či je tento horný odhad optimálny, t.j. či existuje funkcia, pre ktorú $\mathrm{C}_D(f^{(l)}) = l \cdot \mathrm{C}_D(f)$,
2. aký je dolný odhad $\mathrm{C}_D(f^{(l)})$ pomocou $\mathrm{C}_D(f)$,
3. funkciu, pre ktorú by sa $\mathrm{C}_D(f^{(l)})$ čo najviac líšilo od $l \cdot \mathrm{C}_D(f)$, t.j. funkcia, ktorá by ukazovala optimálnosť horného odhadu uvažovaného v bode 2.

V skutočnosti je problém 1 vyriešený, pre problém 2 existuje nejaký dolný odhad, nie je však jasné, či je optimálny. Otázkou teda zostáva buď zlepšiť tento odhad, alebo nájsť nejakú funkciu (ako to popisuje bod 3), ktorá by ukazovala, že nájdený odhad je optimálny.

Na riešenie všetkých troch bodov ale potrebujeme vedieť zdola odhadovať komunikačnú zložitosť funkcie. Preto v ďalšej kapitole uvedieme niektoré techniky na dokazovanie dolných odhadov zložitosti funkcií.

1.3 Metódy dolných odhadov

V tejto podkapitole uvedieme niektoré známe metódy dolných odhadov deterministickej a nedeterministickej komunikačnej zložitosti. Práve existencia vhodných metód na hľadanie dolných odhadov robí z komunikačnej oblasti použiteľný nástroj. Štúdium optimálnosti týchto metód tiež úzko súvisí s problémom amortizovanej zložitosti funkcií.

1.3.1 Monochromatické obdĺžniky

Monochromatický obdĺžnik je kľúčový pojem pri všetkých uvedených metódach dolných odhadov. Teraz zavedieme tento pojem, ukážeme jeho súvislosť s komunikačnými protokolmi a uvedieme základné dolné odhady.

Definícia 1.13 *Nech $f : D_1 \times D_2 \to H$ je funkcia. Množina $R \subseteq D_1 \times D_2$ sa nazýva* **obdĺžnikom**, *ak sa dá zapísať v tvare $R = X \times Y$, kde $X \subseteq D_1$ a $Y \subseteq D_2$.*

Obdĺžnik R sa nazýva **monochromatický**, *ak funkcia f nadobúda na všetkých jeho prvkoch rovnakú hodnotu.*

Lema 1.14 *Nech P je deterministický alebo nedeterministický protokol na výpočet funkcie $f : D_1 \times D_2 \to H$. Pre vrchol v v stromu protokolu P uvažujme množinu všetkých vstupov $(x, y) \in D_1 \times D_2$, pre ktoré existuje výpočet prechádzajúci vrcholom v. Potom pre každý vrchol v je táto množina obdĺžnikom.*

Dôkaz: Postupujme indukciou vzhľadom na hĺbku vrcholu v. Pre koreň stromu tvrdenie triviálne platí, lebo množina všetkých vstupov $D_1 \times D_2$ je obdĺžnik.

Predpokladajme teraz, že tvrdenie platí pre nejaký vrchol u, ktorý nie je listom a dokážeme, že tvrdenie platí aj pre jeho syna v. Nech hrana uv je označená číslom e. Vrchol u je označený dvojicou (i, f), kde i hráč na ťahu a f je funkcia, ktorá určuje ďalšie pokračovanie výpočtu. Predpokladajme bez ujmy na všeobecnosti, že $i = 1$. Vrcholu u zodpovedá podľa indukčného predpokladu obdĺžnik $X \times Y$. Do vrcholu v budú pokračovať také vstupy $(x, y) \in X \times Y$, pre ktoré platí $e \in f(x)$. T.j. ak X' je množina všetkých prvkov $x \in X$, pre ktoré $e \in f(x)$, tak vrcholu v zodpovedá obdĺžnik $X' \times Y$ (ak by bol na ťahu hráč 2, menila by sa množiny Y). $\square$

Definícia 1.15 *Majme funkciu $f : D_1 \times D_2 \to H$.* **Pokrytím** *funkcie f budeme nazývať množinu monochromatických obdĺžnikov, ktorých zjednotenie pokrýva celý definičný obor funkcie f.* **Rozkladom** *funkcie f budeme nazývať rozklad jej definičného oboru na množinu po dvoch disjunktných monochromatických obdĺžnikov, ktorých zjednotenie pokrýva celý definičný obor funkcie f.*

Označme teraz $Rec_N(f)$ počet obdĺžnikov v pokrytí funkcie f s najmenším počtom obdĺžnikov a $Rec_D(f)$ počet obdĺžnikov v rozklade funkcie f s najmenším počtom obdĺžnikov.

Veta 1.16 *Majme funkciu $f : D_1 \times D_2 \to H$. Potom platí:*

$$\lceil \log(Rec_D(f)) \rceil \le \mathrm{C}_D(f)$$
$$\lceil \log(Rec_N(f)) \rceil \le \mathrm{C}_N(f) \le \lceil \log(Rec_N(f)) \rceil + 1.$$

Dôkaz: Uvažujme ľubovoľný deterministický protokol P počítajúci funkciu f. Každému listu stromu P podľa lemy 1.14 prislúcha obdĺžnik obsahujúci všetky vstupy (x, y), ktorých výpočty končia v tomto liste. Nakoľko je protokol deterministický, pre každý vstup je jednoznačne určené, v ktorom liste jeho výpočet skončí. Preto sú tieto obdĺžniky navzájom disjunktné a pokrývajú celý definičný obor funkcie. Tieto obdĺžniky sú takisto monochromatické, lebo každý list stromu už jednoznačne určuje funkčnú hodnotu. Ak teda protokol P má L listov, potom existuje rozklad funkcie f na L monochromatických navzájom disjunktných obdĺžnikov, takže $Rec_D(f) \le L \le 2^{\mathrm{C}_D(P)}$, pričom posledná nerovnosť platí podľa lemy 1.4. Nakoľko to platí pre ľubovoľný protokol P, dostávame prvú nerovnosť vo vete.

Dolný odhad pre $\mathrm{C}_N(f)$ dostaneme podobne, budeme však uvažovať iba listy, ktoré nie sú označené symbolom `fail`. Každému z týchto listov opäť prislúcha monochromatický obdĺžnik, pričom tieto obdĺžniky pokrývajú celý definičný obor, nemusia však byť navzájom disjunktné.

Aby sme dokázali horný odhad pre $\mathrm{C}_N(f)$, uvedieme nedeterministický protokol. Majme množinu $\mathcal{R}$ monochromatických obdĺžnikov, ktorá tvorí minimálne pokrytie funkcie f, t.j $|\mathcal{R}| = Rec_N(f)$. Hráč 1 pre vstup x nájde všetky obdĺžniky $X \times Y$ z $\mathcal{R}$, pre ktoré platí $x \in X$. Nedeterministicky zvolí jeden z týchto obdĺžnikov a pošle jeho číslo zapísané pomocou $\lceil \log(Rec_N(f)) \rceil$ bitov. Hráč 2 nájde obdĺžnik $X \times Y$ prislúchajúci prijatému číslu a pre vstup y zistí, či $y \in Y$. Výsledok testu (bit 0 alebo 1) pošle hráčovi 1. Ak hráč 2 poslal 0, výsledkom výpočtu bude `fail`, ak poslal 1, výsledkom výpočtu bude funkčná hodnota, akú nadobúdajú všetky prvky obdĺžnika $X \times Y$. Uvedomme si, že v tomto prípade $x \in X$ a $y \in Y$, t.j. $(x, y) \in X \times Y$ a teda výsledkom úspešného výpočtu bude vždy hodnota $f(x, y)$. □

Poznámka: Predchádzajúca veta charakterizovala nedeterministickú komunikačnú zložitosť funkcie pomocou miery Rec_N takmer úplne presne. Pre deterministickú zložitosť sme však uviedli len odhad zdola, pričom nie je jasné, nakoľko je tento odhad presný. Najlepší známy odhad zhora je $\mathrm{C}_D(f) = O(\log^2(Rec_D(f)))$. Na druhej strane nie sú známe funkcie, ktorých komunikačná zložitosť by bola od miery $\log(Rec_D(f))$ výrazne vyššia (najlepší známy príklad je funkcia, ktorej zložitosť je konštantným násobkom $\log(Rec_D(f))$).

1.3.2 Metódy dolných odhadov pre nedeterministické protokoly

Nedeterministickú komunikačnú zložitosť sme takmer presne charakterizovali pomocou miery Rec_N. Ak však chceme nájsť dolný odhad zložitosti konkrétnej funkcie, takáto charakterizácia nám stále nemusí pomôcť, pretože odhadnúť zdola počet obdĺžnikov, ktoré musia byť v každom pokrytí funkcie f, môže byť pomerne náročné.

Preto vzniklo niekoľko metód dolných odhadov (spomeňme tzv. fooling set alebo metódu najväčšieho monochromatického obdĺžnika uvedenú nižšie), ktoré sa používajú jednoduchšie, ale ktoré nedávajú presné odhady pre všetky funkcie. Tieto metódy teda dávajú návod, ako sa pokúsiť nájsť pre danú funkciu dôkaz toho, že sa v každom pokrytí musí vyskytovať veľa obdĺžnikov.

V prácach [8, 10] bolo zavedené zovšeobecnenie rôznych metód dolných odhadov, ktoré uvádzame v nasledujúcej definícii.

Označenie 1.17 *Majme funkciu $f : D_1 \times D_2 \to H$ a nech $\mu : D_1 \times D_2 \to \langle 0, 1\rangle$ je rozdelenie pravdepodobnosti na množine $D_1 \times D_2$. Pre $R \subseteq D_1 \times D_2$ označme mieru množiny R*

$$\mu(R) = \sum_{(x,y)\in R} \mu(x, y).$$

Ďalej ak $c = \max(\mu(R))$, kde maximum sa robí zo všetkých monochromatických obdĺžnikov R funkcie f, tak označme

$$B_\mu = \frac{1}{c} \qquad\qquad B_*(f) = \max_\mu(B_\mu).$$

Pre používané metódy dolných odhadov potom možno nájsť nejaké rozdelenie pravdepodobnosti μ tak, aby nimi poskytovaný odhad bol B_μ. Toto zovšeobecnenie má tú výhodu, že nám umožňuje skúmať vlastnosti rôznych metód dolných odhadov súčasne. Príkladom nech je nasledujúca veta, v ktorej pre metódy spadajúce pod naše zovšeobecnenie dokážeme ich správnosť.

Veta 1.18 [8, 10] *Majme funkciu $f : D_1 \times D_2 \to H$ a nech $\mu : D_1 \times D_2 \to \langle 0, 1\rangle$ je rozdelenie pravdepodobnosti na množine $D_1 \times D_2$. Potom platí*

$$\mathrm{C}_N(f) \geq \log B_\mu.$$

Taktiež platí, že $\mathrm{C}_N(f) \geq \log B_*$.

Dôkaz: Miera pravdepodobnosti celého definičného oboru je 1. V každom pokrytí funkcie f musí teda byť súčet mier obdĺžnikov aspoň 1. Nakoľko každý monochromatický obdĺžnik má mieru najviac $1/B_\mu$, potrebujeme aspoň B_μ obdĺžnikov. Podľa vety 1.16 dostávame požadované tvrdenie. Druhá časť tvrdenia je potom už len triviálnym dôsledkom. $\square$

Pozrime sa teraz bližšie na jednu z metód dolných odhadov, konkrétne na metódu najväčšieho monochromatického obdĺžnika.

Označenie 1.19 *Nech $f : D_1 \times D_2 \to H$ je funkcia. Označme λ_f veľkosť (počet prvkov) najväčšieho monochromatického obdĺžnika funkcie f.*

Miera λ_f je špeciálnym prípadom B_μ. Ak totiž zvolíme μ je uniformné rozdelenie pravdepodobnosti, t.j. $\mu(x, y) = \frac{1}{|D_1 \times D_2|}$, monochromatický obdĺžnik s n prvkami má mieru $\frac{n}{|D_1 \times D_2|}$. Teda platí, že $\lambda_f = (1/B_\mu) \cdot |D_1 \times D_2|$. Z toho priamo vyplýva nasledujúca veta.

Veta 1.20 [17] *Nech $f : D_1 \times D_2 \to H$ je funkcia. Potom platí* $\mathrm{C}_D(f) \geq \log |D_1| + \log |D_2| - \log \lambda_f$.

Na záver sa ešte pristavme pri zavedenej miere $B_* = \max_\mu\{B_\mu\}$. Ako sme dokázali vo vete 1.18, táto miera nám taktiež dáva dolný odhad $\mathrm{C}_N(f)$. Miera $B_*(f)$ sa pre danú funkciu odhaduje ťažšie ako B_μ pre konkrétne rozdelenie μ, ale má tú dobrú vlastnosť, že je pomerne presná, pretože platí nasledujúca veta.

Veta 1.21 [8, 10] *Majme funkciu $f : D_1 \times D_2 \to H$. Potom platí*

$$\log B_*(f) \leq \mathrm{C}_N(f) \leq \log B_*(f) + \log\log(D_1 \times D_2) + O(1).$$

1.3.3 Metódy dolných odhadov pre deterministické protokoly

Je zrejmé, že nedeterministická zložitosť funkcie nie je nikdy väčšia ako deterministická, a preto dolný odhad pre $\mathrm{C}_N(f)$ možno použiť aj ako dolný odhad pre $\mathrm{C}_D(f)$. Pre mnohé funkcie takto dostávame metódami uvedenými vyššie pomerne tesné odhady. Vo všeobecnosti sú miery $\mathrm{C}_D(f)$ a $\mathrm{C}_N(f)$ (pre booleovské funkcie) v polynomiálnom vzťahu, čo je jedna z prekvapivých vlastností modelu komunikačnej zložitosti. Nasledujúca veta udáva vzťah medzi $\mathrm{C}_D(f)$ a $\mathrm{C}_N(f)$, pričom je známe, že uvedený odhad je takmer optimálny.

Veta 1.22 [1] *Nech $f : D_1 \times D_2 \to H$ je funkcia. Potom platí*

$$\mathrm{C}_N(f) \leq \mathrm{C}_D(f) = O((\mathrm{C}_N(f))^2).$$

Existuje aj jedna metóda, ktorá odhaduje priamo deterministickú komunikačnú zložitosť (t.j. pomocou ktorej môžeme pre niektoré funkcie nájsť odhad vyšší ako $\mathrm{C}_N(f)$). Je to metóda hodnosti matice. Funkciu $f : D_1 \times D_2 \to H$ si môžeme predstaviť aj ako maticu A typu $|D_1| \times |D_2|$, pričom riadky zodpovedajú jednotlivým prvkom z D_1 a podobne stĺpce zodpovedajú prvkom z D_2. Ďalej zvolíme pole F také, že $H \subseteq F$ a môžeme počítať hodnosť matice A nad poľom F.

Označenie 1.23 *Nech A je matica a F je pole. Budeme označovať $\mathrm{rank}_F(A)$ hodnosť matice A nad poľom F. Ďalej pre funkciu $f : D_1 \times D_2 \to H$ takú, že $H \subseteq F$ označme $rank_F(f) = \mathrm{rank}_F(A)$, kde A je matica nad F zodpovedajúca funkcii f.*

Nasledujúca veta dáva dolný a horný odhad deterministickej komunikačnej zložitosti pomocou miery $rank_F(f)$. Vidíme, že tieto odhady sú od seba veľmi vzdialené. Napriek tomu pre pole reálnych čísel R nebola doteraz nájdená funkcia, ktorej komunikačná zložitosť by sa od $rank_R(f)$ tak veľmi odlišovala a existuje hypotéza, že $\mathrm{C}_D(f) = \log(rank_R(f))^{O(1)}$.

Veta 1.24 [12] *Pre funkciu $f : D_1 \times D_2 \to H$ a pre pole F také, že $H \subseteq F$ platí:*

$$\lceil \log(rank_F(f)) \rceil \leq \mathrm{C}_D(f) \leq rank_F(f) + \lceil \log |H| \rceil .$$

1.4 Odhady pre amortizovanú zložitosť

V tejto podkapitole uvedieme známe výsledky pre amortizovanú zložitosť funkcie a pre mieru $\mathrm{C}_D(f \otimes g)$. V prvej časti sa budeme zaoberať vlastnosťami metód dolných odhadov v kontexte amortizovanej zložitosti. Presnejšie, budeme sa pre rôzne metódy zaoberať otázkou, že ak táto metóda dáva pre funkcie f a f' dolné odhady b a b', aký odhad dáva pre $f \otimes f'$.

V ďalších častiach uvedieme prehľad známych vzťahov medzi komunikačnou zložitosťou a amortizovanou zložitosťou.

1.4.1 Vlastnosti metód dolných odhadov

Ak sme poznamenali v diskusii za lemou 1.12, na odvodenie netriviálnych poznatkov o amortizovanej zložitosti potrebujeme metódy dolných odhadov. Prehľad používaných metód sme uviedli v predchádzajúcej podkapitole. Teraz ukážeme, ako súvisia tieto metódy s problémom amortizovanej zložitosti. Ukáže sa, že pre uvedené metódy pre deterministickú aj nedeterministickú zložitosť, sú dolné odhady **aditívne**, t.j. že ak určitá metóda dáva pre funkcie f a f' dolné odhady b a b', pre $f \otimes f'$ dáva odhad aspoň $b + b'$.

Pre niektoré odhady už bola táto otázka skúmaná v literatúre. V článku [5] autori dokazujú vzťah pre $Rec_N(f)$. V článku [9] autori dokazujú vzťah pre $rank(f)$. V knihe [10] sa uvádza vzťah pre B_* uvedený v dôsledku 1.26. My sme metódy použitú v [10] zovšeobecnili pre B_μ, čím sme dostali vetu 1.25. Z tejto vety už jednoducho vyplýva vzťah pre metódu najväčšieho obdĺžnika (dôsledok 1.27).

Veta 1.25 *Majme funkcie $f : D_1 \times D_2 \to H$ a $f' : D_1' \times D_2' \to H'$ a nech μ a μ' sú rozdelenia pravdepodobnosti na definičných oboroch f a f'. Definujme funkciu $\mu_\otimes$ na definičnom obore funkcie $f \otimes f'$ takto:*

$$\mu_\otimes((x, x'), (y, y')) = \mu(x, y) \cdot \mu'(x', y').$$

Funkcia $\mu_\otimes$ je potom rozdelením pravdepodobnosti a platí

$$B_{\mu_\otimes} = B_\mu B_{\mu'}.$$

Dôkaz: [10] Najprv si uvedomme, že pre množiny $X \subseteq D_1$, $X' \subseteq D_1'$, $Y \subseteq D_2$ a $Y' \subseteq D_2'$ platí

$$\mu_\otimes((X \times X') \times (Y \times Y')) = \mu(X \times Y) \cdot \mu'(X' \times Y').$$

Z toho dostávame, že $\mu_\otimes((D_1 \times D_1') \times (D_2 \times D_2')) = 1 \cdot 1 = 1$ a zobrazenie $\mu_\otimes$ je teda rozdelením pravdepodobnosti.

Podobne môžeme jednoducho dokázať, že $B_{\mu_\otimes} \leq B_\mu B_{\mu'}$. Nech $X \times Y$ je monochromatický obdĺžnik funkcie f s mierou $\mu(X \times Y) = 1/B_\mu$ a nech f na jeho prvkoch nadobúda hodnotu u. Podobne nech $X' \times Y'$ je monochromatický obdĺžnik funkcie f'

s mierou $1/B_{\mu'}$ a nech f' na jeho prvkoch nadobúda hodnotu u'. Zostrojme teraz obdĺžnik $R = (X \times X') \times (Y \times Y')$. Funkcia $f \otimes f'$ na všetkých jeho prvkoch nadobúda hodnotu (u, u') a teda R je monochromatickým obdĺžnikom funkcie $f \otimes f'$. Miera obdĺžnika R je $\mu_\otimes(R) = 1/(B_\mu \cdot B_{\mu'})$. Dokázali sme teda, že $1/B_{\mu_\otimes} \geq 1/(B_\mu B_{\mu'})$, z čoho už máme požadovaný vzťah.

Naopak, nech $R_\otimes = X_\otimes \times Y_\otimes$ je monochromatický obdĺžnik funkcie $f \otimes f'$ s najväčšou mierou a nech $f \otimes f'$ na jeho prvkoch nadobúda hodnotu (u, u'). Označme

$$X = \{x \mid (\exists x')(x, x') \in X_\otimes\} \qquad X' = \{x' \mid (\exists x)(x, x') \in X_\otimes\}.$$

Dokážeme teraz, že $R = (X \times X') \times Y_\otimes$ je monochromatický obdĺžnik, presnejšie, že f na všetkých jeho prvkoch nadobúda hodnotu (u, u'). Majme $((x, x'), (y, y')) \in R$. Z definície R existujú dvojice $(x, x'_1), (x_1, x') \in X_\otimes$. Z toho máme, že $(f \otimes f')((x, x'_1), (y, y')) = (f \otimes f')((x_1, x'), (y, y')) = (u, u')$, čo znamená, že $f(x, y) = f(x_1, y) = u$ a $f'(x'_1, y') = f(x', y') = u'$. Z toho ale máme, že $(f \otimes f')((x, x'), (y, y')) = (u, u')$. Takže obdĺžnik R je monochromatický a $R_\otimes \subseteq R$, takže R má tiež najväčšiu možnú mieru. Analogickým spôsobom z R možno zostrojiť monochromatický obdĺžnik R', ktorý už bude mať tvar $R' = (X \times X') \times (Y \times Y')$ a ktorý bude mať stále rovnakú mieru ako $R_\otimes$.

Dostávame teda

$$\frac{1}{B_{\mu_\otimes}} = \mu_\otimes(R') = \mu(X \times Y)\mu'(X' \times Y') \leq \frac{1}{B_\mu B_{\mu'}},$$

čo znamená, že $B_{\mu_\otimes} \geq B_\mu B_{\mu'}$. □

Dôsledok 1.26 [10] *Nech f_1 a f_2 sú funkcie. Potom platí*

$$B_*(f_1 \otimes f_2) \geq B_*(f_1)B_*(f_2).$$

Dôkaz: Nech μ_1 a μ_2 sú také rozdelenia pravdepodobnosti, že $B_{\mu_1} = B_*(f_1)$ a $B_{\mu_2} = B_*(f_2)$. Pre rozdelenie pravdepodobnosti $\mu_\otimes$ skonštruované podľa vety 1.25 potom platí $B_{\mu_\otimes} = B_*(f_1)B_*(f_2)$. Tvrdenie dostávame z toho, že $B_{\mu_\otimes} \leq B_*(f_1 \otimes f_2)$. □

Vetu 1.25 možno použiť aj na odvodenie aditívnosti metódy najväčšieho obdĺžnika. Táto metóda sa v kontexte amortizovanej zložitosti ešte nespomínala, my ju však budeme potrebovať pri dôkaze vety 1.35.

Dôsledok 1.27 *Majme funkcie $f : D_1 \times D_2 \to H$ a $f' : D'_1 \times D'_2 \to H'$. Potom platí*

$$\lambda_{f \otimes f'} = \lambda_f \lambda_{f'}.$$

Dôkaz: Vieme, že $\lambda_f = (1/B_\mu) \cdot |D_1 \times D_2|$, pričom μ je uniformné rozdelenie pravdepodobnosti na definičnom obore funkcie f. Analogický vzťah platí aj pre funkciu f'.

Ak teraz z uniformných rozdelení μ a μ' zostrojíme zobrazenie $\mu_\otimes$ podľa vety 1.25, dostaneme opäť uniformné rozdelenie. Takže platí

$$\lambda_{f\otimes f'} = \frac{1}{B_{\mu_\otimes}}|(D_1 \times D'_1) \times (D_2 \times D'_2)| = \frac{1}{B_\mu}|D_1 \times D_2|\frac{1}{B_{\mu'}}|D'_1 \times D'_2| = \lambda_f \lambda_{f'}.$$

□

Zostáva nám zaoberať sa metódou $rank_F(f)$, ktorú sme zaviedli pre odhad deterministickej komunikačnej zložitosti. Pri tejto miere vyžadujeme, aby hodnoty funkcie f boli prvkami nejakého poľa F. Tento predpoklad trochu sťažuje situáciu, lebo hodnoty funkcie $f \otimes f'$ sú dvojice. Preto sa nebudeme snažiť vyjadriť $rank_{F'}(f \otimes f')$ pomocou $rank_F(f)$ a $rank_F(f')$, ale vyjadríme priamo $\mathrm{C}_D(f \otimes f')$ pomocou $rank_F(f)$ a $rank_F(f')$.

Veta 1.28 [9] *Majme funkcie $f : D_1 \times D_2 \to H$ a $f' : D'_1 \times D'_2 \to H'$, pričom $H, H' \subseteq F$ pre nejaké pole F. Potom platí*

$$\mathrm{C}_D(f \otimes f') \geq \log(rank_F(f)) + \log(rank_F(f')).$$

Dôkaz: Dôkaz je založený na tom, že zostrojíme funkciu $g : (D_1 \times D'_1) \times (D_2 \times D'_2) \to F$ takú, že $g((x_1, x_2), (y_1, y_2)) = f(x_1, y_1) \cdot f'(x_2, y_@)$ (násobíme v F). Nie je problém ukázať, že $rank_F(g) \geq rank_F(f) \cdot rank_F(f')$. Navyše, ak nejaký protokol počíta $f \otimes f'$, iba zmenou hodnôt v listoch môžeme z neho spraviť protokol pre g a preto platí

$$\mathrm{C}_D(f \otimes f') \geq \mathrm{C}_D(g) \geq \log(rank_F(g)) \geq \log(rank_F(f)) + \log(rank_F(f')).$$

□

1.4.2 Optimálnosť horného odhadu

Ako už vieme z lemy 1.12, platí, že $\mathrm{C}_D(f^{(l)}) \leq l \cdot \mathrm{C}_D(f)$. Poďme najprv dokázať, že tento odhad je optimálny, t.j. že existuje funkcia f taká, že $\mathrm{C}_D(f^{(l)}) = l \cdot \mathrm{C}_D(f)$.

Veta 1.29 *Nech $n = 2^t$ pre $t > 0$ a nech $f : Z_n \times Z_n \to \{0, 1\}$ je funkcia, pre ktorú platí*

$$f(x, y) = \begin{cases} 1 & ak\ x \geq y \wedge x + y < n - 1 \\ 1 & ak\ x \leq y \wedge x + y > n - 1 \\ 0 & inak. \end{cases}$$

Potom platí $\mathrm{C}_D(f^{(l)}) = l(t + 1)$.

Dôkaz: Uvažujme funkciu f a zostrojme na jej definičnom obore rozdelenie pravdepodobnosti μ také, že

$$\mu(x, y) = \begin{cases} 1/(2n) & \text{ak } x = y \\ 1/(2n) & \text{ak } x + y = n - 1 \\ 0 & \text{inak.} \end{cases}$$

1	0	0	0	0	0	0	0
1	1	0	0	0	0	0	1
1	1	1	0	0	0	1	1
1	1	1	1	0	1	1	1
1	1	1	0	1	1	1	1
1	1	0	0	0	1	1	1
1	0	0	0	0	0	1	1
0	0	0	0	0	0	0	1

Vľavo vidíme príklad funkcie f pre $n = 2^3 = 8$. Vo všeobecnosti pre ľubovoľné t má rozdelenie μ nenulové hodnoty na diagonálach, pričom na jednej z nich nadobúda funkcia f hodnoty 0 a na druhej 1. Takže μ dáva nenulové hodnoty pre $2n$ prvkov a je teda rozdelením pravdepodobnosti.

Ďalej platí, že v každom monochromatickom obdĺžniku je najviac jeden prvok (x, y), pre ktorý je $\mu(x, y) \neq 0$. Toto dostaneme jednoduchým rozborom prípadov. Pre $x = y$ platí $f(x, y) = 1$. Každý obdĺžnik, ktorý obsahuje (x, x) aj (x', x') pre $x \neq x'$, obsahuje aj (x, x') a (x', x) a nie je ťažké dokázať, že pre jeden z týchto dvoch prvkov bude hodnota f nula. Takže taký obdĺžnik nebude monochromatický. Ak $x = \bar{y}$, potom $f(x, y) = 0$. Aj v tomto prípade možno podobne ukázať, že každý obdĺžnik, ktorý by obsahoval dva prvky tohto tvaru musí obsahovať aj nejaký prvok, pre ktorý $f(x, y) = 1$.

Dostávame,[2] že miera každého monochromatického obdĺžnika je najviac $1/(2n)$ a teda $B_\mu = 2n$. Podľa vety 1.25 dostávame matematickou indukciou vzhľadom na l, že pre každé l existuje rozdelenie pravdepodobnosti μ_l také, že $B_{\mu_l} = (2n)^l$, čiže $\mathrm{C}_D(f^{(l)}) \geq \log B_{\mu_l} = l(t + 1)$.

Na druhej strane funkciu $f^{(l)}$ možno počítať protokolom s komunikačnou zložitosťou $l(t + 1)$: hráč 1 pošle všetky svoje vstupy hráčovi 2 (ako l binárnych t-bitových reťazcov dĺžky t), hráč 2 vypočíta výsledok a pošle ho späť (l bitov). Takže máme $\mathrm{C}_D(f^{(l)}) = l(t + 1)$. □

Dôsledok 1.30 *Pre funkciu uvedenú vo vete 1.29 platí* $\mathrm{C}_D(f \otimes f) = \mathrm{C}_D(f) + \mathrm{C}_D(f)$, $\mathrm{C}_D(f^{(l)}) \leq l \cdot \mathrm{C}_D(f)$ *a* $\overline{\mathrm{C}_D}(f) = \mathrm{C}_D(f)$.

Poznámka: To, že pre niektoré funkcie je $\overline{\mathrm{C}_D}(f)$ blízko (prípadne rovné) $\mathrm{C}_D(f)$, sa implicitne predpokladá hádam vo všetkých prácach na túto tému a nie je problém ukázať pre mnohé často používané funkcie (ako napr. testovanie rovnosti a pod.), že $\overline{\mathrm{C}_D}(f) \geq \mathrm{C}_D(f) - 1$. Uvedená konštrukcia, ktorá ukazuje presnú rovnosť, je však pôvodná.

1.4.3 Dolný odhad

Dolný odhad pre $\mathrm{C}_D(f \otimes f')$ pomocou $\mathrm{C}_D(f) + \mathrm{C}_D(f')$ dostaneme pomocou analýzy situácie pre nedeterministické protokoly.

Veta 1.31 [5] *Majme funkcie* $f, g : D_1 \times D_2 \to H$. *Potom platí:*

$$\mathrm{C}_N(f \otimes g) \geq \mathrm{C}_N(f) + \mathrm{C}_N(g) - O(\log\log|D_1 \times D_2|)$$
$$\mathrm{C}_N(f^{(l)}) \geq l(\mathrm{C}_N(f) - \log\log|D_1 \times D_2| - O(1)).$$

[2] Na nájdenie dolného odhadu sme použili v podstate metódu fooling set.

Dôkaz: [10] S využitím viet 1.21 a 1.26 dostávame

$$\begin{aligned}\mathrm{C}_N(f)+\mathrm{C}_N(g) &\leq \log B_*(f)+\log B_*(g)+2\log\log|D_1\times D_2|+O(1)\leq\\ &\leq \log B_*(f\otimes g)+2\log\log|D_1\times D_2|+O(1)\leq\\ &\leq \mathrm{C}_N(f\otimes g)+O(\log\log|D_1\times D_2|),\end{aligned}$$

z čoho už plynie prvá dokazovaná nerovnosť. Druhú dokazovanú nerovnosť dostaneme analogicky. □

Vidíme teda, že pomocou známych metód dokazovania dolných odhadov vieme pre nedeterministickú zložitosť dostať pomerne tesný vzťah. Využili sme pritom, že pre nedeterministickú komunikačnú zložitosť máme metódu dolného odhadu B_*, ktorá dáva pomerne tesné odhady a ktorá má navyše vlastnosť aditívnosti pre problém amortizovanej zložitosti.

Nakoľko vieme, že deterministická a nedeterministická zložitosť sú v našom komunikačnom modeli v polynomiálnom vzťahu, dostávame z predchádzajúcej vety aj nasledovné tvrdenie:

Veta 1.32 [5] *Majme funkcie $f,g:D_1\times D_2\to H$. Potom platí:*

$$\begin{aligned}\mathrm{C}_D(f\otimes g) &\geq \Omega\left(\sqrt{\mathrm{C}_N(f)+\mathrm{C}_N(g)}-\log\log(|D_1\times D_2|\right)\\ \mathrm{C}_D(f^{(l)}) &\geq l\cdot\Omega\left(\sqrt{\mathrm{C}_N(f)}-\log\log|D_1\times D_2|\right)\\ \overline{\mathrm{C}_D}(f) &\geq \Omega\left(\sqrt{\mathrm{C}_N(f)}-\log\log|D_1\times D_2|\right).\end{aligned}$$

Dôkaz: Použijeme vety 1.22 a 1.31.

$$\begin{aligned}\mathrm{C}_D(f\otimes g) &\geq \mathrm{C}_N(f\otimes g)\geq \mathrm{C}_N(f)+\mathrm{C}_N(g)-O(\log\log(|D_1\times D_2|)=\\ &=\Omega\left(\sqrt{\mathrm{C}_D(f)}+\sqrt{\mathrm{C}_D(g)}\right)-O(\log\log|D_1\times D_2|).\end{aligned}$$

Teraz si už stačí iba uvedomiť, že $\Omega(\sqrt{a}+\sqrt{b})=\Omega\left(\sqrt{\max\{a,b\}}\right)=\Omega(\sqrt{a+b})$. Druhú časť tvrdenia dostaneme analogicky a tretia časť je dôsledkom druhej. □

1.4.4 Optimálnosť dolného odhadu

Medzi horným odhadom z lemy 1.12 a dolným odhadom z vety 1.32 je veľmi veľký rozdiel. O hornom odhade vieme, že je optimálny, takže zostáva buď dokázať, že aj dolný odhad je optimálny, alebo dolný odhad zlepšiť. Táto otázka je otvoreným problémom. Existuje hypotéza, že $\overline{\mathrm{C}_D}(f)\geq \mathrm{C}_D(f)-\log\log|D_1\times D_2|$.

Nájsť funkciu, ktorej amortizovaná zložitosť je menšia ako jej komunikačná zložitosť, je pomerne ťažké. Potrebujeme totiž dokázať, že $\mathrm{C}_D(f^{(l)})\leq a$ a $\mathrm{C}_D(f)\geq b$, pričom bl je dostatočne väčšie od a. Číslo b musí byť pomerne dobrým dolným odhadom pre funkciu f. Navyše, tento odhad nemôžeme získať tradičnými prostriedkami — ak by sme odhad b dostali pomocou metód ako B_μ alebo $rank_F(f)$, dostávame, že $a\geq bl$. Funkcia f, ktorá by ukazovala rozdiel medzi $\overline{\mathrm{C}_D}$ a C_D by teda zároveň ukazovala aj rozdiel medzi C_D a $\log(rank)$. Na odhad b by bolo potrebné použiť nejakú novú metódu dolných odhadov.

Na záver ešte spomeňme výsledok z článku [5], kde sa autori zaoberali štúdiom čiastočných funkcií. Protokol počíta čiastočnú funkciu f, ak pre všetky vstupy (x, y), pre ktoré je f definovaná dá správny výsledok a pre ostatné vstupy dá ľubovoľný výsledok. V uvedenom článku autori našli čiastočnú funkciu $f : \{0,1\}^n \times \{0,1\} \to \{0,1\}$, pre ktorú $\mathrm{C}_D(f) = \Theta(\log n)$ a $\overline{\mathrm{C}_D}(f) = O(1)$.

1.5 Amortizovaná komunikačná zložitosť väčšiny funkcií

V predchádzajúcich podkapitolách sme uviedli prehľad známych výsledkov o amortizovanej komunikačnej zložitosti funkcií. Takisto sme zaviedli niektoré často používané metódy dolných odhadov funkcií. Zostala však otvorená otázka, ako veľmi sa môže líšiť amortizovaná zložitosť funkcie od komunikačnej zložitosti. V tejto podkapitole dokážeme, že pre väčšinu funkcií sa nelíši o viac ako o malú konštantu. Kvôli jednoduchosti budeme uvažovať iba funkcie, ktoré majú oba vstupy z toho istého definičného oboru a ktorých obor hodnôt je množina $\{0,1\}$.

Označenie 1.33 *Nech D je konečná množina. Potom označme $\mathcal{F}_D$ množinu všetkých funkcií z $D \times D$ do $\{0,1\}$.*

Je známe, že pre väčšinu funkcií z $\mathcal{F}_D$ sa ich komunikačná zložitosť líši od $\log |D|+1$ iba o malú konštantu (pozri [17, 14]). Špeciálne to platí aj pre $D = A^l$. Z toho však nutne nevyplýva, že aj väčšina funkcií tvaru $f^{(l)}$ má veľkú komunikačnú zložitosť. My však dokážeme, že je to tak. Budeme pritom postupovať podobne ako v uvedených článkoch — využijeme metódu najväčšieho obdĺžnika.

Veta 1.34 *Pre väčšinu funkcií z množiny $\mathcal{F}_D$ platí*

$$\lambda_f < 4 \cdot |D|.$$

Dôkaz: [17] Zvoľme pevne obdĺžnik veľkosti $P = 4 \cdot |D|$. Počet funkcií z $\mathcal{F}_D$, pre ktoré je tento obdĺžnik monochromatický, je $2 \cdot 2^{|D \times D| - P}$. Celkovo existuje $2^{|D|} \cdot 2^{|D|}$ všetkých obdĺžnikov, teda počet funkcií, ktoré obsahujú nejaký monochromatický obdĺžnik veľkosti aspoň P je najviac

$$2 \cdot 2^{|D \times D| - P} \cdot 2^{|D|} \cdot 2^{|D|} = 2 \cdot 2^{|D \times D|} \cdot 2^{-2 \cdot |D|}.$$

Všetkých funkcií z $D \times D$ do $\{0,1\}$ je $2^{|D \times D|}$. Podiel funkcií, pre ktoré $\lambda_f \geq P$ a všetkých funkcií je teda najviac $2 \cdot 2^{-2 \cdot |D|}$ a to je menej ako $\frac{1}{2}$. Pre viac ako polovicu všetkých funkcií teda platí $\lambda_f < P$. □

Veta 1.35 *Pre väčšinu funkcií z* $\mathcal{F}_D$ *platí* $\overline{\mathrm{C}_D}(f) \geq \mathrm{C}_D(f) - 4$.

Dôkaz: Označme S_D množinu všetkých funkcií z $\mathcal{F}_D$, pre ktoré platí $\lambda_f < 4 \cdot |D|$. Z vety 1.34 vieme, že S_D obsahuje väčšinu funkcií z $\mathcal{F}_D$.

Nech $f \in S_D$ a nech l je prirodzené číslo. Z dôsledku 1.27 vyplýva, že $\lambda_{f^{(l)}} = (\lambda_f)^l$ a teda $\lambda_{f^{(l)}} < (4 \cdot |D|)^l$. Podľa vety 1.20

$$\mathrm{C}_D(f^{(l)}) \geq 2\log|D^l| - \log\lambda_{f^{(l)}} > 2l\log|D| - \log(4 \cdot |D|)^l = l(\log|D| - 2).$$

Teda $\overline{\mathrm{C}_D}(f) = \limsup_{l\to\infty} \frac{1}{l}\mathrm{C}_D(f^{(l)}) \geq \log|D| - 2$. Naopak pre ľubovoľnú booleovskú funkciu f nad $D \times D$ platí, že $\mathrm{C}_D(f) \leq \lceil\log|D|\rceil + 1 \leq \log|D| + 2$ (hráč 1 pošle hráčovi 2 celý vstup a hráč 2 oznámi výsledok). Pre funkcie z S_D platí

$$\mathrm{C}_D(f) - \overline{\mathrm{C}_D}(f) \leq (\log|D| + 2) - (\log|D| - 2) = 4.$$

$\square$

Kapitola 2

Simultánne protokoly

2.1 Definície

2.1.1 Definície protokolov

Najprv popíšeme protokoly neformálne. Uvažujme nasledujúcu komunikačnú hru. Máme danú funkciu troch premenných $f(x, y, z)$. Ďalej uvažujme štyroch hráčov 1, 2, 3, 4, pričom hráč 1 pozná vstupy y a z, hráč 2 pozná vstupy x a z a hráč 3 pozná vstupy x a y. Hráč 4 nepozná žiaden vstup. Cieľom je vypočítať hodnotu $f(x, y, z)$, pričom hráči postupujú nasledujúcim spôsobom: najprv každý z hráčov 1, 2 a 3 na základe svojich vstupov vypočíta správu a tú pošle hráčovi 4. Hráč 4 potom na základe prijatých správ vypočíta výsledok. Simultánny protokol je predpis, ktorý určuje každému z hráčov 1, 2 a 3 pre každú dvojicu jemu známych vstupov správu, ktorú má poslať a hráčovi 4 určuje pre každú trojicu prídených správ výsledok (funkčnú hodnotu).

Budeme skúmať aj dve obmeny základného simultánneho modelu komunikácie. Simultánny protokol nazveme zúžený, ak hráč 3 neposiela žiadnu správu. Ďalej budeme uvažovať takmer simultánne protokoly. Sú to protokoly, v ktorých hráč 1 a hráč 2 pošlú správu hráčovi 3 a ten vypočíta výsledok (hráča 4 možno vynechať).[1]

Predpokladáme, že protokoly sú prefixové, t.j. množina všetkých možných správ je pre každého hráča bezprefixová. Tento predpoklad zjednodušuje mnohé odhady, pričom nemá veľký vplyv na komunikačnú zložitosť.

Definujme teraz protokoly formálne.

Definícia 2.1 *Nech D_1, D_2, D_3 a H sú konečné množiny.* **Simultánny protokol** *z $D_1 \times D_2 \times D_3$ do H je štvorica funkcií (m_1, m_2, m_3, m_4), kde*

$$\begin{array}{ll} m_1 : D_2 \times D_3 \to \{0,1\}^* & m_2 : D_1 \times D_3 \to \{0,1\}^* \\ m_3 : D_1 \times D_2 \to \{0,1\}^* & m_4 : M \to H, \end{array}$$

[1] Takmer simultánny protokol (almost simultaneous protocol) bol zavedený v [15]. Zúžený protokol sme zaviedli v tejto práci kvôli tomu, že sa v ňom dá zložitosť dobre charakterizovať kombinatorickými objektami.

pričom $M = \{(m_1(y,z), m_2(x,z), m_3(x,y)) \mid x \in D_1, y \in D_2, z \in D_3\}$ *a navyše množiny správ* $H(m_1)$, $H(m_2)$ *a* $H(m_3)$ *sú bezprefixové množiny.*[2]

Nech $P = (m_1, m_2, m_3, m_4)$ *je simultánny protokol z* $D_1 \times D_2 \times D_3$ *do* H. *Vravíme, že* **protokol** P **počíta funkciu** $f : D_1 \times D_2 \times D_3 \to H$, *ak pre všetky* $x \in D_1$, $y \in D_2$ *a* $z \in D_3$ *platí*

$$f(x,y,z) = m_4(m_1(y,z), m_2(x,z), m_3(x,y)).$$

Definícia 2.2 *Nech* D_1, D_2, D_3 *a* H *sú konečné množiny.* **Takmer simultánny protokol** *z* $D_1 \times D_2 \times D_3$ *do* H *je trojica funkcií* (m_1, m_2, m_3), *kde*

$$m_1 : D_2 \times D_3 \to \{0,1\}^* \qquad m_2 : D_1 \times D_3 \to \{0,1\}^*$$
$$m_4 : D_1 \times D_2 \times M \to H,$$

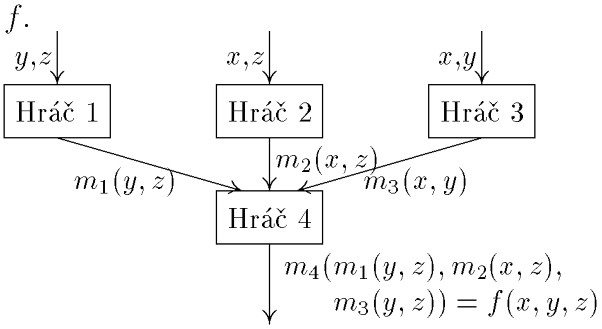
pričom $M = \{(m_1(y,z), m_2(x,z)) \mid x \in D_1, y \in D_2, z \in D_3\}$ *a navyše množiny správ* $H(m_1)$ *a* $H(m_2)$ *sú bezprefixové množiny.*

Nech $P = (m_1, m_2, m_3)$ *je takmer simultánny protokol z* $D_1 \times D_2 \times D_3$ *do* H. *Vravíme, že* **protokol** P **počíta funkciu** $f : D_1 \times D_2 \times D_3 \to H$, *ak pre všetky* $x \in D_1$, $y \in D_2$ *a* $z \in D_3$ *platí*

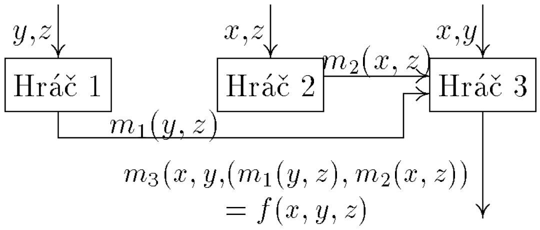
$$f(x,y,z) = m_3(x, y, (m_1(y,z), m_2(x,z)))$$

Definícia 2.3 *Simultánny protokol* $P = (m_1, m_2, m_3, m_4)$ *z* $D_1 \times D_2 \times D_3$ *do* H *nazveme* **zúženým simultánnym protokolom**, *ak pre každé* $x \in D_1$ *a* $y \in D_2$ *platí* $m_3(x,y) = \varepsilon$.

Pre lepšiu orientáciu v jednotlivých obmenách protokolov uvádzame ešte grafické znázornenie práce simultánneho protokolu P, takmer simultánneho protokolu P_A a zúženého simultánneho protokolu P_R, pričom všetky tri protokoly počítajú funkciu f.

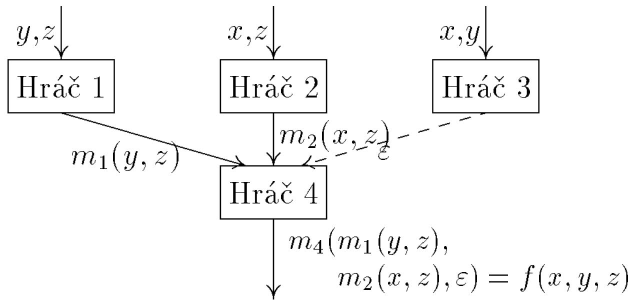


Simultánny protokol P



Takmer simultánny protokol P_A

[2]Symbolom $H(f)$ budeme pre funkciu f označovať množinu všetkých hodnôt, ktoré f nadobúda.



Zúžený simultánny protokol P_R

Simultánne protokoly a ich obmeny sme definovali nad ľubovoľnými konečnými množinami D_1, D_2, D_3 a H. Ďalej sa však obmedzíme na prípad $H = \{0, 1\}$. Ďalej si treba uvedomiť, že pre skúmanie vlastností protokolov nie je podstatné, aké prvky sú v množinách D_1, D_2 a D_3, dôležité sú predovšetkým počty prvkov v týchto množinách. Množiny s rovnakým počtom prvkov sú pre nás ekvivalentné. Preto stačí uvažovať množiny typu $Z_n = \{0, 1, \ldots, n-1\}$.

Označenie 2.4 *Nech p a n sú celé kladné čísla. Označme $\mathcal{F}_{p,n}$ množinu všetkých funkcií $f : Z_p \times Z_p \times Z_n \to \{0, 1\}$.*

Funkcie, súvisiace s otvorenými problémami, ktoré motivovali vznik simultánneho modelu (pozri časť 2.2), a ktoré sú teda v centre našej pozornosti, patria do množiny $\mathcal{F}_{m,2^m}$. Predmetom našich úvah budú ale protokoly počítajúce funkcie z množiny $\mathcal{F}_{p,n}$ pre ľubovoľné p, n. To umožňuje zjednodušiť a zovšeobecniť viaceré definície a dôkazy.

2.1.2 Simultánna komunikačná zložitosť

Definujme teraz dve miery zložitosti pre simultánne protokoly — komunikačnú a správovú zložitosť. Tieto dve miery zložitosti spolu úzko súvisia (pozri lemu 2.8).

Definícia 2.5 *Nech $P = (m_1, m_2, m_3, m_4)$ je simultánny komunikačný protokol z $D_1 \times D_2 \times D_3$ do H.* **Komunikačnú zložitosť protokolu** *P definujeme ako*

$$\mathrm{C}_S(P) = \max\left\{\, |m_1(y,z)| + |m_2(x,z)| + |m_3(x,y)| \,\middle|\, x \in D_1, y \in D_2, z \in D_3 \right\}.$$

Správovú zložitosť protokolu *P definujeme ako*

$$\mathrm{M}_S(P) = \max\left\{ \max\{\, |m_1(y,z)|, |m_2(x,z)|, |m_3(x,y)| \} \,\middle|\, x \in D_1, y \in D_2, z \in D_3 \right\}.$$

Komunikačná zložitosť simultánneho protokolu je teda celkový počet prenesených bitov v najhoršom prípade, správová zložitosť je dĺžka najdlhšej správy protokolu. Analogicky možno zadefinovať komunikačnú a správovú zložitosť takmer simultánneho protokolu.[3]

[3] Zložitosť zúženého simultánneho protokolu zavádzať netreba, lebo každý zúžený simultánny protokol je zároveň simultánnym protokolom.

Definícia 2.6 *Nech* $P = (m_1, m_2, m_3)$ *je takmer simultánny komunikačný protokol z* $D_1 \times D_2 \times D_3$ *do* H. **Komunikačnú zložitosť protokolu** P *definujeme ako*

$$\mathrm{C}_{AS}(P) = \max\left\{|m_1(y,z)| + |m_2(x,z)| | x \in D_1, y \in D_2, z \in D_3\right\}.$$

Správovú zložitosť protokolu P *definujeme ako*

$$\mathrm{M}_{AS}(P) = \max\left\{\max\{|m_1(y,z)|, |m_2(x,z)|\} | x \in D_1, y \in D_2, z \in D_3\right\}.$$

Definovali sme teda komunikačnú a správovú zložitosť simultánneho protokolu a jeho obmien. Teraz zavedieme simultánnu komunikačnú zložitosť funkcie ako komunikačnú zložitosť "najlepšieho" protokolu, ktorý túto funkciu počíta.

Definícia 2.7 *Nech* $f : D_1 \times D_2 \times D_3 \to H$. **Simultánnu komunikačnú zložitosť funkcie** f *definujeme ako*

$$\mathrm{C}_S(f) = \min\left\{\mathrm{C}_S(P) | P \textit{ je simultánny komunikačný protokol počítajúci funkciu } f\right\},$$

simultánnu správovú zložitosť funkcie f *definujeme ako*

$$\mathrm{M}_S(f) = \min\left\{\mathrm{M}_S(P) | P \textit{ je simultánny komunikačný protokol počítajúci funkciu } f\right\}.$$

Analogicky možno definovať takmer simultánnu komunikačnú zložitosť zložitosť funkcie f (označenie $\mathrm{C}_{AS}(f)$) pomocou komunikačnej zložitosti takmer simultánnych protokolov a zúženú simultánnu komunikačnú zložitosť funkcie f (označenie $\mathrm{C}_{\varepsilon S}(f)$) definujeme pomocou komunikačnej zložitosti zúžených simultánnych protokolov.

Podobne definujeme takmer simultánnu správovú a zúženú simultánnu správovú zložitosť funkcie f (označenie $\mathrm{M}_{AS}(f)$ resp. $\mathrm{M}_{\varepsilon S}(f)$) pomocou zodpovedajúcich správových zložitostí.

2.1.3 Základné vlastnosti

V tejto časti uvedieme základné vzťahy medzi zadefinovanými mierami zložitosti protokolov a funkcií a ďalšie pomocné tvrdenia. Lema 2.8 uvádza pre každý z našich troch modelov vzťah medzi komunikačnou a správovou zložitosťou danej funkcie. Vidíme, že tieto miery sa v každom z uvažovaných modelov líšia iba o konštantný násobok. Ak nás teda zložitosť funkcie zaujíma iba asymptoticky, tieto dve miery sú ekvivalentné a môžeme vždy použiť tú z nich, s ktorou sa pre daný problém lepšie pracuje.

Lema 2.8 *Nech* $f \in \mathcal{F}_{p,n}$. *Potom platí:*

$$\begin{aligned}\tfrac{1}{3}\mathrm{C}_S(f) \le \mathrm{M}_S(f) &\le \mathrm{C}_S(f)\\ \tfrac{1}{2}\mathrm{C}_{AS}(f) \le \mathrm{M}_{AS}(f) &\le \mathrm{C}_{AS}(f)\\ \tfrac{1}{2}\mathrm{C}_{\varepsilon S}(f) \le \mathrm{M}_{\varepsilon S}(f) &\le \mathrm{C}_{\varepsilon S}(f).\end{aligned}$$

Dôkaz: Dokážme najprv prvú z nerovností. Nech P je simultánny protokol počítajúci funkciu f. Dokážeme, že platí $\frac{1}{3}\mathrm{C}_S(P) \leq \mathrm{M}_S(P) \leq \mathrm{C}_S(P)$. Požadované tvrdenie potom už dostaneme z definície $\mathrm{C}_S(f)$ a $\mathrm{M}_S(f)$.

$\mathrm{M}_S(P)$ je dĺžka najdlhšej poslanej správy v protokole a $\mathrm{C}_S(P)$ je maximálny súčet dĺžok správ poslaných pre niektorý vstup v protokole. Ak uvažujeme vstup, pre ktorý jeden z hráčov pošle správu dĺžky $\mathrm{M}_S(P)$, tak aj keby ostatní hráči pre tento vstup neposielali nič, celková komunikácia bude aspoň $\mathrm{M}_S(P)$ a teda $\mathrm{C}_S(P) \geq \mathrm{M}_S(P)$. Na druhej strane dĺžka každej jednotlivej správy je najviac $\mathrm{M}_S(P)$ a keďže správy posielajú traja hráči, platí $\mathrm{C}_S(P) \leq 3\mathrm{M}_S(P)$.

Ostatné nerovnosti sa dokážu podobne, treba si len uvedomiť že v takmer simultánnych a zúžených simultánnych protokoloch posielajú (neprázdne) správy iba dvaja hráči. □

V nasledujúcej leme uvedieme vzťah medzi simultánnou komunikačnou zložitosťou funkcie a jej obmenami – takmer simultánnou a zúženou simultánnou zložitosťou.

Lema 2.9 *Nech $f \in \mathcal{F}_{p,n}$. Potom platí:*

$$\mathrm{C}_{AS}(f) \leq \mathrm{C}_S(f) \leq \mathrm{C}_{AS}(f) + 2\lceil \log p \rceil$$
$$\mathrm{C}_{\varepsilon S}(f) - 2\lceil \log p \rceil \leq \mathrm{C}_S(f) \leq \mathrm{C}_{\varepsilon S}(f)$$

Dôkaz: Dokážeme najprv prvé tvrdenie. Majme ľubovoľný simultánny protokol $P = (m_1, m_2, m_3, m_4)$ počítajúci f. Z neho môžeme zostrojiť takmer simultánny protokol $P' = (m'_1, m'_2, m'_3)$ tak, že hráči 1 a 2 nebudú posielať správy hráčovi 4, ale hráčovi 3. Hráč 3 si navyše vypočíta správu, ktorú by posielal v protokole P, takže má k dispozícii všetky tri správy, na základe ktorých už vie podľa protokolu P určiť výsledok. Je zrejmé, že takto zostrojený protokol P' počíta tiež funkciu f. Komunikačná zložitosť protokolu P' neprevyšuje komunikačnú zložitosť protokolu P, teda máme $\mathrm{C}_{AS}(f) \leq \mathrm{C}_S(f)$.

Naopak, majme takmer simultánny protokol $P = (m_1, m_2, m_3)$ počítajúci funkciu f. K nemu zostrojíme simultánny protokol $P' = (m'_1, m'_2, m'_3, m'_4)$ počítajúci funkciu f takto: Hráči 1 a 2 budú posielať správy hráčovi 4 namiesto hráča 3. Navyše hráč 3 pošle hráčovi 4 správu, ktorá bude obsahovať binárny zápis prvých dvoch vstupov funkcie (každé z týchto čísel zapíšeme pomocou $\lceil \log p \rceil$ bitov). Hráč 4 má teda všetky informácie, aké ma v protokole P hráč 3 a vie preto určiť výsledok. Celková komunikácia vzrástla o $2\lceil \log p \rceil$ bitov, máme teda, že $\mathrm{C}_S(f) \leq \mathrm{C}_{AS}(f) + 2\lceil \log p \rceil$.

V druhej časti dôkazu dokážeme druhý zo vzťahov. Uvedomme si najprv, že každý zúžený simultánny protokol je zároveň aj simultánnym protokolom. Z toho priamo dostávame nerovnosť $\mathrm{C}_S(f) \leq \mathrm{C}_{\varepsilon S}(f)$. Vezmime teraz ľubovoľný simultánny protokol $P = (m_1, m_2, m_3, m_4)$. Zostrojíme zúžený simultánny protokol $P' = (m'_1, m'_2, m'_3, m'_4)$, ktorý počíta tú istú funkciu ako P takto: hráč 3 v P' neposiela nič. Správa, ktorú posielal v protokole P, sa však dá vypočítať z hodnôt prvých dvoch vstupov funkcie, pričom každý z hráčov 1 a 2 pozná jeden z týchto vstupov. Títo hráči teda k svojej správe pripoja ešte binárny zápis jednej z týchto dvoch hodnôt. Dĺžka každej správy sa tak predĺži o $\lceil \log p \rceil$ bitov. Hráč 4 potom na základe prijatých prijatých prvých dvoch vstupov dopočíta chýbajúcu správu a určí výsledok. K správam posielaným v protokole P sme takto pridali $2\lceil \log p \rceil$ bitov, máme teda, že $\mathrm{C}_{\varepsilon S}(f) - 2\lceil \log p \rceil \leq \mathrm{C}_S(f)$. □

Dôsledok 2.10 *Nech $f \in \mathcal{F}_{p,n}$. Potom platí:*

$$\mathrm{M}_{AS}(f) \leq \mathrm{M}_S(f) \leq \max\{\mathrm{M}_{AS}(f), 2\lceil \log p \rceil\}$$
$$\mathrm{M}_{\varepsilon S}(f) - \lceil \log p \rceil \leq \mathrm{M}_S(f) \leq \mathrm{M}_{\varepsilon S}(f)$$

Dôkaz: Dôkaz tohoto tvrdenia je obmenou dôkazu predchádzajúcej vety. Použijeme rovnaké konštrukcie, iba namiesto komunikačnej zložitosti budeme počítať správovú zložitosť. □

Poznámka: Ak uvažujeme funkcie $f \in \mathcal{F}_{p,n}$, pre ktoré je veľkosť vstupov x a y (t.j. $\lceil \log p \rceil$) zanedbateľná vzhľadom na komunikačnú zložitosť funkcie v simultánnom modeli, potom všetky uvedené miery zložitosti ($\mathrm{C}_S(f)$, $\mathrm{C}_{AS}(f)$, $\mathrm{C}_{\varepsilon S}(f)$, $\mathrm{M}_S(f)$, $\mathrm{M}_{AS}(f)$ a $\mathrm{M}_{\varepsilon S}(f)$) sú navzájom takmer ekvivalentné.

Lema 2.11 *Ak danú funkciu $f \in \mathcal{F}_{p,n}$ je možné počítať simultánnym protokolom, v ktorom hráč i posiela iba správy dĺžky najviac k, potom existuje protokol na výpočet funkcie f, v ktorom hráč i posiela iba správy dĺžky k (a množiny správ ostatných hráčov sú rovnaké).*

Dôkaz: Nech P je protokol na výpočet funkcie f, v ktorom hráč i poslal iba správy dĺžky najviac k bitov. Keďže protokol P je prefixový, hráč i nemôže posielať viac ako 2^k rôznych správ. Všetkých reťazcov dĺžky k je presne 2^k a žiaden z nich nie je prefixom iného. Hráčovi i možno teda nahradiť každú správu reťazcom dĺžky k tak, aby v novom protokole boli správy posielané pre dva vstupy rovnaké práve vtedy, ak boli pre tieto vstupy rovnaké aj v protokole P. □

2.2 Prehľad známych výsledkov

Simultánne protokoly boli už námetom viacerých článkov. Uvedieme prehľad známych výsledkov v tejto oblasti. Tento prehľad je členený na dve časti. V prvej ukážeme, ako možno výsledky získané v simultánnej zložitosti aplikovať na získanie dolných odhadov pre booleovské obvody. Druhá časť obsahuje horné a dolné odhady komunikačnej zložitosti pre konkrétne funkcie.

2.2.1 Aplikácie v booleovských obvodoch

V tejto časti uvedieme motiváciu, ktorá viedla k skúmaniu simultánneho modelu komunikačnej zložitosti.[4] Bola ňou súvislosť simultánnej komunikačnej zložitosti so vzťahom medzi veľkosťou a hĺbkou booleovského obvodu.

[4] Simultánna komunikačná zložitosť bola zavedená v [13].

Majme funkciu f s $a+b$ bitmi vstupu a c bitmi výstupu a uvažujme obvody, ktoré túto funkciu počítajú. Môžeme sa snažiť nájsť minimálnu veľkosť, akú môže mať obvod počítajúci f, alebo minimálnu hĺbku, akú môže mať obvod počítajúci f. Často sa však stáva, že ak sa snažíme minimalizovať hĺbku obvodu, rastie jeho veľkosť a naopak. Vzniká teda otázka, aký veľký musí byť obvod počítajúci funkciu f, ak má mať určitú danú hĺbku. A táto otázka úzko súvisí so simultánnou komunikačnou zložitosťou. Čo sa týka komunikačnej zložitosti, tú sme zaviedli pre funkcie s tromi vstupmi a jedným bitom výstupu. Preto nebudeme simultánnymi protokolmi počítať priamo funkciu f, ale funkciu bit_f, ktorú z f dostaneme tak, že jej pridáme ďalší argument z množiny Z_c, ktorý bude určovať, ktorý bit výstupu chceme počítať.

Označenie 2.12 *Majme funkciu* $f : \{0,1\}^a \times \{0,1\}^b \to \{0,1\}^c$. *Označme* bit_f *funkciu* $bit_f : Z_c \times \{0,1\}^a \times \{0,1\}^b \to \{0,1\}$, *takú, že pre všetky* i, j, k *platí*

$$bit_f(i,j,k) = (f(j,k))(i).$$

Bolo dokázané (pozri lemu 2.15), že ak sa funkcia f sa dá počítať obvodom s určitou hĺbkou a veľkosťou, tak máme aj horný odhad komunikačnej zložitosti funkcie bit_f. Z toho ale vyplýva, že naopak, ak poznáme dolný odhad simultánnej komunikačnej zložitosti určitej funkcie bit_f, vieme z neho odvodiť, že funkciu f nie je možné počítať obvodmi, ktoré majú pri určitej hĺbke príliš malú veľkosť.

Konkrétne sa uvažoval vzťah pre funkcie s $O(n)$ vstupmi a výstupmi a pre hĺbku obvodu $O(\log n)$ a veľkosť $O(n)$. Otvoreným problémom je dokázať pre niektorú funkciu, ktorá sa dá počítať na (nedeterministickom) Turingovom stroji v polynomiálnom čase, že túto funkciu nie je možné počítať booleovským obvodom s lineárnou veľkosťou a logaritmickou hĺbkou. Pritom existujú jednoduché funkcie, pre ktoré takýto obvod nie je známy.

Práve snaha o riešenie tohto otvoreného problému viedla k skúmaniu modelu simultánnej komunikačnej zložitosti (pozri [13]). V nasledujúcej vete uvedieme horný odhad simultánnej komunikačnej zložitosti pre funkcie s $O(n)$ vstupmi a $O(n)$ výstupmi počítanými booleovskými obvodmi hĺbky $O(\log n)$ a veľkosti $O(n)$. Budeme uvažovať funkcie $f : \{0,1\}^n \times \{0,1\}^{\lceil \log n \rceil} \to \{0,1\}^n$, pretože takéto počty argumentov majú funkcie, ktoré sa v literatúre v tejto súvislosti používali. Príslušná funkcia bit_f má potom dva vstupy dĺžky $\lceil \log n \rceil$ a jeden vstup dĺžky n (patrí teda do množiny funkcií $\mathcal{F}_{\lceil logn \rceil, n}$). Dôkaz vety (najmä lema 2.15) však dáva návod, ako vetu možno modifikovať aj na iné dĺžky vstupov.

Nakoľko z formálneho hľadiska nemá zmysel používať O-notáciu pre funkcie s konečným oborom hodnôt, nasledujúci výsledok budeme formulovať pre nekonečnú postupnosť funkcií $\{f_n\}$ so zväčšujúcim sa oborom hodnôt.

Veta 2.13 [13, 10] *Nech* ε *je pevne dané kladné reálne číslo. Ďalej nech* $\{f_n\}_{n=1}^{\infty}$ *je postupnosť funkcií*

$$f_n : \{0,1\}^{\lceil \log n \rceil} \times \{0,1\}^n \to \{0,1\}^n$$

takých, že f_n *sa dá počítať booleovským obvodom s hĺbkou* $O(\log n)$ *a veľkosťou* $O(n)$. *Potom pre každé* n *existuje simultánny protokol počítajúci funkciu* bit_{f_n}, *pre ktorý platí:*

- *Hráč 1 pošle* $O(n/\log\log n)$ *bitov.*
- *Hráč 2 pošle* $O(n^\varepsilon)$ *bitov.*
- *Hráč 3 pošle* $O(\log n)$ *bitov.*

Poznámka: Vo vete konštanta pri člene $n/\log\log n$ vo výraze $O(n/\log\log n)$ závisí od hodnoty ε (nezávisí však od n).

Skôr, než uvedenú vetu dokážeme, budeme sa podrobnejšie zaoberať jej možným využitím. Ak chceme dokázať, že určitú funkciu f (presnejšie postupnosť funkcií $\{f_n\}$) nie je možné počítať obvodom hĺbky $O(\log n)$ a veľkosti $O(n)$, môžeme to spraviť tak, že dokážeme, že zodpovedajúca funkcia bit_f má komunikačnú zložitosť $\omega(n/\log\log n)$. Podľa vety 2.13 totiž máme, že ak sa f dá počítať obvodom s veľkosťou $O(n)$ a hĺbkou $O(\log n)$, tak bit_f má komunikačnú zložitosť $O(n/\log\log n)$.

Pôvodne sa skúmala funkcia *shift*^{n} (ktorej sa budeme venovať v ďalšej kapitole), o ktorej sa predpokladá, že ju nie je možné počítať obvodom logaritmickej hĺbky a lineárnej veľkosti. Existovala domnienka, že bude možné dokázať, že simultánna komunikačná zložitosť funkcie *shift*^{n} je naozaj $\omega(n/\log\log n)$, a tak že sa vyrieši uvedený otvorený problém.

Avšak, hoci sa pôvodne predpokladalo, že simultánna komunikačná zložitosť funkcie *shift*^{n} je $\Theta(n)$, bol nájdený prekvapivý horný odhad ukazujúci, že jej komunikačná zložitosť je v skutočnosti $o(n/\log\log n)$. Takže vetu 2.13 nie je možné v tomto prípade použiť takto priamočiaro.

Dalo by sa však možno postupovať tak, že by sa uvažovali aj dĺžky správ jednotlivých hráčov. V nájdených protokoloch, ktoré dokazujú tento prekvapivý horný odhad, hráči 1 aj 2 posielajú veľa bitov. Veta 2.13 však hovorí o protokole, v ktorom hráč 1 pošle $O(n/\log\log n)$ bitov, hráč 2 však pošle iba $O(n^\varepsilon)$ bitov pre ľubovoľne malé ε. Či takýto protokol pre funkciu *shift*^{n} existuje, sa ešte nepodarilo ukázať. Ak by sa však ukázalo, že pre niektoré ε takýto protokol neexistuje, potom by sme rovnako dokázali, že pre funkciu *shift*^{n} neexistuje obvod veľkosti $O(n)$ a hĺbky $O(\log n)$. Odhadovať dĺžku správy hráča 2, ak obmedzíme dĺžku správy hráča 1, je však omnoho ťažšie ako odhadovať celkovú komunikačnú zložitosť.

Vetu 2.13 dokážeme pomocou dvoch pomocných liem. Prvá lema (lema 2.14) hovorí o vlastnostiach orientovaných acyklických grafov, ktoré zodpovedajú booleovským obvodom. Túto lemu dokázal Valiant už v roku 1977 v článku [16]. Lema 2.15 ukazuje, ako aplikovať lemu 2.14 na získanie odhadu pre simultánnu komunikačnú zložitosť. Táto lema je v podstate všeobecnejším tvrdením ako veta 2.13, pretože ju možno aplikovať aj na iné hĺbky a veľkosti booleovských obvodov ako $O(\log n)$ a $O(n)$.

Pripomeňme si teraz, že booleovský obvod je vlastne špeciálny orientovaný graf a že jeho hĺbkou rozumieme počet vrcholov na najdlhšej orientovanej ceste v G.

Označením vrcholov grafu G budeme rozumieť priradenie celých čísel vrcholom také, že pre každú hranu (u, v) platí, že vrchol u má priradené menšie číslo ako vrchol v.

Je zrejmé, že graf s hĺbkou d možno označiť číslami z množiny Z_d. Každý vrchol jednoducho označíme dĺžkou najdlhšej orientovanej cesty, ktorá do tohoto vrcholu vchádza. Naopak, ak pre graf G existuje označenie pomocou čísel zo Z_d, tak hĺbka grafu G je najviac d. To preto, že hĺbka grafu je dĺžka najdlhšej cesty a na tejto ceste majú vrcholy priradené navzájom rôzne čísla zo Z_d (každý vrchol má číslo aspoň o jedna väčšie ako jeho predchodca).

Lema 2.14 [16] *Nech $G = (V, E)$ je orientovaný graf s m hranami a hĺbkou d, pričom m a d sú mocniny čísla 2. Potom pre každé $k \leq \log d$ existuje množina hrán $X \subseteq E$ s najviac $mk/\log d$ prvkami taká, že graf $G' = (V, E \setminus X)$ má hĺbku najviac $d/2^k$.*

Dôkaz: Keďže graf G má hĺbku d, existuje označenie hrán grafu G číslami z množiny Z_d. Tieto čísla môžeme zapísať v dvojkovej sústave pomocou $\log d$ bitov. Nech X_i je množina všetkých hrán $(u, v) \in E$ takých, i-ty bit je najvyšší z bitov, v ktorých sa líšia čísla priradené vrcholom u a v. Všetky hrany z množiny E sme takto rozdelili do disjunktných množín X_1, X_2, $\ldots X_{\log d}$.

Uvažujme teraz graf H, ktorý vznikne z grafu G odstránením hrán z množiny X_i. Zostrojíme aj označenie vrcholov grafu H: vrcholu u v grafe priradíme číslo, ktoré vznikne z čísla priradeného vrcholu u v grafe G vynechaním i-teho bitu.

Dokážeme, že týmto spôsobom sme naozaj získali označenie vrcholov grafu H: Majme hranu (u, v) z grafu H a nech b a c sú čísla priradené vrcholom u a v v grafe G. Nech j je najvyšší bit, v ktorom sa čísla b a c líšia. V prípade, že $j < i$, tak i-ty (vynechaný) bit bol v oboch číslach rovnaký a teda aj v grafe H bude mať u menšie číslo ako v. Ak naopak $i > j$, tak po vynechaní i-teho bitu stále zostáva číslo vrcholu u menšie ako číslo vrcholu v, pretože vynechaný bit je menej významný ako bit j. Zostáva prípad $i = j$, ten však nemôže nastať, lebo to by znamenalo, že $(u, v) \in X_i$ a teda táto hrana by bola vynechaná a nepatrila by medzi hrany grafu H.

Takto vzniknuté označenie vrcholov grafu H navyše používa iba čísla, ktorých dvojkový zápis má najviac $\log d - 1$ cifier, t.j. používa čísla z množiny $Z_{d/2}$.

Takýmto spôsobom môžeme postupne odstrániť k z množín X_0, X_1, $\ldots X_{\log d}$. Odstránením každej z množín sa počet cifier v označení vrcholov zníži o 1, takže nakoniec dostaneme graf s vrcholmi označenými pomocou $\log d - k$ cifier, používajú sa teda iba čísla z množiny $Z_{d/2^k}$. Čiže výsledný graf bude mať hĺbku najviac $\frac{d}{2^k}$.

Zvoľme teraz spomedzi množín $X_0, X_1, \ldots X_{\log d}$ takých k množín, ktoré majú najmenší počet prvkov, a odstráňme ich z grafu G. Z predchádzajúcich úvah vyplýva, že sme dostali graf s požadovanou hĺbkou. Zostáva dokázať, že aj počet odstránených hrán spĺňa požiadavky tvrdenia. To je však jednoduché: v množinách X_0, X_1, $\ldots X_{\log d}$ je spolu m prvkov. Ak vyberieme k najmenších množín, môžu mať spolu najviac $\frac{km}{\log d}$ prvkov, čo sa ľahko ukáže sporom. □

Lema 2.15 [13] *Majme funkciu $f : \{0,1\}^a \times \{0,1\}^b \to \{0,1\}^c$ a nech čísla m a d sú mocniny čísla 2. Potom ak je možné počítať funkciu f booleovským obvodom s m hranami a hĺbkou d, potom pre každé $k \leq \log d$ existuje simultánny protokol počítajúci funkciu bit_f, pre ktorý platí:*

- *Hráč 1 pošle najviac* $\frac{km}{\log d}$ *bitov.*
- *Hráči 2 a 3 pošlú spolu najviac* $2^{d/2^k} + 2\lceil \log c \rceil$ *bitov.*

Dôkaz: Nech B je booleovský obvod hĺbky d s m hranami, ktorý počíta funkciu f. Podľa lemy 2.14 existuje množina hrán X veľkosti najviac $\frac{km}{\log d}$, ktorú keď odstránime z obvodu B, dostaneme graf hĺbky najviac $\frac{d}{2^k}$. Požadovaný simultánny protokol zostrojíme takto:

Hráč 1 pozná všetky vstupy obvodu B. Bude teda simulovať činnosť obvodu a pre každú hranu z X pošle hodnotu, ktorá prechádza po tejto hrane v obvode pre dané vstupy. Pošle teda správu dĺžky $\frac{km}{\log d}$.

Hráči 2 a 3 poznajú každý jednu časť vstupov obvodu a každý z nich okrem toho pozná číslo výstupu $i \in Z_c$, ktorého hodnotu treba vypočítať. Hodnotu na výstupe i bude hráč 4 počítať na základe toho, že bude poznať jednak hodnoty na všetkých hranách z X (ktoré pošle hráč 1), číslo i a ďalej hodnoty na tých vstupoch obvodu B, ktoré aj po odstránení hrán z X zostávajú pripojené na vstup i. Takýchto vstupov však nie je viac ako $2^{d/2^k}$, lebo po odstránení hrán z X má obvod hĺbku najviac $d/2^k$ a vstupný stupeň každého vrcholu je najviac 2.

Hráči 2 a 3 teda pošlú hodnoty všetkých vstupov obvodu B, ktoré sú napojené na výstup i (každý pošle tie hodnoty, ktoré pozná) a každý z nich pošle ešte aj vstup i. (Stačilo by síce, aby vstup i posielal iba jeden z hráčov, nebola by však zaručená prefixovosť protokolu).

Hráč 4 z prijatých údajov odsimuluje činnosť potrebnej časti obvodu B a vypočíta výsledok. □

Dôkaz vety 2.13: Ak má obvod veľkosť $O(n)$, potom má aj $O(n)$ hrán, lebo do každého hradla vchádzajú najviac dve hrany. Preto existujú kladné konštanty c, c_1 a c_2, že pre každé n je možné funkciu f_n počítať obvodom s veľkosťou $m \leq cn$ a hĺbkou d (kde $c_1 \log n \leq d \leq c_2 \log n$), pričom čísla m aj d sú mocniny čísla 2.

Pre takýto obvod použijeme lemu 2.15, pričom zvolíme $k = \lceil \log(c_2/\varepsilon) \rceil$, čo je od určitého n menej ako $\log d = \Theta(\log \log n)$. Dostávame protokol, v ktorom prvý hráč pošle najviac $km/\log d$ bitov, čo je $O(n/\log \log n)$ bitov. Druhý a tretí hráč pošlú spolu najviac $2^{d/2^k} + 2\lceil \log n \rceil$ bitov, pričom

$$2^{d/2^k} \leq 2^{c_2 \log n/(c_2/\varepsilon)} = n^{\varepsilon}.$$

Pritom ale obidva vstupy, ktoré pozná hráč 3, sú dĺžky $\lceil \log n \rceil$, takže hráč 3 určite pošle $O(\log n)$ bitov. Hráč 2 pošle $O(n^{\varepsilon})$ bitov. □

2.2.2 Výsledky pre konkrétne funkcie

V tejto časti ukážeme známe horné a dolné odhady simultánnej komunikačnej zložitosti špecifických funkcií. Predovšetkým je to funkcia Shift^n, ktorá dostane na vstupe n-bitový reťazec a číslo $i \in Z_n$ (zapísané v binárnej sústave pomocou $\lceil \log n \rceil$ bitov) a výsledkom bude pôvodný reťazec cyklicky posunutý o i miest doľava. Pre túto funkciu nebol nájdený obvod hĺbky $O(\log n)$ a veľkosti $O(n)$. Otvoreným problémom teda je dokázať, že takýto obvod ani neexistuje. Funkcia *Shift* je pomerne jednoduchá, možno ju však redukovať na mnohé iné prirodzené problémy ako násobenie binárnych čísel, polynómov a podobne. Ak by sa teda ukázalo, že funkciu $Shift^n$ nie je možné počítať obvodom hĺbky $O(\log n)$ a veľkosti $O(n)$, tak by nebolo možné takto počítať ani iné funkcie, na ktoré ju možno redukovať.

Označenie 2.16 *Nech n je prirodzené číslo, $Shift^n$ budeme označovať funkciu $Shift^n : Z_n \times \{0,1\}^n \to \{0,1\}^n$, pre ktorú platí $Shift(i,x) = y$, kde pre j-ty bit reťazca y platí $y(j) = x((i+j) \bmod n)$.*

Ďalej budeme označovať $shift^n$ funkciu bit_{Shift^n}, t.j. funkciu $shift^n : Z_n \times Z_n \times \{0,1\}^n \to \{0,1\}$, pre ktorú platí $shift(i,j,x) = x((i+j) \bmod n)$.

Ako sme už uviedli v prechádzajúcej kapitole, jedným zo spôsobov, ako ukázať, že $Shift^n$ nie je možné počítať obvodom lineárnej veľkosti a logaritmickej hĺbky, je dokázať, že simultánna komunikačná zložitosť funkcie $shift^n$ je $\omega(n/\log\log n)$. Pudlák, Rödl a Sgall však v článku [15] ukázali, že $\mathrm{C}_S(shift^n) = O(n \log\log n/\log n)$. Ich odhad bol ďalej zlepšený v [2].

Skúmala sa tiež zovšeobecnená verzia funkcie $shift^n$ — vo funkcii $shift^n$ dostaneme dve čísla zo Z_n, sčítame ich v Z_n a výsledné číslo určuje poradie výstupného bitu. Zovšeobecnením je uvažovať namiesto Z_n ľubovoľnú grupu rádu n. Dostávame takto zovšeobecnenú adresujúcu funkciu (generalised addressing function, skrátene GAF).

Označenie 2.17 *Nech $(G, \circ)$ je konečná grupa rádu n, pričom $G = \{g_0, g_1, \dots, g_{n-1}\}$. GAF_G budeme označovať funkciu $\mathrm{GAF}_G : G \times G \times \{0,1\}^n$, takú, že pre $g_i, g_j \in G$ a $x \in \{0,1\}^n$ platí $\mathrm{GAF}_G(g_i, g_j, x) = x(k)$, kde $g_i \circ g_j = g_k$.*

Ďalej uvedieme najlepší známy dolný aj horný odhad pre funkciu $shift^n$ a pre $\mathrm{GAF}_{Z_2^t}$, kde Z_2^t je vektorový priestor dimenzie t nad Z_2.

Dolný odhad

Pre obe uvažované funkcie ($shift^n$ aj $\mathrm{GAF}_{Z_2^t}$) ukážeme, že ich správová takmer simultánna zložitosť je $\Omega(\sqrt{n})$. Použijeme postup uvedený v [11, 3]. Poznamenajme ešte, že nakoľko je dolný odhad asymptoticky väčší ako $\log n$, vyplýva zo vzťahov uvedených v lemách 2.9 a 2.8, že správové a komunikačné zložitosti uvažovaných funkcií vo všetkých troch modeloch (simultánnom, takmer simultánnom aj zúženom) budú navzájom ekvivalentné (budú sa líšiť iba o multiplikatívnu konštantu) a je teda jedno, ktorú z uvedených troch mier skúmame.

Označenie 2.18 *Nech $(G, \circ)$ je konečná grupa. Označme*

$$\rho(G) = \min_{H_1, H_2 \subseteq G} \{\rho | \, \rho \geq |H_1| \wedge \rho \geq |H_2| \wedge G = H_1 \circ H_2\},$$

kde pre $H_1, H_2 \subseteq G$ označujeme $H_1 \circ H_2$ množinu $\{h_1 \circ h_2 | \, h_1 \in H_1, h_2 \in H_2\}$.

Veta 2.19 [11] *Nech $(G, \circ)$ je grupa rádu n. Potom platí*

$$\mathrm{M}_{AS}(\mathrm{GAF}_G) \geq \frac{n}{2\rho(G)}.$$

Dôkaz: Z definície $\rho(G)$ vyplýva, že existujú množiny $H_1, H_2 \subseteq G$ také, že $\rho(G) = \max\{|H_1|, |H_2|\}$ a každý prvok $g \in G$ sa dá zapísať aspoň jedným spôsobom v tvare $h_1 \circ h_2$ pre nejaké $h_1 \in H_1$ a $h_2 \in H_2$.

Vezmime teraz ľubovoľný takmer simultánny protokol $P = (m_1, m_2, m_3)$ počítajúci funkciu GAF_G a dokážeme, že $\mathrm{M}_{AS}(P) \geq \frac{n}{2\rho(G)}$.

Zvoľme reťazec $x \in \{0,1\}^n$. Zostrojme reťazce u a v, pričom do u uložíme zreťazenie správ $m_2(h, x)$ postupne pre všetky $h \in H_1$ a podobne do v uložíme správy $m_1(h, x)$ pre všetky $h \in H_2$. Nakoľko množiny správ posielaných jednotlivými hráčmi sú bezprefixové, reťazce u a v vieme jednoznačne rozložiť späť na jednotlivé správy. Navyše, množina reťazcov $u \cdot v$ prislúchajúcich k jednotlivým vstupom $x \in \{0,1\}^n$ je bezprefixová.

Ak poznáme reťazce u a v, vieme z nich určiť pôvodný reťazec x, a to takto. Vezmime bit reťazca x, ktorý zodpovedá prvku $g \in G$. Prvok g vieme napísať ako $h_1 \circ h_2$, pričom $h_1 \in H_1$ a $h_2 \in H_2$. V reťazci u nájdeme správu $m_2(h_1, x)$ posielanú hráčom 2 pre vstup h_1 a v reťazci v nájdeme správu $m_1(h_2, x)$. Zo správ $m_1(h_2, x)$ a $m_2(h_1, x)$ a z hodnôt h_1 a h_2 vieme určiť výsledok protokolu P, ktorým je presne hľadaný bit reťazca x. Pre rôzne prvky $g \in G$ takto získame postupne celý reťazec x.

Pre každé $x \in \{0,1\}^n$ možno na základe príslušných reťazcov u a v toto x jednoznačne určiť. Pre aspoň jedno x musí teda platiť, že $|u| + |v| \geq n$. Ďalej platí, že

$$|u \cdot v| \leq (|H_1| + |H_2|) \cdot \mathrm{M}_{AS}(P) \leq 2\rho(G) \cdot \mathrm{M}_{AS}(P),$$

lebo napríklad reťazec u vznikol zreťazením $|H_1|$ správ dĺžky najviac $\mathrm{M}_{AS}(P)$. Spojením týchto nerovností dostávame $2\rho(G) \cdot \mathrm{M}_{AS}(P) \geq n$ a z toho už priamočiaro vyplýva požadované tvrdenie. □

Dôsledok 2.20

$$\mathrm{M}_{AS}(\mathit{shift}^n) = \Omega(\sqrt{n}).$$

Dôkaz: Vieme, že $\mathit{shift}^n = \mathrm{GAF}_{Z_n}$, t.j. $\mathrm{M}_{AS}(\mathit{shift}^n) \geq n/2\rho(Z_n)$, stačí teda ukázať, že $\rho(Z_n) = O(\sqrt{n})$.

Nech $k = \lceil \sqrt{n} \rceil$. Každé číslo zo Z_n možno zapísať ako najviac dvojciferné číslo v sústave so základom k. Do množiny H_1 dáme všetky čísla zo Z_n, ktoré majú v takomto zápise najnižšiu cifru rovnú nule, podobne do H_2 dáme také čísla zo Z_n, ktoré majú v takomto zápise druhú najnižšiu cifru rovnú nule. V každej množine je teda najviac k čísel. Navyše každé $g \in Z_n$ možno triviálne zapísať ako súčet jedného čísla z H_1 a jedného čísla z H_2. Takže $Z_n = H_1 + H_2$ a teda $\rho(Z_n) \leq \max\{|H_1|, |H_2|\} = O(\sqrt{n})$. □

Dôsledok 2.21 *Nech $n = 2^t$. Potom platí*

$$\mathrm{M}_{AS}(\mathrm{GAF}_{Z_2^t}) = \Omega(\sqrt{n}).$$

Dôkaz: Aj v tomto prípade stačí ukázať, že $\rho(Z_2^t) = O(\sqrt{n})$. Konštrukcia bude podobná ako v predchádzajúcom dôsledku. Prvky Z_2^t sú binárne reťazce dĺžky t. Nech $k = \left\lceil \frac{t}{2} \right\rceil$. Do množiny H_1 dáme všetky reťazce zo Z_2^t, ktoré majú na prvých k miestach nuly (tých je $2^{(t-k)} \leq \sqrt{n}$), podobne do H_2 dáme reťazce zo Z_2^t, ktoré majú nuly na posledných $(t-k)$ miestach (tých je $2^k \leq 2 \cdot \sqrt{n}$). Platí, že $Z_2^t = H_1 + H_2$, takže $\rho(Z_2^t) \leq \max\{|H_1|, |H_2|\} = O(\sqrt{n})$. □

Poznámka: Pomocou vety 2.19 sme pre dve konkrétne grupy rádu n (Z_n a Z_2^t) dokázali, že $\mathrm{M}_{AS}(\mathrm{GAF}_G) = \Omega(\sqrt{n})$. Pre grupu rádu n týmto spôsobom lepší odhad ako $\Omega(\sqrt{n})$ ani získať nemožno, lebo $\rho(G) \geq \sqrt{n}$.

Horný odhad pre *shift*^{n}

Uvedieme teraz najlepší známy protokol pre funkciu *shift*^{n}. Ako sme už uviedli, nájdenie protokolu s komunikačnou zložitosťou $o(n)$ bolo dosť prekvapivé, pretože pôvodne sa predpokladalo, že simultánna komunikačná zložitosť funkcie *shift*^{n} je $\Theta(n)$.

Uvedieme najprv jednoduchý takmer simultánny protokol na výpočet *shift*^{n}, ktorý použije iba $\frac{n}{2} + O(1)$ bitov. Zložitejší protokol, uvedený vo vete 2.23, používa zovšeobecnenie tej istej myšlienky. Lemu 2.22 teda uvádzame kvôli lepšiemu pochopeniu.

V článku [15] bol uvedený protokol so zložitosťou $O(n \log\log n / \log n)$. Táto zložitosť bola ďalej zlepšená v článku [2] (pozri veta 2.23 a jej dôsledok).

Lema 2.22 [15] *Existuje takmer simultánny protokol pre shift^n, v ktorom hráč 1 pošle $\left\lceil \frac{n+1}{2} \right\rceil$ bitov a hráč 2 pošle 1 bit.*

Dôkaz: Počítajme hodnotu *shift*$^n(i,j,x)$, pričom x je n-bitový reťazec. Hráč 1 rozdelí bity reťazca x do dvojíc tak, že u-ty a v-ty bit budú v jednej skupine práve vtedy, keď $(u+v) \bmod n = j$. Pre každé u takéto v existuje, niekedy však môže platiť, že $u = v$. Bity, pre ktoré platí, že $(u+u) \bmod n = j$, budú teda tvoriť samostatné jednoprvkové skupiny.

Ak $(u+u) \bmod n = j$, znamená to, že buď $2u = j$ alebo $2u - n = j$. Teda buď $u = j/2$ alebo $u = (j+n)/2$. Pre nepárne n majú čísla j a $j+n$ rôznu paritu, a teda existuje práve jedna jednoprvková skupina. Ak je n párne, tieto čísla majú rovnakú paritu, a teda existujú buď dve alebo žiadna jednoprvková skupina. Celkový počet vytvorených skupín teda bude najviac $\left\lceil \frac{n+1}{2} \right\rceil$.

Hráč 1 teraz pre každú skupinu bitov spraví súčet bitov (sčítava v Z_2) a výsledné súčty pošle hráčovi 3. Hráč 2 pošle hráčovi 3 iba jeden bit $x(n-i)$. Hráč 3 pozná hodnoty i a j. Určí teda index $k = (i+j) \bmod n$ a medzi súčtami prijatými od hráča 1 nájde súčet skupiny, v ktorej sa bit $x(k)$ nachádza. V tejto skupine je súčet bitov $x(k)$ a $x(n-i)$, lebo $(i+j+n-i) \bmod n = j$. Výsledok teda dostávame po odčítaní bitu $x(n-i)$ od nájdeného súčtu skupiny (v prípade, že skupina bola jednoprvková, máme výsledok priamo, bez odčítania). □

Veta 2.23 [2] *Nech pre k platí $1 \leq k \leq \sqrt{\log n}$. Potom existuje takmer simultánny protokol pre shift^n, v ktorom hráč 1 pošle $O(n/2^k)$ bitov a hráč 2 pošle $O(kn^{1-1/k})$ bitov.*

Dôkaz: Zostrojíme takmer simultánny protokol P_1, ktorý v prípade, že $i + j < n$ vypočíta správne hodnotu $shift^n(i, j, x)$, pričom dĺžky správ poslaných jednotlivými hráčmi budú spĺňať požiadavky uvedené vo vete. Ak máme takýto protokol, protokol P počítajúci hodnotu $shift^n(i, j, x)$ pre ľubovoľné i a j, zostrojíme takto. Hráč 1 pošle správu zostavenú podľa protokolu P_1 pre vstupy j a x a tiež správu zostavenú podľa protokolu P_1 pre vstupy $j' = n - j - 1$ a x', ktorý získame otočením reťazca x. Hráč 2 podobne pošle správu podľa protokolu P_1 pre vstupy i a x a tiež správu pre vstupy $i' = n - i$ a reťazec x'. Hráč 3 pozná i aj j, takže v prípade, že $i + j < n$, určí výsledok podľa pôvodného protokolu P_1 pre vstupy i, j a x. Ak však $i + j \geq n$, tak hráč 3 získa výsledok podľa protokolu P_1 pre vstupy i', j' a x', lebo ak $i + j > n$, tak $i' + j' < n$ a $x'((i' + j') \bmod n) = x((i + j) \bmod n)$. Dĺžky správ protokolu P sa oproti protokolu P' zdvojnásobia, takže stále budú spĺňať ohraničenia dané dokazovanou vetou.

Konštrukcia protokolu P_1. Protokol P_1 má teda správne pracovať pre tie dvojice $i, j \in Z_n$, pre ktoré platí $(i + j) \bmod n = i + j$. Pri konštrukcii použijeme myšlienku z dôkazu lemy 2.22. Presnejšie, pre $k = 1$ je tu skonštruovaný P_1 veľmi podobný na protokol popísaný v leme.

Všetky bity vstupu x funkcie $shift^n(i, j, x)$ rozdelíme do skupín (tentokrát už viacprvkových) a hráč 1 pošle súčty bitov v jednotlivých skupinách. Hráč 2 pošle niekoľko bitov z reťazca x tak, aby poslal všetky bity, ktoré budú v skupine, v ktorej sa nachádza $x(i + j)$, okrem samotného bitu $x(i + j)$. Hráč 3 potom získa $x(i + j)$ odčítaním všetkých ostatných bitov od súčtu príslušnej skupiny.

Zvoľme $m = \lceil \sqrt[k]{n} \rceil$, čiže platí $m^k \geq n > (m - 1)^k$. Každé číslo zo Z_n možno zapísať v sústave so základom m pomocou najviac k cifier (všimnime si, že vzhľadom na ohraničenie k dané vo vete, bude pre $n > 1$ platiť $m \geq 2$ a teda môžeme naozaj používať sústavu so základom m). Označme teraz jednotlivé cifry zápisu čísla i v m-kovej sústave ako $i_0, i_1, \ldots, i_{k-1}$, podobne $j_0, j_1, \ldots j_{k-1}$ sú cifry zápisu čísla j a $l_0, l_1, \ldots l_{k-1}$ nech sú cifry zápisu čísla $l = i + j$. Ďalej budeme využívať fakt, že pre každé $t \in Z_k$ platí $l_t = (i_t + j_t) \bmod m$ alebo $l_t = (i_t + j_t + 1) \bmod m$.

Hráč 1 rozdelí bity reťazca x do skupín. Vezmime $u, v \in Z_n$, pričom cifry čísla u v zápise v m-kovej sústave označme $u_0, \ldots u_{k-1}$ a cifry zápisu čísla v označme $v_0, \ldots v_{k-1}$. Potom bity $x(u)$ a $x(v)$ budú v jednej skupine práve vtedy, keď pre každé $t \in Z_k$ platí

$$u_t = v_t \text{ alebo } (u_t + v_t) \bmod m = j_t.$$

V každej zo skupín vypočíta súčet bitov v Z_2 a tento súčet pošle hráčovi 3.

Odhadnime teraz počet vytvorených skupín. Pre každé t rozdelíme čísla zo Z_m na triedy ekvivalencie, pričom a a b budú v jednej triede práve vtedy, keď $a = b$ alebo $(a + b) \bmod m = j_t$. Pre každé t sú teda triedy určené hodnotou j_t. Počet tried pre každé t je najviac $\left\lceil \frac{m+1}{2} \right\rceil$ (dokázali sme v dôkaze lemy 2.22). Čísla $u, v \in Z_n$ budú v jednej skupine práve vtedy, ak pre každé $t \in Z_k$ sú ich cifry u_t a v_t v jednej triede ekvivalencie určenej číslom j_t. Všetkých skupín je teda $\left\lceil \frac{m+1}{2} \right\rceil^k$.

Protokol pre hráča 2 chceme zostaviť tak, že pošle také bity z reťazca x, aby medzi nimi určite boli všetky bity zo skupiny, v ktorej je $x(l)$, okrem prípadne samotného $x(l)$. V skupine s bitom $x(l)$ sú všetky také bity $x(u)$, že pre každé t platí $u_t = l_t$ alebo $(u_t + l_t) \bmod m = j_t$. Pre každý bit v tejto skupine okrem samotného $x(l)$ však pre aspoň jedno t platí $(u_t + l_t) \bmod m = j_t$. Túto rovnosť môžme upraviť s využitím znalosti, že $l_t = (i_t + j_t) \bmod m$ alebo $l_t = (i_t + j_t + 1) \bmod m$, na tvar

$$(u_t + i_t) \bmod m = 0 \text{ alebo } (u_t + i_t + 1) \bmod m = 0. \tag{2.1}$$

Zistili sme teda, že pre každý bit $x(u)$, ktorý je v skupine s $x(l)$ (okrem samotného $x(l)$), platí pre niektoré $t \in Z_k$ vzťah (2.1). Hráč 2 pošle všetky bity $x(u)$ také, že pre aspoň jedno $t \in Z_k$ platí vzťah (2.1). Medzi týmito bitmi teda budú aj všetky bity, ktoré sú v skupine spolu s $x(l)$.

Hráč 3 už len na základe i a j vypočíta l, zistí, v ktorej skupine sa $x(l)$ nachádza a od jej súčtu odčíta všetky ostatné bity tejto skupiny.

Zložitosť protokolu P_1. Hráč 1 pošle súčty $\left\lceil \frac{m+1}{2} \right\rceil^k$ skupín. Upravujme tento výraz:

$$\left\lceil \frac{m+1}{2} \right\rceil^k \le \frac{((m-1)+3)^k}{2^k} \le \frac{n + \sum_{i=1}^{k} \binom{k}{i} (m-1)^{k-i} 3^i}{2^k}.$$

Označme $S = \sum_{i=1}^{k} \binom{k}{i} (m-1)^{k-i} 3^i$. Stačí dokázať, že $S = O(n)$. Využijeme vzťahy $\binom{k}{i} \le 2^k$, $(m-1)^{k-i} < n \cdot n^{-i/k}$ a $\sum_{i=1}^{k} x^i = (x - x^{k+1})/(1-x)$ a dostávame:

$$\begin{aligned} S &\le 2^k n \textstyle\sum_{i=1}^{k} (3n^{-1/k})^i \le 3 \cdot 2^k n (3n^{-1/k} - 3^{k+1} n^{-\frac{k+1}{k}}) = \\ &= 9(n^{1-1/k+k/\log n} - n^{\log 6/\log n - 1/k}). \end{aligned}$$

Výraz $1 - \frac{1}{k} + \frac{k}{\log n}$ pre pevné n rastie s k, takže najväčší bude pre maximálnu povolenú hodnotu k, čo je $\sqrt{\log n}$. Pre túto hodnotu je však rovný presne 1. Takže dostávame $S \le 9n = O(n)$.

Dokázali sme teda, že počet skupín je $O(n/2^k)$, pre každú pošle hráč 1 jeden bit, pošle teda správu dĺžky $O(n/2^k)$.

Hráč 2 pošle všetky také bity vstupu x, ktorých poradové číslo aspoň pre jednu cifru t spĺňa vzťah (2.1). Počet týchto bitov odhadneme zhora takto. Cifru, ktorá tento vzťah spĺňa, môžeme zvoliť k spôsobmi, pričom vzťah môžu pre dané t spĺňať 2 hodnoty. Ostatné cifry možno zvoliť ľubovoľne zo Z_m. Máme teda, že hráč 2 pošle najviac $2km^{k-1}$ bitov. Z rozboru zložitosti pre hráča 1 vidno, že $m^k = O(n)$ a teda $m^{k-1} = O(n)^{1-1/k} = O(n^{1-1/k})$. Hráč 2 teda pošle $O(kn^{1-1/k})$ bitov. □

Dôsledok 2.24 [2]

$$\mathrm{C}_{AS}(\mathit{shift}^n) = O\left(\frac{n \log^{1/4} n}{2^{\sqrt{\log n}}} \right).$$

Dôkaz: Dostaneme po dosadení $k = \left\lceil \sqrt{\log n} - \frac{\log \log n}{4} \right\rceil$ do vety 2.23. □

Horný odhad pre $\mathrm{GAF}_{Z_2^t}$

Pre funkciu $\mathrm{GAF}_{Z_2^t}$ bol nájdený lepší horný odhad ako pre funkciu GAF_{Z_n} (t.j. $shift^n$). Tento horný odhad využíva vlastnosti grupy Z_2^t, takže ho nemožno priamočiaro použiť pre funkciu $shift^n$.

Veta 2.25 [11] *Nech $n = 2^t$. Potom platí*

$$\mathrm{C}_{AS}(\mathrm{GAF}_{Z_2^t}) = O(n^{0.92}).$$

Dôkaz: Funkcia $\mathrm{GAF}_{Z_2^t}(x, y, f)$ má ako vstup dve čísla $x, y \in Z_2^t$ (t.j. dva t-bitové reťazce) a jeden reťazec f dĺžky n. Reťazec f môžeme chápať ako funkciu $f : \{0,1\}^t \to \{0,1\}$, t.j. každý bit reťazca f určuje funkčnú hodnotu pre jednu t-ticu vstupných bitov. Potom môžeme zapísať výslednú hodnotu protokolu takto (v celom dôkaze $+$ znamená sčítanie v Z_2^t resp. v Z_2):

$$\mathrm{GAF}_{Z_2^t}(x, y, f) = f(x + y).$$

Každá booleovská funkcia t premenných sa však dá zapísať ako polynóm t premenných nad Z_2, pričom tento polynóm bude navyše multilineárny, t.j. ak všetky premenné okrem jednej budeme považovať za parametre, dostaneme lineárnu funkciu jednej premennej. V polynóme zodpovedajúcom f sa teda vyskytujú iba členy tvaru $X_S = \prod_{i \in S} x_i$, kde $S \subseteq Z_t$. Rozdeľme teraz členy polynómu na dve skupiny (sčítame v Z_2):

$$f(x_0, x_1, \ldots, x_{t-1}) = \sum_{S \subseteq Z_t} a_S \cdot X_S = \underbrace{\sum_{|S| > \frac{2}{3}t} a_S \cdot X_S}_{f_1(x_0, \ldots, x_{t-1})} + \underbrace{\sum_{|S| \le \frac{2}{3}t} a_S \cdot X_S}_{f_2(x_0, \ldots, x_{t-1})}.$$

Ak teda x a y sú binárne reťazce dĺžky t, potom $f(x + y) = f_1(x + y) + f_2(x + y)$, kde f_1 je polynóm obsahujúci členy stupňa väčšieho ako $\frac{2}{3}t$, polynóm f_2 obsahuje členy stupňa najviac $\frac{2}{3}t$. Ukážeme dva protokoly P_1 a P_2, pričom pomocou protokolu P_i sa pre vstupy x, y a f vypočíta hodnota $f_i(x, y)$. Je zrejmé, že je možné zostaviť protokol P, počítajúci funkciu $\mathrm{GAF}_{Z_2^t}$, v ktorom hráči 1 a 2 pošlú zreťazenie správ z protokolov P_1 a P_2, hráč 3 vypočíta výsledky týchto protokolov a sčíta ich. Komunikačná zložitosť bude zhora ohraničená súčtom komunikačných zložitostí protokolov P_1 a P_2.

Protokol P_1. Výraz $f_1(x + y)$ bude protokol počítať tak, že hráč 1 na základe vstupu f vypočíta koeficienty a_S pre všetky S také, že $|S| > \frac{2}{3}t$. Tieto koeficienty pošle hráčovi 3. Hráč 3 pozná vstupy x a y, takže spočíta $x + y$ (nad Z_2^t) a vypočíta výsledok.

Protokol P_2. Funkcia f_2 je multilineárnym polynómom stupňa najviac $\frac{2}{3}t$. Ak za vstup dosadíme $x + y = x(0) + y(0), x(1) + y(1), \ldots x(t-1) + y(t-1)$, dostávame

$$f_2(x + y) = \sum_{|S| \le \frac{2}{3}t} a_S \cdot \prod_{i \in S} (x(i) + y(i)) = \sum_{|S| \le \frac{2}{3}t} a_S \cdot \sum_{T \subseteq S} X_T Y_{S \setminus T},$$

kde $X_S = \prod_{i\in S} x(i)$ a $Y_S = \prod_{i\in S} y(i)$. Predchádzajúcu rovnosť môžeme ďalej upraviť:

$$f_2(x+y) = \sum_{|S|\le\frac{2}{3}t} \sum_{|T|\le\frac{2}{3}t} b_{S,T} X_S Y_T,$$

kde $b_{S,T} = a_{S\cup T}$ pre také dvojice $S, T \subseteq Z_t$, že S a T sú disjunktné a ich zjednotenie má najviac $\frac{2}{3}t$ prvkov. Pre ostatné dvojice S a T položíme $b_{S,T} = 0$. Uvedomme si teraz, že $b_{S,T}$ môže byť nenulové iba pre tie dvojice S a T, v ktorých má aspoň jedna množina najviac $\frac{1}{3}t$ prvkov. Sumu teda môžeme rozdeliť na dve časti, do prvej dáme tie členy, ktoré majú $|S| \le \frac{1}{3}t$ a do druhej tie, pre ktoré platí $|T| \le \frac{1}{3}t$ a $|S| > \frac{1}{3}t$ (aby sme niektorý člen nezapočítali dvakrát). Týmto rozdelením a následnou úpravou dostávame:

$$\begin{aligned} f_2(x+y) &= \sum_{|S|\le\frac{1}{3}t} \sum_{|T|\le\frac{2}{3}t} b_{S,T} X_S Y_T + \sum_{|T|\le\frac{1}{3}t} \sum_{\frac{1}{3}t<|S|\le\frac{2}{3}t} b_{S,T} X_S Y_T = \\ &= \sum_{|S|\le\frac{1}{3}t} X_S \cdot \left(\sum_{|T|\le\frac{2}{3}t} b_{S,T} Y_T \right) + \sum_{|T|\le\frac{1}{3}t} Y_T \cdot \left(\sum_{\frac{1}{3}t<|S|\le\frac{2}{3}t} b_{S,T} X_S \right). \end{aligned}$$

Uvedomme si teraz, že koeficienty $b_{S,T}$ závisia iba od vstupu f, ktorý poznajú hráči 1 aj 2. Hráč 1 pre každé $S \subseteq Z_t$ s najviac $\frac{1}{3}t$ prvkami vypočíta hodnotu $\sum_{|T|\le\frac{2}{3}t} b_{S,T} Y_T$, ktorá závisí iba od vstupov f a y a všetky tieto hodnoty pošle hráčovi 3. Podobne hráč 2 pošle hráčovi 3 hodnoty $\sum_{\frac{1}{3}t<|S|\le\frac{2}{3}t} b_{S,T} X_S$ pre všetky $T \subseteq Z_t$ s najviac $\frac{1}{3}t$ prvkami (tieto hodnoty zasa závisia iba od vstupov f a x). Hráč 3 pozná hodnoty x a y, vie teda vypočítať súčiny X_S a Y_S pre každé S a pomocou prijatých koeficientov vie teda vypočítať aj $f_2(x, y)$.

Odhad zložitosti. Pre jednoduchosť budeme uvažovať prípad, že $t = 3m$. V protokole P_1 hráč 1 pošle jeden bit pre každú množinu $S \subseteq Z_t$ s viac ako $2m$ prvkami, celkový počet posielaných bitov je $\sum_{k=2m+1}^{3m} \binom{3m}{k} < \sum_{k=0}^{m} \binom{3m}{k}$.

V protokole P_2 každý z hráčov pošle jeden bit pre každú podmnožinu $S \subseteq Z_t$ s najviac m prvkami, t.j. spolu sa pošle $2\sum_{k=0}^{m} \binom{3m}{k}$ bitov.

Dostávame teda, že celkový počet bitov poslaných v protokole pre výpočet funkcie $\mathrm{GAF}_{Z_2^t}$ je najviac

$$3\sum_{k=0}^{m} \binom{3m}{k}.$$

Na odhad tejto sumy využijeme najprv skutočnosť, že pre $u \le \frac{t}{3}$ platí $\sum_{k=0}^{u} \binom{t}{k} \le 2\binom{t}{u}$. Tento vzťah je možné jednoducho dokázať matematickou indukciou vzhľadom na u s využitím faktu, že $2\binom{n}{m-1} = \binom{n}{m}\frac{2m}{n-m+1} \le \binom{n}{m}$ pre $m \le \frac{n}{3}$. Máme teda, že

$$\mathrm{C}_{AS}(\mathrm{GAF}_{Z_2^{3m}}) \le 6\binom{3m}{m}.$$

Binomický koeficient $\binom{3m}{m}$ ďalej odhadneme podľa Stirlingovej formuly, konkrétne podľa vzťahu

$$n! = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n \left(1 + \frac{\theta_n}{12n}\right),$$

kde $\theta_n \in (0,1)$. Po dosadení (využívajúc, že $n = 2^{3m}$) dostávame

$$\binom{3m}{m} = \sqrt{\frac{3}{4\pi m}} \cdot 2^{3m(\log 3 - \frac{2}{3})} \cdot \frac{1 + \frac{\theta_{3m}}{36m}}{(1 + \frac{\theta_{2m}}{24m})(1 + \frac{\theta_m}{12m})} \leq \frac{n^{\log 3 - \frac{2}{3}}}{\sqrt{\log n}}$$

Nakoľko $\log 3 - \frac{2}{3} = 0.918\ldots$, dostávame, že $\mathrm{C}_{AS}(\mathrm{GAF}_{Z_2^{3m}}) = O(n^{0.92})$. Pre tie hodnoty t, ktoré nie sú deliteľné číslom 3, dostaneme požadované tvrdenie pozorovaním, že počet bitov, ktoré sa v protokole posielajú, tvoria funkciu monotónnu v závislosti od t. □

2.2.3 Zhrnutie

Hoci boli nájdené pomerne prekvapivé a zaujímavé protokoly na výpočet funkcií $shift^n$ a $\mathrm{GAF}_{Z_2^t}$, ich komunikačná zložitosť je pomerne vzdialená od najlepšieho známeho dolného odhadu. Otvorenou otázkou zostáva odstrániť túto medzeru medzi dolným a horným odhadom.

Iným otvoreným problémom zostáva dokázať, že pre niektoré ε neexistuje protokol na výpočet $shift^n$, v ktorom by hráč 1 poslal $O(n/\log\log n)$ a hráč 2 $O(n^\varepsilon)$ bitov (alebo naopak nájsť takýto protokol pre ľubovoľné ε).

V tejto práci sa zaoberáme iba simultánnymi protokolmi pre štyroch hráčov rátajúcimi funkcie troch vstupov. V literatúre však bolo študované aj zovšeobecnenie pre $k+1$ hráčov a k vstupov. Skúmali sa najmä funkcie, pri ktorých počet hráčov rastie s dĺžkou vstupu rýchlejšie ako polylogaritmicky. Ak by sa pre nejakú funkciu ukázal v tomto modeli dolný odhad lepší ako logaritmický, znamenalo by to, že daná funkcia sa nedá počítať ACC^0 obvodom. ACC^0 obvody sú booleovské obvody s konštantnou hĺbkou, polynomiálnou veľkosťou a neohraničeným vstupným stupňom jednotlivých vrcholov. Okrem hradiel *AND*, *OR* a *NOT* sú povolené aj hradlá MOD_m, ktoré zisťujú, či počet jedničiek na ich vstupoch je deliteľný číslom m.

2.3 Odhady pomocou základných parametrov

V tejto podkapitole sa budeme zaoberať niektorými základnými vlastnosťami simultánnej komunikačnej zložitosti funkcií z $\mathcal{F}_{p,n}$ ($\mathcal{F}_{p,n} = Z_p \times Z_p \times Z_n$). Funkciu $f \in \mathcal{F}_{p,n}$ budeme charakterizovať pomocou štyroch jednoduchých parametrov p, n, r a s. Parametre p a n sú jednoducho "rozmery" definičného oboru funkcie. Parametre r a s definujeme takto: funkciu f môžeme chápať ako postupnosť n matíc typu $p \times p$. Parameter r určuje, koľko je medzi týmito n maticami navzájom rôznych matíc. Každá z týchto n matíc je navyše tvorená p riadkami (riadok si môžeme predstaviť napríklad ako slovo z $\{0,1\}^p$). Ak teraz vezmeme všetky riadky zo všetkých matíc dokopy, tak parameter s určuje, koľko je medzi nimi navzájom rôznych riadkov.

V jednotlivých častiach uvedieme charakterizáciu miery $\mathrm{C}_S(f)$ pomocou dvojíc parametrov (p,n), (p,r) a (p,s). Pre každú dvojicu nájdeme horný odhad, kde sa dá aj dolný odhad a pokúsime sa dokázať, že nájdené odhady sú optimálne.

2.3.1 Charakterizácia pomocou p a n

Parametre p a n nehovoria nič o funkčných hodnotách funkcie f. Pre každé p a n existuje funkcia $f \in \mathcal{F}_{p,n}$, ktorá je konštantná a teda na jej výpočet netreba vôbec žiadnu komunikáciu. Z tohto dôvodu pomocou p a n nemožno vyjadriť žiaden (kladný) dolný odhad miery $\mathrm{C}_S(f)$. Uvedieme však horný odhad komunikačnej zložitosti a jeho optimálnosť.

Horný odhad komunikačnej zložitosti

Veta 2.26 *Simultánna komunikačná zložitosť žiadnej funkcie $f \in \mathcal{F}_{p,n}$ nie je väčšia ako*

$$\min\left\{p + \lceil \log p \rceil, \lceil \log n \rceil + 2\lceil \log p \rceil, n + \lceil \log n \rceil\right\}$$

Dôkaz: Uvedieme tri protokoly na výpočet hodnoty $f(x, y, z)$, jeden s komunikačnou zložitosťou $p + \lceil \log p \rceil$, druhý s komunikačnou zložitosťou $\lceil \log n \rceil + 2\lceil \log p \rceil$ a tretí s komunikačnou zložitosťou $n + \lceil \log n \rceil$.

Protokol 1 Hráč 1 (ktorý pozná y a z) pošle hráčovi 4 p-bitový reťazec v taký, že $v(i) = f(i, y, z)$. Hráč 2 pošle hráčovi 4 vstup x (zapísaný $\lceil \log p \rceil$ bitov). Hráč 3 nepošle nič. Hráč 4 ako výsledok vráti $v(x)$.

Protokol 2 Každý hráč pošle jeden zo svojich vstupov hráčovi 4 tak, aby hráč 4 získal celý vstup a na základe toho mohol vypočítať funkčnú hodnotu. Vstup z možno zapísať pomocou $\lceil \log n \rceil$ bitov, vstup x (resp. y) možno zapísať pomocou $\lceil \log p \rceil$ bitov.

Protokol 3 Hráč 3 pošle hráčovi 4 n-bitový reťazec v taký, že $v(i) = f(x, y, i)$. Hráč 1 pošle hráčovi 4 vstup z ($\lceil \log n \rceil$ bitov). Hráč 2 nepošle nič. Hráč 4 ako výsledok vráti $v(z)$. □

Optimálnosť horného odhadu

Ukážeme, že horný odhad uvedený vo vete 2.26 je až na konštantný násobok optimálny. Dokážeme teda, že existujú funkcie s veľkou simultánnou komunikačnou zložitosťou.

Jadro dôkazu sa nachádza v nasledujúcej leme. Tá platí pre ľubovoľné hodnoty p a n. Vo vete 2.26 však dostávame rôzne horné odhady v závislosti od vzájomného vzťahu p a n. Veta 2.28 teda dokazuje optimálnosť horného odhadu pre jednotlivé prípady, aké môžu nastať.

Lema 2.27 *Nech $m = \min\{p, n\}$ a nech k je číslo také, že*

$$7 \cdot 2^k + \frac{kp^2n}{m} - 3 < p^2n. \tag{2.2}$$

Potom existuje funkcia $f \in \mathcal{F}_{p,n}$ so simultánnou komunikačnou zložitosťou väčšou ako k.

Dôkaz: Zvoľme pevne p, n a k. Dokážeme, že ak pre k platí (2.2), potom je počet funkcií z $\mathcal{F}_{p,n}$ vypočítateľných protokolmi s komunikačnou zložitosťou najviac k menší ako počet všetkých funkcií v $\mathcal{F}_{p,n}$.

Protokol s komunikačnou zložitosťou najviac k budeme kódovať pomocou troch binárnych reťazcov u, v a w. Reťazec u obsahuje pre každého hráča množinu správ, aké tento hráč posiela. Pre každého hráča je táto množina správ bezprefixová a každá správa má dĺžku najviac k. Množinu správ jedného hráča budeme kódovať ako binárny reťazec $2^{k+1}-1$, ktorý pre každý zo $2^{k+1}-1$ rôznych reťazcov dĺžky najviac k obsahuje jeden bit. Tento bit určuje, či je daný reťazec v množine správ. Keďže máme troch hráčov, celková dĺžka reťazca u je $3(2^{k+1}-1) = 6 \cdot 2^k - 3$.

Reťazec v obsahuje najprv zreťazenie všetkých správ, ktoré jednotliví hráči posielajú na všetky kombinácie svojich vstupov, pričom reťazec je doplnený nulami na dĺžku $\frac{kp^2n}{m}$ (neskôr dokážeme, že dĺžka zreťazenia správ nepresiahne túto hodnotu). Začiatok reťazca v je tvorený zreťazením pn správ, ktoré pošle hráč 1 na jednotlivé kombinácie vstupov y a z. Ďalej nasleduje zreťazenie pn správ, ktoré posiela hráč 2 na všetky kombinácie svojich vstupov a nakoniec zreťazenie p^2 správ, ktoré posiela hráč 3. Ak poznáme reťazec u (a čísla n a p), vieme reťazec v jednoznačne rozložiť na jednotlivé správy, lebo množiny správ jednotlivých hráčov sú bezprefixové a teda vieme určiť, kde v reťazci v končí ktorá správa. Tieto dva reťazce spolu teda jednoznačne určujú, čo bude ktorý hráč posielať pre ktorý vstup.

Zostáva dokázať, že reťazec bude mať vždy dĺžku $\frac{kp^2n}{m}$, t.j. že dĺžka zreťazenia všetkých správ všetkých hráčov nepresiahne túto hodnotu. Označme dĺžku zreťazenia všetkých správ q. Vytvorme tabuľku tak, že pre každú z p^2n možných kombinácií vstupov funkcie uvedieme reťazec, ktorý vznikne zreťazením správ poslaných jednotlivými hráčmi pre tento vstup. Veľkosť každého riadku je najviac k, takže celá tabuľka obsahuje najviac kp^2n znakov. Správa poslaná hráčom i je taká istá vo všetkých riadkoch, v ktorých sa mení iba vstup číslo i. Pre hráčov 1 a 2 je takýchto riadkov p, pre hráča 3 je takýchto riadkov n. Teda každá správa z reťazca v sa v tabuľke nachádza na aspoň $m = \min\{p, n\}$ rôznych miestach. Dĺžka tabuľky je preto aspoň mq. Máme teda, že $q \leq \frac{kp^2n}{m}$, čo sme chceli dokázať.

Reťazec w popisuje, aký výsledok hráč 4 ohlási po prijatí určitej trojice správ od ostatných hráčov. Reťazec w obsahuje jeden bit pre každý reťazec z $\{0,1\}^k$ (t.j. $|w| = 2^k$). Hráč 4 spojí správy prijaté od hráčov 1, 2 a 3 do jedného reťazca (ktorý bude mať dĺžku najviac k) a doplní znakom 0 na dĺžku k. Potom nájde vo w bit prislúchajúci získanému reťazcu a ten vyhlási za výsledok. Pre každú trojicu správ zostaví hráč 4 iný reťazec, lebo správy hráčov sú z bezprefixových množín. Každé možné správanie sa hráča 4 v prefixovom protokole s komunikačnou zložitosťou najviac k možno teda popísať takýmto reťazcom.

Každý protokol s komunikačnou zložitosťou najviac k teda možno popísať reťazcom uvw, pričom pre rôzne protokoly dostávame rôzne reťazce. Dĺžka reťazca uvw je $7 \cdot 2^k - 3 + \frac{kp^2n}{m}$. Protokol však jednoznačne určuje počítanú funkciu. Teda počet funkcií vypočítateľných protokolom s komunikačnou zložitosťou najviac k neprevyšuje počet rôznych reťazcov uvw vhodnej dĺžky, ktorý je

$$2^{|uvw|} = 2^{(7 \cdot 2^k - 3 + \frac{kp^2n}{m})}$$

Počet všetkých funkcií $Z_p \times Z_p \times Z_n \to \{0,1\}$ je ale $2^{p^2 n}$. Teda ak pre nejaké k platí (2.2), potom existuje funkcia s komunikačnou zložitosťou väčšou ako k. $\square$

Veta 2.28 *Nech $n, p \geq 4$. Potom platí:*

- *Ak $p \leq \log n$, tak existuje funkcia $f \in \mathcal{F}_{p,n}$ taká, že $\mathrm{C}_S(f) \geq p$.*
- *Ak $\log n \leq p \leq n$, tak existuje funkcia $f \in \mathcal{F}_{p,n}$ taká, že $\mathrm{C}_S(f) \geq \lceil \log n \rceil - 1$.*
- *Ak $n \leq p \leq 2^n$, tak existuje funkcia $f \in \mathcal{F}_{p,n}$ taká, že $\mathrm{C}_S(f) \geq \lceil \log p \rceil - 1$.*
- *Ak $2^n \leq p$, tak existuje funkcia $f \in \mathcal{F}_{p,n}$ taká, že $\mathrm{C}_S(f) \geq n - 1$.*

Dôkaz: Jednotlivé prípady dokážeme pomocou lemy 2.27.

- Nech $p \leq \log n$. Dokážeme, že pre $k = p - 1$ platí vzťah (2.2), t.j. existuje funkcia so simultánnou komunikačnou zložitosťou aspoň p. Upravujme ľavú stranu:
$$7 \cdot 2^k + \frac{kp^2 n}{m} - 3 = 7 \cdot 2^{p-1} + \frac{(p-1)p^2 n}{p} - 3 \leq \frac{7}{2}n + p^2 n - pn - 3 < p^2 n$$
- Nech $\log n \leq p \leq n$. Dokážeme, že pre $k = \log n - 1$ platí vzťah (2.2), t.j. existuje funkcia s komunikačnou zložitosťou aspoň $\lceil \log n \rceil - 1$. Upravujme ľavú stranu:
$$7 \cdot 2^k + \frac{kp^2 n}{m} - 3 = 7 \cdot 2^{\log n - 1} + \frac{(\log n - 1)p^2 n}{p} - 3 \leq \frac{7}{2}n + p^2 n - pn - 3 < p^2 n$$
- Nech $n \leq p \leq 2^n$. Dokážeme, že pre $k = \log p - 1$ platí vzťah (2.2), t.j. existuje funkcia s simultánnou komunikačnou zložitosťou aspoň $\lceil \log p \rceil - 1$. Upravujme ľavú stranu:
$$7 \cdot 2^k + \frac{kp^2 n}{m} - 3 = 7 \cdot 2^{\log p - 1} + \frac{(\log p - 1)p^2 n}{n} - 3 \leq \frac{7}{2}p + p^2 n - p^2 - 3 < p^2 n$$
Nerovnosť $\frac{7}{2}p - p^2 - 3 < 0$ platí pre každé $p > 2$.
- Nech $2^n \leq p$. Dokážeme, že pre $k = n - 1$ platí vzťah (2.2), t.j. existuje funkcia so simultánnou komunikačnou zložitosťou aspoň n. Upravujme ľavú stranu:
$$7 \cdot 2^k + \frac{kp^2 n}{m} - 3 = 7 \cdot 2^{n-1} + \frac{(n-1)p^2 n}{n} - 3 \leq \frac{7}{2}p + p^2 n - p^2 - 3 < p^2 n$$

$\square$

Dôsledok 2.29 *Nech $p, n \geq 4$ a nech $g(p,n)$ je horný odhad simultánnej komunikačnej zložitosti funkcie z $\mathcal{F}_{p,n}$ uvedený vo vete 2.26, t.j.*

$$g(p,n) = \min\{p + \lceil \log p \rceil, \lceil \log n \rceil + 2\lceil \log p \rceil, n + \lceil \log n \rceil\}$$

Potom existuje funkcia so simultánnou komunikačnou zložitosťou aspoň $\frac{1}{3}g(p,n) - 1$.

Dôkaz: Dostaneme jednoduchým rozborom jednotlivých prípadov vo vete 2.28. $\square$

2.3.2 Charakterizácia pomocou p a r

Nech $f \in \mathcal{F}_{p,n}$. Pre každé $x \in Z_n$ nech B_x je binárna matica typu $p \times p$ taká, že $B_x(i,j) = f(i,j,x)$. Nech číslo r označuje počet rôznych matíc B_x definovaných pre danú funkciu f (t.j. $r = |\{B_x \mid x \in Z_n\}|$). Nakoľko počet všetkých binárnych matíc typu $p \times p$ je 2^{p^2}, musí platiť, že $1 \leq r \leq 2^{p^2}$.

V tejto časti zostrojíme dolný a horný odhad simultánnej komunikačnej zložitosti danej funkcie pomocou parametrov p a r a dokážeme optimálnosť týchto odhadov.

Horný odhad

Veta 2.30 *Nech $f(i,j,x) \in \mathcal{F}_{p,n}$ a nech číslo r označuje počet rôznych matíc B_x definovaných pre danú funkciu f. Potom platí*

$$\mathrm{C}_S(f) \leq \min\{p + \lceil \log p \rceil, \lceil \log r \rceil + 2\lceil \log p \rceil, r + \lceil \log r \rceil\}$$

Dôkaz: Protokol s komunikačnou zložitosťou $p + \lceil \log p \rceil$ sme zostrojili v dôkaze vety 2.26. Stačí teda uviesť dva protokoly, jeden s komunikačnou zložitosťou $\lceil \log r \rceil + 2\lceil \log p \rceil$, druhý s komunikačnou zložitosťou $r + \lceil \log r \rceil$.

Nech všetky rôzne matice B_x pre funkciu f sú $A_1, A_2, \ldots A_r$.

1. Hráč 1 na základe vstupu x zistí k také, že $B_x = A_k$ a pošle číslo k ($\lceil \log r \rceil$ bitov). Hráč 3 pošle vstupy i a j – na každý z nich je potrebných $\lceil \log p \rceil$ bitov. Hráč 2 neposiela nič. Hráč 4 nájde $A_k(i,j)$.
2. Hráč 1 na základe vstupu x zistí k také, že $B_x = A_k$ a pošle číslo k ($\lceil \log r \rceil$ bitov). Hráč 3 pošle r-bitový reťazec v, ktorého l-ty bit je $A_l(i,j)$. Hráč 4 vyberie k-ty bit reťazca v.

□

Optimálnosť horného odhadu

Ukážeme, že horný odhad uvedený vo vete 2.30 je optimálny až na konštantný násobok.

Veta 2.31 *Pre ľubovoľné prirodzené p a r také, že $r \leq 2^{p^2}$ označme*

$$h(p,r) := \min\{p + \lceil \log p \rceil, \lceil \log r \rceil + 2\lceil \log p \rceil, r + \lceil \log r \rceil\}$$

Potom pre každé p a r ($r \leq 2^{p^2}$, $p, r \geq 4$) existuje funkcia $f \in \mathcal{F}_{p,n}$ s parametrom r a so simultánnou komunikačnou zložitosťou aspoň $\frac{1}{3}h(p,r) - 1$.

Dôkaz: Nech p a r sú čísla splňujúce predpoklady vety. Podľa dôsledku 2.29 existuje funkcia $f \in \mathcal{F}_{p,r}$, pre ktorú platí

$$\mathrm{C}_S(f) \geq \frac{1}{3}\min\{p + \lceil \log p \rceil, \lceil \log r \rceil + 2\lceil \log p \rceil, r + \lceil \log r \rceil\} - 1$$

To je však presne $\frac{1}{3}h(p,r)-1$. Môže sa však stať, že počet rôznych matíc definovaných pre funkciu f je menší ako r. V takom prípade rozšírime funkciu f na funkciu $f' \in \mathcal{F}_{p,n}$ pre vhodné $n > r$ tak, aby počet rôznych matíc vo funkcii f' bol presne r. Simultánna komunikačná zložitosť funkcie f' je aspoň taká, ako simultánna komunikačná zložitosť funkcie f, f' teda spĺňa naše požiadavky. □

Dolný odhad

Pomocou parametrov p a r je možné dokázať aj dolný odhad komunikačnej zložitosti, ktorý uvádzame v nasledujúcej vete. Pri dôkaze tejto vety je použitá informačno teoretická myšlienka analogická dôkazu tvrdenia 2.3. z [15].

Veta 2.32 *Nech $f(i,j,x) \in \mathcal{F}_{p,n}$ a nech číslo r označuje počet rôznych matíc B_x definovaných pre danú funkciu f. Potom platí:*

$$\mathrm{C}_S(f) \geq \frac{\lceil \log r \rceil}{p}$$

Dôkaz: Nech P je ľubovoľný takmer simultánny komunikačný protokol pre funkciu f s komunikačnou zložitosťou k. Dokážeme, že $k \geq \lceil \log r \rceil / p$. Keďže z každého simultánneho protokolu možno vyrobiť takmer simultánny protokol s tou istou komunikačnou zložitosťou, komunikačná zložitosť funkcie f je tiež aspoň $k \geq \lceil \log r \rceil / p$.

Zvoľme pevne jednu z r rôznych matíc B_x. Zostavme tabuľku, ktorá bude pre každé $i = 0, 1, \ldots, p-1$ obsahovať správy, ktoré hráči 1 a 2 pošlú podľa protokolu P, ak vstupy, ktoré každý z nich vidí, sú i a x. Tieto dve správy spolu tvoria komunikáciu, aká v protokole prebehne pre vstup (i,i,x). Preto každý riadok tejto tabuľky obsahuje najviac k bitov. Celkovo teda tabuľka obsahuje najviac kp bitov.

Ak však poznáme takúto tabuľku pre konkrétne x, vieme z nej určiť celú maticu B_x. Pre ľubovoľne zvolené i a j vezmeme správu vyslanú hráčom 1 z riadku j tabuľky a správu vyslanú hráčom 2 z riadku i tabuľky. Tieto správy tvoria komunikáciu na vstup (i,j,x) v protokole P. Podľa protokolu na základe týchto správ a čísel i a j vieme jednoznačne určiť $B_x(i,j)$.

Počet navzájom rôznych matíc B_x je r. Keďže každú z týchto matíc je možné jednoznačne určiť tabuľkou obsahujúcou najviac kp bitov, musí platiť, že $kp \geq \lceil \log r \rceil$. Teda máme

$$k \geq \frac{\lceil \log r \rceil}{p}$$

□

Poznámka: Dokázaný dolný odhad je optimálny (ako ukážeme neskôr), je však pomerne slabý, pretože pre $r \leq 2^p$ nedáva odhad komunikačnej zložitosti väčší ako 1. Pre funkcie $f \in \mathcal{F}_{m,2^m}$, ktoré sú predovšetkým predmetom nášho záujmu, sa nedá teda vôbec použiť.

Optimálnosť dolného odhadu

Dokážeme, že dolný odhad uvedený vo vete 2.32 je optimálny v tom zmysle, že ak pre nejaké parametre p a r dáva táto veta odhad k, tak existuje funkcia s týmito parametrami, ktorá má simultánnu komunikačnú zložitosť najviac $k + \lceil \log k \rceil$.

Veta 2.33 *Pre každé p a r ($1 < r \leq 2^{p^2}$) a pre každé $n \geq r$ existuje funkcia $f \in \mathcal{F}_{p,n}$ s parametrom r, pre ktorú platí $\mathrm{C}_S(f) \leq \left\lceil \frac{\log r}{p} \right\rceil + \left\lceil \log \left\lceil \frac{\log r}{p} \right\rceil \right\rceil$.*

Dôkaz: Nech $k = \left\lceil \frac{\log r}{p} \right\rceil$. Zostrojíme funkciu, pre ktorú existuje simultánny protokol s komunikačnou zložitosťou $k + \lceil \log k \rceil$. Nech $A = \{0,1\}^{k \cdot p}$. Veľkosť množiny A je

$$|A| = 2^{k \cdot p} = 2^{\lceil \frac{\log r}{p} \rceil p} \geq 2^{\log r} = r$$

K reťazcu $v \in A$ zostrojíme maticu A_v typu $p \times p$ nasledovne: do riadkov $0, 1, \ldots, k-1$ uložíme v (t.j. $A_v(i,j) = v(i \cdot p + j)$), ďalšie riadky budú zhodné s riadkom $k-1$. Všimnime si, že reťazec v sa do matice A_v vždy zmestí, lebo $k \leq p$:

$$k = \left\lceil \frac{\log r}{p} \right\rceil \leq \left\lceil \frac{\log 2^{p^2}}{p} \right\rceil = p$$

Pre každé dva rôzne reťazce v a w z A sú aj zodpovedajúce matice rôzne. Z množiny $\{A_v | v \in A\}$ teda môžeme vybrať r navzájom rôznych matíc. Z vybraných r rôznych matíc zostavíme funkciu f tak, že každému číslu zo Z_n priradíme teda jednu takúto maticu (niektoré matice môžeme použiť aj viackrát, každú však aspoň raz).

Takto zostavenú funkciu budeme počítať nasledovným protokolom. Hráč 1 na základe vstupu x určí maticu A_v zodpovedajúcu vstupu x. Ako správu pošle bity $A_v(0,j), A_v(1,j) \ldots A_v(k-1,j)$. Hráč 3 v prípade, že $i < k$, pošle číslo i, v opačnom prípade pošle $k-1$. Posiela teda číslo z množiny $\{0, 1, \ldots, k-1\}$, čo je možné spraviť pomocou $\lceil \log k \rceil$ bitov. Hráč 4 po prijatí reťazca u od hráča 1 a čísla l od hráča 3 vráti ako odpoveď l-tý bit reťazca u.

Takto vypočítaná odpoveď je určite správna: pre $i < k$ sa vypočíta $u(l) = A_v(l,j) = A_v(i,j)$. Pre $i \geq k$ sa vypočíta $A_v(l,j) = A_v(k-1,j) = A_v(i,j)$, lebo všetky riadky od riadku k počnúc sa rovnajú riadku $k-1$. □

Poznámka: Z dôkazu vety 2.32 vyplýva, že uvedený dolný odhad platí aj pre takmer simultánne protokoly. Simultánny protokol uvedený v predchádzajúcom dôkaze ľahko možno zmeniť na takmer simultánny protokol so zložitosťou k, čo je teda skutočne takmer simultánna zložitosť zostrojenej funkcie. V takmer simultánnom prípade teda možno zostrojiť funkcie, ktoré sa od uvedeného dolného odhadu vôbec nelíšia.

Rozbor zložitosti konkrétnej funkcie

Ako sme už poznamenali, dolný odhad pomocou p a r je pomerne slabý. Napríklad pre $r \leq 2^p$ nedáva vôbec žiadnu informáciu. Ak je však r veľmi veľké (blízke 2^{p^2}), náš odhad začína byť zaujímavý. Skúsme ho teraz aplikovať na funkciu s maximálnym možným r.

Nech $n = 2^{p^2}$. Nech $B_0, B_1, \ldots, B_{n-1}$ sú všetky rôzne binárne matice typu $p \times p$. Uvažujme funkciu $f \in \mathcal{F}_{p,n}$ takú, že $f(i,j,x) = B_x(i,j)$. Podľa vety 2.26 je zložitosť tejto funkcie najviac $p + \lceil \log p \rceil$. Naopak podľa vety 2.32 je zložitosť tejto funkcie aspoň $\frac{\lceil \log n \rceil}{p} = p$. Zložitosť tejto funkcie je teda $\Theta(p)$. Pre túto konkrétnu funkciu nám teda nami dokázané odhady dali pomerne presný odhad zdola aj zhora.

Máme teda funkciu $f \in \mathcal{F}_{p,n}$ pre $n = 2^{p^2}$, ktorej simultánna komunikačná zložitosť je $\Theta(p)$. Otvorený problém, ktorý viedol k skúmaniu simultánnej zložitosti, vyžaduje nájsť (nedeterministicky polynomiálne počítateľnú) funkciu z $\mathcal{F}_{p,n}$ pre $n = 2^p$ so simultánnou komunikačnou zložitosťou $\Theta(p)$ (pozri podkapitolu 2.2). Na tento problém sa môžeme pozerať aj tak, že potrebujeme z vyššie uvedenej funkcie f vynechať $2^{p^2} - 2^p$ matíc tak, aby sa simultánna komunikačná zložitosť tejto funkcie príliš neznížila. Existujú určité dvojice matíc také, že ak je funkcia A vo funkcii, tak ak maticu B odoberieme, tak sa komunikačná zložitosť nezníži. Takže určité zníženie parametra n by bolo možné spraviť. Problémom je, že takto potrebujeme vylúčiť z funkcie f veľmi veľký počet funkcií, čo už naráža na ťažkosti.

2.3.3 Charakterizácia pomocou p a s

Nech $f \in \mathcal{F}_{p,n}$. Pre každé $x \in Z_n$ a $i \in Z_p$ nech $r_{x,i}$ je binárny reťazec dĺžky p taký, že $r_{x,i}(j) = f(i,j,x)$. Ak funkciu f reprezentujeme binárnymi maticami $B_0, B_1, \ldots, B_{n-1}$ typu $p \times p$, tak $r_{x,i}$ je i-ty riadok funkcie B_x.

Nech číslo s označuje počet rôznych riadkov $r_{x,i}$ definovaných pre danú funkciu, t.j. veľkosť množiny $\{r_{x,i} \,|\, x \in Z_n, i \in Z_p\}$. Keďže každý riadok má dĺžku p, počet rôznych riadkov je najviac 2^p. Teda musí platiť $1 \le s \le 2^p$.

Horný odhad

Veta 2.34 *Nech $f(i,j,x) \in \mathcal{F}_{p,n}$ a nech číslo s označuje počet rôznych riadkov $r_{x,i}$ definovaných pre danú funkciu f. Potom platí*

$$\mathrm{C}_S(f) \le \min\{\lceil \log s \rceil + \lceil \log p \rceil, s + \lceil \log s \rceil\}$$

Dôkaz: Uvedieme dva simultánne protokoly, jeden s komunikačnou zložitosťou $\lceil \log s \rceil + \lceil \log p \rceil$, druhý s komunikačnou zložitosťou $s + \lceil \log s \rceil$.

Nech všetky rôzne riadky pre funkciu f sú $a_1, a_2, \ldots a_s$.

1. Hráč 2 na základe vstupov x a i zistí k také, že $a_k = r_{x,i}$, t.j. že a_k je i-ty riadok matice B_x. Hráč 2 pošle hráčovi 4 číslo k (zapísané pomocou $\lceil \log s \rceil$ bitov). Hráč 3 pošle vstup j — na to je potrebných $\lceil \log p \rceil$ bitov. Hráč 1 neposiela nič. Hráč 4 nájde j-ty prvok riadku a_k.

2. Hráč 2 na základe vstupov x a i zistí k také, že $a_k = r_{x,i}$ a pošle číslo k ($\lceil \log s \rceil$ bitov). Hráč 1 pošle s-bitový reťazec v, ktorého l-ty bit je $a_l(j)$. Hráč 4 vyberie k-ty bit reťazca v.

□

Optimálnosť horného odhadu

Veta 2.35 *Pre ľubovoľné p a s (také, že $s \leq 2^p$) označme*

$$h'(p,s) = \min\left\{\lceil \log s\rceil + \lceil \log p\rceil, s + \lceil \log s\rceil\right\}.$$

Potom pre každé p a s také, že $p \leq s \leq 2^p$ existuje pre nejaké n funkcia $f \in \mathcal{F}_{p,n}$ s parametrom s, ktorej simultánna komunikačná zložitosť je aspoň $\frac{1}{2}h'(p,s)$.

Dôkaz: Zvoľme ľubovoľnú množinu s navzájom rôznych riadkov dĺžky p a zostavme funkciu f, ktorá bude obsahovať všetky matice typu $p \times p$, ktoré obsahujú len riadky z tejto množiny. Počet takýchto matíc je s^p, lebo na každý z p riadkov matice môžeme použiť každý z s rôznych riadkov.

Funkcia f má teda parameter r (počet rôznych matíc) rovný s^p. Podľa vety 2.32 platí

$$\mathrm{C}_S(f) \geq \frac{\lceil \log r\rceil}{p} = \frac{\lceil \log s^p\rceil}{p} \geq \log s$$

Keďže $\mathrm{C}_S(f)$ je celé číslo veľké aspoň $\log s$, platí, že $\mathrm{C}_S(f) \geq \lceil \log s\rceil$. Nakoľko predpokladáme, že $p \leq s$, platí, že $h'(p,s) \leq 2\lceil \log s\rceil \leq 2\mathrm{C}_S(f)$, čiže $\mathrm{C}_S(f) \geq \frac{1}{2}h'(p,s)$. □

Poznámka: Pre $p \leq s$ sme dokázali optimálnosť horného odhadu. Z dôkazu však vyplýva, že aj pre $s < p$ platí, že existuje funkcia so zložitosťou aspoň $\lceil s\rceil$. Takýto odhad už však neukazuje optimálnosť horného odhadu pre $s < p$.

Dolný odhad

Pomocou parametrov p a r sa nám pre funkcie s veľkým r podarilo nájsť dolný odhad simultánnej komunikačnej zložitosti. V tejto časti dokážeme, že pomocou parametrov p a s žiaden netriviálny odhad nemožno nájsť, presnejšie, že pre každé hodnoty p a s ($1 \leq s \leq 2^p$) existuje funkcia s týmito parametrami, ktorá má komunikačnú zložitosť najviac 1.

Čo sa týka dolného odhadu pomocou p a s, môžeme teda povedať iba toto: pre $s = 1$ môže byť $\mathrm{C}_S(f)$ aj 0 (konštantná funkcia), pre $s > 1$ už funkcia nemôže byť konštantná a teda $\mathrm{C}_S(f)$ je aspoň 1.

Veta 2.36 *Nech p a s sú prirodzené čísla, $1 < s \leq 2^p$ a nech $n = s$. Potom existuje funkcia $f \in \mathcal{F}_{p,n}$ s parametrom s a so simultánnou komunikačnou zložitosťou najviac 1.*

Dôkaz: Funkciu $f(i,j,x)$ zostrojíme tak, že každá matica B_x bude mať všetky riadky rovnaké (tak, aby celkový počet rôznych riadkov resp. rôznych matíc bol s). V každej matici B_x teda každý stĺpce obsahuje buď samé nuly alebo samé jednotky. Hráč 1, ktorý pozná x aj j, vie určiť hodnotu funkcie a tú poslať hráčovi 4 ako jeden bit. □

Poznámka: Odhady pomocou p a s symetricky platia aj pre počet rôznych stĺpcov. Môžeme zaviesť aj novú mieru s', ktorá by určovala minimum z počtov rôznych stĺpcov

Parametre p a n	
Horný odhad	$h(p,n) = \min\{p + \lceil \log p \rceil, \lceil \log n \rceil + 2\lceil \log p \rceil, n + \lceil \log n \rceil\}$
Optimálnosť	$\frac{1}{3}h(p,n)$
Dolný odhad	$d(p,n) = 0$
Optimálnosť	$d(p,n)$
Parametre p a r	
Horný odhad	$h(p,r) = \min\{p + \lceil \log p \rceil, \lceil \log r \rceil + 2\lceil \log p \rceil, r + \lceil \log r \rceil\}$
Optimálnosť	$\frac{1}{3}h(p,r)$
Dolný odhad	$d(p,r) = \lceil \log r \rceil / p$
Optimálnosť	$d(p,r) + \lceil \log d(p,r) \rceil$
Parametre p a s	
Horný odhad	$h(p,s) = \min\{\lceil \log s \rceil + \lceil \log p \rceil, s + \lceil \log s \rceil\}$
Optimálnosť	$\frac{1}{2}h(p,s)$ pre $s > p$
Dolný odhad	$d(p,s) = 1$ pre $s > 1$
Optimálnosť	$d(p,s)$

Tabuľka 2.1: Prehľad odhadov pre simultánnu zložitosť

a riadkov. V takom prípade by ale tiež existovala funkcia, ktorá má pre ľubovoľne veľké s' simultánnou komunikačnú zložitosť 2. Použili by sme funkciu $f' \in \mathcal{F}_{p,2n}$, kde $n = s'$, takú že pre $x \in Z_n$ platí $f'(i,j,x) = f(i,j,x)$ a $f'(i,j,x+n) = f(j,i,x)$, kde f je funkcia z predchádzajúceho dôkazu. Každý z hráčov 1 a 2 pošle 1 ak stĺpec resp. riadok určený jeho vstupmi obsahuje aj 0 aj 1. Ak je jeho stĺpec/riadok konštantný, pošle jeho hodnotu. Hráč 4 spočíta hodnotu funkcie ako súčin poslaných bitov.

2.3.4 Zhrnutie

Uviedli sme dolné a horné odhady simultánnej komunikačnej zložitosti pomocou dvojíc parametrov (p,n), (p,r) a (p,s). Parametre p, n, r a s sú veľmi jednoduché a pomerne ľahko sa pre danú funkciu určia. Na jednej strane takto môžeme pre funkciu získať aspoň nejaké odhady simultánnej komunikačnej zložitosti. Na druhej strane sú tieto odhady pomerne nepresné (je veľký rozdiel medzi dolným a horným odhadom), čo je spôsobené tým, že zvolené parametre nepopisujú dostatočne tie črty funkcie, ktoré určujú jej komunikačnú zložitosť. Naše odhady teda môžu poskytnúť prvú orientáciu, hrubý odhad, ktorý je potom potrebné zlepšovať inými technikami. Pre niektoré špeciálne prípady (pozri na strane 47) však dostávame aj pomocou týchto odhadov uspokojivé výsledky.

V tabuľke 2.1 vidíme prehľad dosiahnutých výsledkov pre všetky tri skúmané dvojice parametrov. Uvádzame vždy príslušný odhad a aj jeho optimálnosť, t.j. pre horné odhady dolný odhad zložitosti nejakej funkcie, ktorý nie je príliš vzdialený od daného horného odhadu a pre dolný odhad naopak horný odhad zložitosti nejakej funkcie.

Z dokázaných tvrdení je asi najzaujímavejšia veta 2.28, ktorá ukazuje, že existuje funkcia s vysokou simultánnou komunikačnou zložitosťou. Zaujímavá je tiež aj veta 2.32, pomocou ktorej môžeme odhadovať zdola komunikačnú zložitosť aspoň tých funkcií, ktoré majú veľmi vysoké r. Otvoreným problémom zostáva optimálnosť horného odhadu pomocou parametrov p a s pre $s < p$.

Celkovo sa nám podarilo získať nie príliš dobrý dolný odhad pre p a r a nezískali sme prakticky žiaden odhad pre parametre p a s (resp. p a s'). Môže sa však zdať, že pomocou vhodnej kombinácie r a s by sme možno získali aj lepší dolný odhad. Napríklad keď sme dokazovali optimálnosť dolného odhadu pomocou p a r, použili sme funkciu, ktorá mala dosť málo rôznych stĺpcov a navyše v jednej matici mohlo byť aj veľmi veľa rovnakých riadkov. Môžeme sa zaoberať napríklad otázkou, či ak by sme zakázali matice, v ktorých sa jednotlivé riadky opakujú, či vieme ešte zostrojiť príklad s tak malou simultánnou komunikačnou zložitosťou.

To, že takéto úvahy pravdepodobne nevedú k lepším odhadom sa pokúsime ukázať v nasledujúcom texte. Ukážeme funkciu, pre ktorú existuje protokol, v ktorom každý hráč pošle iba jeden bit a pritom táto funkcia má veľké parametre r aj s a navyše má v každej matici všetky riadky aj stĺpce navzájom rôzne.

Funkcia so správou zložitosťou 1

Skúmajme teraz, aké vlastnosti musí mať funkcia $f \in \mathcal{F}_{p,n}$, aby platilo $\mathrm{M}_S(f) = 1$. Znamená to, že existuje simultánny protokol $P = (m_1, m_2, m_3, m_4)$, v ktorom každý z hráčov 1, 2 a 3 pre ľubovoľný vstup pošle práve jeden bit. Oborom hodnôt funkcií m_1, m_2 a m_3 bude teda množina $\{0,1\}$ a funkcia m_4 bude funkciou z $\{0,1\}^3$ do $\{0,1\}$.

Kvôli lepšej predstavivosti si funkcie m_1, m_2 a m_3 budeme reprezentovať ako matice. Hráčovi 1 takto možno priradiť binárnu maticu M_1 typu $n \times p$, takú že $M_1(y,z) = m_1(y,z)$. Podobne hráčovi 2 priradíme maticu M_2 typu $p \times n$ a hráčovi 3 maticu M_3 typu $p \times p$. Pre všetky x, y, z musí pritom platiť vzťah $f(x,y,z) = m_4\left(M_1(y,z), M_2(x,z), M_3(x,y)\right)$.

Naopak, ak pre nejakú funkciu existujú takéto binárne matice a funkcia m_4, jej simultánna správová zložitosť je najviac 1.

Veta 2.37 *Pre každé $p > 2$ a $n = 2^{2p}$ existuje funkcia $f \in \mathcal{F}_{p,n}$, ktorá je vypočítateľná simultánnym protokolom, v ktorom každý hráč pošle jeden bit a ktorá má 2^p rôznych riadkov aj stĺpcov, 2^{2p-1} rôznych matíc a v každej matici sú všetky riadky navzájom rôzne aj všetky stĺpce navzájom rôzne.*

Dôkaz: Nech matica M_3 je jednotková matica, t.j. $M_3(i,j) = 1$ práve vtedy, keď $i = j$. Nech $v_0, v_1, \dots v_{n-1}$ sú všetky binárne reťazce dĺžky $2p$. Potom $M_1(y,z)$ bude y-tý bit reťazca v_z a $M_2(x,z)$ bude $(x+p)$-ty bit reťazca v_z. To znamená, že matice M_1 a M_2 volíme tak, že ak pre všetky z vezmeme stĺpec z z matice M_1 a stĺpec z z matice M_2, tak dostávame všetky navzájom rôzne dvojice binárnych reťazcov dĺžky p. Nakoniec zvoľme $m_4(x,y,z) = (x+y+z) \bmod 2$.

O funkcii definovanej vzťahom $f(x,y,z) = m_4\left(M_1(y,z), M_2(x,z), M_3(x,y)\right)$ dokážeme, že má požadované vlastnosti. Označme B_z maticu, pre ktorú platí $B_z(x,y) = f(x,y,z)$

Dokážme najprv, že každý z 2^p možných binárnych riadkov dĺžky p sa v niektorej matici B_z vyskytuje. Zvoľme teda binárny reťazec $r = r(0)r(1)\dots r(p-1)$. Nech z je také číslo, že prvých $p+1$ bitov reťazca v_z je $\overline{r(0)}r(1)\dots r(p-1)0$. Potom nultý riadok matice B_z je zhodný s reťazcom r. Platí totiž, že

$$B_z(0,0) = (M_1(0,z) + M_2(0,z) + M_3(0,0)) \bmod 2 = (\overline{r(0)} + 0 + 1) \bmod 2 = r(0)$$

a pre $i > 0$ dostávame

$$B_z(0,i) = (M_1(i,z) + M_2(0,z) + M_3(0,i)) \bmod 2 = (r(i) + 0 + 0) \bmod 2 = r(i)$$

Analogicky možno dokázať, že reťazec r sa v niektorej matici B_z vyskytuje aj ako stĺpec – zvolíme jednoducho nultý stĺpec matice B_z, kde v_z začína nulou a končí reťazcom $\overline{r(0)}r(1)\dots r(p-1)$.

Ďalej dokážeme, že v každej matici B_z sú všetky riadky navzájom rôzne. Zvoľme teda z. Nech B'_z je matica, pre ktorú platí $B'_z(x,y) = (M_1(y,z) + M_2(x,z)) \bmod 2$, t.j. $B_z(x,y) = (B'_z(x,y) + M_3(x,y)) \bmod 2$. Ak je $(p+x)$-tý bit v_z nula, potom riadok x matice B'_z je zhodný s prvými p bitmi reťazca v_z, v opačnom prípade obsahuje tieto bity negované. Každé dva riadky matice B'_z sú teda buď negáciou jeden druhého alebo sú zhodné. Všimnime si teraz, že i-te riadky matíc B_z a B'_z sa líšia iba v bite i. Nech teraz $i \neq j$. Dokážeme, že existuje k také, že i-ty a j-ty riadok matice B_z sa líšia v k-tom stĺpci. Ak sú i-ty a j-ty riadok matice B'_z zhodné, tak môžeme zvoliť $k = i$ alebo $k = j$. Na týchto indexoch sa oproti matici B'_z zmení v matici B_z práve jeden z riadkov. V prípade, že i-ty a j-ty riadok matice B'_z sú negáciou jeden druhého, môžeme za k zvoliť ľubovoľný index rôzny od i aj j (taký určite existuje, lebo $p > 2$. V k-tom stĺpci sa líšia vybrané dva riadky aj v matici B_z aj v B'_z.

Zostáva dokázať, že počet navzájom rôznych matíc vo funkcii f je $2^{2p-1} = n/2$. Vezmime ľubovoľnú maticu B_z a skúmajme veľkosť množiny $R_z = \{z' \in Z_n \mid B_{z'} = B_z\}$. Dokážeme, že $|R_z| = 2$ pre každé $z \in Z_n$. Platí, že $z' \in R_z$ práve vtedy, keď platí

$$(\forall x, y \in Z_p)\,(B_z(x,y) = (v_{z'}(y) + v_{z'}(p+x) + M_3(x,y)) \bmod 2) \tag{2.3}$$

Z tohoto vzťahu je zrejmé, že ak $z' \in R_z$ a $v_{z''}$ vznikne zo $v_{z'}$ negáciou všetkých bitov, tak aj $z'' \in R_z$. To znamená, že R_z obsahuje vždy minimálne dva prvky – z a prvok zodpovedajúci negácii v_z. Dokážeme teraz, že ak pre dva prvky $z', z'' \in R_z$ platí, že reťazce v'_z a v''_z sa zhodujú v prvom bite, tak sa zhodujú aj v ostatných bitoch a teda sa rovnajú aj z' a z''. Keďže $z' \in R_z$, na základe vzťahu (2.3) dostávame pre každé $x \in Z_p$:

$$v_{z'}(p+x) = (B_z(x,0) + v_{z'}(0) + M_3(x,0)) \bmod 2$$

Podobne pre $y \in Z_p$ platí:

$$\begin{aligned} v_{z'}(y) &= (B_z(0,y) + v_{z'}(p) + M_3(0,y)) \bmod 2 = \\ &= (B_z(x,0) + B_z(0,y) + v_{z'}(0) + M_3(x,0) + M_3(0,y)) \bmod 2 \end{aligned}$$

Dostávame teda, že všetky ostatné bity reťazca $v_{z'}$ sú jednoznačne určené nultým bitom tohto reťazca, ktorý je zhodný pre z' aj z''. Dokázali sme teda, že $|R_z| = 2$ pre každé z, takže počet navzájom rôznych matíc je $n/2$. □

Príklad: Uvedieme príklad funkcie zostrojenej v dôkaze pre $p = 3$ (a teda $n = 2^{2p} = 64$). Táto funkcia je už veľmi rozsiahla, takže ju nemôžeme uviesť celú, zobrazíme však, ako sa vytvára. V ľavom stĺpci vidíme matice časť matíc M_1 a M_2 a maticu M_3. Matice M_1 a M_2 sú typu 3×64. Nakoľko v dôkaze nie je úplne presne určené, ako majú tieto matice vyzerať (nie je dané poradie reťazcov), zostrojíme ich tak, že jednotlivé stĺpce zľava doprava budú tvoriť čísla 0 až 63 v binárnej sústave, pričom riadok 0 matice M_1 obsahuje najvyššie cifry a riadok 2 matice M_2 obsahuje najnižšie cifry. V maticiach sú zobrazené stĺpce 39, 40 a 41.

V pravom stĺpci vidíme matice B_z zostrojenej funkcie f, pre $z = 39, 40, 41$. $B_z(x,y) = (M_1(y,z) + M_2(x,z) + M_3(x,y)) \bmod 2$. V riadku pod tým vidíme matice $B'_z(x,y) = (M_1(y,z) + M_2(x,z)) \bmod 2$.

Matica M_1:

$$\begin{array}{|c|}\hline \cdots\cdots\ 1\ 1\ 1\ \cdots\cdots \\ \cdots\cdots\ 0\ 0\ 0\ \cdots\cdots \\ \cdots\cdots\ 0\ 1\ 1\ \cdots\cdots \\ \hline\end{array}$$

Matica M_2:

$$\begin{array}{|c|}\hline \cdots\cdots\ 1\ 0\ 0\ \cdots\cdots \\ \cdots\cdots\ 1\ 0\ 0\ \cdots\cdots \\ \cdots\cdots\ 1\ 0\ 1\ \cdots\cdots \\ \hline\end{array}$$

Matica M_3:

$$\begin{array}{|ccc|}\hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ \hline\end{array}$$

Matice B_z funkcie f pre $z = 39, 40, 41$:

$$\begin{array}{ccc} z=39 & z=40 & z=41 \\ \begin{array}{|ccc|}\hline 1&1&1\\0&0&1\\0&1&0\\\hline\end{array} & \begin{array}{|ccc|}\hline 0&0&1\\1&1&1\\1&0&0\\\hline\end{array} & \begin{array}{|ccc|}\hline 0&0&1\\1&1&1\\0&1&1\\\hline\end{array} \end{array}$$

Matice B'_z funkcie f pre $z = 39, 40, 41$:

$$\begin{array}{ccc} z=39 & z=40 & z=41 \\ \begin{array}{|ccc|}\hline 0&1&1\\0&1&1\\0&1&1\\\hline\end{array} & \begin{array}{|ccc|}\hline 1&0&1\\1&0&1\\1&0&1\\\hline\end{array} & \begin{array}{|ccc|}\hline 1&0&1\\1&0&1\\0&1&0\\\hline\end{array} \end{array}$$

2.3.5 Simultánna správová zložitosť

Doteraz sme sa zaoberali simultánnou komunikačnou zložitosťou funkcií, teda súčtom dĺžok správ poslaných jednotlivými hráčmi. V tejto časti budeme skúmať správovú zložitosť funkcií, t.j. maximálnu dĺžku správy poslanej v protokole. Podľa lemy 2.8 vieme, že odhady nájdené pre komunikačnú zložitosť platia až na konštantný násobok aj pre správovú zložitosť. Takto priamo dostávame pre správovú zložitosť odhady pomocou parametrov p, n, r a s. Tieto odhady by sa dali ešte zlepšiť tak, že by sme uvažovali jednotlivé vety, v ktorých sa dokazovali odhady pre komunikačnú zložitosť a v ich dôkazoch by sme spočítali správovú zložitosť uvádzaných protokolov.

Tu sa však zameriame iba na jeden problém. Odvodíme akúsi analógiu vety 2.28, t.j. že existujú funkcie s veľkou správovou zložitosťou. Budeme však predpokladať, že $p = n$, t.j. všetky tri vstupy sú rovnako veľké. Tento predpoklad nám umožní spraviť presnejší odhad, ako vo vete 2.28, kde sme počítali s ľubovoľnými parametrami p a n. Takisto dokážeme, že funkcií s veľkou simultánnou správovou zložitosťou je väčšina.

Pre $p = n$ je možné každú funkciu vypočítať tak, že každý hráč pošle najviac $\lceil \log n \rceil$ bitov (pošle jeden zo svojich vstupov). Aké je ale najmenšie d také, že je možné každú funkciu vypočítať tak, že každý hráč pošle najviac d bitov? Dokážeme, že $\lceil \log n \rceil - 1 \le d \le \lceil \log n \rceil$, takže dokážeme že triviálny horný odhad je optimálny až na aditívnu konštantu 1.

Veta 2.38 *Nech $n \ge 4$ a $p = n$. Potom existuje funkcia $f \in \mathcal{F}_{p,n}$, ktorej simultánna* *správová zložitosť je* $\lceil \log n \rceil - 1$. *Navyše, takýchto funkcií je väčšina z celkového počtu funkcií v* $\mathcal{F}_{p,n}$.

Dôkaz: Označme $m = \lceil \log n \rceil$. Podobne ako v leme 2.27, aj v tejto vete dokážeme, že počet funkcií, ktoré sú vypočítateľné protokolom so správovou zložitosťou najviac $m-2$, je menší ako počet všetkých funkcií. Keďže $p = n$, každý hráč má presne n^2 rôznych kombinácií vstupov. Podľa lemy 2.11 môžeme predpokladať, že každý hráč posiela iba správy dĺžky $m-2$. Pre každú z n^2 dvojíc vstupov môže poslať ľubovoľnú z 2^{m-2} možných správ dĺžky $m-2$. Teda pre svoje vstupy sa každý hráč môže správať presne $(2^{m-2})^{n^2}$ spôsobmi. Hráč 4 musí pre každú trojicu správ, ktorá mu príde od ostatných hráčov vedieť určiť výsledok. Počet takýchto trojíc je najviac $(2^{m-2})^3$, a teda počet správaní pre tohoto hráča je najviac $2^{(2^{m-2})^3}$. Celkový počet funkcií, vypočítateľných protokolmi, v ktorých žiaden hráč nepošle viac ako $m-2$ bitov je najviac

$$\left((2^{m-2})^{n^2}\right)^3 \cdot 2^{(2^{m-2})^3}$$

Upravujme tento výraz (použijeme vzťah $m - 2 = \lceil \log n \rceil - 2 \leq \log n - 1$ a teda $2^{m-2} \leq \frac{n}{2}$):

$$\left((2^{m-2})^{n^2}\right)^3 \cdot 2^{(2^{m-2})^3} \leq 2^{3(\log n - 1)n^2} \cdot 2^{\left(\frac{n}{2}\right)^3} = 2^{3(\log n-1)n^2+n^3/8}$$

Nech x je pomer počtu funkcií, vypočítateľných protokolmi, v ktorých žiaden hráč nepošle viac ako $m-2$ bitov a počtu všetkých funkcií. Dokážeme, že $x < \frac{1}{2}$.

$$x \leq \frac{2^{3(\log n-1)n^2+n^3/8}}{2^{n^3}} = 2^{3(\log n-1)n^2+n^3/8-n^3} = 2^{n^2(3(\log n-1)-\frac{7}{8}n)}$$

Ľahko sa overí, že pre každé celé $n \geq 4$ je $(3(\log n - 1) - \frac{7}{8}n) < -\frac{1}{16}$ a teda $x < 2^{4^2-1/16} \leq \frac{1}{2}$. □

2.4 Charakterizácia simultánnej zložitosti

Uvedieme niektoré charakterizácie komunikačnej zložitosti simultánnych protokolov (presnejšie takmer simultánnych protokolov a zúžených simultánnych protokolov) pomocou pojmov z teórie grafov a z kombinatoriky.

2.4.1 Grafová charakterizácia zložitosti takmer simultánnych protokolov

V tejto časti uvedieme charakterizáciu komunikačnej zložitosti takmer simultánnych protokolov pomocou chromatického čísla určitej množiny grafov.

Označenie 2.39 *Majme funkciu* $f \in \mathcal{F}_{p,n}$. *Označme* G_f *bipartitný graf* $G_f = (V_f, E_f)$ *definovaný takto:*

$$\begin{aligned} V_f = \ & \{(1, y, z_1, z_2) \mid y \in Z_p, z_1, z_2 \in Z_n, z_1 \neq z_2\} \cup \\ & \cup \{(2, x, z_1, z_2) \mid x \in Z_p, z_1, z_2 \in Z_n, z_1 \neq z_2\} \end{aligned}$$

$$E_f = \{\{(1,y,z_1,z_2),(2,x,z_1,z_2)\} \,|\, x,y \in Z_p, z_1,z_2 \in Z_n, z_1 \neq z_2, \\ f(x,y,z_1) \neq f(x,y,z_2)\}$$

Ďalej nech $V \subseteq V_f$. *Graf* $G_V = (V_V, E_V)$ *definujeme takto:*

$$V_V = \{(1,y,z) \,|\, y \in Z_p, z \in Z_n\} \cup \{(2,x,z) \,|\, x \in Z_p, z \in Z_n\}$$

$$E_V = \{\{(i,x,z_1),(i,x,z_2)\} \,|\, i \in \{1,2\}, x \in Z_p, z_1,z_2 \in Z_n, (i,x,z_1,z_2) \in V\}$$

Ak je dvojica $\{(1,y,z_1,z_2),(2,x,z_1,z_2)\}$ hranou v grafe G_f, znamená to, že buď musí hráč 1 poslať rozličné správy na vstupy (y,z_1) a (y,z_2), alebo musí hráč 2 poslať rozličné správy na vstupy (x,z_1) a (x,z_2), lebo $f(x,y,z_1) \neq f(x,y,z_2)$ a ak by obaja hráči na uvedené dvojice vstupov posielali rovnaké správy, hráč 3 by nevedel určiť funkčnú hodnotu (pozná iba x a y).

V dôkaze nasledujúcej vety nájdeme korešpondenciu medzi takmer simultánnymi protokolmi a vrcholovými pokrytiami grafu G_f. Pritom počet navzájom rôznych správ poslaných v protokole P zhruba zodpovedá chromatickému číslu[5] grafu G_V, kde V je vrcholové pokrytie zodpovedajúce protokolu P.

Veta 2.40 *Nech* $f \in \mathcal{F}_{p,n}$ *a nech*

$$m = \min\{\chi(G_V) |\, V \subseteq V_f \text{ je vrcholové pokrytie grafu } G_f\}$$

Potom platí $\mathrm{M}_{AS} = \lceil \log m \rceil$.

Dôkaz: Nech Π je množina všetkých takmer simultánnych protokolov počítajúcich funkciu f. Ďalej nech P je protokol z Π. Označme počet navzájom rôznych správ posielaných hráčom 1 v protokole P ako $M_{P,1}$ a podobne počet navzájom rôznych správ posielaných hráčom 2 ako $M_{P,2}$. Ďalej nech M_P je maximum z čísel $M_{P,1}$ a $M_{P,2}$.

Nech M je najmenšie číslo také, že v každom protokole $P \in \Pi$ niektorý z hráčov posiela aspoň M navzájom rôznych správ, t.j. $M = \min\{M_P | P \in \Pi\}$. Dokážeme, že $M = m$. Ak má hráč poslať M navzájom rôznych správ, pričom množina týchto správ je bezprefixová, potom niektorá z týchto správ musí mať dĺžku aspoň $\lceil \log M \rceil$, t.j. dostávame, že naozaj $\mathrm{M}_{AS} = \lceil \log m \rceil$.

Zvyšok dôkazu rozdelíme na dve časti. Najprv dokážeme, že $M \geq m$ (pre každý protokol zostrojíme zodpovedajúce vrcholové pokrytie V) a v druhej časti dokážeme, že $m \geq M$ (pre každé vrcholové pokrytie V zostrojíme protokol).

1. časť: $M \geq m$

Nech P je protokol z Π. Nájdeme vrcholové pokrytie V grafu G_f také, že graf G_V bude M_P-zafarbiteľný, t.j. dokážeme, že $M_P \geq \chi(G_V) \geq m$. Keďže tento vzťah platí pre všetky čísla M_P, platí aj ich pre minimum – číslo M.

Majme teda protokol $P \in \Pi$. Zostrojme teraz hľadané vrcholové pokrytie V takto: vrchol $(1,y,z_1,z_2) \in G_f$ bude patriť do V práve vtedy, keď hráč 1 pre

[5] Chromatické číslo grafu G budeme označovať $\chi(G)$.

dvojice svojich vstupov (y, z_1) a (y, z_2) posiela navzájom rôzne správy v protokole P. Podobne vrchol $(2, x, z_1, z_2) \in G_f$ bude patriť do V práve vtedy, keď hráč 2 posiela rôzne správy pre dvojice svojich vstupov (x, z_1) a (x, z_2).

Nie je ťažké nahliadnuť, že graf G_V je M_P-zafarbiteľný. Pre každého hráča priradíme rôznym správam, ktoré tento hráč v protokole používa, farby $1, 2, \ldots$. Vrchol (i, x, z) ofarbíme farbou priradenou správe, ktorú posiela hráč i ak dostane dvojicu vstupov (x, z). Z konštrukcie množiny V vyplýva, že žiadne dva vrcholy spojené hranou nebudú ofarbené rovnakou farbou. Použitých farieb je najviac M_P, lebo žiaden z hráčov nepoužíva viac správ.

Zostáva dokázať, že V je vrcholovým pokrytím grafu G_f. Postupujme sporom: nech existuje hrana $e = \{(1, y, z_1, z_2), (2, x, z_1, z_2)\} \in E_f$, ktorá nie je pokrytá množinou V. To znamená, že v protokole P hráč 1 posiela rovnaké správy pre vstupy (y, z_1) aj (y, z_2) a podobne hráč 2 posiela rovnaké správy pre vstupy (x, z_1) aj (x, z_2). Keďže však e je hrana grafu G_f, platí $f(x, y, z_1) \neq f(x, y, z_2)$. Pre trojice vstupov (x, y, z_1) a (x, y, z_2) však hráč 3 dostane od oboch hráčov rovnakú informáciu a on sám vidí iba vstupy x a y, ktoré sú pre obe trojice rovnaké. Hráč 3 musí teda v oboch prípadoch vypočítať rovnaký výsledok, takže protokol P nepočíta funkciu f, čo je spor.

2. časť: $m \geq M$

Nech V je vrcholové pokrytie grafu G_f. Zostrojíme protokol $P \in \Pi$, v ktorom žiaden hráč nepošle správu dlhšiu ako $\chi(G_V)$. Dokážeme teda, že $M_P \leq \chi(G_V)$ a keďže $M \leq M_P$, platí aj $M \leq \chi(G_V)$. Keďže táto nerovnosť platí pre každé vrcholové pokrytie V, platí aj vzťah $M \leq m$.

Hľadaný protokol P zostrojíme jednoducho. Vezmime ľubovoľné farbenie grafu G_V, ktoré používa $\chi(G_V)$ farieb (predpokladajme, že farby sú čísla $1, 2, \ldots, k$). Hráč i pošle pre dvojicu svojich vstupov (x, z) číslo farby vrcholu (i, x, z). Predpokladajme teraz, že hráč 3 vidí dvojicu vstupov (x, y) a od hráčov 1 a 2 dostane správy m_1 a m_2 zostrojené uvedeným spôsobom. Potom zvolí z také, že vrchol $(1, y, z)$ je ofarbený farbou m_1 a vrchol $(2, x, z)$ je ofarbený farbou m_2 a za výsledok vyhlási hodnotu $f(x, y, z)$. Takéto z vždy existuje, čo vyplýva z konštrukcie protokolu pre x a y.

Treba ešte dokázať, že uvedený protokol naozaj počíta funkciu f. Predpokladajme sporom, že existuje vstup (x, y, z), pre ktorý protokol P vypočíta výstup rôzny od $f(x, y, z)$. Hráč 3 teda musel zvoliť výsledok ako hodnotu $f(x, y, z')$, kde $f(x, y, z') = a \neq f(x, y, z)$, pričom hráč 1 posiela pre dvojice vstupov (y, z) a (y, z') rovnaké správy a hráč 2 posiela rovnaké správy na dvojice vstupov (x, z) a (x, z').

Keďže hráč 1 posiela pre dvojice vstupov (y, z) a (y, z') rovnaké správy, vrcholy $(1, y, z)$ a $(1, y, z')$ v grafe G_V sú ofarbené rovnakou farbou, teda nie sú spojené hranou a teda vrchol $(1, y, z, z')$ nepatrí do V. Analogicky možno dokázať, že ani vrchol $(2, x, z, z')$ nepatrí do V. To ale znamená, že tieto dva vrcholy nie sú v grafe G_f spojené hranou (ak by boli spojené hranou, V by nebolo vrcholové pokrytie). Z definície grafu G_f ale dostávame, že teda $f(x,y,z) = f(x,y,z')$, čo je spor. $\square$

2.4.2 Charakterizácia zložitosti zúžených simultánnych protokolov

Nasleduje niekoľko charakterizácií správovej zložitosti zúžených komunikačných protokolov. Najprv uvedieme úzky vzťah medzi zúženými simultánnymi protokolmi a protokolmi na výpočet relácií. Z neho potom odvodíme charakterizáciu zložitosti funkcie pomocou matíc a bipartitných grafov.

Charakterizácia pomocou komunikačnej zložitosti relácií

Uvažujme reláciu $R \subseteq Z_p \times Z_p \times Z_n \times Z_n \times \{0,1\}$. Simultánny protokol na výpočet relácie R bude pracovať nasledovným spôsobom: Hráč 1 dostane vstupy $y \in Z_p$ a $z_1 \in Z_n$, hráč 2 dostane vstupy $x \in Z_p$ a $z_2 \in Z_n$. Každý z hráčov na základe svojich vstupov zostaví správu, tú pošle hráčovi 4 (hráča 3 neuvažujeme). Hráč 4 nepozná žiaden zo vstupov a iba na základe prijatých správ má vypočítať hodnotu $i \in \{0,1\}$ takú, že $(x,y,z_1,z_2,i) \in R$. Navyše požadujeme, aby množina všetkých správ, ktoré môže poslať hráč 1 (resp. hráč 2) bola bezprefixová.

Formálne je možné zadefinovať takéto protokoly a ich zložitosť podobne ako simultánne protokoly (resp. zúžené simultánne protokoly). Tento model má však ešte jeden výrazný rozdiel (okrem toho, že nepočítame funkciu, ale reláciu) oproti štandardnému simultánnemu modelu – informácia daná hráčom 1 a 2 sa neprekrýva. Táto vlastnosť spôsobuje, že zložitosť výpočtu takýchto relácií vieme pomerne dobre charakterizovať. Navyše, zúžená simultánna správová zložitosť funkcie sa nelíši od simultánnej správovej zložitosti vhodne zvolenej relácie.

Veta 2.41 *Nech $f \in \mathcal{F}_{p,n}$ a nech $R \subseteq Z_p \times Z_p \times Z_n \times Z_n \times \{0,1\}$ je relácia definovaná takto:*

$$\begin{aligned} R = \;& \{(x,y,z,z,f(x,y,z)) \mid x,y \in Z_p, z \in Z_n\} \\ & \cup \{(x,y,z_1,z_2,i) \mid x,y \in Z_p, z_1,z_2 \in Z_n, z_1 \neq z_2, i \in \{0,1\}\} \end{aligned}$$

Potom $\mathrm{M}_{\varepsilon S}(f)$ je rovná simultánnej správovej zložitosti relácie R.

Dôkaz: Nech P je simultánny protokol počítajúci reláciu R. Zostrojíme teraz zúžený simultánny protokol P' počítajúci funkciu f. Funkcie m_1 a m_2, ktoré pre jednotlivé dvojice vstupov určujú poslanú správu, budú v oboch protokoloch rovnaké. Funkcia m_3 v protokole P' je z definície konštantne rovná ε. Funkciu m_4 pre P' (určujúcu pre hráča 4, aký výsledok má oznámiť pre rôzne trojice správ) získame z funkcie m_4 pre P zúžením iba na tie dvojice správ, ktoré môžu pri protokole P' nastať (treba ešte doplniť tretí argument, ten je však v celom definičnom obore m_4 rovný ε).

Protokol P', ktorý sme zostrojili týmto spôsobom, vráti pre vstup (x,y,z) výsledok $m_4(m_1(y,z), m_2(x,z))$. Rovnaký výsledok však vráti aj protokol P na vstup (x,y,z,z). Podľa definície R však $(x,y,z,z,i) \in R$ práve vtedy, keď $i = f(x,y,z)$ a teda protokol P' vráti správny výsledok.

Naopak nech P je zúžený simultánny protokol počítajúci funkciu f. Zostrojíme simultánny protokol P' počítajúci reláciu R. Podobne ako v predchádzajúcom prípade, funkcie m_1 a m_2 budú v oboch protokoloch rovnaké. Funkciu m_4 pre P' získame rozšírením funkcie m_4 pre P na všetky dvojice správ z $H(m_1) \times H(m_2)$. Pritom pre dvojice správ, pre ktoré pôvodná funkcia m_4 nie je definovaná, môžeme doplniť ľubovoľné hodnoty.

Aby sme dokázali, že protokol P' naozaj počíta reláciu R, stačí dokázať, že dá správnu odpoveď pre štvorice (x, y, z_1, z_2), pre ktoré $z_1 = z_2$ (pre ostatné dvojice je totiž z definície relácie R každá odpoveď správna). Pre takéto štvorice však protokol P' vráti rovnaký výsledok ako vráti protokol P pre trojicu x, y, z_1, čo je naozaj správna odpoveď.

V oboch konštrukciách mal skonštruovaný protokol P' rovnaké množiny správ $H(m_1)$ a $H(m_2)$ ako pôvodný protokol P, takže správová zložitosť bola pre oba protokoly rovnaká. Z toho vyplýva, že aj správová zložitosť funkcie f a relácie R (v uvažovaných modeloch) je rovnaká. $\square$

Matice a bipartitné grafy – pojmy a označenia

Pri ďalších charakterizáciách zúženej správovej zložitosti budeme veľa pracovať s binárnymi maticami, pričom si budeme všímať najmä rozklad ich množiny riadkov na množiny rovnakých riadkov, počty rôznych riadkov a podobné pojmy zadefinované pre stĺpce. Budeme taktiež uvažovať bipartitné grafy. Preto teraz zavedieme niekoľko označení na uľahčenie takýchto úvah.

Majme binárnu maticu A typu $n \times m$. Zavedieme reláciu ekvivalencie riadkov $\sim_r \subseteq Z_n \times Z_n$ takto:

$$i \sim_r j \iff (\forall k \in Z_m)(A(i,k) = A(j,k)),$$

t.j. čísla i a j budú ekvivalentné práve vtedy, ak im zodpovedajúce riadky v A sú rovnaké. Relácia ekvivalencie $\sim_r$ nám určuje rozklad množiny Z_n na triedy ekvivalencie. Triedu ekvivalencie obsahujúcu číslo i budeme označovať $[i]_{r,A}$. Množinu všetkých navzájom rôznych riadkov matice A môžeme stotožniť s množinou $\{[i]_{r,A} | \, i \in Z_n\}$. Analogicky tiež môžeme zaviesť reláciu ekvivalencie stĺpcov $\sim_s \subseteq Z_m$, triedy ekvivalencie $[i]_{s,A}$ a množinu všetkých navzájom rôznych stĺpcov matice A stotožníme s množinou $\{[i]_{s,A} | \, i \in Z_m\}$.

Uvedieme jednu pomerne triviálnu lemu, ktorú však v nasledujúcich dôkazoch budeme často používať:

Lema 2.42 *Nech A je binárna matica typu $n \times m$ a nech $i, i' \in Z_n$ a $j, j' \in Z_m$ sú také čísla, že $i' \in [i]_{r,A}$ a $j' \in [j]_{s,A}$. Potom platí $A(i,j) = A(i',j')$.*

Dôkaz: Z definície množiny $[i]_{r,A}$ vyplýva, že $A(i,j) = A(i',j)$. Podobne z definície $[j]_{s,A}$ vyplýva, že $A(i',j) = A(i',j')$. Z toho už dostávame požadované tvrdenie. $\square$

Inak povedané lema vraví, že ak vezmeme jednu triedu ekvivalencie riadkov a jednu triedu ekvivalencie stĺpcov, tak na priesečníku ľubovoľných dvoch prvkov z týchto tried bude vždy to isté číslo. Na základe tohto pozorovania môžeme zaviesť pojem redukcie matice – z matice vyškrtáme viacnásobné výskyty rovnakých riadkov a stĺpcov. Riadky a stĺpce v takto získanej matici potom zodpovedajú triedam ekvivalencie a na priesečníku určitého riadku a stĺpca v redukovanej matici je hodnota, ktorá bola v pôvodnej matici na všetkých priesečníkoch prvkov príslušných tried ekvivalencie (podľa predchádzajúcej lemy). Formálnejšie môžeme uvedený pojem zaviesť takto:

Definícia 2.43 *Nech A je binárna matica typu $n \times m$. Maticu A' typu $n' \times m'$ budeme nazývať* **redukciou matice** *A, ak existujú bijekcie $\psi_r : \{[i]_{r,A} | \, i \in Z_n\} \to Z_{n'}$ a $\psi_s : \{[i]_{s,A} | \, i \in Z_m\} \to Z_{m'}$ také, že pre každé $i \in Z_n$ a pre každé $j \in Z_m$ platí*

$$A(i,j) = A'(\psi_r([i]_{r,A}), \psi_s([j]_{s,A})).$$

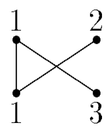
Maticu nazveme **redukovanou**, *ak je sama sebe redukciou.*

Na základe lemy 2.42 vidíme, že pre každú maticu existuje redukcia, pričom táto redukcia je až na poradie riadkov a stĺpcov daná jednoznačne. Ľahko tiež dokázať, že redukcia ľubovoľnej matice má všetky riadky aj stĺpce navzájom rôzne, je teda redukovanou maticou.

Teraz poďme venovať pozornosť bipartitným grafom. Štandardne sa bipartitnými grafmi rozumie určitá špeciálna trieda grafov, my si však tento pojem kvôli jednoduchšiemu značeniu zavedieme trochu odlišne.

Pod bipartitným grafom budeme rozumieť usporiadanú trojicu $G = (U, V, E)$, kde U a V sú konečné množiny vrcholov a E je množina hrán, pričom $E \subseteq U \times V$. Znamená to teda, že v bipartitných grafoch budeme uvažovať fixné rozdelenie vrcholov do partícií (a to aj pre grafy, kde existuje viacero možných rozdelení) a navyše budeme medzi oboma partíciami rozlišovať. Takisto množiny U a V nemusia byť nutne disjunktné – ak sa však nejaký prvok nachádza v množine U aj vo V, tak reprezentuje dva rôzne vrcholy grafu, pričom tieto vrcholy môžu a nemusia byť spojené hranou.

Príklad:



Graf G

Na obrázku máme znázornený graf $G = (U, V, E)$, kde $U = \{1, 2\}$, $V = \{1, 3\}$ a $E = \{(1, 3), (2, 1), (1, 1)\}$. Vrcholy partície U sú zobrazené na vrchnom riadku, vrcholy partície V sú zobrazené na spodnom riadku. Takýmto spôsobom budeme bipartitné grafy zobrazovať aj v nasledujúcich príkladoch.

Ďalej sa budeme zaoberať korešpondenciou medzi binárnymi maticami a bipartitnými grafmi. V nasledujúcej definícii zostrojíme k danej matici A bipartitný graf, ktorý bude mať v partícii U všetky navzájom rôzne riadky matice A, partícia V bude množina všetkých navzájom rôznych stĺpcov matice A a hrany budú zodpovedať jednotkám v matici.

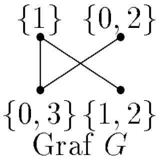
Definícia 2.44 *Nech A je binárna matica typu $n \times m$.* **Bipartitný graf priradený** *k matici A je graf $G = (U, V, E)$, pre ktorý platí*

$$U = \{[i]_{r,A} | \, i \in Z_n\} \qquad V = \{[i]_{s,A} | \, i \in Z_m\}$$
$$E = \{([i]_{r,A}, [j]_{s,A}) | \, i \in Z_n \wedge j \in Z_m \wedge A(i,j) = 1\}.$$

Príklad: Bipartitný graf G je priradený k matici A. Matica A' je redukciou matice A. Po vhodnom preznačení vrcholov grafu G dostaneme graf G' priradený k matici A'.

$$\boxed{\begin{array}{cccc} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{array}}$$

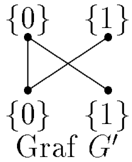
Matica A



Graf G

$$\boxed{\begin{array}{cc} 1 & 1 \\ 1 & 0 \end{array}}$$

Matica A'



Graf G'

Nakoniec ešte budeme uvažovať určité vzťahy medzi vybranými podmaticami matice A a podgrafmi jej priradenému bipartitnému grafu G. Maticu A' nazveme vybranou podmaticou matice A, ak ju z matice A môžeme dostať vynechaním niektorých riadkov a stĺpcov a prípadnou zmenou poradia zostávajúcich riadkov a stĺpcov. Nižšie uvádzame formálnu definíciu vybranej podmatice a tiež definíciu bipartitne indukovaného podgrafu, čo je špeciálny prípad indukovaného podgrafu:

Definícia 2.45 *Nech A_1 je binárna matica typu $n_1 \times m_1$ a A_2 binárna matica typu $n_2 \times m_2$. Hovoríme, že matica A_1 je* **vybranou podmaticou** *matice A_2, ak existujú injektívne zobrazenia $\phi_r : Z_{n_1} \to Z_{n_2}$ a $\phi_s : Z_{m_1} \to Z_{m_2}$ také, že platí*

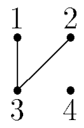
$$(\forall i \in Z_{n_1})(\forall j \in Z_{m_1})(A_1(i,j) = A_2(\phi_r(i), \phi_s(j))).$$

Definícia 2.46 *Majme bipartitné grafy $G_1 = (U_1, V_1, E_1)$ a $G_2 = (U_2, V_2, E_2)$. Hovoríme, že graf G_1 je* **bipartitne indukovaný podgraf** *grafu G_2, ak existujú injektívne zobrazenia $\phi_U : U_1 \to U_2$ a $\phi_V : V_1 \to V_2$ také, že platí*

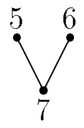
$$(\forall u \in U_1)(\forall v \in V_1)((u,v) \in E_1 \iff (\phi_U(u), \phi_V(v)) \in E_2).$$

Graf G_1 je teda bipartitne indukovaným podgrafom grafu G_2 práve vtedy, keď je jeho indukovaným podgrafom (resp. je izomorfný s nejakým jeho indukovaným podgrafom), pričom navyše požadujeme, aby vrcholy z prvej partície grafu G_1 sa zobrazovali na vrcholy prvej partície grafu G_2 a podobne pre druhé partície. Z definície vidno, že relácia "byť bipartitne indukovaným podgrafom" je tranzitívna, t.j že ak G je bipartitne indukovaným podgrafom G' a G' je bipartitne indukovaným podgrafom G'', tak G je bipartitne indukovaným podgrafom G''.

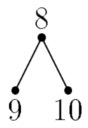
Príklad: Uvažujme bipartitné grafy G_1, G_2, G_3 a G_4 zobrazené na obrázku. Bipartitný graf G_2 je bipartitne indukovaným podgrafom grafu G_1 (požadované zobrazenia zostrojíme napr. takto: $\phi_U(5) = 2$, $\phi_U(6) = 1$, $\phi_U(7) = 3$) Graf G_3 ani graf G_4 však nie sú bipartitne indukovanými podgrafmi grafu G_1, hoci oba sú jeho podgrafmi v zvyčajnej grafovej terminológii a graf G_4 je dokonca aj jeho indukovaným podgrafom.



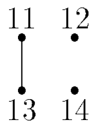
Graf G_1



Graf G_2



Graf G_3



Graf G_4

Lema 2.47 *Nech A je binárna matica typu $n \times m$ a A' nech je binárna matica typu $n' \times m'$. Ďalej nech G je bipartitný graf priradený k A a G' nech je priradený k A'.*

Potom ak A' je vybranou podmaticou matice A, tak G' je bipartitne indukovaný podgraf grafu G.

Naopak, ak G' je bipartitne indukovaný podgraf grafu G a A' je redukovaná matica, potom A' je vybranou podmaticou matice A.

Dôkaz: Majme teda grafy $G = (U, V, E)$ a $G' = (U', V', E')$ a matice A a A' spĺňajúce predpoklady vety. Dokážeme najprv prvú časť, potom druhú časť vety.

Prvá časť dôkazu. Nech A' je vybranou podmaticou matice A a nech $\phi_r : Z_{n'} \to Z_n$ a $\phi_s : Z_{m'} \to Z_m$ sú zobrazenia z definície vybranej podmatice (t.j. ϕ_r dáva pre každý riadok matice A' zodpovedajúci riadok matice A a podobne ϕ_s pre stĺpce). Dokážeme, že G' je bipartitne indukovaným podgrafom grafu G.

Zostrojíme zobrazenia $\phi_U : U' \to U$ a $\phi_V : V' \to V$ a dokážeme, že sú injektívne a že pre ne platí vzťah

$$(\forall u \in U')(\forall v \in V')((u, v) \in E' \iff (\phi_U(u), \phi_V(v)) \in E). \tag{2.4}$$

To ale znamená, že tieto zobrazenia spĺňajú všetky podmienky z definície bipartitne indukovaného podgrafu a teda G' je bipartitne indukovaným podgrafom grafu G.

Pre každý vrchol $u \in U'$ zvolíme $i \in Z_{n'}$ také, že $u = [i]_{r,A'}$ a položíme

$$\phi_U(u) = [\phi_r(i)]_{r,A}$$

Analogicky pre $v \in V'$, zvolíme $j \in Z_{m'}$ také, že $v = [j]_{s,A'}$ a položíme $\phi_V(v) = [\phi_s(j)]_{s,A}$.

Najprv treba dokázať, že zostrojené zobrazenia sú injektívne. To dokážeme iba pre ϕ_U, pre ϕ_V je dôkaz analogický. Pre ľubovoľné navzájom rôzne u a v z množiny U' dokážeme, že platí, že $\phi_U(u) \neq \phi_U(v)$. Nech sme pri konštrukcii $\phi_U(u)$ zvolili i spomedzi hodnôt, pre ktoré $u = [i]_{r,A'}$, a podobne nech j je hodnota zvolená pre v. Keďže $u \neq v$, platí, že $[i]_{r,A'} \neq [j]_{r,A'}$ a teda riadky i a j matice A' sú rôzne. Potom ale aj riadky $\phi_r(i)$ a $\phi_r(j)$, ktoré riadkom i a j zodpovedajú v matici A, sú navzájom rôzne. Preto $[\phi_r(i)]_{r,A} \neq [\phi_r(j)]_{r,A}$, čo je požadované tvrdenie, lebo $\phi_U(u) = [\phi_r(i)]_{r,A}$ a $\phi_U(v) = [\phi_r(j)]_{r,A}$.

Nakoniec dokážeme, že platí vzťah (2.4). Zvoľme ľubovoľné $u \in U'$ a $v \in V'$. Ďalej nech pri konštrukcii $\phi_U(u)$ sme zvolili hodnotu $i \in Z_{n'}$ a pri konštrukcii $\phi_V(v)$ nech sme zvolili hodnotu $j \in Z_{m'}$. Vrcholy u a v sú v grafe G' spojené hranou práve vtedy, keď $A'(i, j) = 1$. Z definície vybranej podmatice máme $A'(i, j) = A(\phi_r(i), \phi_s(j))$. Na dokončenie dôkazu poznamenajme, že

$$A(\phi_r(i), \phi_s(j)) = 1 \iff ([\phi_r(i)]_{r,A}, [\phi_s(j)]_{s,A}) \in E,$$

pričom platí, že $([\phi_r(i)]_{r,A}, [\phi_s(j)]_{s,A}) = (\phi_U(u), \phi_V(v))$.

Druhá časť dôkazu. Nech G' je bipartitne indukovaným podgrafom grafu G a nech A' je redukovaná. Nech $\phi_U : U' \to U$ a $\phi_V : V' \to V$ sú zobrazenia z definície bipartitne indukovaného podgrafu. Dokážeme, že A' je podmaticou A.

V tejto časti dôkazu budeme postupovať podobne ako v predchádzajúcej – zostrojíme zobrazenia $\phi_r : Z_{n'} \to Z_n$ a $\phi_s : Z_{m'} \to Z_m$ a dokážeme, že sú injektívne a že pre ne platí vzťah

$$(\forall i \in Z_{n'})(\forall j \in Z_{m'})(A'(i,j) = A(\phi_r(i), \phi_s(j))). \tag{2.5}$$

Dostaneme teda, že zostrojené zobrazenia spĺňajú podmienky z definície vybranej podmatice a teda A' je vybranou podmaticou matice G.

Majme teda $i' \in Z_{n'}$. Nech $u \in U$ je vrchol grafu G zodpovedajúci vrcholu $[i']_{r,A'}$ grafu G', t.j.

$$u = \phi_U([i']_{r,A'}).$$

Ako $\phi_r(i')$ zvolíme niektorú hodnotu $i \in Z_n$, pre ktorú platí $u = [i]_{r,A}$. Analogicky pre stĺpce: pre $j' \in Z_{m'}$ nech $v = \phi_V([j']_{s,A'})$ a ako $\phi_s(j')$ zvolíme niektoré $j \in Z_m$, pre ktoré platí $v = [j]_{s,A}$.

Dokážme teraz injektívnosť ϕ_r (dôkaz pre ϕ_s je analogický). Nech $i', j' \in Z_{n'}$ sú navzájom rôzne, dokážeme, že $\phi_r(i') \neq \phi_r(j')$. Keďže A' je redukovaná, všetky jej riadky sú navzájom rôzne a teda $[i']_{r,A'} = \{i'\} \neq \{j'\} = [j']_{r,A'}$. Z injektívnosti zobrazenia ϕ_U máme, že $\phi_U([i']_{r,A'}) \neq \phi_U([j']_{r,A'})$. Prvky $\phi_U([i']_{r,A'})$ a $\phi_U([j']_{r,A'})$ sú však triedami ekvivalencie $[i]_{r,A}$ a $[j]_{r,A}$ pre nejaké $i, j \in Z_n$. Nakoľko sú tieto triedy navzájom rôzne, znamená to, že sú disjunktné. Hodnoty $\phi_r(i')$ a $\phi_r(j')$ boli zvolené ako prvky týchto tried ekvivalencie a musia byť teda navzájom rôzne.

Zostáva dokázať jedine vzťah (2.5). Majme teda $i' \in Z_{n'}$ a $j' \in Z_{m'}$. $A'(i', j') = 1$ práve vtedy, keď dvojica $([i']_{r,A'}, [j']_{s,A'})$ je hranou grafu G'. Z definície indukovaného podgrafu však máme, že táto dvojica je hranou práve vtedy, keď dvojica $(\phi_U([i']_{r,A'}), \phi_V([j']_{s,A'}))$ je hranou grafu G. Keďže graf G je priradený k A, pre ľubovoľné $i \in \phi_U([i']_{r,A'})$ a pre ľubovoľné $j \in \phi_V([j']_{s,A'})$ platí, že uvedená dvojica je hranou práve vtedy, keď $A(i,j) = 1$. Platí to teda aj pre i a j zvolené pri konštrukcii zobrazení ϕ_r a ϕ_s. Z uvedených ekvivalencií dostávame požadovaný vzťah. □

Lema 2.48 *Nech A je binárna matica typu $n \times m$ a A' nech je binárna matica typu $n' \times m'$. Ďalej nech G je bipartitný graf priradený k A a G' nech je priradený k A'.*

Potom ak A' je redukciou matice A, tak G je bipartitne indukovaný podgraf grafu G'.

Dôkaz: Nech $G = (U, V, E)$ a nech $G' = (U', V', E')$. Ďalej nech $\psi_r : \{[i]_{r,A} | i \in Z_n\} \to Z_{n'}$ a $\psi_s : \{[i]_{s,A} | i \in Z_m\} \to Z_{m'}$ je dvojica zobrazení z definície redukcie matice, ktoré pre triedu ekvivalencie $\sim_r$ resp. $\sim_s$ matice A vrátia príslušný riadok resp. stĺpec matice A'.

Teraz pre grafy G a G' zostrojíme zobrazenia $\phi_U : U \to U'$ a $\phi_V : V \to V'$ z definície bipartitne indukovaného podgrafu.

Vezmime teda vrchol $u \in U$ a hľadajme hodnotu $\phi_U(u)$. Vzhľadom na to, že G je graf priradený k matici A, vrchol u je triedou ekvivalencie $\sim_r$ pre maticu A. Vrchol u teda možno zobraziť zobrazením ψ_r na nejaký riadok i matice A'. Matica A' je redukovaná, takže trieda $[i]_{r,A'}$ je jednoprvková (obsahuje iba i). Množina $\{i\}$ je ale súčasne vrcholom z množiny U', bude teda výslednou hodnotou. Zobrazenia ϕ_U a ϕ_V teda definujeme takto:

$$\phi_U(u) = \{\psi_r(u)\} \qquad \phi_V(v) = \{\psi_s(v)\}$$

Nakoľko zobrazenia ψ_r aj ψ_s sú injektívne, nie je ťažké vidieť, že aj ϕ_U a ϕ_V sú injektívne. Zostáva dokázať, že pre všetky $u \in U$ a $v \in V$ platí, že dvojica (u, v) je hranou v G práve vtedy, keď dvojica $(\phi_U(u), \phi_V(v))$ je hranou v G'. Avšak z vlastností použitých funkcií a z predchádzajúcich úvah vyplýva:

$$\begin{aligned}(u,v) \in E \iff & (\forall i \in u)(\forall j \in v)(A(i,j) = 1) \iff A'(\psi_r(u), \psi_s(v)) = 1 \iff \\ \iff & (\{\psi_r(u)\}, \{\psi_s(v)\}) \in E' \iff \\ \iff & (\phi_U(u), \phi_V(v)) \in E'.\end{aligned}$$

□

Charakterizácia pomocou matíc I.

Vráťme sa teraz späť k charakterizácii správovej zložitosti funkcií. Vo vete 2.41 sme k funkcii $f \in \mathcal{F}_{p,n}$ zostrojili reláciu R, ktorá má rovnakú správovú zložitosť. Teraz ukážeme ako možno charakterizovať simultánnu správovú zložitosť relácie R. Myšlienku tejto charakterizácie popíšeme najprv neformálne, potom uvedieme vetu s podrobným dôkazom.

Uvažujme nejakú podmnožinu g relácie R, ktorá by bola funkciou, t.j. pre každú štvoricu (x, y, z_1, z_2) by existovalo práve jedno i také, že $(x, y, z_1, z_2, i) \in g$. Správovú zložitosť takejto funkcie možno pomerne jednoducho charakterizovať. Zostrojme k funkcii g maticu takú, že jej riadky budú zodpovedať dvojiciam vstupov prvého hráča, stĺpce dvojiciam vstupov druhého hráča a jednotlivé prvky matice budú funkčné hodnoty. Ak pre nejaké dve dvojice vstupov hráča 1 sú zodpovedajúce riadky matice navzájom rôzne, hráč 1 musí poslať pre tieto dvojice navzájom rôzne správy. Podobne hráč 2 musí rozlíšiť rôznymi správami také dvojice vstupov, pre ktoré sú zodpovedajúce stĺpce rôzne. Optimálny protokol pre g teda použije $\lceil \log a \rceil + \lceil \log b \rceil$ bitov, kde a resp. b je počet rôznych riadkov resp. stĺpcov uvažovanej matice.

Ľubovoľný simultánny protokol počítajúci reláciu R však počíta aj nejakú funkciu $g \subseteq R$, pretože pre každú štvoricu vstupov dá protokol jednoznačnú odpoveď (protokol je deterministický) — táto odpoveď bude funkčnou hodnotou funkcie g pre danú štvoricu vstupov. Simultánnu komunikačnú zložitosť relácie R je teda možno charakterizovať ako minimum zo simultánnych komunikačných zložitostí funkcií, ktoré sú podmnožinami relácie R.

Označenie 2.49 *Nech $f \in \mathcal{F}_{p,n}$. Označme $\mathcal{M}_f$ množinu binárnych matíc A typu $pn \times pn$ takých, že pre každé $i, j \in Z_p$ a $k \in Z_n$ platí*

$$A(kp + j, kp + i) = f(i, j, k).$$

Matice v $\mathcal{M}_f$ sú teda matice zodpovedajúce funkciám, ktoré sú podmnožinou relácie R.

Veta 2.50 *Nech $f \in \mathcal{F}_{p,n}$. Potom*

$$\mathrm{M}_{\varepsilon S}(f) = \min_{A\in\mathcal{M}_f}\{\max\{\lceil\log b\rceil, \lceil\log c\rceil\} | \, b \text{ je počet rôznych riadkov v } A, \; c \text{ je počet rôznych stĺpcov v } A\}.$$

Dôkaz: Dokážeme najprv, že uvedený výraz je horným ohraničením zúženej simultánnej správovej zložitosti funkcie f. Vezmime maticu A, na ktorej sa dosahuje minimum. Nech má táto matica b rôznych riadkov a c rôznych stĺpcov. Zostrojíme protokol, v ktorom rôznym riadkom v A (t.j. rôznym triedam ekvivalencie $[i]_{r,A}$) priradíme rôzne správy dĺžky $\lceil\log b\rceil$ a rôznym stĺpcom v A priradíme rôzne správy dĺžky $\lceil\log c\rceil$. Pripomeňme, že riadkom resp. stĺpcom zodpovedajú vstupy (y, z) resp. (x, z). Hráč 1, ak dostane vstup (y, z), pošle správu, ktorá zodpovedá triede ekvivalencie $[pz + y]_{r,A}$ a podobne hráč 2 pre vstup (x, z) pošle správu prislúchajúcu k triede ekvivalencie $[pz + x]_{s,A}$. Hráč 4 po prijatí trojice správ (v_1, v_2, ε) nájde riadok i a stĺpec j, také, že ich triedam ekvivalencie zodpovedajú správy v_1 a v_2 a ako výsledok oznámi hodnotu $A(i, j)$.

Takto zostrojený protokol má požadovanú správovú zložitosť $\max\{\lceil\log b\rceil, \lceil\log c\rceil\}$. Zostáva si uvedomiť, že naozaj vždy vráti správny výsledok. To dokážeme sporom – predpokladajme, že pre nejakú trojicu vstupov (x, y, z) protokol vráti nesprávny výsledok. To ale znamená, že pri zostavovaní funkcie m_4 sme použili hodnotu, ktorá nie je na priesečníku riadku $i = pz + y$ a stĺpca $j = pz + x$, ale hodnotu, ktorá je na priesečníku riadku i' a j', pričom ale $i' \in [i]_{r,A}$ a tiež $j' \in [j]_{s,A}$. Teda s využitím lemy 2.42 dostávame $f(x, y, z) = a_{i,j} = a_{i',j'} \neq f(x, z, y)$, čo je spor, takže protokol naozaj počíta funkciu f.

Vezmime teraz zúžený simultánny protokol $P = (m_1, m_2, m_3, m_4)$ počítajúci f so simultánnou správovou zložitosťou $\mathrm{M}_{\varepsilon S}$. K tomuto protokolu zostrojíme maticu $A \in \mathcal{M}_f$, ktorá bude mať najviac $b = |H(m_1)|$ rôznych riadkov a najviac $c = |H(m_2)|$ rôznych stĺpcov (kde $H(m_i)$ je množina všetkých správ posielaných hráčom i). Keďže $\mathrm{M}_{\varepsilon S}(f) = \mathrm{M}_{\varepsilon S}(P) \geq \max\{\lceil\log b\rceil, \lceil\log c\rceil\}$, je výraz uvedený vo vete aj dolným odhadom miery $\mathrm{M}_{\varepsilon S}(f)$.

Zostrojme maticu A: nech $i, j \in Z_{pn}$. Potom i možno zapísať ako $pz_1 + y$ ($y = i \bmod p$ a $z_1 = \lfloor i/p\rfloor$) a podobne j možno zapísať ako $pz_2 + x$. Nech teraz $v_1 = m_1(y, z_1)$ a $v_2 = m_2(x, z_2)$. Ak je funkcia m_4 pre vstup (v_1, v_2, ε) definovaná, potom $A(i, j)$ bude rovné $m_4(v_1, v_2, \varepsilon)$, v opačnom prípade položíme $A(i, j) = 0$.

O takto zostrojenej matici A najprv ukážeme, že skutočne patrí do množiny $\mathcal{M}_f$. Vezmime teda $x, y \in Z_p$ a $z \in Z_n$ ľubovoľné. Dostávame $A(zp + y, zp + x) = m_4(m_1(y, z), m_2(x, z)) = f(x, y, z)$ (druhá rovnosť vyplýva z korektnosti protokolu P).

Zostáva ukázať, že počet rôznych riadkov matice je najviac b a počet rôznych stĺpcov je najviac c. Uvedomme si, že ak pre nejaké dve dvojice vstupov (y_1, z_1) a (y_2, z_2) hráč 1 pošle rovnakú správu v_1, tak zodpovedajúce riadky ($pz_1 + y_1$ a $pz_2 + y_2$) budú rovnaké (hodnota $A(i, j)$ závisí iba od v_1 a v_2, pričom v_2 závisí iba od čísla stĺpca, nie od riadku). Počet rôznych riadkov v matici A teda nepresiahne počet rôznych správ posielaných hráčom 1 v protokole P, čo je presne hodnota b. Symetricky možno dokázať, že počet rôznych stĺpcov v A nepresiahne hodnotu c. $\square$

Neformálne si charakterizáciu uvedenú v predchádzajúcej vete môžeme predstaviť tak, že zostrojíme maticu typu $pn \times pn$, ktorá bude mať hodnoty 0, 1 a nedefinované. Hodnoty 0 a 1 budú na tých miestach, ktoré zodpovedajú funkčným hodnotám funkcie f (t.j. prvky tvaru $A(pk+i, pk+j)$ pre $k \in Z_n$ a $i, j \in Z_p$). Na ostatných miestach budú nedefinované hodnoty. Definované hodnoty teda tvoria n podmatíc typu $p \times p$ umiestnených okolo hlavnej uhlopriečky matice. $\mathcal{M}_f$ je množina všetkých matíc, ktoré dostaneme nahradením nedefinovaných hodnôt hodnotami 0 a 1. Úlohu minimalizovať počet správ posielaných jednotlivými hráčmi sme teda previedli na úlohu doplniť 0 a 1 do takejto nedoplnenej matice tak, aby sme minimalizovali počet rôznych riadkov a stĺpcov.

Príklad: Ako príklad uvedieme maticu zodpovedajúcu funkcii $\mathit{shift}^p(x, y, z) = z((x+y) \bmod p)$ (pozri označenie 2.16), kde z predstavuje p-bitový reťazec, $z(i)$ je jeho i-ty bit a x a y sú čísla zo Z_p.

Vľavo vidíme hodnoty nedoplnenej matice. Voľné miesta zodpovedajú nedefinovaným hodnotám. Vpravo je jedna z matíc z $\mathcal{M}_{\mathit{shift}^p}$. V celej matici existujú dva rôzne riadky a dva rôzne stĺpce, t.j. pre $p = 2$ môžeme funkciu počítať protokolom, v ktorom každý pošle iba jeden bit.

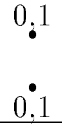
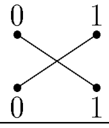
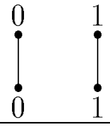
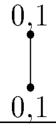
$$
\begin{array}{|cc|cc|cc|cc|}
\hline
0 & 0 & & & & & & \\
0 & 0 & & & & & & \\
\cline{1-4}
 & & 0 & 1 & & & & \\
 & & 1 & 0 & & & & \\
\cline{3-6}
 & & & & 1 & 0 & & \\
 & & & & 0 & 1 & & \\
\cline{5-8}
 & & & & & & 1 & 1 \\
 & & & & & & 1 & 1 \\
\hline
\end{array}
\qquad
\begin{array}{|cc|cc|cc|cc|}
\hline
\mathbf{0} & \mathbf{0} & 0 & 1 & 1 & 0 & 0 & 0 \\
\mathbf{0} & \mathbf{0} & 0 & 1 & 1 & 0 & 0 & 0 \\
\cline{1-4}
0 & 0 & \mathbf{0} & \mathbf{1} & 1 & 0 & 0 & 0 \\
1 & 1 & \mathbf{1} & \mathbf{0} & 0 & 1 & 1 & 1 \\
\cline{3-6}
0 & 0 & 0 & 1 & \mathbf{1} & \mathbf{0} & 0 & 0 \\
1 & 1 & 1 & 0 & \mathbf{0} & \mathbf{1} & 1 & 1 \\
\cline{5-8}
1 & 1 & 1 & 0 & 0 & 1 & \mathbf{1} & \mathbf{1} \\
1 & 1 & 1 & 0 & 0 & 1 & \mathbf{1} & \mathbf{1} \\
\hline
\end{array}
$$

Charakterizácia pomocou bipartitných grafov

V predchádzajúcej časti sme charakterizovali správovú zložitosť pomocou počtu rôznych riadkov a stĺpcov určitých matíc. V tejto časti budeme v úvahách pokračovať a prevedieme túto charakterizáciu do teórie grafov.

Označenie 2.51 *Nech $f \in \mathcal{F}_{p,n}$ a nech $k \in Z_n$. Označme $X_{f,k}$ binárnu maticu typu $p \times p$, pre ktorú platí $X_{f,k}(i, j) = f(j, i, k)$. Ďalej označme $G_{f,k} = (U_{f,k}, V_{f,k}, E_{f,k})$ bipartitný graf priradený matici $X_{f,k}$.*

Príklad: Uvažujme opäť funkciu $f = \mathit{shift}^p$ z množiny $\mathcal{F}_{p,2^p}$, t.j. pre funkciu f platí $f(x, y, z) = z((x+y) \bmod p)$, kde parameter z budeme chápať ako binárny zápis čísla zo Z_{2^p}. Nasledujúca tabuľka pre $p = 2$ obsahuje pre každé $z \in Z_{2^p}$ v druhom riadku maticu $X_{f,k}$ a v treťom riadku graf $G_{f,z}$. V grafoch $G_{f,z}$ je vždy horná partícia $U_{f,z}$ a dolná $V_{f,z}$. Vrcholy grafu $G_{f,z}$ sú triedy ekvivalencie $\sim_r$ a $\sim_s$ pre maticu $X_{f,z}$. Na obrázku sú jednotlivé vrcholy označené zoznamom prvkov príslušnej triedy ekvivalencie. V grafoch $G_{f,00}$ a $G_{f,11}$ sú oba riadky aj oba stĺpce rovnaké, takže príslušná trieda ekvivalencie je dvojprvková, ostatné triedy ekvivalencie sú jednoprvkové.

Binárny zápis z	00	01	10	11
Matica $X_{f,z}$	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$
Graf $G_{f,z}$				

Označenie 2.52 *Nech* $f \in \mathcal{F}_{p,n}$*. Označme* $\mathcal{G}_f$ *množinu bipartitných grafov* $G = (U, V, E)$ *takých, že pre každé* $z \in Z_n$ *je graf* $G_{f,z}$ *bipartitne indukovaným podgrafom grafu* G*.*

Veta 2.53 *Nech* $f \in \mathcal{F}_{p,n}$*. Potom*

$$\mathrm{M}_{\varepsilon S}(f) = \min\left\{\max\{\lceil \log |U| \rceil,\ \lceil \log |V| \rceil\} \mid \exists G = (U, V, E) \in \mathcal{G}_f\right\}.$$

Dôkaz: V dôkaze využijeme vetu 2.50. V prvej časti dôkazu pre každú maticu $A \in \mathcal{M}_f$ zostrojíme bipartitný graf $G = (U, V, E) \in \mathcal{G}_f$ taký, že veľkosť množiny U bude rovnaká ako počet rôznych riadkov v A a veľkosť množiny V bude rovnaká ako počet rôznych stĺpcov v A.

V druhej časti dôkazu naopak k ľubovoľnému grafu $G = (U, V, E) \in \mathcal{G}_f$ zostrojíme maticu $A \in \mathcal{M}_f$ s najviac $|U|$ rôznymi riadkami a najviac $|V|$ rôznymi stĺpcami.

Takto odvodíme rovnosť:

$$\begin{aligned} & \min\{\max\{\lceil \log b \rceil,\ \lceil \log c \rceil\} \mid (\exists A \in \mathcal{M}_f)(b \text{ je počet rôznych riadkov v } A \text{ a} \\ & \qquad\qquad\qquad\qquad\qquad\qquad\qquad c \text{ je počet rôznych stĺpcov v } A)\} = \\ = \ & \min\{\max\{\lceil \log |U| \rceil,\ \lceil \log |V| \rceil\} \mid \exists G = (U, V, E) \in \mathcal{G}_f\} \end{aligned}$$

Z tejto rovnosti už podľa vety 2.50 dostávame požadované tvrdenie.

Prvá časť dôkazu. Majme maticu $A \in \mathcal{M}_f$. Hľadaným grafom $G = (U, V, E)$ bude bipartitný graf priradený k matici A. Vrcholy z partície U teda zodpovedajú navzájom rôznym riadkom matice A a podobne vrcholy z partície B zodpovedajú navzájom rôznym stĺpcom matice A. Množiny U a V majú teda požadované počty prvkov.

Treba ešte ukázať, že graf G patrí do množiny $\mathcal{G}_f$, t.j. pre každé $z \in Z_n$ je graf $G_{f,z} = (U_{f,z}, V_{f,z}, E_{f,z})$ jeho bipartitne indukovaným podgrafom.

Zvoľme $z \in Z_n$. Pre maticu $X_{f,z}$ z definície platí $X_{f,z}(i,j) = f(j,i,z) = A(pz + i, pz + j)$, je teda vybranou podmaticou matice A. Ďalej podľa definície je graf $G_{f,z}$ grafom priradeným matici $X_{f,z}$. Z lemy 2.47 teda dostávame, že graf $G_{f,z}$ je bipartitne indukovaným podgrafom grafu G.

Druhá časť dôkazu. Majme bipartitný graf $G = (U, V, E) \in \mathcal{G}_f$. Zostrojíme k nemu maticu $A \in \mathcal{M}_f$ typu $pn \times pn$, ktorá bude mať najviac $|U|$ rôznych riadkov a najviac

$|V|$ rôznych stĺpcov. Maticu A budeme konštruovať takto: zostrojíme zobrazenie $\psi_r : Z_{pn} \to U$, ktoré každému riadku priradí vrchol z partície U a zobrazenie $\psi_s : Z_{pn} \to V$, ktoré každému stĺpcu priradí vrchol z partície V. Potom hodnota $A(j,l)$ bude 1, ak sú vrcholy $\psi_r(j)$ a $\psi_s(l)$ spojené hranou a 0 v opačnom prípade.

Pre m-tý riadok (resp. stĺpec) matice A, kde $m = kp+i$, ($k \in Z_n$, $i \in Z_p$), určíme hodnoty $\psi_r(m)$ (resp. $\psi_s(m)$) takto. Nech $G_{f,k} = (U_{f,k}, V_{f,k}, E_{f,k})$ je bipartitne indukovaný podgraf grafu G, ktorý je priradený matici $X_{f,k}$. Pripomeňme, že vrcholy z $U_{f,k}$ (z $V_{f,k}$) sú triedy ekvivalencie riadkov (stĺpcov) matice $X_{f,k}$. Nech ϕ_U a ϕ_V sú injektívne zobrazenia z definície bipartitne indukovaného podgrafu, t.j. nech pre ne platí

$$(\forall u \in U_{f,k})(\forall v \in V_{f,k})((u,v) \in E_{f,k} \iff (\phi_U(u), \phi_V(v)) \in E). \tag{2.6}$$

Hodnoty $\psi_r(kp+i)$ a $\psi_s(kp+i)$ zostrojíme takto:

$$\psi_r(kp+i) = \phi_U([i]_{r,X_{f,k}}) \qquad \psi_s(kp+i) = \phi_V([i]_{s,X_{f,k}})$$

Hodnotu $\psi_r(kp+i)$ teda dostaneme takto: vezmeme maticu $X_{f,k}$ (ktorá obsahuje hodnoty funkcie f, ak je tretím vstupom k) a vyberieme z nej i-ty riadok. Graf $G_{f,k}$ je bipartitný graf priradený k $X_{f,k}$, t.j. prvky partície $U_{f,k}$ zodpovedajú navzájom rôznym riadkom matice $X_{f,k}$. Vezmime vrchol $v \in U_{f,k}$, ktorý zodpovedá riadku i matice $X_{f,k}$ ($v = [i]_{r,X_{f,k}}$). K riadku matice A sme teda najprv našli riadok matice $X_{f,k}$ a potom k nemu prislúchajúci vrchol v grafu $G_{f,k}$. Nakoniec využijeme vzťah grafu $G_{f,k}$ ku grafu G určený zobrazením ϕ_U a položíme $\psi_r(kp+i)$ rovné $\phi_U(v)$.

Treba ešte ukázať, že takto definované zobrazenia spĺňajú naše požiadavky, t.j. že pomocou nich skonštruovaná matica A patrí do množiny $\mathcal{M}_f$ a že má najviac $|U|$ riadkov a $|V|$ stĺpcov.

Druhá z podmienok sa dokáže veľmi jednoducho. Ľahko totiž možno nahliadnuť, že ak pre nejaké i a j platí $\psi_r(i) = \psi_r(j)$, potom sa i-ty a j-ty riadok matice A rovnajú. Zobrazenie ψ_r však nadobúda najviac $|U|$ rôznych hodnôt, preto je v matici A najviac $|U|$ navzájom rôznych riadkov. Podobne možno postupovať pre stĺpce.

Dokážme teda, že $A \in \mathcal{M}_f$. Znamená to dokázať, že pre všetky $k \in Z_n$ a pre všetky $i,j \in Z_p$ platí $A(kp+i, kp+j) = f(j,i,k)$. Nech $X^* = X_{f,k}$ a nech ϕ_U a ϕ_V sú zobrazenia spĺňajúce vzťah (2.6).

Hodnota $A(kp+i, kp+j)$ je rovná jednej práve vtedy, keď $(\psi_r(kp+i), \psi_s(kp+j)) \in E$. Vieme však, že $\psi_r(kp+i) = \phi_U([i]_{r,X^*})$ a $\psi_s(kp+j) = \phi_V([j]_{s,X^*})$. Z tohoto faktu a zo vzťahu (2.6) máme, že

$$(\psi_r(kp+i), \psi_s(kp+j)) \in E \iff ([i]_{r,X^*}, [j]_{s,X^*}) \in E_{f,k}.$$

Nakoľko $G_{f,k}$ je bipartitný graf priradený matici X^*, platí

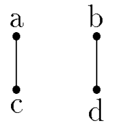
$$([i]_{r,X^*}, [j]_{s,X^*}) \in E_{f,k} \iff X^*(i,j) = 1.$$

Nakoniec dodajme, že $X^*(i,j) = f(j,i,k)$ a teda máme

$$A(kp+i, kp+j) = 1 \iff f(j,i,k) = 1,$$

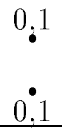
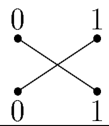
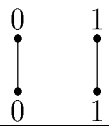
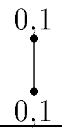
takže $A \in \mathcal{M}_f$. □

Príklad: Tento príklad nadväzuje na príklad zo strany 65. Vtedy sme pre funkciu $f = \mathit{shift}^p$ ukázali jednotlivé grafy $G_{f,k}$ a matice $X_{f,k}$ Teraz pre túto funkciu ukážeme graf $G \in \mathcal{G}_f$ a k tomuto grafu zostrojíme maticu A tak, ako je to popísané v druhej časti dôkazu predchádzajúcej vety.



Graf G

Na obrázku vidíme graf $G = (U, V, E)$, pričom $U = \{a, b\}$ a $V = \{c, d\}$. Dole v tabuľke je pre každé k znázornená matica $X_{f,k}$, bipartitný graf $G_{f,k}$ aj zobrazenia ϕ_U a ϕ_V, ktoré dokumentujú, že príslušný graf $G_{f,k}$ je bipartitne indukovaným podgrafom grafu G.

Binárny zápis z	00	01	10	11
Matica $X_{f,z}$	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$
Graf $G_{f,z}$				
Zobrazenie ϕ_U	$\phi_U(0,1) = a$	$\phi_U(0) = a$, $\phi_U(1) = b$	$\phi_U(0) = a$, $\phi_U(1) = b$	$\phi_U(0,1) = a$
Zobrazenie ϕ_V	$\phi_V(0,1) = d$	$\phi_V(0) = d$ $\phi_V(1) = c$	$\phi_V(0) = c$ $\phi_V(1) = d$	$\phi_V(0,1) = c$

V konštrukcii matice A najprv potrebujeme zostrojiť zobrazenia ψ_r a ψ_s. Tie zostavíme jednoducho podľa predchádzajúcej tabuľky - hodnotu $\phi_r(zp + i)$ získame tak, že v tabuľke vezmeme stĺpec zodpovedajúci z, v tomto stĺpci nájdeme vrchol grafu, ktorý zodpovedá i-temu riadku matice X a výsledkom bude hodnota ϕ_U pre tento vrchol:

z	0		1		2		3	
i	0	1	0	1	0	1	0	1
$x = zp + i$	0	1	2	3	4	5	6	7
$\psi_r(x)$	a	a	a	b	a	b	a	a
$\psi_r(x)$	d	d	d	c	c	d	c	c

Teraz už položíme $m_{i,j}$ rovné 1 práve vtedy, keď v grafe G sú vrcholy $\psi_r(i)$ a $\psi_s(j)$ spojené hranou. Dostávame maticu A uvedenú vpravo. Hodnoty 1 sú v tejto matici na priesečníkoch riadkov označených a a stĺpcov označených c a tiež na priesečníkoch b a d. Ako vidíme, je to naozaj matica z $\mathcal{M}_f$ a má dva rôzne riadky a dva rôzne stĺpce.

$$
\begin{array}{c|cccccccc|}
 & d & d & d & c & c & d & c & c \\
\hline
a & \mathbf{0} & \mathbf{0} & 0 & 1 & 1 & 0 & 1 & 1 \\
a & \mathbf{0} & \mathbf{0} & 0 & 1 & 1 & 0 & 1 & 1 \\
a & 0 & 0 & \mathbf{0} & \mathbf{1} & 1 & 0 & 1 & 1 \\
b & 1 & 1 & \mathbf{1} & \mathbf{0} & 0 & 1 & 0 & 0 \\
a & 0 & 0 & 0 & 1 & \mathbf{1} & \mathbf{0} & 1 & 1 \\
b & 1 & 1 & 1 & 0 & \mathbf{0} & \mathbf{1} & 0 & 0 \\
a & 0 & 0 & 0 & 1 & 1 & 0 & \mathbf{1} & \mathbf{1} \\
a & 0 & 0 & 0 & 1 & 1 & 0 & \mathbf{1} & \mathbf{1} \\
\hline
\end{array}
$$

Charakterizácia pomocou matíc II.

Doteraz sme mieru $\mathrm{M}_{\varepsilon S}(f)$ charakterizovali pomocou matíc a bipartitných grafov. V tejto časti sa vrátime späť k maticiam, pričom poskytneme inú charakterizáciu. V predchádzajúcej charakterizácii pomocou matíc sme hľadali maticu, v ktorej boli matice $X_{f,k}$ podmaticami na vopred daných štvorcových výsekoch. Počet rôznych správ v protokole potom zodpovedal počtu navzájom rôznych riadkov a stĺpcov v takto zostrojenej matici. Teraz budeme postupovať inak: namiesto matíc $X_{f,k}$ budeme uvažovať ich redukcie a správovú zložitosť funkcie budeme charakterizovať pomocou množiny matíc, pre ktoré sú všetky redukcie matíc $X_{f,k}$ vybranými podmaticami.

Uvedomme si ešte, že ak je niektorá redukcia matice A vybranou podmaticou matice B, tak každá redukcia matice A je vybranou podmaticou matice B (jednotlivé redukcie sa líšia len poradím riadkov a stĺpcov).

Označenie 2.54 *Nech $f \in \mathcal{F}_{p,n}$. Označme $\mathcal{M}'_f$ množinu všetkých binárnych matíc A takých, že pre každé $k \in Z_n$ je redukcia matice $X_{f,k}$ vybranou podmaticou matice A.*

Veta 2.55 *Nech $f \in \mathcal{F}_{p,n}$. Potom*

$$\mathrm{M}_{\varepsilon S}(f) = \min_{A \in \mathcal{M}'_f} \{\max\{\lceil \log b \rceil, \lceil \log c \rceil\} \mid A \text{ je typu } b \times c\}.$$

Dôkaz: Dôkaz rozdelíme na dve časti. V prvej časti dokážeme, že výraz na pravej strane je horným ohraničením $\mathrm{M}_{\varepsilon S}(f)$ a druhej časti, že je aj dolným ohraničením.

Prvá časť dôkazu. V tejto časti využijeme vetu 2.53. Majme $A \in \mathcal{M}'_f$ typu $b \times c$ a zostrojíme bipartitný graf $G = (U, V, E) \in \mathcal{G}_f$ taký, že $|U| \leq b$ a $|V| \leq c$. Podľa vety 2.53 existuje protokol so správovou zložitosťou najviac $\max\{\lceil \log |U| \rceil, \lceil \log |V| \rceil\}$, z čoho vyplýva, že tento protokol má zložitosť $\max\{\lceil \log b \rceil, \lceil \log c \rceil\}$.

Hľadaný graf G bude bipartitný graf priradený k matici A. Množina U teda obsahuje triedy ekvivalencie $[i]_{r,A}$, tých je však najviac b. Podobne množina V má najviac c prvkov. O grafe G stačí dokázať už iba to, že patrí do množiny $\mathcal{G}_f$, t.j. že každý z grafov $G_{f,k}$ je bipartitne indukovaným podgrafom grafu G.

Vezmime teda $k \in Z_n$. Nech matica X je redukciou matice $X_{f,k}$ a H nech je bipartitný graf priradený k X. Keďže $A \in \mathcal{M}'_f$, matica X musí byť vybranou podmaticou matice A. Podľa lemy 2.47 dostávame, že H je bipartitne indukovaným podgrafom grafu G.

Máme teda maticu $X_{f,k}$ a jej redukciu X, ďalej graf $G_{f,k}$ priradený k matici $X_{f,k}$ a graf H priradený k X. Z lemy 2.48 dostávame, že graf $G_{f,k}$ je bipartitne indukovaným podgrafom grafu H.

Dokázali sme teda, že graf $G_{f,k}$ je bipartitne indukovaným podgrafom grafu H a H je bipartitne indukovaným podgrafom grafu G. Z tranzitívnosti relácie "byť bipartitne indukovaným podgrafom" dostávame, že $G_{f,k}$ je bipartitne indukovaným podgrafom grafu G.

Druhá časť dôkazu. Podľa vety 2.50 vieme, že

$$\mathrm{M}_{\varepsilon S}(f) = \min_{A \in \mathcal{M}_f}\{\max\{\lceil \log b \rceil, \lceil \log c \rceil\} \mid b \text{ je počet rôznych riadkov v } A, \; c \text{ je počet rôznych stĺpcov v } A\}.$$

Stačí teda pre ľubovoľnú maticu $A \in \mathcal{M}_f$ nájsť maticu $A' \in \mathcal{M}'_f$ takú, že ak A má b rôznych riadkov a c rôznych stĺpcov, tak A' má b riadkov a c stĺpcov.

Hľadaná matica A' je redukcia matice A. Pre každé $k \in Z_n$ je $X_{f,k}$ vybranou podmaticou matice A. Ľahko sa nahliadne, že keďže A' je redukciou A, tak redukcia $X_{f,k}$ bude vybranou podmaticou A'. Teda $A' \in \mathcal{M}'_f$. □

Príklad: Aj v tomto príklade budeme uvažovať funkciu $f = \mathit{shift}^2$. Označme A' maticu

$$A' = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Overíme, že matica A' je naozaj z $\mathcal{M}'_f$. Tabuľka nižšie zobrazuje redukcie jednotlivých matíc $X_{f,k}$ a ich redukcie.

Binárny zápis z	00	01	10	11
Redukcia $X_{f,z}$	$\begin{pmatrix} 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 \end{pmatrix}$

Ľahko vidno, že všetky matice uvedené v tabuľke sú naozaj vybranými podmaticami matice A'. Matica A' je pritom redukciou matice $A \in \mathcal{M}_f$ uvedenej v príklade na strane 68. Naopak, graf $G \in \mathcal{G}_f$ uvedený v tom istom príklade je (po vhodnom preznačení vrcholov) bipartitným grafom priradeným k A'.

2.4.3 Zhrnutie

Ukázali sme charakterizáciu dvoch obmien základného modelu simultánnej komunikačnej zložitosti pomocou pojmov z teórie grafov, resp. pomocou matíc. Nepodarilo sa nám, žiaľ, túto charakterizáciu využiť na nájdenie metódy dolného odhadu simultánnej zložitosti, takže táto otázka zostáva otvorená.

Chceli by sme ešte upozorniť na jednu závažnú vlastnosť uvedených charakterizácií. V diskusii k vete 2.13 sme uviedli, že jedným zo spôsobov, ako ukázať, že funkcia

Shift^n sa nedá počítať obvodom veľkosti $O(n)$ a hĺbky $O(\log n)$ je dokázať, že ak má hráč 1 poslať iba $O(n/\log\log n)$ bitov, tak hráč 2 musí poslať aspoň $\Omega(n^\varepsilon)$ bitov pre niektoré kladné ε. Znamená to zaviesť zložitosť protokolu ako dvojicu (i, j), kde i je dĺžka najdlhšej správy hráča 1 a j je dĺžka najdlhšej správy hráča 2 a skúmať, ktoré dvojice (i, j) sú možnými zložitosťami protokolu pre výpočet skúmanej funkcie f.

Vety v časti 2.4.2 síce všetky charakterizujú správovú zložitosť funkcie, z ich dôkazov sa však ľahko nahliadne, že nimi možno charakterizovať zložitosť funkcie aj ako dvojicu (napr. $(\lceil\log b\rceil, \lceil\log c\rceil)$, kde b je počet riadkov a c je počet stĺpcov nejakej matice z $\mathcal{M}'_f$.

Naše charakterizácie teda neposkytujú iba metódy na výpočet správovej simultánnej zložitosti, ale aj na charakterizáciu zložitosti funkcie pomocou dvojice, a teda možno ich použiť aj na ďalšie skúmanie otvoreného problému, či sa dá *Shift*^{n} počítať booleovským obvodom veľkosti $O(n)$ a hĺbky $O(\log n)$.

Záver

V práci sme sa zaoberali amortizovanou komunikačnou zložitosťou a simultánnou zložitosťou. V obidvoch oblastiach sme uviedli definíciu modelu, prehľad známych výsledkov ako i vlastné čiastkové výsledky.

V oblasti amortizovanej komunikačnej zložitosti sme ukázali, že pre väčšinu funkcií sa amortizovaná komunikačná zložitosť príliš nelíši od komunikačnej zložitosti. Taktiež sme zostrojili funkciu, ktorej amortizovaná zložitosť je presne rovná komunikačnej zložitosti.

V oblasti simultánnej komunikačnej zložitosti sme ukázali odhady zložitosti pomocou základných parametrov a ich optimálnosť a tiež kombinatoricko-grafovú charakterizáciu simultánnej komunikačnej zložitosti.

Aj keď uvedené výsledky neriešia hlavné otvorené problémy v skúmaných oblastiach, prinášajú nové poznatky o skúmaných modeloch súvisiace s týmito problémami. Kombinatorická charakterizácia simultánnej zložitosti by možno mohla byť pomôckou pri hľadaní metód dolných odhadov pre simultánny model.

Literatúra

[1] Alfred V. Aho, Jeffrey D. Ullman, and Mihalis Yannakakis. On notions of information transfer in VLSI circuits. In *Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing*, s. 133–139, Boston, Massachusetts, 25.–27. apríl 1983.

[2] Andris Ambainis. Upper bounds on multiparty communication complexity of shifts. In *13th Annual Symposium on Theoretical Aspects of Computer Science*, vol. 1046 of *Lecture Notes in Computer Science*, s. 631–642, Grenoble, France, 22.–24. február 1996. Springer Verlag.

[3] László Babai, Peter G. Kimmel, and Satyanarayana V. Lokam. Simultaneous messages vs. communication. In *12th Annual Symposium on Theoretical Aspects of Computer Science*, vol. 900 of *Lecture Notes in Computer Science*, s. 361–372, Munich, Germany, 2.–4. marec 1995. Springer Verlag.

[4] Jeff Edmonds, Steven Rudich, Russell Impagliazzo, and Jiří Sgall. Communication complexity towards lower bounds on circuit depth. In *32nd Annual Symposium on Foundations of Computer Science*, s. 249–257, San Juan, Puerto Rico, 1.–4. október 1991. IEEE.

[5] Tomàs Feder, Eyal Kushilevitz, Moni Naor, and Noam Nisan. Amortized communication complexity. *SIAM Journal on Computing*, 24(4):736–750, august 1995.

[6] Juraj Hromkovič. *Communication Complexity and Parallel Computing.* Springer Verlag, 1997.

[7] Russell Impagliazzo, Ran Raz, and Avi Wigderson. A direct product theorem. In *Proceedings of the Ninth Annual Structure in Complexity Theory Conference*, s. 88–96, Amsterdam, The Netherlands, 28. jún–1. júl 1994. IEEE Computer Society Press.

[8] Mauricio Karchmer, Eyal Kushilevitz, and Noam Nisan. Fractional covers and communication complexity (extended abstract). In *Proceedings of the Seventh Annual Structure in Complexity Theory Conference*, s. 262–274, Boston, Massachusetts, 22.–25. jún 1992. IEEE Computer Society Press,.

[9] Mauricio Karchmer, Ran Raz, and Avi Wigderson. Super-logarithmic depth lower bounds via the direct sum in communication complexity. *Computational Complexity*, 5(3/4):191–204, 1995.

[10] Eyal Kushilevitz and Noam Nisan. *Communication Complexity*. Cambridge University Press, 1997.

[11] Satyanarayana V. Lokam. *Algebraic Methods in Computational Complexity: Arithmetic Circuits, Communication Complexity, and Interactive Proof Systems*. PhD thesis, University of Chicago, 1996.

[12] Kurt Mehlhorn and Erik M. Schmidt. Las Vegas is better than determinism in VLSI and distributed computing (extended abstract). In *Proceedings of the Fourteenth Annual ACM Symposium on Theory of Computing*, s. 330–337, San Francisco, California, 5.–7. máj 1982.

[13] Noam Nisan and Avi Wigderson. Rounds in communication complexity revisited. *SIAM Journal on Computing*, 22(1):211–219, február 1993.

[14] A. Orlitsky and A. El Gamal. Communication complexity. In *Yaser S. Abu-Mostafa, Complexity in Information Theory*, s. 16–61. Springer-Verlag, 1988.

[15] Pavel Pudlák, Vojtěch Rödl, and Jiří Sgall. Boolean circuits, tensor ranks, and communication complexity. *SIAM Journal on Computing*, 26(3):605–633, jún 1997.

[16] Leslie G. Valiant. Graph-theoretic arguments in low-level complexity. In J. Gruska, editor, *Mathematical Foundations of Computer Science, 6th Symposium*, vol. 53 of *Lecture Notes in Computer Science*, s. 162–176, Tatranská Lomnica, 5.–9. september 1977. Springer-Verlag.

[17] Andrew C.-C. Yao. Some complexity questions related to distributive computing. In *Conference Record of the Eleventh Annual ACM Symposium on Theory of Computing*, s. 209–213, Atlanta, Georgia, 30. apríl–2. máj 1979.