Algebrai módszerek a Boole-hálózatok elméletében

Szakdolgozat

Írta:	Témavezető:
Varga Dániel	Friedl Katalin

1996.

Tartalomjegyzék

1. Bevezetés

Dolgozatunkban bonyolultságelméleti alsó becsléseket adó módszereket mutatunk be különböző Boole-hálózati modellekre. Ezen módszerek bonyolultságelméleti szempontból közös gyökerűek, de meglepően változatosak az alkalmazott klasszikus matematikai apparátust tekintve. Bizonyításainkban felhasználjuk többek között a lineáris algebra, a lineáris egyenlőtlenségrendszerek elmélete, az approximációelmélet, a racionális törtfüggvények approximációelmélete és a klasszikus többváltozós analízis egyes alapvető eredményeit.

A 2. Fejezetben áttekintjük a Boole-hálózatok bonyolultságelméletének legalapvetőbb fogalmait.

A 3. Fejezetben ismertetjük a dolgozatunk fő tárgyát képező algebrai módszercsalád első és máig leggfontosabb alkalmazását, Smolensky tételét a konstans mélységű, szubexponenciális méretű Boole-hálózatokról [Smo].

A 4. Fejezetben bemutatjuk a diszkrét Fourier-transzformációs technikát, amely az 5., 6. és 7. fejezetben alapvető segédeszközünk lesz. Illusztrációként bizonyítjuk Bruck tételét [Bru].

Az 5. Fejezetben ismertetjük Aspnes, Beigel, Furst és Rudich tételét [ABFR], amely mind a bizonyítás technikáját, mind az eredményt tekintve Smolensky tételének valós számtest feletti analogonja.

A 6. Fejezetben az ε-közelítés fogalmát vizsgáljuk. Egy n-változós polinom akkor ε-közelít egy Boole-függvényt, ha a Boole-függvény értelmezési tartományán legfeljebb ε-nal térnek el. Nisan és Szegedy [NS] nyomán alsó becslést adunk a logikai $Vagy$ függvényt ε-közelítő polinomok fokszámára. A bizonyítás approximációelméleti technikákon alapul.

A 7. Fejezet a szerző önnálló eredményeit tartalmazza az ε-közelítésről. A Farkas Lemma felhasználásával szükséges és elégséges feltételt adunk egy Boole-függvény adott fokszámú polinommal való ε-közelíthetőségére. Megmutatjuk, hogy ez az ereddmény speciális esetként tartalmazza Aspnes et al. 5. Fejezetben tárgyalt Alternatívatételét. Kós Géza eredményére [Kós] támaszkodva valamelyest megjavítjuk a Nisan és Szegedy tételében szereplő konstansokat. A bizonyítás —szemben Nisan és Szegedy bizonyításával— teljesen elemi konstrukción alapul.

A 8. Fejezetben Paturi és Saks [PS] nyomán a paritásfüggvényt számító 2 mélységű THR-hálózatokat vizsgáljuk. Ennek kapcsán bemutatunk egy rokon elemi geometriai problémát, és az azzal kapcsolatos legfontosabb eredményeket. A THR-hálózatok vizsgálatára ezután bevezetjük és alkalmazzuk a racionális törtfüggvényekkel való közelítés mószerét.

A 9. Fejezetben Smolensky tételét [Smo] ismertetjük szimmetrikus kapukat használó hálózatok számítási erejéről. A bizonyítás során az elemi többváltozós analízis módszereit használjuk, a Boole-függvényt interpoláló analitikus függvények k-adrendű parciális deriváltjait vizsgálva.

2. A Boole-hálózatok bonyolultságelméletének alapfogalmai

2.1. Jelölések

Bevezetünk néhány jelölést, amelyek a kombinatorikában és a bonyolultságelméletben standardnak tekinthetők.

$[n]$	$:= \{1, ..., n\}$
2^X	jelöli X hatványhalmazát
$\binom{X}{k}$	jelöli X összes k-elemű halmazainak halmazát
$\binom{X}{\leq k}$	jelöli X összes legfeljebb k-elemű halmazainak halmazát
$\binom{n}{\leq k}$	$:= \sum_{i \in [k]} \binom{n}{i} \quad \left(= \left\lvert \binom{[n]}{\leq k} \right\rvert\right)$

A bonyolultságelméletben a kvantitatív eredményeket hagyományosan ordó-jelölések használatával adják meg, hiszen a bonyolultsági mértékek nagyságrendje legtöbbször lényegesebb, mint az egzakt értékük. Emlékeztetőül:

2.1. Definíció.
$f(n) = O(g(n))$ azt jelenti, hogy létezik olyan $c \in \mathbb{R}, c > 0$, hogy $|f(n)| \leq$ $\leq c|g(n)|$ minden n-re.

$f(n) = o(g(n))$ azt jelenti, hogy minden $c \in \mathbb{R}, c > 0$ számhoz létezik olyan $m \in \mathbb{N}$, hogy minden $n \geq m$-re $|f(n)| < c|g(n)|$.

$f(n) = \Omega(g(n))$ azt jelenti, hogy létezik olyan $c \in \mathbb{R}, c > 0$, hogy $|f(n)| \geq$ $\geq c|g(n)|$ minden n-re.

$f(n) = \Theta(g(n))$ azt jelenti, hogy $f(n) = \Omega(g(n))$ és $f(n) = \Theta(g(n))$.

Önnálló jelölést vezetünk be néhány gyakran előforduló nagyságrendre:

$$\begin{array}{lcl} const & := & O(1) \\ poly(n) & := & n^{O(1)} \\ lin(n) & := & O(n) \\ polylog(n) & := & log(n)^{O(1)} \\ subexp(n) & := & 2^{n^{o(1)}} \\ qpoly(n) & := & 2^{polylog(n)} \; (= n^{polylog(n)}) \end{array}$$

A továbbiakban — hacsak külön nem jelezzük az ellenkezőjét — a dolgozatban szereplő függvénysorozatok függő változója mindig n, az éppen vizsgált Boole-függvény változóinak száma. Ezért, ha ez nem okoz zavart, az n argumentumot nem írjuk ki.

2.2. Boole-hálózat, Elemi Boole-függvények

2.2. Definíció. $V := \{-1, +1\}$. **Boole-függvénynek** *nevezünk egy tetszőleges $V^n \longrightarrow V$ függvényt. A V^n-et néha kockának, elemeit csúcsoknak fogjuk nevezni.*

Megjegyzés. Ezen definíció mellett a $+1$ a hagyományosan használt $Igaz$ és a -1 a $Hamis$ logikai értéknek felel meg.

A Boole-hálózat legáltalánosabb definíciója a következő:

2.3. Definíció. **Boole-hálózatnak** *nevezünk egy aciklikus irányított gráfot, amelynek nem forrás csúcsai Boole-függvényekkel vannak címkézve, méghozzá úgy, hogy a csúcsba menő élek azonosítva vannak a Boole-függvény változóival. A nem forrás csúcsokat* **kapuknak** *nevezzük. Feltesszük, hogy a hálózatnak csak egy nyelője van. A hálózat forrásait* **bemeneteknek**, *nyelőjét* **kimenetnek** *nevezzük. A hálózat által kiszámított függvény értelemszerűen, rekurzíve definiálódik a bemenetektől a kimenetig. Egy kapu* **bemenetei** *azok a kapuk, amelyekből él indul az adott a kapuba. A kapu* **ősei** *az összes kapuk, melyekből az adott kapu elérhető irányított úton.*

Mint látjuk, a Boole-hálózat minden csúcsa, és a hálózat maga is egy-egy Boole-függvényt számít.

2.4. Definíció. *A hálózat k-***dik szintje** *azon kapuk halmaza, amelyek minden ősüktől legfeljebb k távolságra vannak, de van olyan ősük, amelytől pontosan k távolságra vannak.* **Szintezettnek** *nevezzük a hálózatot, ha csak egymás utáni szintek között megy él benne.*

Ha a kimenet kiszámítását időbeli folyamatnak tekintjük, akkor a k-dik szint azokból a kapukból áll, amelyek a számítás k-dik fázisában számítják ki a kimenetüket.

2.5. Definíció. **Topologikus sorrendnek** *nevezzük a kapuk egy tetszőleges felsorolását, amely kompatibilis a hálózat gráfjával, tehát amelyben minden kaput megelőznek az ősei.*

A Boole-hálózat definíciója megengedi a kapukban tetszőleges Boole-függvények használatát. Bonyolultságelméleti szempontból az érdekes helyzet az, ha a csúcsokban nem engedünk meg akármilyen függvényt, csak valamilyen értelemben egyszerűeket. Attól függően, hogy milyen függvényeket engedünk meg, különféle hálózatosztályokhoz juthatunk.

Megjegyzés. Egy olyan függvény, mint például az AND, valójában függvények családját jelenti, hiszen AND van kétváltozós, háromváltozós...

2.6. Definíció. *A leggyakrabban használt Boole-függvények:*

AND:	$+1$, *ha minden bemenet* $+1$, -1 *egyébként.*
OR:	-1, *ha minden bemenet* -1, $+1$ *egyébként.*
MAJ:	$+1$, *ha a bemenetek legalább fele* $+1$, -1 *egyébként.*
MOD_m:	$+1$, *ha az egyesek száma osztható* m*-mel,* -1 *egyébként.*
$EXACT_k$:	$+1$, *ha az egyesek száma pontosan* k, -1 *egyébként.*
PAR:	*a bemenetek szorzata. Ez egy* ± 1 *szorzótól eltekintve éppen* MOD_2.

Az eddig említettek mind **szimmetrikus** Boole-függvények, tehát a kimenet csak a bemenenet egyeseinek számától függ. A szimmetrikus Boole-függvények családját $SYMM$-mel jelöljük.

THR: (lineáris küszöbfüggvény) A MAJ általánosítása. A bemenetek valamely lineáris kombinációjából kivon egy küszöbértéket, és pontosan akkor ad 1-et, ha az eredmény nemnegatív.

2.7. Definíció. *Ha* $GATE_1, GATE_2, ...$ *Boole-függvény-osztályok, akkor* $\{GATE_1, GATE_2, ...\}$**-hálózatnak** *nevezzük azon Boole-hálózatok osztályát, amelyeknek a kapui ezen Boole-függvény-osztályok elemei.*

Például $\{AND, NOT\}$-hálózat azon Boole-hálózatok összességét jelenti, amelyeknek kapui kizárólag AND és NOT függvényeket számítanak.

2.3. A Boole-hálózatok mértékei

2.8. Definíció.
A hálózat **mérete** *a kapuk száma,*
A hálózat **mélysége** *a szintek száma.*
A **befok** *a maximális befok a hálózat gráfjának csúcsain.*
A **rend** *a maximális befok az első szintű kapuk között.*

Ha feltesszük, hogy a THR-függvény küszöbértéke és bemeneteinek súlyai egész számok, az ugyan nem változtat a THR függvényosztályon, de ekkor vizsgálhatjuk a kapu egy érdekes mértékét:

2.9. Definíció. *Egy THR-kapu* **súlya** *az együtthatók (beleértve a küszöbértéket) abszolútérték-összege.*

A Boole-hálózat definíciójában megengedtük a párhuzamos éleket is. Ezekre a gyakorlatban azért nincs szükség, mert az építőelemként használt függvények számítási képességét ez általában nem növeli. Például egy AND kapuba futó párhuzamos élek egyszerűen egy kivételével elhagyhatók, és egy PAR kapuba futó párhuzamos élek esetében csak a darabszámuk paritása számít.

Más a helyzet a MAJ kapukkal. Ha modellünkben MAJ kapukat használunk, és nem teszünk megkötést a párhuzamos élekről, akkor könnyen modellezhetjük az általános THR-függvényt egyetlen MAJ-kapuval. Ezért MAJ-kapukat használó modellekben hasznos mérték a gráf éleinek száma. Ezt szokták a hálózat **élkomplexitásának** nevezni. A párhuzamos éleket használó MAJ kapuról THR kapukra áttérve ez lényegében éppen a hálózat THR-kapuinak összsúlya, amit a THR-hálózat **súlyának** nevezünk.

2.4. Függvénysorozatok, Hálózat-sorozatok

2.10. Definíció. **Boole-függvény-sorozatnak** *nevezzünk egy $\{f_{n_i} : i \in \mathbb{N}\}$ sorozatot, ha f_{n_i} egy n_i-változós Boole-függvény, és $\{n_i\}$ természetes számok egy szigorúan monoton növő sorozata.*

2.11. Definíció. **Hálózat-sorozatnak** *nevezünk egy $\{H_{n_i} : i \in \mathbb{N}\}$ sorozatot, ha H_{n_i} egy n_i bemenetű hálózat, és $\{n_i\}$ természetes számok egy szigorúan monoton növő sorozata.*
Értelemszerű módon a hálózatsorozat akkor **számítja** *a függvénysorozatot, ha minden i-re H_{n_i} kimenete f_{n_i}.*

2.5. Bonyolultsági osztályok

Tekintsünk egy modellt, egy vagy több mértékkel. Ha a mértékekre valamilyen felső korlátokat követelünk meg, ahol a felső korlát lehet akár egzakt (például 3 mélységű hálózat), akár nagyságrendi (például *qpoly* méretű hálózat), akkor **hálózat-osztályt** definiáltunk.

Felhívjuk a figyelmet arra, hogy a hálózat-osztály nevével ellentétben nem hálózatok, hanem hálózat-sorozatok halmaza.

A hálózat-osztály definiálása után definiálhatjuk a megfelelő nyelvosztályt, azon nyelvek halmazát, amelyeket a hálózat-osztály valamely eleme számít.

A klasszikus nyelvosztály, AC^0, a konstans mélységű, polinom méretű $\{AND, OR, NOT\}$-hálózatokkal számítható nyelvek osztálya jelölésünkkel így fest:

2.12. Definíció. *AC^0 := ($\{AND, OR, NOT\}$-hálózat,poly méret, const mélység)*

Ha kicsit pongyolán például azt írjuk, hogy $SYMM \subseteq AC^0$, az alatt azt értjük, hogy $SYMM$ függvényekből alkotott tetszőleges függvénysorozat számítható AC^0-ban.

Példa. Később találkozni fogunk többek közt a következő hálózat-osztályokkal:
($\{AND, OR, NOT, MOD_3\}$-hálózat, k mélység, $2^{o(n^{1/2k})}$)
(THR-hálózat,$poly$ súly, 2 mélység, lin méret)
($SYMM$-hálózat,$m(n)$ befok, $k(n)$ méret)

2.6. Történeti kitekintés

A konstans mélységű, polinom méretű Boole-hálózatok vizsgálatát Furst-Saxe-Sipser [FSS], és Ajtai [Aj] kezdeményezte. 1981-ben egymástól függetlenül belátták, hogy a 2.12.-ban definiált AC^0 hálózatok nem képesek a paritásfüggvény kiszámítására.

2.13. Tétel. **(Furst-Saxe-Sipser,Ajtai)** $PAR \notin AC^0$

A tétel végső változata Yao [Y] és Håstad [Ha] munkája:

2.14. Tétel. **(Yao,Håstad)**
$PAR \notin (\{AND, OR, NOT\}-$hálózat$, d$ mélység$, 2^{o(n^{1/(d+1)})})$

Egyszerű konstrukció mutatja, hogy ez az eredmény konstansoktól eltekintve éles.

Furst et al., Ajtai, Yao és Hastad bizonyításai nem algebrai, hanem valószínűségszámítási technikákon alapulnak, ezért dolgozatunkban nem tárgyaljuk azokat, de az 2.13. Tételre két polinomiális módszert alkalmazó bizonyítást is adunk majd. Az egyik Smolensky [Smo], a másik Aspnes et al. [ABFR] eredménye.

Bár dolgozatunkban nem tárgyaljuk, mindenképpen említést érdemel, hogy mint arra már Furst-Saxe-Sipser rámutatott, a konstans mélységű hálózatokra vonatkozó alsó becslések lefordíthatók a bonyolultságelmélet egy másik ágának, az orákulumos Turing-gépek elméletének nyelvezetére, és ott értékes eredményeket adnak. Lásd például [KVVY][Bei2].

3. A polinomiális módszer első alkalmazása

Ebben a fejezetben Smolensky [Smo] nyomán bizonyítjuk Yao és Håstad tételének egy valamivel gyengébb konstansokat adó, de általánosabb változatát. Egyelőre csak kimondjuk a tételt.

3.1. Tétel. (Smolensky)
$PAR \notin (\{AND, OR, NOT, MOD_3\}$–hálózat, k mélység, $2^{o(n^{1/2k})})$.

Most lássunk egy naív kísérletet Furst et al. eredeti állításának bizonyítására a polinomok alkalmazásával:

Az egyszerűbb tárgyalás kedvéért az OR-kapukat a De Morgan-szabály szerint lecseréljük AND-ekre és NOT-okra. Látható, hogy ez legfeljebb háromszorozza a kapuk számát, ami eredményeinket nem érinti.

3.2. Állítás. *A $2\prod_{i\in[n]}(x_i+1)/2-1$ polinom n-edfokú, és a V^n halmazra megszorítva éppen az AND Boole-függvénnyel egyenlő.* □

A hálózathoz rendelt polinomot a bemenetektől a kimenet felé induktíve definiáljuk, a hálózat egy topologikus sorrendje szerint haladva végig a kapukon. A i. bemenet polinomja legyen az x_i polinom. Ha egy NOT-kapu bemenetének a p polinom felel meg, akkor a kimenetének feleltessük meg a $-p$ polinomot. Ha egy AND-kapu bemeneteinek a $p_1, p_2, ..., p_m$ polinomokat feleltettük meg, akkor a kimenetnek feleltessük meg a fenti $2\prod_{i\in[m]}(p_i+1)/2-$ -1 polinomot. Vegyük észre, hogy ez a polinom V^n-re megszorítva éppen a megfelelő AND-kapu kimenetét adja. Az eljárást az összes kapura elvégezve elérjük, hogy az n bemenettel rendelkező hálózathoz hozzárendelt

n-változós polinom V^n-re megszorítva pontosan a hálózat által számított Boole-függvényt adja meg.

Ha ezek után a konstruált polinom fokszámát felülről tudjuk becsülni a hálózat méretének és mélységének valamilyen függvényével, és van alsó becslésünk arra, hogy hanyadfokú polinommal lehet interpolálni a számítandó Boole-függvényt, akkor alsó becslést nyertünk a függvényt számító Boole-hálózat méretére.

Sajnos ezt az ígéretes program nem vezet eredményre. Ha ugyanis valamelyik kapu bemeneteinek száma n-nél nagyobb, akkor a hozzárendelt polinom fokszáma azonnal n fölé nő, és a becslés triviálissá válik, hiszen — mint hamarosan látni fogjuk — minden Boole-függvény interpolálható legfeljebb n-edfokú polinommal.

Razborov [Ra] 1985-ös cikkében 'megmenti' az ötletet. (Bár ő eredményét egy másik formalizmusban, a mátrixalgebrák nyelvén fogalmazta meg.) Razborov új gondolata a következő: Esetünkben a kapu kimenetét pontosan tudtuk reprezentálni a bemeneteket reprezentáló polinomok polinomjával, de ezen lépés során a fokszám kezelhetetlenül nőtt. Azonban lehetséges a kimenet reprezentálása sokkal kisebb fokszámú polinomjával is a bemeneti polinomoknak, ha megengedjük, hogy a kimenet néhány — kevés — bemenetre hibás legyen. Ez esetben olyan alsó becslésre van szükség, amely azt szavatolja, hogy a kérdéses függvény nem lehet sok helyen egyenlő egy kis fokszámú polinommal.

Smolensky [Smo] volt az, aki Razborov bizonyítását az általunk is használt nyelven újrafogalmazta és némileg továbbfejlesztette.

Razborov egy másik jelentős eredménye alsó becslés a klikkfüggvényt számoló $\{AND, OR\}$-hálózat méretére [Ra2]. Ez a bizonyítás szintén azon alapul, hogy a kapu kimenetét közelítjük egy olyan függvénnyel, amelynek bizonyos kombinatorikai paraméterei jól becsülhetők.

Karchmer [Kar] észrevette, hogy több ilyen jellegű bizonyítás mögött közös kombinatorikai jelenség húzódik meg, és az approximációs technikának megfogalmazta a legáltalánosabb keretét. Ezt Karchmer és Wigderson [Wig] fúziós módszernek nevezte el. A fúziós módszer segítségével a 'dinamikus' bonyolultsági kérdéseket átfogalmazhatjuk 'statikus' kérdésekké — bizonyos nagy halmazrendszerek lefogási problémáivá. Sajnálatos, de nem meglepő módon a kapott kombinatorikai problémák az esetek többségében éppen úgy kezelhetetlennek bizonyulnak, mint az eredeti bonyoluultságelméleti kérdések.

3.1. Approximáció véges test felett

A továbbiakban p rögzített páratlan prímszám, és $\mathbb{Z}_p$ a p-elemű test. A Boole-függvények továbbra is $V^n \to V$ függvények, de V-t most $\mathbb{Z}_p$ részének tekintjük.

3.3. Definíció. *Legyen $S \subseteq \mathbb{Z}_p^n$. Legyen f S-ről $\mathbb{Z}_p$-be képező függvény, és r valamilyen $S \subseteq S' \subseteq \mathbb{Z}_p^n$ halmazról $\mathbb{Z}_p$-be képező függvény. Azt mondjuk, hogy r S* **felett reprezentálja** *f-et, ha S-re megszorítva f és r azonosan egyenlőek.*

3.4. Definíció. *Ha f a V^n kockán van értelmezve, és r V^n felett reprezentálja, akkor egyszerűen azt mondjuk, hogy r* **reprezentálja** *f-et.*

Ennek a reprezentációnak van egy fontos tulajdonsága, amit a későbbiekben (a valós számtest esetén) a 4. Fejezetben részletesen fogunk tanulmányozni, de most csak kimondunk és bizonyítunk.

3.5. Definíció. *Egy n-változós polinomot* **multilineárisnak** *nevezünk, ha minden változójában lineáris.*

3.6. Definíció. **Multilinearizálásnak** *nevezzük azt a műveletet, amikor egy többváltozós polinom monomjaiban a páros kitevőket 0-ra, a páratlanokat 1-re cseréljük.*

Látható, hogy p multilinearizáltja V^n-en azonosan egyenlő p-vel, hiszen 1 és -1 hatványai csak a kitevő paritásától függenek.

3.7. Állítás. *Minden V^n-ről $\mathbb{Z}_p$-be képező függvény — speciálisan minden Boole-függvény — egyértelműen reprezentálható multilineáris polinommal.*

Bizonyítás.
Egzisztencia: f-hez először interpolációval találhatunk egy reprezentáló polinomot, ami nem feltétlenül multilineáris. Ennek a multilinearizáltja bizonyítja a létezést.
Unicitás: Létezési eredményünket úgy is fogalmazhatjuk, hogy a multilineáris monomok (azaz a $\prod_{j \in J} x_j$ alakú függvények) generálják a V^n-ről $\mathbb{Z}_p$-be menő függvények 2^n-dimenziós vektorterét. A multilineáris monomok száma 2^n, hiszen $[n]$ minden részhalmazához egyértelműen tartozik multilineáris monom. Mivel a monomok generálják a vektorteret, és darabszámuk éppen a vektortér dimenziója, ezért függetlenek is, amiből pedig már következik az egyértelműség. □

3.8. Definíció. *Egy f Boole-függvényt egy $r : V^n \to \mathbb{Z}_p$ függvény ε hibával* **approximál**, *ha legfeljebb $2^n\varepsilon$ darab csúcs kivételével megegyeznek a V^n kockán.*

Smolensky eredménye szerint ha f kis fokszámú polinom $\mathbb{Z}_p$ felett, akkor a $PAR = \prod_{j\in[n]} x_j$ Boole-függvényt nem approximálhatja kis hibával. Pontosabban:

3.9. Tétel. (Smolensky) *Ha a $\mathbb{Z}_p$ feletti n-változós r polinom fokszáma $\sqrt{n}$, akkor r PAR-t $\Omega(1)$ hibával approximálja.*

Bizonyítás.

Tegyük fel, hogy a $\sqrt{n}$ fokú r polinom az $S \subseteq V^n$ halmaz felett reprezentálja a $x_1x_2\cdots x_n$ függvényt. Az S-ből $\mathbb{Z}_p$-be képező függvények $\mathbb{Z}_p$ feletti $|S|$ dimenziós vektorteret alkotnak. Célunk, hogy ezeket a függvényeket $n/2 + \sqrt{n}$ fokú polinomokkal reprezentáljuk S felett.

Először válasszunk egy tetszőleges multilineáris reprezentációt. Ezt megtehetjük a 3.7. Állítás szerint, hiszen $S \subseteq V^n$. Ezt a reprezentáló polinomot fogjuk módosítani, minden monomját külön-külön. Ha egy monom $n/2$-nél nem nagyobb fokú, ne változtassuk meg. Legyen az m monom $n/2$-nél nagyobb fokú, azaz valamilyen $|J| > n/2$-re

$$m(x) = \prod_{j\in J} x_j = x_1x_2\cdots x_n \prod_{j\notin J} x_j^{-1}$$

Ez utóbbi az $x \in S$ pontokon éppen

$$r(x)\prod_{j\notin J} x_j.$$

Ez egy legfeljebb $n/2+\sqrt{n}$ fokú polinom. Ezt a helyettesítést minden $n/2$-nél nagyobb fokú monomra elvégezve tetszőleges S-ből $\mathbb{Z}_p$-be képező függvény reprezentálható a kívánt fokú polinommal. Mint már korábban láttuk, a monomok lineárisan függetlenek. A d-fokú monomok száma éppen $\binom{n}{d}$. E szerint a d-nél nem nagyobb fokú polinomok egy $\mathbb{Z}_p$ feletti $\binom{n}{\le d}$-dimenziós vektorteret alkotnak. Tehát

$$|S| \le \binom{n}{\le \frac{n}{2} + \sqrt{n}}.$$

A tétel ezután következik az alábbi ismert becslésből.

3.10. Lemma. (Chernoff-korlát)

$$\frac{1}{2^n}\binom{n}{\le \frac{n-k}{2}} \le e^{-k^2/2n}$$

$\square$

3.2. AND approximálása

Ezen alfejezet eredményeit a tárgyalás egyszerűsítése végett a háromelemű test felett mondjuk ki, bár kis változtatással minden $\mathbb{Z}_p$ test felett is érvényesek. Emlékeztetünk rá, hogy AND az a Boole-függvény, amely 1, ha minden változó 1, és -1 egyébként. Most belátjuk, hogy az AND Boole-függvény approximálható kis fokszámú polionommal, nem túl nagy hibával. A figyelmes olvasó észreveheti, hogy ez az állítás ebben a formában érdektelen, hiszen az azonosan -1 nulladfokú polinom $\frac{1}{2^n}$ hibával approximálja AND-et, és ennél jobb eredmény nem is várható. Hogy állításunkat pontossá —és persze a későbbiekben alkalmazhatóvá— tegyük, kiterjesztjük az approximáció definícióját.

3.11. Definíció. *Legyen π valószínűségeloszlás a V^n halmazon. f legyen a szokásos módon a kockáról $\mathbb{Z}_p$-be képező függvény, és r n-változós polinom. Azt mondjuk, hogy r az f-et ε hibával* **approximálja a π bemeneti eloszlás mellett**, *ha $Pr_\pi(f(x) \neq r(x)) \leq \varepsilon$*

Látható, hogy eredeti approximáció-fogalmunk ennek az a speciális esete, amikor π-nek az egyeletes eloszlást választjuk.

3.12. Tétel. (Smolensky) *Legyen l pozitív egész, és π tetszőleges valószínűségeloszlás V^n-en. Ekkor létezik $\mathbb{Z}_3$ feletti $2l$-fokú polinom, amely $1/2^l$ hibával approximálja az n-változós AND-függvényt a π bemeneti eloszlás mellett.*

Bizonyítás. A konstrukció alapgondolata azonos az alábbi gyakan használt ötlettel: (Kommunikációs bonyolultságelméleti alkalmazására jó példa [Nis]): Egy véges test feletti x vektorról kell eldöntenünk, hogy az azonosan 0 vektor-e. Megengedett megkérdeznünk a skalárszorzatát egy tetszőleges általunk adott vektorral. Algoritmusunk: Előállítunk l darab egymástól független véletlen ± 1-vektort, és mindegyiket skalárszorozzuk x-szel. Ha van nemnulla skalárszorzat, akkor x nemnulla. Ha minden skalárszorzat nulla, akkor legfeljebb $1/2^l$ tévedési valószínűség mellett kijelenthetjük, hogy $x = 0$.

Válasszuk ki $[n]$ egy J véletlen részhalmazát, minden részhalmazt egyforma valószínűséggel választva. Tekintsük az

$$s_J(x) := \left(\sum_{j\in J}(x_j - 1)\right)^2 + 1$$

másodfokú polinomot.

3.13. Lemma. *Ha* $x = (1,1,...,1)$*, akkor* $Pr(s_J(x) = 1) = 1$ *Ha* $x \neq$ $\neq (1,1,...,1)$*, akkor* $Pr(s_J(x) = -1) \geq \frac{1}{2}$ *(a valószínűséget* J *véletlen választására nézve tekintjük)*

A Lemma bizonyítása. Az állítás első része triviális. A második rész bizonyításához rögzítsünk egy x nem azonosan 1 bemenetet. Nevezzünk **jónak** egy J halmazt, ha $s_J(x) = -1$. J pontosan akkor jó, ha $\sum_{j\in J}(x_j - 1) \neq 0$. Két esetet különböztetünk meg x választása szerint.
I. eset: $\sum_{j\in[n]}(x_j - 1) \neq 0$.
Állítsuk párba a J halmazokat úgy, hogy mindegyik kerüljön párba a komplementerével.

$$\sum_{j\in J}(x_j - 1) + \sum_{j\in[n]\setminus J}(x_j - 1) \neq 0,$$

ezért J és $[n] \setminus J$ közül legalább az egyik jó. Ezzel az állítást az I.esetre beláttuk.
II. eset: $\sum_{j\in[n]}(x_j - 1) = 0$ Feltettük, hogy x nem csupa-1 vektor, legyen mondjuk $x_n = -1$.

$$\sum_{j\in[n-1]}(x_j - 1) = -1$$

Az I. esethez hasonlóan állítsuk párba $[n-1]$ részhalmazait, és jegyezzük meg, hogy melyek a jó halmazok. Most minden részhalmazhoz vegyük hozzá az n elemet. A részhalmazhoz tartozó összeg ezáltal $x_n - 1 =$ 1-gyel nő. Az eredetileg jó halmazokból, amelyekre az összeg nemnulla volt, ennek hatására lehet jó is, rossz is. Ellenben az eredetileg rossz halmazokból, amelyekre az összeg nulla volt, biztosan jó keletkezik. Így most is legalább annyi jó halmaz van, mint rossz. □

A Tétel bizonyítása Láttuk, hogy egy véletlenszerűen választott s_J másodfokú polinom legalább 1/2 eséllyel egyenlő $AND(x)$-szel minden fix x-re. A hibát ismétléssel csökkentjük. Legyen $\{J_i : i \in [l]\}$ egymástól függetlenül választott véletlen részhalmazok családja. Tekintsük a

$$\prod_{i\in[l]}(s_{J_i}+1)-1$$

$2l$ fokú polinomot. Ez éppen az $AND(s_{J_1}, s_{J_2}, ..., s_{J_l})$ Boole-függvényt reprezentálja. A lemmából azonnal következik, hogy ez a valószínűségi változó-polinom minden x bemenetre legfeljebb $1/2^l$ valószínűséggel hibázik. Van tehát egy polinomcsaládunk, amely csupa $2l$ fokú polinomból áll, és minden x-re legalább az $(1-1/2^l)$-edrészük jól reprezentálja AND-et az adott x-en. A tétel bizonyításához már csak egy kettős leszámlálást kell alkalmazni. Ebből következik, hogy van olyan eleme a polinomcsaládnak, amely a π bemeneti eloszlás mellett $(1-1/2^l)$ valószínűséggel egyenlő AND-del. Ezzel az állítást bizonyítottuk. □

3.3. Boole-hálózatból polinom

Az AND-re vonatkozó approximáció birtokában megadunk egy eljárást, amely egy k mélységű, S méretű $\{AND, OR, NOT, MOD_3\}$ -hálózathoz konstruál egy kis fokszámú polinomot, amely approximálja a hálózat által számított függvényt.

Első lépésként a deMorgan-szabály alkalmazásával az OR-kapukat lecseréljük AND és NOT kapukra. Ez a hálózat méretét legfeljebb megháromszorozza.

A hálózatot a bemenetektől a kimenetek felé haladva topologikus sorrendben (2.4. Definíció) kapunként alakítjuk polinommá. Kezdőlépésként az x_i bemeneteket az x_i polinomokkal reprezentáljuk. ($i \in [n]$).

A rekurzió során folyamatosan fenntartjuk az approximáló polinomoknak azt a tulajdonságát, hogy minden $x \in V^n$ bemeneten V-beli értéket adnak.

Ha egy kapu sorra kerül, akkor a topologikus sorrend definíciója szerint a bemeneteire már megadtuk az approximáló polinomokat. Legyenek ezek $g_1(x), g_2(x), ..., g_m(x)$. Három esetet különböztetünk meg aszerint, hogy milyen kapuról van szó.

I. eset: NOT-kapu

A kimenet ekkor 0 hibával reprezentálható a $-g_1$ polinommal, amely a bemenet elsőfokú polinomja.

II. eset: MOD_3-kapu

A kimenet szintén 0 hibával reprezentálható a

$$\left(\sum_{i\in[m]}(g_i+1)^2\right)^2+1$$

negyedfokú polinommal. Ugyanis $(g_i+1)^2$ akkor 1, ha $g_i=1$, és akkor 0, ha $g_i=-1$. Az összeg eszerint pontosan akkor 0, ha az 1 értékű g_i-k száma hárommal osztható.

III. eset: AND-kapu

A hálózat bemeneteinek V^n halmazán vett egyenletes eloszlás indukál egy π eloszlást a $(g_1(x), g_2(x), ..., g_m(x))$ vektorra nézve.

Példa.

$$g_1(x_1,x_2,x_3) := (x_1+1)(x_2+1)-1 \quad (= OR(x_1,x_2)),$$

$$g_2(x_1,x_2,x_3) := (x_2+1)(x_3+1)-1 \quad (= OR(x_2,x_3)),$$

Ekkor V^3 egyenletes eloszlása $AND(g_1,g_2)$ alábbi bemeneti eloszlását indukálja:

$$Pr(g_1(x)=-1, g_2(x)=-1) = 1/8$$
$$Pr(g_1(x)=-1, g_2(x)=+1) = 1/8$$
$$Pr(g_1(x)=+1, g_2(x)=-1) = 1/8$$
$$Pr(g_1(x)=+1, g_2(x)=+1) = 5/8$$

Az indukált π eloszlásra alkalmazzuk a 3.12. Tételt. Ez egy olyan h m-változós polinomot ad, amely $1-1/2^l$ π-valószínűséggel a g_i bemenetek AND-függvénye lesz. π választása és az indukált eloszlás definíciója miatt a $h(g_1(x), ...g_m(x))$ polinom $1/2^l$ hibával approximálja az $AND(g_1(x), ...g_m(x))$ Boole-függvényt, ha az x-et egyenletes eloszlással választjuk V^n-ből.

Ezzel a három esetet egyenként kezeltük. Összefoglalva: a kapu kimenete minden esetben közelíthető a kapu bemeneteinek legfeljebb $(2l)$-fokú polinomjával, úgy, hogy a hálózat azon inputjainak aránya, amelyekre ez a kapu hibás eredményt ad, legfeljebb $1/2^l$.

A polinommá alakítást az összes kapura elvégezve egy polinomot kapunk, amely approximálja a hálózat által számított függvényt. Két kérdés maradt: mekkora hibával számít, és mennyi a fokszáma?

Mindkét kérdés egyszerűen megválaszolható. Az i. szinten az előző szintek kapuiból alkotott polinomok legfeljebb $(2l)$-fokú polinomjai szerepelnek. Így a fokszám minden szinten az előző szint maximális fokszámának $(2l)$-dik hatványával becsülhető. A teljes fokszám tehát legfeljebb $(2l)^k$.

Minden egyes kapu a bemenetek (nem a saját bemenetei, hanem az egész hálózat bemenetei) legfeljebb $1/2^l$-ed részén hibázik. Így a globális hiba legfeljebb $N/2^l$.

Eddigi eredményeinket tétellé fogalmazzuk:

3.14. Tétel. *Legyen $l \in N$. Ha egy $\{AND, OR, NOT, MOD_3\}$-hálózat mérete N és mélysége k, akkor a hálózat kimenete approximálható $N/2^l$ hibával egy $\mathbb{Z}_3$ feletti $(2l)^k$ fokszámú polinommal.* $\square$

Válasszuk l-et $(\frac{1}{2}n^{1/2k})$-nak, és alkalmazzuk a tételt a PAR Boole-függvényt számító hálózatra. Ekkor a nyert polinom fokszáma éppen $\sqrt{n}$, és a polinom $N/2^{\frac{1}{2}n^{1/2k}}$ hibával approximálja PAR-t. A 3.9. Tétel szerint egy $\sqrt{n}$ fokú polinom PAR-t $\Omega(1)$ hibával képes csak approximálni. Tehát

$$N = \Omega(2^{\frac{1}{2}n^{1/2k}}),$$

és ezzel a 3.1. Tétel bizonyítását befejeztük. $\square$

4. A Fourier-apparátus

Az előző fejezetben már találkoztunk azzal a gondolattal, hogy egy test felett egy V^n-en értelmezett függvény egyértelműen interpolálható multilineáris polinommal (3.7. Állítás). Ebben a fejezetben az $\mathbb{R}$ test esetében részletesen vizsgáljuk az interpoláló polinom tulajdonságait.

4.1. Multilineáris polinomok, Fourier-transzformáció

A további fejezetekben a valós számok teste felett dolgozunk.

4.1. Definíció. *Saks nyomán, némileg nehézkesen,* **pszeudo-Boole függvénynek** *nevezünk egy f függvényt, ha a V^n kocka csúcsaiból a valós számokba képez, azaz ha $f \in \mathbb{R}^{V^n}$.*

A pszeudo-Boole függvények algebrát alkotnak a valósok felett az elemenkénti szorzással. Ennek az algebrának természetes bázisát adják V^n egyelemű részhalmazainak karakterisztikus függvényei.

A pszeudo-Boole függvények terén skalárszorzatot definiálunk.

$$\langle f|g\rangle := \sum_{x\in V^n} f(x)g(x)$$

4.2. Definíció. *Egy $J \subseteq [n]$ halmazra $\pi_J := \prod_{j\in J} x_j$ A π_J függvényeket* **paritás-** *vagy* **monomfüggvényeknek** *fogjuk nevezni.*

Két, sokat használt tulajdonságuk:

$$\pi_J \cdot \pi_K = \pi_{J \triangle K}$$

($J \triangle K$ a két halmaz szimmetrikus differenciája)

$$\sum_v \pi_J(v) = \begin{cases} 2^n & J = 0 \\ 0 & J \neq 0 \end{cases}$$

Ebből a két azonosságból könnyen levezethető legfontosabb tulajdonságuk, hogy ortogonális bázisát alkotják $\mathbb{R}^{V^n}$-nek a fent bevezetett skalárszorzásra nézve:

4.3. Állítás.

$$\langle \pi_J | \pi_K \rangle = \begin{cases} 2^n & J = K \\ 0 & J \neq K \end{cases}$$

Páronként ortogonálisak, és 2^n a darabszámuk, tehát bázist alkotnak. Így minden pszeudo-Boole függvény egyértelműen felírható

$$r = \frac{1}{2^n} \sum_{J \subseteq [n]} \langle r | \pi_J \rangle \, \pi_J$$

alakban. Ezt nevezzük r **spektrális felírásának** vagy **spektrális alakjának**. Bevezetjük a következő jelölést:

4.4. Definíció. *Az $r \in \mathbb{R}^{V^n}$ függvényhez definiáljuk az $\hat{r} \in \mathbb{R}^{2^{[n]}}$ függvényt:*

$$\hat{r}(J) := \frac{1}{2^n} \langle r | \pi_J \rangle$$

Az $r \mapsto \hat{r}$ leképezés lineáris transzformáció $\mathbb{R}^{V^n}$ és $\mathbb{R}^{2^{[n]}}$ között. Ezt **Fourier-transzformációnak** *nevezzük.*

$$r = \sum_{J \subseteq [n]} \hat{r}(J) \pi_J$$

Dolgozatunk legnagyobb részét ezen transzformáció vizsgálatának, illetve alkalmazásainak szenteljük.

A spekrális felírást mint multilineáris polinomot azonosítjuk a megfelelő $\hat{r}$ függvénnyel, így beszélünk például az r-et reprezentáló $\hat{r}$ polinomról.

$\hat{r}$-nak, mint polinomnak a szokásos módon definiáljuk a fokszámát és sűrűségét. Formálisan:

4.5. Definíció.
$\hat{r}$ **foka** $\deg\hat{r} = \max\{|J| : \hat{r}(J) \neq 0\}$
$\hat{r}$ **sűrűsége** $\mathrm{dns}\hat{r} = |\{J : \hat{r}(J) \neq 0\}|$

4.6. Definíció. *A spektrális alak egyértelműsége miatt egy tetszőleges pszeudo-Boole függvénynek definiálhatjuk a fokszámát és sűrűségét, mint a spektrális felírásának fokszámát illetve sűrűségét.*

4.7. Definíció. **Spektráltartónak** *nevezzük a spektrális alak nemnulla együtthatójú monomjainak halmazát:* $S(r) := \{J \in 2^{[n]} : \hat{r}(J) \neq 0\}$

4.8. Definíció. *Legyen* $\mathcal{S} \subseteq 2^{[n]}$*, és* $r \in \mathbb{R}^{V^n}$*.* r **spektrális projekciója** $\mathcal{S}$*-re az* r *merőleges vetítése a pszeudo-Boole függvények vektorteréből az* $\mathcal{S}$ *tartójú pszeudo-Boole függvények alterébe. Azaz*

$$r|_{\mathcal{S}} := \frac{1}{2^n} \sum_{J \in \mathcal{S}} \langle r | \pi_J \rangle \, \pi_J$$

Az alábbiakban megadjuk a Fourier-transzformációnak mint az $\mathbb{R}^{V^n}$-ből $\mathbb{R}^{2^{[n]}}$-be menő lineáris transzformációnak a mátrixát.

A mátrix sorai az $[n]$ részhalmazaival, oszlopai a V^n csúcsaival vannak indexelve. Tudjuk, hogy $\hat{r}(J) = \frac{1}{2^n} \langle r | \pi_J \rangle$. Ebből látszik, hogy a mátrix J-vel indexelt sora éppen az $\frac{1}{2^n}\pi_J$ vektor. Így a mátrix J-dik sorának v-dik eleme $\frac{1}{2^n}\pi_J(v)$.

4.9. Definíció.

$$H_n(J)(v) := \pi_J(v) \quad v \in V^n, J \subseteq [n]$$

4.10. Állítás.

$$\hat{r} = \frac{1}{2^n} H_n \, r$$

$$r = H_n^T \, \hat{r}$$

□

Most megadunk egy megfeleltetést $2^{[n]}$ és V^n elemei között.

4.11. Definíció. *A* $K \in 2^{[n]}$ *halmazhoz rendeljük a* $v_K \in V^n$ *csúcsot:*

$$v_K[k] := \begin{cases} -1 & k \in K \\ 0 & k \notin K \end{cases}$$

4.12. Állítás.

$$\pi_J(v_K) = (-1)^{|J \cap K|}$$

$\square$

Ebből azonnal látszik, hogy ha a csúcsokat is a részhalmazokkal címkézzük — ezzel a mátrix sorait és oszlopait megfeleltetve egymásnak —, akkor szimmetrikus mátrixot kapunk. Ha a részhalmazokat lexikografikusan rendezzük, akkor H_n-ből egy hagyományosan indexelt $2^n \times 2^n$-es mátrixot kapunk. Könnyen ellenőrizhető, hogy ez az alábbi rekurzióval adható meg.

$$\begin{aligned} H_0 &:= \begin{bmatrix} 1 \end{bmatrix} \\ H_1 &:= \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \\ H_{n+1} &:= \begin{bmatrix} H_n & H_n \\ H_n & -H_n \end{bmatrix} \end{aligned}$$

A H_n mátrixokat **Sylvester-féle Hadamard mátrixoknak** nevezzük.

Megjegyzés. Hadamard-mátrixnak az ortogonális ± 1-mátrixokat nevezzük.

Mindez a spektrális felírás alábbi egyszerű induktív előállításának felel meg.

$$\begin{aligned} r^+(x_1, x_2, ..., x_{n-1}) &:= r(x_1, x_2, ..., x_{n-1}, +1) \\ r^-(x_1, x_2, ..., x_{n-1}) &:= r(x_1, x_2, ..., x_{n-1}, -1) \end{aligned}$$

Ha r^+ az $\hat{r}^+$, r^- pedig az $\hat{r}^-$ polinommal reprezentált, akkor r-et reprezentálja az

$$\hat{r}(x_1, ..., x_n) := \frac{1 - x_n}{2}\, \hat{r}^-(x_1, ..., x_{n-1}) + \frac{1 + x_n}{2}\, \hat{r}^+(x_1, ..., x_{n-1})$$

polinom.

4.13. Tétel. **(Parseval azonosság)** $\langle f | g \rangle = 2^n \sum_{J \subseteq [n]} \hat{f}(J) \hat{g}(J)$

Bizonyítás. f-et és g-t írjuk fel spektrális alakban. A skalárszorzat linearitása és a monomok ortogonalitása miatt elég az állítást arra az esetre belátni, ha f és g monomok. Erre pedig az állítás következik az 4.3. Állításból. $\square$

A Parseval azonosságot az $f = g$ speciális esetre alkalmazva kapjuk, hogy

4.14. Állítás.

$$\sum_{J \subseteq [n]} (\hat{f}(J))^2 = 1$$

4.2. Erős és gyenge előjelreprezentáció

4.15. Definíció. *Egy r pszeudo-Boole függvényről azt mondjuk, hogy az f Boole-függvényt* **erősen előjelreprezentálja**, *ha* $\forall x \in V^n : \operatorname{sgn} r(x) = f(x)$. *(Ezt röviden* $\operatorname{sgn} r = f$*-nek írjuk.)*

4.16. Definíció. *Egy r pszeudo-Boole függvényről azt mondjuk, hogy az f Boole-függvényt* **gyengén előjelreprezentálja**, *ha r nem azonosan 0, és azon $x \in V^n$-ekre, amelyekre $r(x) \neq 0$, $\operatorname{sgn} r(x) = f(x)$.*

Tekinthetjük úgy, hogy az r 'nem foglal állást' azokról az x-ekről, amelyekre $r(x) = 0$.

Az erős és gyenge előjelreprezentáció (szemben a spektrális reprezentációval) természetesen nem egyértelmű, egy Boole-függvényt sok pszeudo-Boole függvény reprezentálhat. Mi bizonyos értelemben egyszerűeket keresünk majd. A spektrális felírás sugall két természetes bonyolultsági mértéket: a fokszámot és a sűrűséget.

4.17. Definíció. *f* **erős foka**: $\deg_s(f) := \min\{\deg(r) :$ *r erősen előjelreprezentálja f-et* $\}$

4.18. Definíció. *f* **erős sűrűsége**: $\operatorname{dns}_s(f) := \min\{\operatorname{dns}(r) :$ *r erősen előjelreprezentálja f-et* $\}$

4.19. Definíció. *f erősen előjelreprezentálható $\mathcal{S}$ spektráltartóval, ha létezik r, amely erősen előjelreprezentálja, és $S(r) \subseteq \mathcal{S}$.*

A **gyenge fok** ($\deg_w(f)$) és a **gyenge sűrűség** ($\operatorname{dns}_w(f)$), és a gyengén előjelreprezentálhatóság definíciója a fentiekkel teljesen analóg.

Példa. Definíció szerint minden nemtriviális THR-függvénynek 1 az erős foka, és minden nemtriviális paritásfüggvénynek 1 az erős sűrűsége.

Valamivel összetettebb példa az $EXACT_k$ függvény, amelynek erős foka legfeljebb 2, mint azt az $\frac{1}{2} - \left(\sum_{i\in[n]} x_i - k\right)^2$ előjelreprezentáló polinom mutatja. Konvexitási megfontolásokból könnyen levezethető, hogy ha $k \neq 0, n$, akkor $EXACT_k$ erős foka nagyobb 1-nél.

Triviális kapcsolatok definícióink között:

4.20. Állítás. $\deg_w(f) \leq \deg_s(f) \leq \deg(f)$ □

4.21. Állítás. $\deg_s(f) \leq d$ *pontosan akkor, ha f erősen előjelreprezentálható $\binom{[n]}{\leq d}$ spektráltartóval.* □

4.3. Motiváció: a perceptronok

A számítási modell leggyakrabban segédeszköz bonyolulságelméleti kérdések vizsgálatára, és nem azzal az igénnyel alkotják, hogy műszaki kivitelezésre kerüljön. Van azonban egy modell, amely nagyban hasonlít bizonyos gyakorlatban is használt számítási eszközökre. Ez a modell a perceptron.

4.22. Definíció. *A perceptron 2 mélységű szintezett hálózat, amelynek első szintje AND-kapukból áll, második szintjén pedig egy THR-kapu van.*

A perceptront a 40-es évek óta vizsgálják, mint az egyszerű neuronhálózatok, speciálisan a látóidegek leegyszerűsített modelljét [MCP]. A perceptronok irodalmának máig legfontosabb forrásműve Minsky és Papert 1968-ban megjelent monográfiája [MP]. Ebben jelennek meg elsőként a előjelreprezentáló polinomok, és ez a polinomok első egzakt alkalmazása bonyolultságelméleti kérdések megválaszolására.

Történeti érdekesség, hogy a szerzők művüket a perceptronok elleni vitairatnak szánták [Cla]. A hatvanas évek mesterséges intelligencia-kutatásának egyik népszerű irányzata a perceptront az agy modellálására alkalmas univerzális számítási eszköznek tekintette, és rövid távú célként tűzte ki valós gondolkodási feladatokat megoldó perceptronok építését. Minsky és Papert egy másik irányzatot képviseltek, amely a gondolkodás nemfolytonos, szimbólummanipulációs oldalát hangsúlyozta, és hasonlóan rövid távú célja volt gondolkodó digitális számítógépek építése. Minsky és Papert bonyolultsági alsó becsléseiket bizonyítéknak tekintették arra, hogy az ellentábor reményei nem megalapozottak. Természetesen ma már senki sem akar gondolkodó perceptront építeni, de Minsky és Papert filozófiai végkövetkeztetése is idejét múlta, hiszen a mesterséges intelligencia-kutatásban ma már az általuk preferált szimbólummanipulációs megközelítésnél nagyobb a szerepe van a neuronhálózatok elvén alapuló analóg, nemtriviális kódolású modelleknek.

A Perceptronok meggyőzte a mesterséges intelligencia-kutatókat a perceptronok gyenge számítási képességéről, és ez évekkel vetette vissza a mesterséges neuronhálózatok kutatását, pedig azok ártatlanok voltak a perceptron legnagyobb hibájában, hogy kicsi a mélysége.

Ha a Boole-függvények definiálásakor $Igaz$ és $Hamis$ igazságértékeket az általunk használt $(+1, -1)$ helyett a $(1, 0)$ számokkal reprezentáljuk, akkor az AND a szorzásnak felel meg. Könnyen láthatjuk, hogy ekkor a perceptron egy polinom előjelét számítja, ahol az egyes monomok az első szint kapuinak felelnek meg. A perceptron mérete éppen eggyel nagyobb a polinom sűrűségénél, a perceptron rendje — azaz első szintjének max-befoka — éppen a polinom fokszáma. A perceptron THR-kapujának súlya pedig a polinom együtthatóinak abszolútérték-összege. Így a perceptron bonyolultságelméleti vizsgálata közvetlenül visszavezethető a megfelelő polinomok algebrai vizsgálatára.

Sajnálatos módon a $(1,0)$-reprezentációra nem igazán alkalmazható a Fourier-technika. Ezért az előjelreprezentálással kapcsolatos általunk ismertetett eredmények a $(+1,-1)$-reprezentáció esetére vonatkoznak. Látható, hogy ez az algebrailag kezelhetőbb eset annak a mesterkéltebb Boole-hálózatosztálynak felel meg, amelynek az első szintjén PAR-kapuk vannak, a másodikon pedig egy THR-kapu. Vegyük észre viszont, hogy az egyik reprezentációról a másikra való áttérés a bementi vektor egy affin transzformációjának felel meg, ezért nem érinti a reprezentáló polinom fokszámát. E szerint egy függvény erős foka egyenlő a függvényt számoló optimális rendű perceptron rendjével. A $(+1,-1)$-reprezentációra való áttérés azonban teljesen megváltoztathatja mind a polinom sűrűségét, mind az együtthatók abszolútértékösszegét, és így hasonló állítás nem igaz a perceptron méretére vagy súlyára.

4.4. Bruck lemmája

A pszeudo-Boole függvények terén definiálunk egy normát. Ez nem a már definiált skalárszorzat által indukált norma lesz, hanem egy másik, amely különösen alkalmas az előjelreprezentáció vizsgálatára. Később további normákat is vizsgálunk majd.

4.23. Definíció. *Az $r \in \mathbb{R}^{V^n}$ függvény* **standard l_1-normája***:*

$$\|r\| := \sum_{x \in V^n} |r(x)|$$

Ez lesz a messze leggyakrabban használt normánk, így ezt egyszerűen normának fogjuk nevezni.

A most következő lemma szinte azonnali következménye a Parseval azonosságnak (4.13. Állítás), de az előjelreprezentációval kapcsolatos összes eredményünknek ez fog kiindulópontjául szolgálni.

4.24. Lemma. **(Bruck lemmája)** *$r \in \mathbb{R}^{V^n}$ gyengén előjelreprezentálja $f \in V^{V^n}$-t akkor és csakis akkor, ha*

$$\|r\| = 2^n \sum_{J \subseteq [n]} \hat{f}(J)\hat{r}(J).$$

r erősen előjelreprezentálja f-et akkor és csakis akkor, ha

$$\|r\| = 2^n \sum_{J \subseteq [n]} \hat{f}(J)\hat{r}(J),$$

és $\forall x \in V^n : r(x) \neq 0$.

Bizonyítás. Világos, hogy ha r gyengén előjelreprezentálja f-et, akkor

$$\forall v \in V^n : f(x)r(x) \geq 0.$$

Ez ekvivalens azzal, hogy

$$\|r\| = \langle r|f\rangle .$$

Alkalmazva a 4.13. Parseval azonosságot éppen a bizonyítandó állítást kapjuk.

Az erős előjelreprezántációra vonatkozó állítás ezek után triviális. □

A következő, szintén sokat használt állítás jól demonstrálja a Lemma alkalmazhatóságát. Tartalma az, hogy a monomfüggvények nem csak lineárisan függetlenek, de nem állhatnak elő más monomfüggvények lineáris kombinációjának signumaként sem.

4.25. Állítás. *Ha r gyengén előjelreprezentálja a π_K paritásfüggvényt, akkor $K \in S(r)$. Speciálisan, $\deg_w(PAR) = n$.*

Bizonyítás. Tegyük fel, hogy r gyengén előjelreprezentálja π_K-t, és spektráltartója nem tartalmazza K-t. Bruck lemmája szerint

$$\|r\| = 2^n \sum_{J\subseteq[n]} \hat{r}(J)\widehat{\pi_K}(J) = 2^n\hat{r}(K) = 0.$$

Ez ellentmond annak, hogy r nem azonosan 0. □

Egy további érdekes alkalmazás az alábbi:

4.26. Tétel. (Rekonstruálhatósági tétel) *Legyen f Boole-függvény, és r az f erős előjelreprezentánsa. Legyen továbbá $\mathcal{S} = S(r)$. Ekkor $f|_{\mathcal{S}}$ — f spektrális projekciója $\mathcal{S}$-re —, egyértelműen meghatározza f-et.*

Bizonyítás. Tegyük fel, hogy létezik egy g Boole-függvény is, amelyre $g|_{\mathcal{S}} = f|_{\mathcal{S}}$. Ekkor g és r is kielégítik az

$$\|r\| = 2^n \sum_{J\subseteq[n]} \hat{r}(J)\hat{g}(J)$$

egyenlőséget, ezért r g-t is erősen előjelreprezentálja. Tehát $g = \operatorname{sgn} r = f$. □

4.5. Alkalmazás: $PT_1 \subsetneq LT_2$

Most a Fourier-transzformációs technika egyik legelső bonyolultságelméleti alkalmazásával ismerkedünk meg. Bruck [Bru] definiálta elsőként az úgynevezett Polinom-küszöb (Polynomial Threshold) függvényeket.

4.27. Definíció. *PT_1 azon Boole-függvény-sorozatok bonyolultsági osztálya, amelyeknek erős sűrűsége a bemenetek számának polinomja.* [1]

A perceptronok nyelvén PT_1 azon függvény-sorozatok osztálya, amelyek számíthatóak olyan 2 mélységű, polinom méretű szintezett Boole-hálózattal, amelynek az első szintjén PAR-kapuk, a második szintjén egy THR-kapu van.

PT_1 nagyon bő függvénycsalád, szinte minden általunk eddig definiált Boole-függvény-sorozat benne van. Nyilvánvalóan benne van minden monomfüggvény, minden küszöbfüggvény, és minden konstans erős fokú Boole-függvény, mint például $EXACT_k$.

Bruck vette észre elsőként, hogy a PT_1 függvények számíthatóak 2 mélységű, polinom méretű THR-hálózatokkal.

4.28. Definíció. $LT_2 :=$ *(THR-hálózat,poly méret,2 mélység)*

Az LT_2 osztály nagyon fontos tulajdonsága:

4.29. Állítás. *$SYMM \subseteq LT_2$, azaz minden szimmetrikus Boole-függvény számítható LT_2 hálózattal.*

Bizonyítás. Az első szinten a $\operatorname{sgn}(f_k)$ függvényeket számítjuk, amelyek azt állapítják meg, hogy a bemenet egyeseinek száma legalább k-e:

$$f_k(x) := \sum_{i\in[n]} \frac{x_i+1}{2} - k - \frac{1}{2} \quad (k \in \{0, ..., n+1\})$$

Vegyük észre, hogy

$$\frac{\operatorname{sgn} f_k(x) - \operatorname{sgn} f_{k+1}(x)}{2}$$

egyenlő 1-gyel, ha x egyeseinek száma k, minden más esetben pedig 0. A szimmetrikus Boole-függvény értéke csak a bemenet 1-eseinek számától függ. Legyen $s(k)$ az a függvény, amely a számítandó Boole-függvény értékét adja

[1] Az egyes index az elnevezésben arra utal, hogy Bruck definiálta a PT_1 kapukat használó k-mélységű, polinom méretű hálózatok osztályát, PT_k-t is.

a k darab 1-ből álló bemeneten. Ekkor a Boole-függvény éppen egyenlő a következő kifejezéssel:

$$\sum_{k=0}^{n} s(k)\frac{\operatorname{sgn} f_k(x) - \operatorname{sgn} f_{k+1}(x)}{2}$$

$\square$

4.30. Tétel. **(Bruck)** $PT_1 \subseteq LT_2$

Bizonyítás. A tétel bizonyítása azon a megfigyelésen alapul, hogy az előbbi konstrukcióban nem használtuk ki az LT_2 teljes erejét. Ugyanis a második szinten csak összegeztünk, de az eredménynek nem kellett a signumát vennünk. Az előző bizonyításban bevezetett jelöléssel

$$PAR(x) = 1 + 2\sum_{k\in[n]} (-1)^k \operatorname{sgn} f_k(x).$$

A 8. fejezetben részleges bizonyítást adunk arra a kevéssé meglepő tényre, hogy ez a konstrukció lényegében optimális LT_2 hálózatot ad PAR-ra a kapuk számát tekintve.

Mint említettük, ez a hálózat a második szinten már csak összegez. Ez alapján a polinom-küszöbfüggvény számítása egyszerűen úgy történhet, hogy minden monomjára külön felépítünk egy az előbb bemutatott PAR-hálózatot, a második szint összegeit beszorozzuk a monom együtthatójával, és az összes második szintű kaput összevonjuk egyetlen összeggé. Az eredményül kapott hálózat mérete a polinom-küszöbfüggvény monomjai számának legfeljebb $(n + 1)$-szerese. $\square$

Bruck a Fourier-transzformációs technikák ötletes alkalmazásával bebizonyította, hogy a $PT_1 \subseteq LT_2$ tartalmazás valódi. Megmutatta, hogy az általa teljes kvadratikus függvénynek (CQ) nevezett szimmetrikus Boole-függvény nem eleme PT_1-nek. Az 4.29. Állítás ezek után adja a tartalmazás valódiságát.

Ezt az eredményt úgy interpretálhatjuk, hogy a *poly* méretű, 2 mélységű hálózatok, amelyeknek mindkét szintje THR-kapukból áll, határozottan erősebb számítási képességű, mint azok a *poly* méretű, 2 mélységű hálózatok, amelyeknek első szintjén csak PAR-kapuk vannak, a második szintjén pedig egy THR-kapu.

4.31. Tétel. **(Bruck)** $PT_1 \subsetneq PL_2$.

A bizonyításhoz visszatérünk az előző fejezetben folytatott vizsgálatainkhoz. Az alábbiakban a pszeudo-Boole függvényeknek más normáit is fogjuk használni, mint az eddig megismert $\|\cdot\|$ standard l_1-normát.

4.32. Definíció.
A **spektrális** l_∞**-norma** *vagy* $\hat{l}_\infty$**-norma***:*

$$|\!|\!| r |\!|\!|_\infty := \max_{J\subseteq[n]} |\hat{r}(J)|$$

A **spektrális** l_1**-norma** *vagy* $\hat{l}_1$**-norma***:*

$$|\!|\!| r |\!|\!|_1 := \sum_{J\subseteq[n]} |\hat{r}(J)|$$

Elsőként egy hasznos lemmát bizonyítunk a pszeudo-Boole függvények normáiról. Ez az állítás egyébként az úgynevezett Haussdorff-Young egyenlőtlenség speciális esete.

4.33. Lemma. $\|r\| \geq 2^n |\!|\!| r |\!|\!|_\infty$

Bizonyítás. Legyen $J \in [n]$ rögzített halmaz.

$$\|r\| = \|\pi_J \cdot r\| = \sum_{x:(\pi_J\cdot r)(x)>0} (\pi_J \cdot r)(x) - \sum_{x:(\pi_J\cdot r)(x)<0} (\pi_J \cdot r)(x) =$$

$$= \sum_x (\pi_J \cdot r)(x) - 2 \sum_{x:(\pi_J\cdot r)(x)<0} (\pi_J \cdot r)(x) \geq \sum_x (\pi_J \cdot r)(x) = 2^n \hat{r}(J)$$

□

A lemma segítségével alsó becslést adunk egy Boole-függvény erős sűrűségére.

4.34. Tétel. $\forall f \in V^{V^n} : \mathrm{dns}_s(f) \geq 1/|\!|\!| f |\!|\!|_\infty$

Bizonyítás. Ha r erősen előjelreprezentálja f-et, akkor

$$|\!|\!| f |\!|\!|_\infty |\!|\!| r |\!|\!|_1 \geq \sum_{J\subseteq[n]} \hat{f}(J)\hat{r}(J) = \frac{1}{2^n}\|r\| \geq |\!|\!| r |\!|\!|_\infty \geq \frac{|\!|\!| r |\!|\!|_1}{|S(r)|}$$

Itt az első egyenlőtlenség triviális, a második éppen Bruck lemmája, a harmadik az 4.33 Lemma, és az utolsó ismét triviális a spektráltartó definíciója alapján. □

Ez a tétel motiválja az alábbi definíciót:

4.35. Definíció. *PL_∞ jelöli azon Boole-függvények (függvénysorozatok) családját, amelyekre $1/\|f\|_\infty$ felülről becsülhető n polinomjával.*

A 4.14. Állításból tudjuk, hogy a spektrális együtthatók négyzetösszege 1. PL_∞ tehát azokból a Boole-függvényekből áll, amelyeknek spektrális együtthatói nem egyenletesen kicsik, hanem vannak köztük kiugróan magasak.

4.36. Következmény. $PT_1 \subseteq PL_\infty$ □

Megjegyzés. A 4.34. Tétel alsó becslés az erős sűrűségre a spektrális norma függvényében. Bruck és Smolensky a véletlen módszer felhasználásával ellentétes irányú becslést adott. Ezt az eredményt csak kimondjuk.

4.37. Tétel. (Bruck-Smolensky) $\forall f \in V^{V^n} : \mathrm{dns}_s(f) \leq 2n(\|f\|_1)^2$

A **nem** PL_∞-beli Boole-függvények egy érdekes osztálya a **görbe függvények**, amelyekre

$$\forall J \subseteq [n] : |\hat{f}(J)| = 2^{n/2}$$

4.38. Definíció. $CQ(x_1, x_2, ..., x_n) := \bigoplus_{i<j}(x_i \wedge x_j)$

Nyilvánvaló, hogy CQ szimmetrikus függvény, tehát a 4.29. Állítás szerint benne van LT_2-ben.

Ahhoz, hogy belássuk, hogy $CQ \notin PT_1$, elég belátni,hogy CQ görbe függvény:

4.39. Tétel. (Bruck) *Ha n páros, akkor*

$$\forall J \subseteq [n] : |\widehat{CQ_n}(J)| = 2^{n/2},$$

azaz CQ_n görbe függvény.

A teljesen elemi, de számolásigényes bizonyítást nem közöljük, megtalálható [Bru]-ban.

Ezzel a 4.31. Tételt beláttuk, $PT_1 \subsetneq PL_2$. □

5. Előjelreprezentáció és approximáció

Smolensky eredményének algebrai része minden véges testre működött. Analóg eredmény valósok felett is igaz, Aspnes et al. [ABFR] a Fourier-transzformáció elemi tulajdonságait felhasználva bizonyítja. Valósok felett viszont (a lineáris egyelőtlenségrendszerek bizonyos tulajdonságainak köszönhetően) hasonló erdmények nem csak a paritásfüggvényre igazolhatók. Erről szól Aspnes et al. elegáns Alternatívatétele. A hálózatból polinommá alakítás is hasonló Smolensky konstrukciójához, bár az a konstrukció nem alkalmazható közvetlenül, hiszen a 3.12. Tétel erősen kihasználta az alaptest végességét. Ezt a problémát Valiant és Vazirani egy korábbi eredményére építve hidalják át.

Csupán megemlítjük, hogy ez a konstrukció bizonyos értelemben — a felhasznált véletlen bitek számát tekintve — jobb eredményt ad Smolensky véges test feletti konstrukciójánál. Ennek a ténynek a felhasználásával többeknek ([AH],[KVVY],[Tar2]) sikerült az eredetinél jóval egyszerűbb bizonyítást adni Toda híres tételére [To].

5.1. Az Alternatívatétel és következményei

A lineáris egyenlőtlenségrendszerek elméletének legalapvetőbb eredménye a **Farkas-lemma**. A Farkas-lemmának sok ekvivalens verziója létezik, mi az alábbit fogjuk felhasználni:

5.1. Lemma. *Legyen U az $\mathbb{R}^m$ vektortér tetszőleges altere. Ekkor a következő két állítás közül pontosan egy teljesül:*

1. *Létezik $q \in U$, amelyre $q \neq 0, q \geq 0$.*
2. *Létezik $p \in U^{\perp}$, amelyre $p > 0$.*

Bár ez az általunk használt alakból nem látható azonnal, Farkas-lemmájának geometriai tartalma: Rögzítsünk le egy zárt konvex poliédert. Ekkor egy pont akkor és csak akkor nem eleme a poliédernek, ha létezik zárt féltér, amely tartalmazza a poliédert, de nem tartalmazza a pontot.

A bizonyítás megtalálható bármely lineáris programozással foglalkozó monográfiában, például [Chv]-ban.

Látni fogjuk, hogy Farkas Lemmájának szinte közvetlen következménye egy olyan állítás, amelynek segítségével sok Boole-függvény (például minden szimmetrikus Boole-függvény) gyenge és erős fokát meghatározhatjuk.

5.2. Állítás. *Legyen $f \in V^{V^n}$, és U legyen a $\mathbb{R}^{V^n}$ vektortér tetszőleges altere. A következő két állítás közül pontosan egy teljesül:*

f gyengén előjelreprezentálható U-beli pszeudo-Boole függvénnyel.
f erősen előjelreprezentálható $U^{\perp}$-beli pszeudo-Boole függvénnyel.

Bizonyítás. Vegyük észre, hogy az állítást elég arra az esetre bizonyítani, amikor az f az azonosan 1 Boole-függvény. (Ezt a függvényt a továbbiakban $\underline{1}$-gyel jelöljük.) Ugyanis választhatunk egy σ ortogonális transzformációt psz-en, amely az f-et $\underline{1}$-be viszi, és erre $(\sigma(U))^{\perp} = \sigma(U^{\perp})$.

Alkalmazva Farkas Lemmáját ezután pontosan a bizonyítandó állítást kapjuk. □

Fontos speciális eset, amikor az U néhány monom által generált altér. Ennek további speciális esete, amikor U a legfeljebb d fokú monomok által generált altér. Kimondjuk a tétel ezen speciális eseteknek megfelelő változatait.

5.3. Tétel. *Legyen $f \in V^{V^n}$, és $\mathcal{S} \subseteq 2^{[n]}$. A következő két állítás közül pontosan egy teljesül:*

1. *f gyengén előjelreprezentálható $\mathcal{S}$ spektráltartóval.*
2. *f erősen előjelreprezentálható $2^{[n]} \setminus \mathcal{S}$ spektráltartóval.*

□

5.4. Tétel. *Legyen $f \in V^{V^n}$, $d \in \{0, ..., n\}$ A következő két állítás közül pontosan egy teljesül:*

1. $\deg_w(f) \leq d$
2. $\deg_s(f \cdot PAR) \leq n - d$

Másként fogalmazva: Minden $f \in V^{V^n}$-re

$$\deg_w(f) + \deg_s(f \cdot PAR) = n.$$

Bizonyítás. Alkalmazzuk az 5.3. Tételt az $\mathcal{S} = \binom{n}{\leq d}$ esetre. Az állítás bizonyításához ezután csak arra a megfigyelésre van szükség, hogy f pontosan akkor erősen előjelreprezentálható $\{S : S \subseteq [n], |S| > d\}$ spektráltartóval, ha $f \cdot PAR$ erősen reprezentálható $\binom{n}{\leq n-d}$ spektráltartóval, hiszen

$$x_J \cdot PAR = x_{[n] \setminus J}.$$

□

Most az 5.4. Tétel alkalmazásaként meghatározzuk egy tetszőleges szimmetrikus Boole-függvény gyenge és erős fokát. Ehhez előbb egy definíció.

5.5. Definíció. *Legyen f szimmetrikus Boole-függvény. f előjelváltásainak számát úgy definiáljuk, mint az*

$$a_0 := f(-1, -1, -1, ..., -1),$$

$$a_1 := f(+1, -1, -1, ..., -1),$$

$$a_2 := f(+1, +1, -1, ..., -1),$$

$$\vdots$$

$$a_n := f(+1, +1, +1, ..., +1)$$

sorozat előjelváltásainak számát.

5.6. Következmény. *Legyen f szimmetrikus Boole-függvény. f gyenge és erős foka egyaránt egyenlő f előjelváltásainak számával.*

Bizonyítás. Legyen az f előjelváltásainak száma k. Ekkor könnyen konstruálhatunk olyan g egyváltozós polinomot, amelynek a signuma az m helyen azonos az előző definícióban megadott $\{a\}$ sorozat m-dik tagjával, és fokszáma k. A

$$g\left(\sum_{i\in[n]} \frac{x_i + 1}{2}\right)$$

legfeljebb k fokú polinom erősen előjelreprezentálja f-et.

Ezzel beláttuk, hogy $\deg_s(f) \leq k$. A fordított irányú egyenlőtlenség bizonyításához tekintsük az $f \cdot PAR$ Boole-függvényt. $f \cdot PAR$ előjelváltásainak száma láthatóan éppen $n - k$. A fentiek szerint tehát $\deg_s(f \cdot PAR) \leq n - k$.

$$(n-k) + k \geq \deg_s(f \cdot PAR) + \deg_s(f) \geq \deg_s(f \cdot PAR) + \deg_w(f) = n.$$

Itt az első egyenlőtlenség előbbi meggondolásaink eredménye, a második a triviális 4.20, a harmadik pedig éppen az 5.4. Tétel.

Mindenütt egyenlőség áll, amiből a bizonyítandó állítás azonnal következik. $\square$

Az állításból látszik, hogy egy tipikus szimmetrikus Boole-függvény gyenge foka $n/2$. Feltehetjük a kérdést általános Boole-függvényekre is. Aspnes et al. az alábbi meglepő sejtést fogalmazza meg.

5.7. Sejtés. **(Aspnes et al.)** *A $2m$-változós f Boole-függvények* $(1-o(1))$ *részére* $\deg_w(f) = m$.

A $2m+1$*-változós f Boole-függvények* $(1/2 - o(1))$ *részére* $\deg_w(f) = m$, *és másik* $(1/2 - o(1))$ *részére* $\deg_w(f) = m+1$.

Ebben az irányban Gotsman [Got] is ért el eredményeket, de a legerősebb becslés Razborov és Rudich [RR] munkája. Érdekességként megjegyezzük, hogy Razborovék ezen eredmény alapján bizonyos negatív következtetéseket vontak le Aspnes et al. módszereinek élesíthetőségéről.

5.8. Tétel. **(Razborov-Rudich)** *Az n-változós f Boole-függvények* $(1 - o(1))$ *részére*

$$\deg_w(f) \geq n/20.$$

Ezt az állítást nem bizonyítjuk.

5.2. Approximáció a valósok felett

5.9. Definíció. *Az f Boole-függvényt az r pszeudo-Boole függvény ε hibával* **approximálja**, *ha legfeljebb $2^n\varepsilon$ darab $x \in V^n$ csúcs kivételével $r(x) = f(x)$.*
Az f Boole-függvényt az r pszeudo-Boole függvény ε hibával **előjelapproximálja**, *ha legfeljebb $2^n\varepsilon$ darab $x \in V^n$ csúcs kivételével* $\operatorname{sgn} r(x) = f(x)$.

Felhívjuk a figyelmet a 3.8. Definícióval való analógiára. Később, az 5.13 Definícióban, csakúgy mint a $\mathbb{Z}_3$ feletti approximáció definícióját, ezt is kiterjesztjük tetszőleges bemeneti valószínűségeloszlás esetére.

Most következő tételünkkel kapcsolatba hozzuk egy függvény előjelapproximálhatóságát a gyenge fokával.

5.10. Tétel. **(Aspnes et al.)** *Tegyük fel, hogy egy f Boole-függvényt egy r polinom úgy előjelapproximál, hogy a hibázó pontok halmaza $S \subset V^n$. Legyen $k \in [n]$ a legkisebb olyan szám, amelyre*

$$|S| < \binom{n}{\leq k}.$$

Ekkor

$$\deg(r) \geq \deg_w(f) - 2k$$

Bizonyítás. A bizonyítás azon alapul, hogy az S halmazhoz keresünk egy olyan polinomot, amelynek kicsi a fokszáma, sehol sem negatív, nem azonosan 0, de S minden elemén 0. Ezzel megszorozva az előjelapproximáló polinomot az eredmény gyengén előjelreprezentálja f-et.

Nem meglepő módon ezt a sehol sem negatív polinomot egy olyan polinom négyzeteként fogjuk keresni, amelynek kicsi a fokszáma, nem azonosan 0, de S minden elemén 0. Ennek létezését szavatolja az alábbi lemma.

5.11. Lemma. *Ha $S \subset V^n$, és $|S| < \binom{n}{\leq k}$, akkor létezik olyan $p(x)$ nem azonosan 0, k-adfokú polinom, amely S-en azonosan 0.*

A Lemma bizonyítása. Egy n-változós k-adfokú polinomnak $\binom{n}{\leq k}$ együtthatója van, és V^n egyes pontjain felvett értékei ezeknek lineáris kombinációi. (Ezeket a lineáris kombinációkat egzakt módon meg is adtuk a 4.10. Állításban.) Így az, hogy a polinom értéke egy adott pontban 0, egy homogén lineáris egyenlőséggel írható fel, melynek változói a polinom k-nál nem nagyobb fokú monomjainak együtthatói. Az, hogy a p az egész S-en eltűnik, e szerint azzal ekvivalens, hogy p együtthatói egy $|S|$ sorból és $\binom{n}{\leq k}$ oszlopból álló homogén lineáris egyenletrendszert kielégítenek. Az $|S| < \binom{n}{\leq k}$ feltétel miatt ennek létezik nemtriviális megoldása, ami éppen a keresett polinomnak felel meg. □

A Tétel bizonyítása. Szorozzuk meg r-et az előző lemma által adott p polinom négyzetével. Az eredmény fokszáma $\deg(r) + 2k$, és gyengén előjelreprezentálja f-et. A gyenge fok definíciója szerint

$$\deg(r) + 2k \geq \deg_w(f)$$

□

Most alkalmazzuk a PAR függvényre a fentieket, megkapva ezzel a 3.9. Tétel megfelelőjét a valós előjelapproximáció esetére.

5.12. Következmény. *Egy $\sqrt{n}$ fokú pszeudo-Boole függvény a PAR Boole-függvényt csak $\Omega(1)$ hibával képes előjelapproximálni.*

Bizonyítás. Tegyük fel, hogy az r pszeudo-Boole függvény fokszáma $\sqrt{n}$, és az $S \subset V^n$ halmaz pontjaitól eltekintve előjelreprezentálja PAR-t. A 4.25. Következmény szerint $\deg_w(PAR) = n$. Alkalmazzuk az 5.10. Tételt:

$$\sqrt{n} \geq n - 2k,$$

ahol k a legkisebb olyan szám, amelyre $|S| < \binom{n}{\leq k}$.

$$k \geq \frac{n}{2} - \frac{\sqrt{n}}{2}$$

A Chernoff-korlát (3.10. Állítás) alkalmazásával éppen a bizonyítandó állítást kapjuk. $\square$

5.3. AND approximálása

Most bizonyítjuk azt a tételt, amely Smolensky 3.12. Tételének közvetlen megfelelője a valós számtest feletti approximáció-fogalomra. 1990-91-ben egymástól többé-kevésbé függetlenül több kutatócsoport is [BGS2][ABFR] [Tar2][AH] megalkotta a tételt lényegében azonos formában.

Emlékeztetünk rá, hogy a 3.12. Tétel szerint az AND tetszőleges bemeneti eloszlás mellett kis hibával approximálható a $\mathbb{Z}_3$ feletti kis fokszámú polinommal.

Először megadjuk a 3.11. Definíció megfelelőjét a valós esetre.

5.13. Definíció. *Legyen π valószínűségeloszlás a V^n halmazon. f legyen Boole-függvény, r pszeudo-Boole függvény.*
Azt mondjuk, hogy r az f-et ε hibával **approximálja** *a π bemeneti eloszlás mellett, ha $Pr_\pi(f(x) = r(x)) \leq \varepsilon$*
Azt mondjuk, hogy r az f-et ε hibával **előjelapproximálja** *a π bemeneti eloszlás mellett, ha $Pr_\pi(f(x) = \operatorname{sgn} r(x)) \leq \varepsilon$*

Beigel-Reingold-Spielman, Aspnes-Beigel-Furst-Rudich, Tarui, Allender-Hertrampf eredménye:

5.14. Tétel. *Legyen l pozitív egész, és π tetszőleges valószínűségeloszlás V^n-en. Ekkor az n-változós AND-függvényhez létezik a racionálisok feletti $l \log n$-fokú polinom, amely $(2/3)^l$ hibával approximálja a π bemeneti eloszlás mellett.*

Megjegyzés. Hangsúlyozzuk, hogy nem előjelaprroximációról, hanem approximációról van szó.

Bizonyítás. A bizonyítás hasonlít a 3.12. Tétel bizonyításához, de szükség van egy új ötletre. Ez Valiant és Vazirani egy korábbi lemmája [VV].

Az alfejezet hátralévő részében $k := \lceil \log n \rceil + 1$. Legyen $J \subseteq [n]$, $J \neq \emptyset$. Definiáljuk a $\{Z_i : i \in [k]\}$ véletlen halmazsorozatot az alábbi módon:
$Z_1 := [n]$, és Z_{i+1}-et úgy kapjuk Z_i-ből, hogy Z_i minden elemét egymástól függetlenül $\frac{1}{2}$ valószínűséggel kihagyjuk.

5.15. Lemma. **(Valiant-Vazirani)**

$$Pr(\exists i \in [k] : |Z_i \cap J| = 1) \geq 1/3$$

A lemmának megadjuk egy Lukács Andrástól származó szemléletes átfogalmazását: Egy radioaktív atom felezési ideje pontosan egy nap. Előállítunk belőle egy tetszőleges dózist. Ezek után minden nap pontban délben megvizsgáljuk az elbomlatlan anyag mennyiségét. Ekkor Valiant és Vazirani lemmája szerint legalább 1/3 valószínűséggel lesz olyan nap, amikor a déli vizsgálat pontosan egy atomot talál.

A Lemma bizonyítása.

A tömörebb tárgyalás kedvéért bevezetjük az alábbi jelölést: $p_i := |Z_i \cap J|$ Az alábbi három eset közül pontosan egy áll fenn.

I. eset. $p_1 = 1$.

II. eset. $p_i > 1$ minden $i \in [k]$-ra. Ennek valószínűsége legfeljebb $n2^{-k} \leq$ $\leq 1/2$.

III. eset. Valamilyen $i \in [k-1]$-re $p_i > 1$, de $p_{i+1} \leq 1$.

Tetszőleges j-re az alábbi feltételes valószínűségek:

$$Pr(p_{j+1} = 0 | p_j = m) = 2^{-m}$$

$$Pr(p_{j+1} = 1 | p_j = m) = m2^{-m}$$

Ezért $m \geq 2$ esetén

$$Pr(p_{j+1} = 0 \mid (p_j = m) \wedge (p_{j+1} = 0 \vee 1)) = \frac{2^{-m}}{m2^{-m} + 2^{-m}} = \frac{1}{m+1} \leq \frac{1}{3}$$

E szerint arra az i-re, amelyre $p_i > 1$, és $p_{i+1} \leq 1$, legalább 2/3 valószínűséggel $p_{i+1} = 1$.

A I. és III. eset együtt legalább 1/2 valószínűségű, tehát legalább 1/3 annak a valószínűsége, hogy valamely $i \in [k]$-ra $p_i = 1$. $\square$

A lemma segítségével k-adfokú véletlen polinomot alkotunk, amely legalább 1/3 valószínűséggel -1, ha a bemenet nem azonosan 1, és mindig 1, ha a bemenet azonosan 1. Legyen $\{Z_i : i \in [k]\}$ a lemmában szereplő véletlen halmazsorozat. p_i-vel most polinomot jelölünk.

$$p_i(x) := \sum_{-x_j \in Z_i} \frac{x_j + 1}{2} \qquad i \in [k]$$

$p_i(x)$ éppen az x-ben Z_i-beli pozícióban levő (-1)-ek számával egyenlő.

Definiáljuk a p véletlen, k-adfokú polinomot:

$$p := \prod_{i=0}^{k} (1 - p_i)$$

Ha x azonosan 1, akkor minden $p_i(x) = 0$, tehát $p(x) = 1$. Ellenkező esetben a Lemma szerint legalább 1/3 valószínűséggel valamelyik $p_i(x)$ egyenlő 1-gyel, és a szorzat nulla lesz. $2p - 1$ tehát legalább 1/3 valószínűséggel egyenlő $AND(x)$-szel.

Innen a bizonyítás technikája azonos a 3.12. Tétel bizonyításával; először ismétléssel csökkentjük a hibát, majd kettős leszámlálást alkalmazunk.

A hiba csökkentéséhez válasszuk a $p^{(1)}, p^{(2)}, ..., p^{(l)}$ polinomokat úgy, hogy a definiáló $\{Z_i\}$ véletlen halmazsorozatok egymástól függetlenek legyenek. Tekintsük a

$$2\left(\prod_{i\in[l]} \frac{p^{(i)} + 1}{2}\right) - 1$$

polinomot. Ez a valószínűségi változó-polinom minden x bemenetre legfeljebb $(2/3)^l$ valószínűséggel hibázik. Van tehát egy polinomcsaládunk, amely csupa $l \log n$ fokú polinomból áll, és minden x-re legalább az $(1 - (2/3)^l)$-edrészük jól reprezentálja AND-et. A tétel bizonyításához már csak egy kettős leszámlálást kell alkalmazni. Ebből következik, hogy van olyan eleme a polinomcsaládnak, amely a π bemeneti eloszlás mellett $(1 - (2/3)^l)$ valószínűséggel egyenlő AND-del. Ezzel az állítást bizonyítottuk.

5.4. Boole-hálózatból polinom

Ez a fejezet szintén hasonlítani fog a megfelelő 3.3. Fejezetre. Ott a véges test használata lehetővé tette a MOD_3-kapuk használatáról szóló 3.1 általánosítását a klasszikus 2.13. Tételnek. Mint látni fogjuk, itt a valósok használata egy más irányú általánosítást tesz lehetővé.

5.16. Lemma. *Legyen $l \in \mathbb{N}$. Ha egy $\{AND, OR, NOT\}$-hálózat mérete N és mélysége k, akkor a hálózat approximálható $N/2^l$ hibával egy valósok feletti $(2l)^k$ fokszámú polinommal.*

Bizonyítás. Első lépésként a deMorgan-szabály alkalmazásával az OR-kapukat lecseréljük AND és NOT kapukra. Ez a hálózat méretét legfeljebb megháromszorozza.

A hálózatot a bemenetektől a kimenetek felé haladva topologikus sorrendben (2.4. Definíció) kapunként alakítjuk polinommá. Kezdőlépésként az x_i bemeneteket az x_i polinomokkal reprezentáljuk. ($i \in [n]$).

Ha egy kapu sorra kerül, akkor a topologikus sorrend definíciója szerint a bemeneteire már megadtuk az approximáló polinomokat. Legyenek ezek $g_1(x), g_2(x), ..., g_m(x)$. Két esetet különböztetünk meg aszerint, hogy milyen kapuról van szó.

I. eset: NOT**-kapu** A kimenet ekkor 0 hibával reprezentálható a $-g_1$ polinommal, amely a bemenet elsőfokú polinomja.

II. eset: AND**-kapu** A V^n halmazon vett egyenletes eloszlás indukál egy π eloszlást a $(g_1(x), g_2(x), ..., g_m(x))$ vektorra nézve.

Az indukált π eloszlásra alkalmazzuk a 5.14. Tételt. Ez egy olyan h m-változós polinomot ad, amely $1 - 1/2^l$ π-valószínűséggel a g_i bemenetek AND függvénye lesz. π választása és az indukált eloszlás definíciója miatt a $h(g_1(x), ...g_m(x))$ polinom $1/2^l$ hibával approximálja az $AND(g_1(x), ...g_m(x))$ függvényt, ha az x-et egyenletes eloszlással választjuk V^n-ből.

Összefoglalva: a kapu kimenete minden esetben approximálható a kapu bemeneteinek legfeljebb $(2l)$-fokú polinomjával, úgy, hogy a hálózat azon inputjainak aránya, amelyekre ez a kapu hibás eredményt ad, legfeljebb $1/2^l$.

Az i. szinten az előző szintek kapuiból alkotott polinomok legfeljebb $(2l)$-fokú polinomjai szerepelnek. Így a fokszám minden szinten az előző szint maximális fokszámának $(2l)$-dik hatványával becsülhető. A teljes fokszám tehát legfeljebb $(2l)^k$.

Minden egyes kapu a bemenetek (nem a saját bemenetei, hanem a legalsó szint bemenetei) legfeljebb $1/2^l$-ed részén hibázik. Így a globális hiba legfeljebb $N/2^l$. □

5.17. Tétel. *PAR nem számítható olyan k mélységű, $2^{o(n^{1/2k})}$ méretű $\{AND, OR, NOT\}$-Boole-hálózattal, amelynek a legfelső szintjén egy THR-kapu van.*

Bizonyítás. Válasszuk l-et $(\frac{1}{2}n^{1/2k})$-nak, és alkalmazzuk az előző lemmát a PAR Boole-függvényt számító hálózat legfelső THR kapujának összes bemenetére. Ezek után értelemszerű módon a hálózat kimenetét **előjel**-approximálhatjuk a polinomok egy lineáris függvényével. Ekkor a nyert polinom fokszáma éppen $\sqrt{n}$, és a polinom $N/(2^{1/2n^{1/2k}})$ hibával előjel-approximálja PAR-t. A 5.12. Tétel szerint egy $\sqrt{n}$ fokú polinom PAR-t $\Omega(1)$ hibával képes csak approximálni. Tehát

$$N = \Omega(2^{\frac{1}{2}n^{1/2k}}),$$

és ezzel a 5.17. Tétel bizonyítását befejeztük. □

6. ε-közelítés

A Boole-függvények eddig bevezetett algebrai reprezentációi és azoknak megfelelő bonyolultsági mértékei (az approximálhatóság különböző verziói, gyenge és erős fok) után most egy olyant tárgyalunk, amely talán még az előbbieknél is természetesebb.

6.1. Definíció. *Legyen $0 \le \varepsilon < 1$. Az f Boole-függvényt az r pszeudo-Boole függvény* ε**-közelíti**, *ha*

$$\forall x \in V^n : |f(x) - r(x)| \le \varepsilon.$$

6.2. Definíció. *Az f Boole-függvény* ε**-közelítő foka**, $\deg_\varepsilon(f)$ *a legkisebb fokú pszeudo-Boole függvény foka, amely ε-közelíti f-et.*

Definíciónk azonnali következményei:

6.3. Állítás. $\deg_0(f) = \deg(f) \qquad \deg_\varepsilon(f) \le \deg(f)$

Felmerül a kérdés, hogy becsülhető-e alulról nemtriviális módon $\deg(f)$-nek valamilyen függvényével $\deg_\varepsilon(f)$? Ezt a kérdést válaszolja meg Nisan és Szegedy dolgozata [NS].

6.4. Tétel. (Nisan-Szegedy) *Minden fix $0 \le \varepsilon < 1$ mellett*

$$\deg(f) = O(\deg_\varepsilon^8(f))$$

minden f Boole-függvényre,

A Tétel szerint tehát ha egy függvény fokszáma nagy, akkor közelíteni sem lehet sokkal kisebb fokszámmal.

Nisan és Szegedy bizonyításában a kulcslemma nem más, mint a tétel bizonyítása egy speciális esetben. Mi a következő alfejezetben [NS] nyomán bizonyítjuk ezt a speciális esetet. (6.15. Tétel)

A becsléshez Nisan és Szegedy ezután több egyenlőtlenséget ékel közbe, melyek Nisan [Nis2] illetve Blum-Impagliazzo [BI] korábbi eredményei. Érdekes módon bár a becslés két algebrai jellegű mennyiséget hoz kapcsolatba, a közbeékelt mennyiségek között van kombinatorikai (a blokkszenzitivitás), és bonyolultságelméleti jellegű (a döntési fa mélység és CREW PRAM bonyolultság). Ezeket a mennyiségeket nem definiáljuk.

Éppen a többlépcsős becslés az oka, hogy a meglehetősen nagy 8-as kitevő megjelenik a becslésben. Nisan és Szegedy azt sejtik, hogy ez távol van az optimálistól:

6.5. Sejtés. (Nisan-Szegedy) *Minden fix $0 \le \varepsilon < 1$ mellett*

$$\deg(f) = O(\deg_\varepsilon^2(f))$$

minden f Boole-függvényre.

Most definiáljuk az approximációelméletben alapvető fontosságú Csebisev polinomokat.

6.6. Definíció. *Ha $|x| \le 1$, akkor*

$$T_n(x) := \cos(n \text{ arc } \cos x).$$

Ha $|x| \ge 1$, akkor

$$T_n(x) := \text{ch}\,(n \,\text{arch}\, x).$$

T_n éppen egyenlő egy n-edfokú polinommal. Ezt nevezzük az **n-dik Csebisev polinomnak**.

A Csebisev-polinomok legfontosabb tulajdonságait összefoglaljuk. Bizonyításuk megtalálható bármelyik approximációelméleti monográfiában, mint például [Riv].

6.7. Állítás.

I. tulajdonság. $|T_n(x)| \le 1$, *ha* $|x| \le 1$.

II. tulajdonság. $|T_n'(x)| \le n^2$, *ha* $|x| \le 1$.

III. tulajdonság. $|T_n'(x)| \ge n^2$, *ha* $|x| \ge 1$.

A Csebisev-polinomok segítségével könnyen konstruálhatunk kis fokszámú, az OR függvényt közelítő pszeudo-Boole függvényt.

6.8. Állítás. *Minden elég nagy n-re*

$$\deg_\varepsilon(OR) \le \frac{1}{\sqrt{2}}\text{arch}\left(\frac{2}{\varepsilon}\right)\sqrt{n}.$$

Bizonyítás. Legyen c pozitív valós, és $k := c\sqrt{n}$. Tekintsük a

$$p(x) := \frac{T_k\left(\frac{x}{n-1}\right)}{T_k\left(\frac{n}{n-1}\right)}$$

egyváltozós polinomot. Elemi becslésekből levezethető, hogy

$$T_k\left(\frac{n}{n-1}\right) \geq \operatorname{ch}\left(\sqrt{2}\frac{k}{\sqrt{n}}\right) = \operatorname{ch}(\sqrt{2}c).$$

Ez a p polinom tehát az n-ben 1, és $0 \leq x \leq n-1$-re $p(x)$ abszolút értékben legfeljebb $1/\operatorname{ch}(\sqrt{2}c)$. Ebből következik, hogy a

$$1 - 2p\left(n - \sum_{i\in[n]} \frac{x_i+1}{2}\right)$$

pszeudo-Boole függvény $2/\operatorname{ch}(\sqrt{2}c)$ hibával közelíti az OR függvényt. Ha adott az ε hiba, akkor a megfelelő c ebből kiszámítható, és éppen az állításban megköveteltnek adódik. □

Ez a példa mutatja, hogy az 6.5. Sejtés tovább nem élesíthető, hiszen $\deg OR = n$.

6.1. A Szimmetrizációs Lemma

Legyen f szimmetrikus pszeudo-Boole függvény. Ekkor f-nek megfeleltethetjük azt az $\tilde{f}$ legfeljebb n-edfokú egyváltozós polinomot, amelyre

$$\tilde{f}(k) = f(-1,-1,...,-1,+1,,...,+1,+1)$$

ahol a $+1$-ek száma k. Az $\tilde{f}$ polinom egyértelmű, hiszen $(n+1)$ ponton interpolál.

6.9. Állítás. $\deg f = \deg \tilde{f}$

Bizonyítás. Világos, hogy a

$$g(x) := \tilde{f}\left(\sum_{i\in[n]} \frac{x_i+1}{2}\right)$$

$\deg\tilde{f}$-fokú polinom interpolálja az f pszeudo-Boole függvényt. Ez a polinom nem feltétlenül multilineáris. Multilinearizáltját jelöljük h-val. (3.6. Definíció). A multilinearizálás a fokszámot csak csökkentheti, ami mutatja, hogy $\deg f \leq \deg\tilde{f}$. A g maximális fokú monomjai a

$$\left(\sum_{i\in[n]} \frac{x_i+1}{2}\right)$$

kifejezés $\deg\tilde{f}$-edik hatványra emelésével állnak elő. A hatványozást elvégezve látható, hogy h maximális fokú monomjai éppen a n változóból képezett $\deg\tilde{f}$ darab csupa különböző tényezőből álló szorzatok, azonos együtthatóval. Ebből azonnal következik, hogy

$$\deg h = \deg\tilde{f}.$$

A spektrális alak egyértelműsége miatt f azonos h-val. □

Most definiáljuk egy függvény szimmetrizáltját. A definíció Minsky és Papert nevéhez fűződik [MP]. Ők az alább bizonyítandó Szimmetrizációs Lemmát arra használták, hogy levezessék a $\deg_s(PAR) = n$ egyenlőséget, dolgozatunk 4.25. Állítását.

6.10. Definíció. *Legyen $r \in \mathbb{R}^{V^n}$. r* **szimmetrizáltja**

$$r^{symm}(x_1, ..., x_n) := \frac{1}{n!} \sum_{\pi \in S_n} r(x_{\pi(1)}, ..., x_{\pi(n)}).$$

(S_n az $[n]$ permutációcsoportja.)
Ugyanez a formula definiálja egy n-változós polinom szimmetrizáltját.

A szimmetrizáció egy pszeudo-Boole függvényhez hozzárendeli azt a pszeudo-Boole függvényt, amely az összes k darab $+1$-et tartalmazó bemenetre ugyanazt az értéket veszi fel: az eredeti függvénynek a k darab $+1$-et tartalmazó bemeneteken vett átlagát. Világos, hogy egy pszeudo-Boole függvény szimmetrizáltja szimmetrikus pszeudo-Boole függvény, és egy polinom szimmetrizáltja szimmetrikus polinom. Szimmetrikus pszeudo-Boole függvény szimmetrizáltja önmaga. A szimmetrizáció talán legfontosabb tulajdonsága, hogy nem növeli a fokszámot:

6.11. Lemma. $\deg r^{symm} \le \deg r$.

Bizonyítás. Ha r spektrális alakja a multilineáris $\hat{r}$ polinom, akkor r szimmetrizáltjának spektrális alakja éppen az $(\hat{r})^{symm}$ multilineáris polinom. Ez utóbbi az $\hat{r}(x_{\pi(1)}, ..., x_{\pi(n)})$ polinomok átlaga, és ezek mindannyian $\deg r$ fokú polinomok. Ebből az állítás következik. □

Az $f \mapsto \tilde{f}$ leképezést eddig csak szimmetrikus pszeudo-Boole függvényekre definiáltuk.

6.12. Definíció. *Egy f tetszőleges pszeudo-Boole függvényre a $\tilde{f}$ egyváltozós polinomot a $\widetilde{f^{symm}}$ képlettel definiáljuk.*

A 6.9. Állítás és a 6.11. Lemma következménye:

6.13. Lemma. **(Szimmetrizációs Lemma)** $\deg\tilde{f} \le \deg f$. □

6.2. Becslés az OR függvényre

Először bizonyítás nélül kimondunk egy alapvető approximációelméleti lemmát.

6.14. Lemma. (Markov) *Legyen p egyváltozós d fokú valós polinom, és $[a_1, a_2]$ tetszőleges intervallum. Legyen b olyan pozitív valós, hogy minden $a_1 \leq x \leq a_2$-re $-b \leq p(x) \leq b$. Ekkor $[a_1, a_2]$ minden x elemére*

$$|p'(x)| \leq \frac{2d^2 b}{a_2 - a_1}.$$

Nisan és Szegedy ezt a lemmát felhasználva alsó becslés adnak egy speciális Boole-függvény-osztály közelítő fokára. Fontos megjegyeznünk, hogy az OR függvény benne van ebben az osztályban.

6.15. Tétel. (Nisan-Szegedy) *Ha az f Boole-függvény a csupa -1 csúcsban -1, és az összes szomszédos csúcsban $+1$, akkor*

$$\deg_\varepsilon(f) \geq \sqrt{\frac{1-\varepsilon}{2} n}.$$

Bizonyítás. Tegyük fel, hogy r a kívánt mértékben közelíti f-et. Alkalmazzuk a Szimmetrizációs Lemmát (6.13. Lemma) r-re. Egy $p := \tilde{r}$ egyváltozós polinomot kapunk, amelynek fokszámát jelöljük d-vel. p a következő tulajdonságokkal rendelkezik:

0. $d \leq \deg r$.

I. $-1-\varepsilon \leq p(0) \leq -1+\varepsilon$. (hiszen $p(0) = r(-1, -1, ..., -1)$)

II. $+1-\varepsilon \leq p(1) \leq +1+\varepsilon$.

III. $-1-\varepsilon \leq p(k) \leq +1+\varepsilon$, ha $2 \leq k \leq n$ egész.

I.-ből és II.-ből a Lagrange-féle középértéktétel szerint következik, hogy létezik olyan $0 \leq x \leq 1$, hogy
IV. $|p'(x)| \geq \frac{(+1-\varepsilon)-(-1+\varepsilon)}{1-0} = 2(1-\varepsilon)$.

Be fogjuk látni, hogy a III. és IV. feltételt kielégítő polinom legalább $\sqrt{\frac{1-\varepsilon}{2} n}$ fokú.

Ha egy intervallumon egy polinom mindenütt kicsi, de a deriváltja nem mindenütt kicsi, akkor a Markov-lemma szavatolja, hogy a polinom fokszáma nagy. Mi a III. feltétel szerint nem egy intervallumon, hanem csak egy intervallum egész pontjain tudjuk a polinomról, hogy kicsi. Most kiterjesztjük a

becslést a teljes intervallumra:
$c := \max\{|p'(x)| : 0 \leq x \leq n\}$ (IV. szerint $c \geq 2(1-\varepsilon)$.)

III.-ból a Lagrange-féle középértéktétel segítségével következik

$$-1-\varepsilon-c/2 \leq p(x) \leq +1+\varepsilon+c/2.$$

Most már alkalmazhatjuk a Markov-lemmát:

$$c \leq \frac{2d^2(1+\varepsilon+c/2)}{n}$$

Átrendezve:

$$d^2 \geq \frac{cn}{c+2+2\varepsilon} \geq \frac{2(1-\varepsilon)n}{2(1-\varepsilon)+2+2\varepsilon} = \frac{1-\varepsilon}{2}n.$$

Ebből az O. állítás alapján a bizonyítandó állítás már következik. □

A 6.8. Állítást figyelembe véve ezzel megkaptuk, hogy

6.16. Következmény. *Minden rögzített* $0 < \varepsilon < 1$*-re*

$$\deg_\varepsilon(OR) = \Theta(\sqrt{n}).$$

A 7. Fejezetben még visszatérünk az OR függvény közelítő fokának kérdésére.

Bár a 6.15. Tétel csak egy meglehetősen speciális függvényosztályra ad alsó becslést, de Nisan és Szegedy megmutatták, hogy ez alapján már minden Boole-függvény közelítő fokára adható becslés. Mint már említettük, mi ezt nem bizonyítjuk.

Most bemutatjuk a 6.15. Tétel egy 'továbbfejlesztett változatát' [Pat].

6.17. Tétel. (Paturi) *Egy f szimmetrikus Boole-függvényre*

$$\Gamma(f) := \min\{|2k-n+1| : \tilde{f}(k) \neq \tilde{f}(k-1), 0 \leq k < n\}.$$

Ekkor

$$\deg_{2/3}(f) = \Theta(\sqrt{n(n-\Gamma(f))}).$$

Speciálisan

$$\deg_{2/3}(MAJ) = \Omega(n).$$

Itt $\Gamma(f)$ nem más, mint annak az $n/2$-re szimmetrikus, egész intervallumnak a hossza, amelyen $\tilde{f}$ konstans.

Paturi tételének bizonyítása Markov lemmájához (6.14. Lemma) hasonló nemtriviális approximációelméleti alsó becsléseken alapul. Ezek az eredmények szintén polinomok intervallumon való viselkedéséről szólnak. Nisan és Szegedy bizonyításában fontos lépés a 'diszkretizáció'. (Így nevezzük a bizonyításnak azt a lépését, amikor a $[0, n]$ intervallumon való viselkedésről szóló approximációelméleti eredményből hasonló eredményre következtetünk a $\{0, ..., n\}$ véges halmazon.) Nisan és Szegedy bizonyításában a diszkretizáció a Lagrange-féle középértéktétel alapján lényegében nyilvánvaló volt. Paturi bizonyításában a nehézség abból adódik, hogy ez esetben az éles eredmény eléréséhez nem elegendő a középértéktétel használata. Paturi bizonyos trigonometrikus polinomok konstruálásának segítségével hidalja át ezt a nehézséget, amelyekkel beszorozva a szimmetrizáltat az eredetileg csak egész pontokban kicsi polinom a teljes intervallumon kicsivé válik, miközben a derivált egy kitüntetett pontban nem csökken.

7. ε-közelítés adott spektráltartóval

Most azt a kérdést fogjuk vizsgálni, hogy adott $f \in V^{V^n}$, adott $0 \leq \varepsilon < 1$ és adott $\mathcal{S}$ spektráltartó mellett létezik-e olyan $r \in \mathbb{R}^{V^n}$, amely $\mathcal{S}$ spektráltartóval ε-közelíti f-et. Eredményünk egy Aspnes et al. tételéhez (5.3. Tétel) hasonló alternatívatétel lesz, amelynek a következő fejezetben bemutatjuk néhány alkalmazását is.

7.1. Alternatívatétel az ε-közelítésről

Az, hogy egy $r \in \mathbb{R}^{V^n}$ egy $f \in V^{V^n}$ Boole-függvényt ε-közelít, egy lineáris egyenlőtlenségrendszerrel írható le. Azt, hogy $S(r) \subseteq \mathcal{S}$ (speciálisan hogy r foka $\leq d$), egy homogén lineáris egyenletrendszerrel fejezhetjük ki. Írjuk fel ezeket. A felíráshoz egyaránt szükségünk lesz a standard és a spektrális alakra. Mint már láttuk (4.10 . Állítás), ha r-et a csúcsokkal indexelt, és $\hat{r}$-ot a monomokkal indexelt 2^n-dimenziós vektornak tekintjük, akkor a Fourier-transzformáció egy olyan lineáris transzformáció, melynek átmenetmátrixa egy Sylvester-féle H Hadamard-mátrix:

$$\hat{r} = \frac{1}{2^n} H r \qquad\qquad r = H\hat{r}$$

Ha kikötjük, hogy $S(r) \subseteq \mathcal{S}$, akkor az $\hat{r}$ vektor $\mathcal{S}$-en kívüli elemei eltűnnek. Ekkor $\hat{r}$ helyett tekinthetjük azt az $\hat{r}|_{\mathcal{S}}$ vektort, amelynek elemei $\mathcal{S}$

elemeivel vannak indexelve. Ez esetben az $r = H\hat{r}$ transzformációs képlet természetesen az $r = H|_{\mathcal{S}}\,\hat{r}|_{\mathcal{S}}$ alakba megy át, ahol $H|_{\mathcal{S}}$ az a mátrix, amely H $\mathcal{S}$ elemeivel indexelt oszlopaiból áll. A rövidség kedvéért $\hat{r}|_{\mathcal{S}}$ helyett írjunk x-et. Az, hogy létezik $\mathcal{S}$ tartójú, f-et ε-közelítő r, ezek után így írható:

$\exists x \in \mathbb{R}^{\mathcal{S}}$:

$$(☺) \qquad H|_{\mathcal{S}}\, x \le f + \varepsilon\underline{1} \qquad\qquad -H|_{\mathcal{S}}\, x \le -f + \varepsilon\underline{1}$$

(Itt $\underline{1}$ az azonosan 1 Boole-függvényt jelöli.)
Farkas lemmájának egyik változatát (5.1. Lemma) már alkalmaztuk Aspnes et al. Alternatívatételének (5.3. Tétel) bizonyításakor. Most egy másik változatot fogunk használni, és a megfogalmazás módját is megváltoztatjuk, alkalmazkodva fejezetünk nyelvezetéhez.

7.1. Tétel. *Legyen $A \in \mathbb{R}^{[n]\times[m]}$, $b \in \mathbb{R}^{[n]}$. Definiálunk két egyenlőtlenségrendszert. Primál: $Ax \le b \quad (x \in \mathbb{R}^{[n]})$ Duál: $yA = 0$, $\langle y|b\rangle < 0 \quad (y \in \mathbb{R}^{[m]})$ A primál és a duál egyenlőtlenségrendszer közül pontosan egy oldható meg.*

Ha (☺)-ot választjuk a primál egyenlőtlenségrendszernek, akkor a duális egyenlőtlenségrendszer könnyen láthatóan

$$(☹) \qquad \begin{aligned} y_1 H|_{\mathcal{S}} + y_2(-H|_{\mathcal{S}}) &= 0 \\ \langle y_1|f + \varepsilon\underline{1}\rangle + \langle y_2| - f + \varepsilon\underline{1}\rangle &< 0 \end{aligned}$$

Itt $y_1, y_2 \in \mathbb{R}^{V^n}$, és ezek sorvektornak tekintendők.

Átrendezés után:

$$(y_1 - y_2)H|_{\mathcal{S}} = 0$$

$$\langle y_1 - y_2|f\rangle + \varepsilon\,\langle y_1 + y_2|\underline{1}\rangle < 0$$

Ebből az alakból látható, hogy ha y_1, y_2 megoldás, és egy $v \in V^n$ indexre $y_1(v) > 0$, $y_2(v) > 0$, akkor mindkettőből egy kis valós számot levonva y_1, y_2 megoldás marad, hiszen $y_1 - y_2$ nem változik, $\langle y_1 + y_2|\underline{1}\rangle$ pedig csökken. Így tehát feltehetjük, hogy olyan megoldásunk van (☹)-ra, amelyre $\forall v \in V^n : y_1(v)y_2(v) = 0$

Ezután $y := y_2 - y_1$, és ekkor $(y_1 + y_2)(v) = |y(v)|$, amiből $\langle y_1 + y_2|\underline{1}\rangle = \|y\|$ következik.

Eddigi átalakításaink eredménye:

(☹)pontosan akkor oldható meg, ha létezik $y \in \mathbb{R}^{V^n}$: $yH|_{\mathcal{S}} = 0$ $\langle y|f\rangle >$ $> \varepsilon\|y\|$

Az $yH|_{\mathcal{S}} = 0$ feltétel könnyen értelmezhető. Éppen azt jelenti, hogy $S(y)$ diszjunkt $\mathcal{S}$-től. Az $\langle y|f\rangle > \varepsilon\|y\|$ feltétel viszont annyira lényeges lesz későbbi vizsgálataink során, hogy erre önnálló definíciót vezetünk be:

7.2. Definíció. *Legyen $0 \leq \varepsilon < 1$. Egy $y \in \mathbb{R}^{V^n}$* **ε-fedi** *az $f \in V^{V^n}$ függvénnyel, ha $\langle y|f\rangle > \varepsilon\|y\|$.*

A szokásos módon azt mondjuk, hogy f **ε-fedhető $\mathcal{S}$ spektráltartóval**, *ha létezik $r \in \mathbb{R}^{V^n}$, ami ε-fedi f-et, és $S(r) \subseteq \mathcal{S}$.*

A fedésnek ez a definíciója nem igazán szemléletes, nem látszik belőle az sem, hogy itt valamilyen értelemben közelítésről van szó. Ezért megadunk egy nyilvánvalóan ekvivalens, de átláthatóbb definíciót is:

7.3. Definíció. *Egy $y \in \mathbb{R}^{V^n}$* **ε-fedi** *az $f \in V^{V^n}$ függvényt, ha*

$$(1-\varepsilon)\sum\{|y(x)| : x \in V^n, \operatorname{sgn} y(x) = f(x)\} >$$
$$(1+\varepsilon)\sum\{|y(x)| : x \in V^n, \operatorname{sgn} y(x) \neq f(x)\}$$

Az ε-fedés tehát azt jelenti, hogy azon pontok, amelyeken y előjelreprezentálja f-et, $|y|$-súlyukat tekintve többségben vannak a pontok között. (Szemben Aspnes et al. approximáció-definíciójával, ahol darabszámra vannak többségben, de a 'hibázó' pontokon $|y|$ nagy is lehet.)

Új definíciónk birtokában kimondjuk Alternatívatételünket:

7.4. Tétel. *Egy f Boole-függvényre a következő két állítás közül pontosan az egyik teljesül:*

(☺) *f ε-közelíthető $\mathcal{S}$ spektráltartóval.*
(☹) *f ε-fedhető $2^{[n]} \setminus \mathcal{S}$ spektráltartóval.*

Külön kimondjuk tételünk legfontosabb speciális esetét:

7.5. Tétel. *Egy f Boole-függvényre a következő két állítás közül pontosan az egyik teljesül:*

(☺D) $\deg_\varepsilon(f) \leq d$.
(☹D) *$PAR \cdot f$ ε-fedhető $(n-d)$-fokú polinommal.*

Bizonyítás. A bizonyítás teljesen analóg az 5.4. Tétel bizonyításával. Alkalmazzuk a 7.4. Alternatívatételt az $\mathcal{S} = \binom{[n]}{\leq d}$ esetben. $\square$

Most tételünkből speciális esetként levezetjük Aspnes et al. 5.3. Alternatívatételét. Ehhez két lemmát bizonyítunk, amelyek megvilágítják az ε-közelítés, a ε-fedés, illetve a gyenge és erős előjelreprezentáció kapcsolatát. Az első lemma bizonyítása kerekítési, a másodiké kompaktsági jellegű.

7.6. Lemma. *A következő két állítás ekvivalens:*

1. *f erősen előjelreprezentálható $\mathcal{S}$ spektráltartóval.*
2. *Létezik olyan $0 \leq \varepsilon < 1$, amelyre f ε-közelíthető $\mathcal{S}$ spektráltartóval.*

7.7. Lemma. *A következő két állítás ekvivalens:*

1. *f gyengén előjelreprezentálható $\mathcal{S}$ spektráltartóval.*
2. *f minden $0 \leq \varepsilon < 1$-re ε-fedhető $\mathcal{S}$ spektráltartóval.*

A két lemmából és az 7.4. Tételből nyilvánvalóan következik a 5.3. Tétel.

Az 7.6 Lemma bizonyítása. A $\Leftarrow$ irány nyilvánvaló. A $\Rightarrow$ irány bizonyításához tegyük fel, hogy r erősen előjelreprezentálja f-et $\mathcal{S}$ spektráltartóval.

$$c := \min\{|r(v)| : v \in V^n\}$$

$$d := \max\{|r(v)| : v \in V^n\}$$

Nyilvánvaló, hogy az $\frac{1}{d}r$ függvény értékei abszolút értékben $\frac{1}{cd}$ és 1 közé esnek, tehát $1 - \frac{1}{cd}$-közelíti f-et. $\square$

Az 7.7 Lemma bizonyítása. Egy f Boole-függvényt egy r pszeudo-Boole függvény pontosan akkor gyengén előjelreprezentál, ha $\langle f|r\rangle = \|r\|$. Ekkor nyilván minden 1-nél kisebb ε-ra $\langle f|r\rangle > \varepsilon \|r\|$. Ezzel a $\Leftarrow$ irányt beláttuk.

A $\Rightarrow$ irány bizonyításához tekintsük az 1 l_1-normájú pszeudo-Boole függvények halmazát. Ez kompakt részhalmaza a pszeudo-Boole függvényeknek az l_1-norma által indukált topológiában. Messük el ezt a halmazt azon pszeudo-Boole függvények lineáris terével, amelyeknek spektráltartója benne van $\mathcal{S}$-ben. Ez a lineáris tér zárt részhalmaza $\mathbb{R}^{V^n}$ -nek a fenti topológiában, tehát a metszet is kompakt. Jelölje a metszetet K. K-n értelmezzük az alábbi folytonos funkcionált:

$$\Phi(r) := \langle r|f\rangle$$

Ha r ε-fedi f-et, akkor $r/\|r\|$ is, tehát feltehetjük, hogy az f-et fedő r függvény K-ban van. Az, hogy f minden $0 \leq \varepsilon < 1$-re ε-fedhető $\mathcal{S}$ spektráltartóval, ezek után azzal ekvivalens, hogy $\sup_D \Phi = 1$. Ebből viszont D kompaktsága és Φ folytonossága miatt következik, hogy létezik $r \in D$, amelyre $\langle r|f\rangle = 1$. r nem azonosan 0, hiszen normája 1. Ez az r előjelreprezentálja f-et $\mathcal{S}$ spektráltartóval. □

7.2. Az Alternatívatétel alkalmazása

Most bemutatjuk az 7.5. Tétel egy alkalmazását, amely némileg megjavítja Nisan és Szegedy megfelelő eredményének, a 6.15. Tételnek az OR függvényre való alkalmazását.

7.8. Tétel. *A következő két állítás közül pontosan egy teljesül:*

1. $\deg_\varepsilon(OR) \leq d$.
2. *Létezik olyan f egyváltozós, $n-d$ fokú polinom, amelyre*

$$2f(0) > \varepsilon \sum_{k=0}^{n} \binom{n}{k} |f(k)|$$

Bizonyítás. A 7.5. Tétel szerint OR pontosan akkor **nem** ε-közelíthető d fokú polinommal, ha létezik olyan $r \in \mathbb{R}^{V^n}$, $\deg r \leq n-d$, amelyre

$$\langle r|OR \cdot PAR\rangle > \varepsilon \|r\|.$$

Feltéve, hogy $d \geq 1$, látható, hogy a keresett r-re $\langle r|PAR\rangle = 0$. Ezt kivonva az előző egyenlőtlenségből:

$$\varepsilon \|r\| < \langle r|PAR \cdot (\underline{1} - OR)\rangle = \langle r|\underline{1} - OR\rangle = 2r(-1,-1,...,-1)$$

Azt kaptuk, hogy a keresett r olyan pszeudo-Boole függvény, amelynek l_1-normája majdnem teljesen a csupa-(-1) csúcsba összpontosul. r-et a szimmetrizációs technika szellemében

$$r(x) = f\left(\sum_{i\in[n]} \frac{x_i+1}{2}\right)$$

alakban keressük, ahol f egyváltozós polinom. Ekkor könnyen láthatóan

$$\|r\| = \sum_{k=0}^{n} \binom{n}{k} |f(k)|.$$

f-nek ki kell elégítenie egyrészt a $\deg f \leq n - d$ feltételt, másrészt a következő egyenlőtlenséget:

$$2f(0) > \varepsilon \sum_{k=0}^{n} \binom{n}{k} |f(k)|$$

A Szimmetrizációs Lemma (6.13. Lemma) triviális következménye, hogy a keresett r létezése ekvivalens a megfelelő paraméterű f egyváltozós polinom létezésével, más szóval nem önkényes választás r-et ilyen speciális alakban keresni. □

A feltételeket kielégítő, lényegében optimális f polinom konstrukciója Kós Géza eredménye [Kós], az ő szíves hozzájárulásával közöljük.

7.9. Tétel. **(Kós Géza)** *Ha n elég nagy, $c \leq 1.37$, és $m = c\sqrt{n}$, akkor létezik olyan f legfeljebb $n - m$ fokú egyváltozós polinom, amelyre*

$$2f(0) > \varepsilon(c) \sum_{k=0}^{n} \binom{n}{k} |f(k)|,$$

ahol

$$\varepsilon(c) = \frac{1}{\mathrm{ch}\,(2c) + 1/2}.$$

A bizonyítás Csebisev polinomok elemi tulajdonságat felhasználó konstrukció, és mellőzzük.

Ebből az eredményből eddigi meggondolásaink alapján könnyen kiszámolható:

7.10. Tétel. *Ha n elég nagy, és $\varepsilon \geq 0.1911$, akkor*

$$\deg_\varepsilon(OR) \geq \frac{1}{2}\mathrm{arch}\left(\frac{1}{\varepsilon} - \frac{1}{2}\right)\sqrt{n}.$$

Néhány konkrét ε értékre kiszámoljuk a konstansokat:

7.11. Következmény. *Elég nagy n-re*

$$\deg_{0.2}(OR) \geq 1.0923\sqrt{n}$$

$$\deg_{0.3}(OR) \geq 0.8509\sqrt{n}$$

$$\deg_{0.4}(OR) \geq 0.6585\sqrt{n}$$

Ezek a becslések valamivel megjavítják Nisan és Szegedy megfelelő eredményeit, melyek szerint

7.12. Állítás. *Elég nagy n-re*

$$\deg_{0.2}(OR) \geq 0.6324\sqrt{n}$$

$$\deg_{0.3}(OR) \geq 0.5616\sqrt{n}$$

$$\deg_{0.4}(OR) \geq 0.5477\sqrt{n}$$

A 6.8. Állítás által adott megfelelő felső becslések:

7.13. Állítás. *Elég nagy n-re*

$$\deg_{0.2}(OR) \leq 2.1165\sqrt{n}$$

$$\deg_{0.3}(OR) \leq 1.8276\sqrt{n}$$

$$\deg_{0.4}(OR) \leq 1.6210\sqrt{n}$$

Megjegyezzük, hogy nagy ε értékekre Nisan és Szegedy tétele ad jobb eredményt.

8. Közelítés racionális törtfüggvényekkel

Ebben a fejezetben a PAR függvényt számoló 2 mélységű szintezett THR-hálózatokkal foglalkozunk, amelyekkel már találkoztunk a a 4.5. Alfejezetben. Ott a 4.29. Állításban megadtunk egy konstrukciót, amely n kapuval számolja PAR-t. Természetes várakozás, hogy ez optimális a kapuk számát tekintve az ilyen hálózatok között. Azonban ez az egyszerűnek tűnő állítás nehéznek bizonyul, máig megoldatlan. Mi most egy gyengébb állítást fogunk belátni. Ez Paturi és Saks [PS] eredménye.

8.1. Tétel. (Paturi-Saks) *PAR nem számítható szintezett, 2 mélységű, $n/\log^2 n$ méretű, poly súlyú THR-hálózattal.*

Az eredmény nem igazán erős, a bizonyítás azonban érdekes ötleten alapul, amely a későbbiekben több jelentős eredmény [BGS1][Bei3] kiindulópontjául szolgált. Ezek Ez az ötlet a racionális törtfüggvényekkel való közelítés használata. A 8.1. Tétel erősebb, súly-megkötéssel nem élő változatát azonban nem ezzel, hanem a véletlen megszorítások módszerével bizonyították Impagliazzo, Paturi és Saks [IPS].

8.1. Kockaszeletelés

Egy küszöb-kapunak megfelel egy hipersík, a kaput definiáló lineáris kifejezés nullhelyeinek halmaza. Az általánosság megszorítása nélkül feltehetjük, hogy ez nem tartalmaz csúcsot.

Paturi és Saks első, sikertelennek bizonyult bizonyítási ötlete a következő egyszerű megfigyelésen alapult:

8.2. Állítás. *Egy 2 mélységű, PAR-t számoló szintezett THR-hálózat első szintjén lévő kapuinak megfelelő hipersíkok elmetszik a V^n kocka minden élét.*

Megjegyzés. A metszés alatt egyetlen belső pontban való metszést értünk.

Bizonyítás. A hipersíkok $\mathbb{R}^n$-t konvex tartományokra bontják. Ha két pont azonos tartományba esik, akkor a második szintű kapu számára 'egyformán viselkednek'. A PAR függvény jellemzője, hogy a kocka szomszédos csúcsain különböző értékeket vesz fel. Tehát a kocka szomszédos csúcsai nem eshetnek azonos tartományba, akkor viszont van őket elválasztó a hipersíkok között. Ez természetesen elmetszi az őket összekötő élet. □

8.3. Definíció. *Az n-dimenziós kocka* **nyesési száma**, *$N(n)$, azon hipersíkok minimális száma, amelyek együtt elmetszik a kocka összes élét.*

A fentiek szerint $N(n)$ alsó becslés a 2 mélységű, PAR-t számoló THR-hálózat első szintjén lévő kapuinak számára. Paturi és Saks azt sejtették, hogy $N(n) = \Omega(n)$, ami konstans szorzótól eltekintve optimális becslést adott volna az eredeti kérdésre. Ezt azonban nem tudták bebizonyítani, sőt $N(n)$ értékére a későbbiekben sem születtek elég jó becslések. Az alábbiakban összefoglaljuk a kocka-nyesési probléma jelenlegi állását.

Az $N(n) =?$ kérdést először O'Neil fogalmazta meg 1971-ben [ON], majd egymástól függetlenül többen is újra feltették.

$N(n) \leq n$, amit három alapvetően különböző konstrukció is mutat. Ezek közül kettő triviális, és a harmadik is egyszerű. Az első az $\{x_k = 0 : k \in [n]\}$ hipersíkcsalád, azaz a kocka felező merőleges hipersíkjai.

A második, az

$$f_k(x) := \sum_{i\in[n]} \frac{x_i + 1}{2} - k - \frac{1}{2} \quad (k \in [n])$$

hipersíkcsalád, amely egymással párhuzamos, a kockára 'átlós' állású síkokból áll, és amellyel már találkoztunk a 4.29. Állítás bizonyítása során.

A harmadik, amelyet csak páratlan n-re definiálunk, úgy kapható, ha az $x_1 + x_2 + ... + x_{\lfloor \frac{n}{2} \rfloor} - x_{\lceil \frac{n}{2} \rceil} - x_{\lceil \frac{n}{2} \rceil + 1} - ... - x_n = 0$ hipersíkra alkalmazzuk az $x_1 \to x_2 \to ... \to x_n \to x_1$ lineáris leképezés hatványait.

Minthogy ezen három konstrukció olyan hipersíkcsaládokat ad, amelyek nem csökkenthetők a kocka-nyesési tulajdonság elvesztése nélkül, és mivel nem volt ismert ezeknél jobb konstrukció, ezért azok a kutatók, akik feltettek az $N(n)$ nagyságára vonatkozó kérdést, egyben megkockáztatták az $N(n) = n$ sejtést is. Ez az $n \leq 3$ esetben könnyen ellenőrizhető, és $n = 4$-re Emamy-Khansary [Em] bizonyította. Ezután meglepetésként hatott Paterson következő konstrukciója, amely cáfolja a sejtést $n = 6$-ra. [Alo][Sak]

8.4. Állítás. **(Paterson)** *A V^6 kockát nyesi az alábbi hipersíkrendszer:*

$$\begin{array}{rcrcrcrcrcrcr}
y_1 & := & +2x_1 & + & 2x_2 & + & 2x_3 & + & 6x_4 & + & 6x_5 & - & 8x_6, \\
y_2 & := & -4x_1 & - & 4x_2 & - & 4x_3 & + & 6x_4 & + & 6x_5 & - & 2x_6, \\
y_3 & := & +6x_1 & + & 6x_2 & + & 6x_3 & + & 2x_4 & + & 2x_5 & - & 8x_6, \\
y_4 & := & -2x_1 & - & 2x_2 & - & 2x_3 & + & 6x_4 & + & 6x_5 & + & 12x_6, \\
y_5 & := & +6x_1 & + & 6x_2 & + & 6x_3 & + & 2x_4 & + & 2x_5 & + & 16x_6.
\end{array}$$

8.5. Állítás. *$N(n)$ szubadditív, azaz $N(n+m) \leq N(n) + N(m)$*

Bizonyítás. Ha $\{a^k(x_1, x_2, ..., x_n) : k \in K\}$ nyeső síkcsalád V^n-hez, és $\{b^l(x_1, x_2, ..., x_n) : l \in L\}$ nyeső síkcsalád V^m-hez, akkor

$$\{a^k(x_1, ..., x_n) : k \in K\} \cup \{b^l(x_{n+1}, x_{n+2}, ..., x_{n+m}) : l \in L\}$$

nyeső síkcsalád V^{n+m}-hez. $\square$

8.6. Következmény. $N(n) \leq \lceil \frac{5}{6} n \rceil$

Ez a legjobb ismert felső becslés $N(n)$-re. A legjobb ismert alsó becslés O'Neil egy tételének [ON] teljesen triviális alkalmazásával adódik. Ezt a tételt nem bizonyítjuk.

8.7. Tétel. **(O'Neil)** *Egy hipersíkkal a kockának legfeljebb $\lceil n/2 \rceil \binom{n}{\lceil n/2 \rceil}$ élét metszhetjük el.*

Megjegyzés. Ez a becslés éles is a fentebb definiált $f_{\lfloor \frac{n}{2} \rfloor}$ síkra.

A kocka éleinek számát, $n2^{n-1}$-t elosztva ezzel a számmal megkapjuk az alábbi alsó becslést $N(n)$-re:

8.8. Következmény. $N(n) = \Omega(\sqrt{n})$ $\square$

8.2. THR közelítése törtfüggvénnyel

Racionális törtfüggvénynek nevezzük két n-változós polinom hányadosát. Mindig olyan polinomokat választunk nevezőnek, amelyek a szokásos értelmezési tartományon, V^n-en nem tűnnek el. Így a racionális törtfüggvény meghatároz egy pszeudo-Boole függvényt. A törtfüggvény **fokszámát** mint a számláló és a nevező fokszámának összegét definiáljuk.

A 6.17. Tétel szerint egy THR-függvényt általában nem lehet $o(n)$ fokszámú polinommal ε-közelíteni. Mint látni fogjuk, racionális törtfüggvényekkel sokkal jobb a helyzet.

Az alábbiakban bemutatjuk Newman [New] konstrukcióját az abszolútérték függvényt közelítő kis fokszámú racionális törtfüggvényre.

$$\xi := e^{-1/\sqrt{k}}$$

$$p(x) := \prod_{i=0}^{k-1} (x + \xi^i)$$

$$R_k(x) := x \frac{p(x) - p(-x)}{p(x) + p(-x)}$$

8.9. Tétel. **(Newman)** *R_k egy $(2k+1)$ fokú racionális törtfüggvény.*

$$\forall x \in [-1,1] : ||x| - R_k(x)| \leq 3e^{-\sqrt{k}}$$

Newman tételét nem bizonyítjuk. Segítségével a nem túl nagy súlyú THR-függvény ε-közelítésére könnyen konstrukciót adhatunk.

Legyen az $f \in THR$ az $f(x) = \operatorname{sgn}\left(\sum_{i\in[n]} w_i x_i + w_0\right)$ kifejezéssel definiálva, ahol a w_i súlyok egészek, és abszolútérték-összegük, azaz f súlya legyen u.

8.10. Tétel. **(Paturi-Saks)** *Legyen $k \in \mathbb{N}$ A fenti f közelíthető $2k+2$ fokú racionális törtfüggvénnyel $3ue^{-\sqrt{k}}$ hibával.*

Bizonyítás. Vegyük észre, hogy V^n-re megszorítva

$$f(x) = |\sum_{i\in[n]} w_i x_i + w_0| / (\sum_{i\in[n]} w_i x_i + w_0).$$

Osszuk el a számlálót és a nevezőt u-val. u definíciója szerint ekkor a számláló és a nevező egyaránt -1 és $+1$ közötti szám lesz, ha $x \in V^n$. A számlálót a 8.9. Tétel szerint közelíthetjük az

$$R_k(\sum_{i\in[n]} w_i x_i + w_0)$$

$2k+1$ fokú racionális törtfüggvénnyel, legfeljebb $3e^{-\sqrt{k}}$ hibával. A nevező $(\sum_{i\in[n]} w_i x_i + w_0)/u$. Feltettük, hogy ez sehol nem 0 a kockán. A súlyok egészek, tehát $|(\sum_{i\in[n]} w_i x_i + w_0)/u|$ legalább $1/u$.

$$R_k(\sum_{i\in[n]} w_i x_i + w_0)/((\sum_{i\in[n]} w_i x_i + w_0)/u)$$

tehát legfeljebb $3ue^{-\sqrt{k}}$ hibával közelíti f-et. □

8.3. THR-hálózatból törtfüggvény

Ha a $p(x)/q(x)$ k-adfokú racionális törtfüggvény előjelreprezentálja az f Boole-függvényt, akkor a $p(x)q(x)$ k-adfokú polinom is előjelreprezentálja f-et. Ezt az egyszerű észrevételt kombinálva a 4.25. Következménnyel a következőt kapjuk:

8.11. Lemma. *PAR nem erősen előjelreprezentálható n-nél kisebb fokú racionális törtfüggvénnyel.* □

Most 8.10. Tétel segítségével, racionális törtfüggvénnyel előjelreprezentálunk egy 2-szintes THR-hálózatot.

8.12. Lemma. *A 2 mélységű szintezett $N+1$ kapus, U súlyú THR-hálózat kimenete előjelreprezentálható $N(2k+2)$ fokú polinommal, feltéve hogy $3U^2e^{-\sqrt{k}} < 1$.*

Bizonyítás. Legyenek az első szintű THR-kapuk $h_1, h_2, ..., h_N$, a kimeneti THR-kapu pedig

$$\operatorname{sgn} g(y) := \operatorname{sgn}\left(\sum_{m\in[N]} w_m y_m + w_0\right).$$

Ennek súlyát jelöljük u-val. Az első szintű h_m THR-kaput a 8.10. Tétel segítségével $3ue^{-\sqrt{k}}$ hibával közelítjük a $\tilde{h}_m$ $2k+2$-fokú racionális törtfüggvénnyel. A

$$G(x) := g(h_1(x), h_2(x), ..., h_N(x))$$

függvényt ezután közelítsük a következővel:

$$\tilde{G}(x) := g(\tilde{h}_1(x), \tilde{h}_2(x), ..., \tilde{h}_N(x))$$

$\tilde{G}$ éppen N darab $2k+2$-fokú racionális törtfüggvény lineáris kombinációja, ebből azonnal következik, hogy legfeljebb $N(2k+2)$ fokú. Másrészt a közelítés hibája legfeljebb u-szorosa az egyes kapuk közelítéséből adódó hibáknak, ahol u a legfelső kapu súlya. Az $U^2 e^{-\sqrt{k}} < 1/3$ feltétel miatt tehát a $\tilde{G}$ egynél kisebb hibával közelíti G-t. G nullától különböző egész szám, tehát G és $\tilde{G}$ előjele azonos, $\tilde{G}$ előjelreprezentálja a hálózat által számított függvényt. $\square$

A **8.1. Tétel bizonyítása** Tegyük fel, hogy egy a 8.1. Tétel feltételeinek eleget tevő hálózat-sorozat számolja a PAR függvényt. A hálózatok súlya $poly(n)$, azaz létezik c, hogy minden n-re az n. hálózat súlya legfeljebb n^c. Ekkor könnyen látható. hogy létezik olyan elég nagy c' konstans, hogy ha $k = c' \log^2 n$, akkor a 8.12. Lemmát alkalmazva a hálózatainkból $O(N(n) \log^2 n)$ fokú racionális törtfüggvényeket kapunk, amelyek előjelreprezentálják a PAR függvényt. Alkalmazva a 8.11. Lemmát éppen a bizonyítandó állítást kapjuk:

$$N(n) = \Omega(n/\log^2 n)$$

$\square$

9. Interpoláció analitikus függvényekkel

Smolensky [Smo2] nevéhez fűződik egy más jellegű kísérlet az analízis technikáinak felhasználására bonyolultsági alsó becslésekhez. Ebben a modellben $\mathbb{C}^n$-beli analitikus függvényekkel reprezentáljuk a Boole-függvényt. A reprezentáció talán a legtermészetesebb: a reprezentáló függvény V^n-re megszorítva azonos a reprezentálandó függvénnyel. A bevezetett bonyolultsági mérték, a differenciáldimenzió ellenben nem hasonlít az eddig tárgyalt mértékekre.

9.1. A differenciáldimenzió

Legyen $S \subset \mathbb{C}^n$ véges halmaz, és jelöljük T-vel az S-ből $\mathbb{C}$-be képező függvények terét.

9.1. Definíció. *Egy $f : \mathbb{C}^n \to \mathbb{C}$ analitikus függvény differenciáldimenziója (röviden diffdimenziója) az S halmaz felett az f minden rendű parciális deriváltfüggvényei által feszített függvénytér S-re való megszorításának dimenziója a T térben.*

9.2. Definíció. *$f : S \to \mathbb{C}$ diffdimenziója a diffdimenziók minimuma az összes analitikus függvényeken, melyeknek S-re való megszorítása f.*

Alkalmazásainkban S-et V^n-nek fogjuk választani, de a fogalom megértéséhez lássunk egy egyszerű példát $n = 1$-re és $S = [m] - re$.

Példa. Mennyi $f : [m] \to \mathbb{C}$ diffdimenziója, ha $f(k)$-t a k. Fibonacci-számnak választjuk? Ismeretes, hogy $f(k)$ alkalmas $\lambda_1, \lambda_2, c_1, c_2$ konstansokkal $c_1\lambda_1^k + c_2\lambda_2^k$ alakba írható. A $c_1\lambda_1^x + c_2\lambda_2^x$ analitikus függvénynek tetszőleges rendű deriváltja is ilyen alakú, csak a c_1 és c_2 értéke változik. Tehát az összes derivált benne van a λ_1^x és λ_2^x által generált függvénytérben. Az f függvény diffdimenziója tehát 2.

9.3. Definíció. *Egy $v \in \mathbb{C}^n$ vektorra definiáljuk az f analitikus függvény* **eltoltját** *a következőképpen: $f_v(x) := f(x - v)$*

Most új mértékünk egy ekvivalens definícióját adjuk.

9.4. Állítás. *A parciális deriváltak által T-ben feszített altér azonos az f összes eltoltja által T-ben feszített altérrel. f diffdimenziója tehát egyenlő a z f összes eltoltja által V-ben feszített altér dimenziójával.*

A Taylor-sorfejtésen alapuló egyszerű bizonyítást nem részletezzük. □

9.5. Következmény. *Ha találunk k darab $v \in \mathbb{C}^n$ vektort, amelyekre az $f_v|_S$ függvények lineárisan függetlenek, akkor az f diffdimenziója legalább k.*

Ennek segítségével mutatunk egy konkrét Boole-függvényt, amelynek nagyon nagy a diffdimenziója.

9.6. Állítás. *$EQ(x) := AND((x_1x_2), (x_3x_4), ..., (x_{n-1}x_n))$ diffdimenziója legalább $2^{n/2}$. ($S := V^n$)*

Bizonyítás. Legyen f az EQ-t interpoláló analitikus függvény. Egy $\omega = (\varepsilon_1, ..., \varepsilon_{n/2})$ nulla-egy-vektorhoz definiáljuk az f_ω eltoltat:

$$f_\omega(x_1, x_2, ..., x_n) := f(x_1, x_2 + 2\varepsilon_1, x_3, x_4 + 2\varepsilon_2, ..., x_{n-1}, x_n + 2\varepsilon_{n/2})$$

Azt állítjuk, hogy ezek az eltoltak lineárisan függetlenek. Tekintsük V^n-nek azt a részkockáját, amelynek páros koordinátái (-1)-ek. f_ω ezen a kockán -1 értéket vesz fel mindenütt, kivéve az $(1-2\varepsilon_1, -1, 1-2\varepsilon_2, -1, ..., 1-2\varepsilon_{n/2}, -1)$ helyen. A 9.5. Következményből az állítás nyilvánvaló. □

Smolensky-t az motiválta a definíció megalkotásakor, hogy olyan mértéket keresett, amely minden szimmetrikus függvényre kicsi, de bizonyos függvényekre nagy értékeket is felvehet.

9.7. Tétel. *Szimmetrikus Boole-függvény diffdimenziója legfeljebb $n+1$.*

Bizonyítás. A Young-tétel szerint egy szimmetrikus függvény k-adrendű parciális deriváltjai egyenlőek. Egy a kockán értelmezett szimmetrikus függvény interpolálható legfeljebb n-edfokú szimmetrikus polinommal. Ennek pedig a Young tétel miatt csak $n+1$ különböző parciális deriváltja van, hiszen az n-nél magasabb rendű deriváltak azonosan nullák. □

9.2. $SYMM$-hálózatból analitikus függvény

9.8. Tétel. *Egy k méretű, m befokú $SYMM$-hálózat által számított Boole-függvény diffdimenziója (a V^n halmaz felett) legfeljebb $(m+1)^k$.*

Bizonyítás. Jelöljük σ_j-vel a j-dik kapu bemeneteinek összegét. Könnyen látható, hogy a j-dik kapu kimenete interpolálható

$$y_j(x) := e^{\frac{2\pi i}{m+1}\sigma_j(x)}$$

egy polinomjával.

Vizsgáljuk meg y_k parciális deriváltját x_l szerint.

$$\frac{\partial}{\partial x_l} e^{\frac{2\pi i}{m+1}\sigma_k(x)} = \left(\frac{\partial}{\partial x_l}\frac{2\pi i}{m+1}\sigma_k(x)\right) y_k$$

σ_k maga is y_j-k lineáris kombinációja ($j < k$). Ezért a parciális deriválást végig elvégezve az y_j függvények szorzataiból alkotott kifejezések lineáris kombinációját kapjuk. Ez igaz marad akkor is, ha a valamelyik változó szerinti parciális deriválást ismételten elvégezzük. Más szóval a kimeneti Boole-függvényt interpoláltuk egy olyan analitikus függvénnyel, amelyre a minden rendű parciális deriváltfüggvények által feszített függvényteret a

$$\prod_{j=1}^{k} y_j^{d_j} \qquad (d_j \in \mathbb{N})$$

függvények generálják.

Vegyük észre, hogy mivel σ_j a V^n halmazon csak egész értékeket vesz fel, ezért minden j-re

$$y_j^{m+1}(x) = 1 \qquad (x \in V^n)$$

Tehát a d_j kitevőkről feltehetjük, hogy $(m+1)$-nél kisebbek. Így az egész függvényteret generálni tudtuk $(m+1)^k$ függvénnyel. Éppen ezt akartuk bizonyítani. □

Az alsó és a felső becslés triviális kombinálásával a következő tételt kapjuk:

9.9. Tétel. **(Smolensky)** *Az EQ Boole-függvényt számító, m befokú $SYMM$-hálózat mérete* $\Omega(n/\log m)$. □

10. Köszönetnyilvánítás

A szerző a legkülönbözőbb okokból köszönetet mond Antal Kálmánnénak, Király Zoltánnak, Tardos Gábornak, Katona Gyulának, Frank Andrásnak, Hídvégi Zoltánnak, ifj. Antal Kálmánnak, Fleiner Balázsnak, Wiener Gábornak, de legfőképpen Friedl Katalinnak és Kós Gézának.

Irodalom

[Aj] M. Ajtai. σ_1^1-formulae on finite structures. Annals of Pure and Applied Logic, 24:1-48, 1983.

[All] E. Allender. A note on the power of threshold circuits. In Proc. 30th FOCS, pp. 580-584, 1989.

[AH] E. Allender, U. Hertrampf. On the power of uniform families of constant depth threshold circuits. In Proc. 15th International Symp. on Math. Foundations of Computer Science, pp. 158-164, 1990.

[Alo] N. Alon. Személyes Beszélgetés

[ABFR] J. Aspnes, R. Beigel, M. Furst, S. Rudich. The expressive power of voting polynomials. In Proc. 23rd STOC, pp. 402-409, 1991.

[Bei1] R. Beigel. The Polynomial Method in Circuit Complexity. In. Proc 8th Structure, pp. 82-95, 1993.

[Bei2] R. Beigel. Perceptrons, PP, and the polynomial hierarchy. In Proc. 7th Structures, pp. 14-19, 1992.

[Bei3] R. Beigel. When do extra majority gates help? polylog(n) majority gates are equivalent to one. In Proc. 24th STOC, pp. 450-454, 1992.

[BGS1] R. Beigel, N. Reingold, D. Spielman. PP is closed under intersection. In Proc. 23th STOC, pp. 1-9, 1991.

[BGS2] R. Beigel, N. Reingold, D. Spielman. The perceptron strikes back. In Proc. 6th Structures, pp. 286-291, 1991.

[BI] M. Blum, R. Impagliazzo. Generic oracles and oracle classes. In Proc 28th FOCS, pp. 118-126, 1987.

[Bru] J. Bruck. Harmonic analysis of polynomial threshold functions. SIAM J. of Discrete Math., 3(2):168-177, May 1990.

[BS] J. Bruck, R. Smolensky. Polynomial threshold functions, AC^0 functions and spectral norms. SIAM J. of Discrete Math., 21:33-42, 1992.

[Chv] V. Chvatal. Linear Programming. W. H. Freeman and Company, 1983.

[Cla] A. Clarke. A megismerés építőkövei, Osiris, Budapest, 1996.

[Em] M. R. Emamy-Khansary. On the cuts and the cut number of the 4-cube. Journal of Combinatorial Theory Series A, 41:221-227, 1986.

[FSS] M. Furst, J. B. Saxe, M. Sipser. Parity, circuits, and the polynomial-time hierarchy. Math. Systems Theory, 17(1):13-27, 1984.

[GHR] M. Goldmann, J. Håstad, A. A. Razborov. Majority gates vs. general weighted threshold gates. In Proc. 7th Structures, pp. 2-13, 1992.

[GK] M. Goldmann, M. Karpinski. Simulating threshold circuits by majority circuits. In Proc. 25th STOC, pp. 551-560, 1993.

[Got] C. Gotsman. On boolean functions, polynomials and algebraic threshold functions. Manuscript, 1992.

[HMPSG] A. Hajnal, W. Maas, P. Pudlak, M. Szegedy, G. Turan. Threshold circuits od bounded depth. In Proc. 28th FOCS, pp. 99-110, 1987.

[Ha] J. Håstad. Almost optimal lower bounds for small depth circuits. In Advances in Computing Research 5: Randomness and Computation, pp. 143-170, JAI Press, Greenwich, CT, 1989.

[IPS] R. Impagliazzo, M. Paturi, M. Saks. Size-depth trade-offs for threshold circuits. In Proc. 25th STOC, pp. 541-550, 1993.

[KVVY] R. Kannan, H. Venkateswaran, V. Vinay, A. C. Yao. A circuit-based proof of Toda's Theorem. Inf. & Comp., 1993.

[Kar] M. Karchmer. On proving lower bounds for circuit size. In Proc. 8th Structure, pp. 112-118, 1993.

[KL] R. M. Karp, R. J. Lipton. Some connections between nonuniform and uniform complexity classes. In Proc 12th STOC, pp. 302-309, 1980.

[Kós] Kós Géza. Személyes Beszélgetés

[LMN] N. Linial, Y. Mansour, N. Nisan. Constant depth circuits, fourier transforms and learnability. In Proc. 30th FOCS, pp. 574-579, 1989.

[MCP] W. S. McCulloch, W. Pitts. A logical calculus for the ideas immanent in nervous activity. Bull. of Math. Biophysics, 5:115-133, 1943.

[MP] M. Minsky, S. Papert. Perceptrons. MIT Press, Cambridge, Mass., 1969. Expanded edition, 1988.

[New] D. J. Newman. Rational approximation to $|x|$. Michigan Math. Journal, 11:11-14, 1964.

[Nis] N. Nisan. The communication complexity of threshold gates. Manuscript, 1993.

[Nis2] N. Nisan. CREW PRAMs and decision trees. In Proc. 21th STOC, pp. 327-335, 1989.

[NS] N. Nisan, M. Szegedy. On the degree of boolean functions as real polynomials. In Proc. 24th STOC, pp. 462-467, 1992.

[ON] P. O'Neil. Hyperplane cuts of an n-cube. Discrete Math., 1:193-195, 1971.

[Pat] R. Paturi. On the degree of polynomials that approximate symmetric boolean functions. In Proc. 24th STOC, pp. 468-474, 1992.

[PS] R. Paturi, M. Saks. On threshold circuits for parity. In Proc 31st FOCS, pp. 397-404, 1990.

[Ra] A. A. RAZBOROV. Lower bounds for the size of circuits of bounded depth with basis $\{\wedge, \oplus\}$. Math. Notes of the Academy of Sciences of the USSR, 41:(4):333-338, September 1987.

[Ra2] A. A. RAZBOROV. Lower bounds for the monotone complexity of some Boolean functions. Soviet Math. Dokl., 31:354-357, 1985.

[RR] A. A. RAZBOROV, S. RUDICH. Natural Proofs. In Proc. 26th STOC, pp. 204-213, 1994.

[Riv] T. J. RIVLIN. Chebyshev Polynomials. Wiley and Sons, 2nd edition, 1990.

[Sak] M. SAKS. Slicing the hypercube. Manuscript

[Sip] M. SIPSER. Lecture notes on Compexity Theory. Manuscript

[Smo] R. SMOLENSKY. Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In Proc. 19th STOC, pp. 77-92, 1987.

[Smo2] R. SMOLENSKY. On interpolation by analytic functions with special properties and some weak lower bounds on the size of circuits with symmetric gates. In Proc. 31th FOCS, pp. 628-631, 1990.

[Sze] M. SZEGEDY. Algebraic Methods in Lower Bounds for Computational Models with Limited Computations. PhD thesis, The University of Chicago, 1989.

[Tar1] J. TARUI. Degree complexity of Boolean functions and its applications to relativized separations. In Proc. 6th Structures, pp. 382-390, 1991.

[Tar2] J. TARUI. Probabilistic polynomials, AC^0 functions, and the polynomial-time hierarchy. Theoretical Computer Science, pp. 167-183, 1993.

[To] S. TODA. PP is as hard as the polynomial hierarchy. SIAM Journal on Computing, 20(5):865-877, 1991.

[VV] L. G. VALIANT, V. V. VAZIRANI. NP is as easy as detecting unique solutions. Theoretical Computer Science, 47:85-93, 1986.

[Wig] A. WIGDERSON. The fusion method for lower bounds in circuit complexity, Manuscript, 1993.

[Y] A. C. YAO. Separating the polynomial-time hierarchy by oracles. In Proc. 31th FOCS, pp. 1-10, 1985.