TARTALOMJEGYZÉK

Yet now and then your men of wit
Will condescend to take a bit.
— JONATHAN SWIFT, *Cadenus és Vanessa* (1713) [?]

Egy kettes számrendszerbeli számjegy angolul „binary digit”,
röviden – Turkey javaslatára – bit.
— CLAUDE E. SHANNON, (1948) [42]

bit (bit), n . . . fárasztó eszköz . . .
— JESS STEIN és LAURENCE URDANG, *Random House Dictionary of the English Language* (1966) [?]

7.1. Nullák és egyesek

KOMBINATORIKAI ALGORITMUSOK tervezése során általában nagyon oda kell figyelni a hatékonyságra. A szükséges gyorsaság elérésének egyik fontos módszere a megfelelő adatreprezentáció. Érdemes tehát ismereteinket az alapvető reprezentációs technikák területén megerősíteni, mielőtt nekikezdünk a kombinatorikai algoritmusok részletes tanulmányozásának.

A mai számítógépek többnyire a bináris számrendszeren alapulnak az ember által előnyben részesített tízes számrendszer közvetlen alkalmazása helyett. A gépek ugyanis különös ügyességgel kezelik a kétállapotú kapcsolókat – ezek állapotait rendszerint a 0 és az 1 számjegyekkel jelöljük. Az első 6 fejezetben nem használtuk ki, hogy a bináris számítógépek számos olyan dolgot gyorsan meg tudnak csinálni, amit a decimális számítógépek nem. Egy bináris gép a „logikai” vagy „bitenkénti” műveleteket általában éppen olyan könnyedén tudja végrehajtani, mint amilyen könnyen összead vagy kivon. Ezt a lehetőséget eddig azonban ritkán aknáztuk ki. épet bizonyos értelemben arra kértük, hogy „félkézzel” dolgozzon. Láttuk, hogy a bináris és decimális számítógépek sok tekintetben nem különböznek lényegesen egymástól, de a bináris számítógépet bizonyos értelemben arra kértük, hogy „félkézzel” dolgozzon.

A nulláknak és egyeseknek az a meghökkentő képessége teszi a bináris számok tanulmányozását különösen értékessé, hogy kódolni lehet velük az információt éppúgy, mint az objektumok közötti logikai relációkat, sőt még magukat az információt feldolgozó algoritmusokat is. Valójában nem csak a kombinatorikai algoritmusok erősítésére használjuk majd a bitenkénti műveleteket, hanem azt is látni fogjuk, hogy a kétértékű logika tulajdonságai olyan új kombinatorikai problémákhoz vezetnek, amelyek önmagukban is nagyon érdekesek.

A számítástudománnyal foglalkozó kutatók lépésről lépésre egyre jobban megszelídítik a zabolátlan nullákat és egyeseket, és hasznos trükkökre használják fel őket. De mint ahogyan egy epizodista a színpadon, mi is jobban tesszük, ha alaposan megértjük a bináris számok elemi tulajdonságait, mielőtt nekifognánk a magasabb szintű fogalmak és technikák tanulmányozásának. Ezért azoknak az alapvető eljárásoknak a vizsgálatával kezdünk, melyek segítségével biteket és bitsorozatokat kezelhetünk.

7.1.1. Logikai alapok

16 különböző lehetséges olyan $f(x, y)$ függvény van, amelyik adott két bitből, mondjuk az x és az y bitekből, egy harmadik $z = f(x, y)$ bitet állít elő, hiszen az $f(0, 0)$, $f(0, 1)$, $f(1, 0)$ és $f(1, 1)$ függvényértékek mindegyikét kétféleképpen választhatjuk meg. A 7.1. táblázat azokat az elnevezéseket és jelöléseket tartalmazza, amelyeket a formális logikában ezekkel a függvényekkel kapcsolatban hagyományosan használnak; feltéve, hogy 1 az „igaz” és 0 a „hamis” igazságértéket jelöli. A négy függvényértékből álló $f(0, 0)f(0, 1)f(1, 0)f(1, 1)$ sorozatot szokás az f függvény *igazságtáblájának* hívni.

És akkor képzeljünk el egy olyan algebrát, amelyben az x, y, z és a c szimbólumok
a 0 és 1 értékeket és egyedül ezeket veszik fel.
– GEORGE BOOLE, *An investigation of the Laws of Thought* (1854) [?, 2. fejezet 15. alfejezete]

Ellenkezőleg viszont – folytatta Subidu – ha így volna, akkor így lehetne,
ha így lenne, akkor így lehetett volna, de mivel nincs így, hát nem így van. Ez logikus.
– LEWIS CARROLL, *Alice Tükörországban* (1871) [?, 4. fejezet]

Ezeket a függvényeket gyakran „Boole-műveleteknek” nevezzük George Boole [?, ?] iránti tiszteletből. Ő vette először észre, hogy a nullákkal és egyesekkel végzett algebrai műveleteket fel lehet használni egy olyan kalkulus megalkotására, mely támogatja a logikai következtetéseket. Boole azonban sohasem dolgozott a „logikai vagynak” nevezett $\vee$ művelettel, szigorúan a nullákkal és egyesekkel végzett szokásos aritmetikai műveletekhez tartotta magát. Így hát a diszjunkció kifejezésére $x + y$-t írt, de de ügyelt arra, hogy csak akkor használja a jelölést, ha x és y kölcsönösen kizárták egymást (nem volt egyszerre mindkettő 1). Ha pedig szükséges volt, $x + (1-x)y$-t írt, így biztosítva, hogy a diszjunkció eredménye ne lehessen 2.

Amikor Boole angol nyelven előadást tartott, a $+$ műveletről beszélve olykor azt mondta, „and” (és), máskor pedig „or” (vagy). Ez a gyakorlat egy mai matematikus számára különösnek tűnhet, míg rá nem jön, hogy a szóhasználat tulajdonképpen teljesen normális; azt mondjuk ugyanis például, hogy „a kisfiúk és kislányok gyerekek”, ugyanakkor „a gyerekek kisfiúk vagy kislányok”.

Jevons [?, 69. §] kiterjesztette a Boole-kalkulust a szokatlan $x + x = x$ szabállyal, és megmutatta, hogy ha ezt az új $+$ műveletet használjuk, $(x + y)z$ egyenlő $xz + yz$-vel. Azonban a disztributivitás másik, $xy + z = (x + z)(y + z)$ törvényét Jevons nem ismerte fel. Gyaníthatóan a használt jelölés miatt nem vette észre, hisz a második disztributivitási törvénynek nincs megfelelője az aritmetikában. A 7.1. táblázatbeli szimmetrikusabb $x \wedge y$ és $x \vee y$ jelölések könnyebbé teszik számunkra, hogy mindkét disztributivitási törvényt megjegyezzük:

$$(x \vee y) \wedge z \;=\; (x \wedge z) \vee (y \wedge z), \tag{1}$$

$$(x \wedge y) \vee z \;=\; (x \vee z) \wedge (y \vee z). \tag{2}$$

A (2) törvényt Peirce [35] vezette be, aki Jevonstól függetlenül rájött, hogyan kell kiterjeszteni a Boole-kalkulust. Egyébként amikor Peirce [36, 32. oldal] néhány évvel később ezekről a korai eredményekről írt, hivatkozott is a „Jevons-féle összeadással dolgozó *Booli* algebrára”. A „Boole-i” jelző manapság szokatlannak tűnő írásmódja hosszú éveken át

7.1. táblázat.
A TIZENHAT KÉTVÁLTOZÓS LOGIKAI MŰVELET

igazság-tábla	régi és új jelölések	műveleti jel	megnevezések
0000	0	$\perp$	ellentmondás; hamisság; konstans 0
0001	xy, $x \wedge y$, $x \& y$	$\wedge$	konjunkció; … és …; „and”
0010	$x \wedge \bar{y}$, $x \not\supset y$, $[x > y]$, $x \dot{-} y$	$\overline{\supset}$	differencia; …, de … nem
0011	x	$\llcorner$	bal projekció, első diktátor
0100	$\bar{x} \wedge y$, $x \not\subset y$, $[x < y]$, $y \dot{-} x$	$\overline{\subset}$	nem …, de …
0101	y	R	jobb projekció, második diktátor
0110	$x \oplus y$, $x \not\equiv y$, $x\hat{\ }y$	$\oplus$	exkluzív diszjunkció; kizáró vagy; „xor”
0111	$x \vee y$, $x \mid y$	$\vee$	(inkluzív) diszjunkció; … vagy …; „or”
1000	$\bar{x} \wedge \bar{y}$, $\overline{x \vee y}$, $x \mathbin{\overline{\vee}} y$, $x \downarrow y$	$\overline{\vee}$	együttes tagadás; sem …, sem …; „nor”
1001	$x \equiv y$, $x \leftrightarrow y$, $x \Leftrightarrow y$	$\equiv$	ekvivalencia; … akkor és csak akkor, ha …
1010	$\bar{y}$, $\neg y$, $!y$, $\sim y$	$\overline{\mathsf{R}}$	jobb komplemens
1011	$x \vee \bar{y}$, $x \subset y$, $x \Leftarrow y$, $[x \geq y]$, x^y	$\subset$	fordított implikáció; …, ha
1100	$\bar{x}$, $\neg x$, $!x$, $\sim x$	$\overline{\llcorner}$	bal komplemens
1101	$\bar{x} \vee y$, $x \supset y$, $x \Rightarrow y$, $[x \leq y]$, y^x	$\supset$	implikáció; csak akkor …, ha …; ha …, akkor …
1110	$\bar{x} \vee \bar{y}$, $\overline{x \wedge y}$, $x \mathbin{\overline{\wedge}} y$, $x \mid y$	$\overline{\wedge}$	egyszerre nem … és …; „nand”
1111	1	$\top$	tautológia; érvényesség; konstans 1

használatban volt olyannyira, hogy Funk és Wagnalls nagyszótárában még 1963-ban is így jelent meg.

Igazságértékekkel számolni valójában sokkal régebbi dolog, mint a Boole-algebra. A görög filozófusok már a Kr. előtti negyedik században kidolgozták az ítéletlogikát. Figyelemre méltó viták folytak akkoriban arról, hogy mi lesz adott x és y állítások esetén a „ha x, akkor y” állítás helyénvaló igazságértéke. Megarai Philo [?] Kr. e. kb. 300-ban a 7.1. táblázatbeli igazságtáblának megfelelően definiálta ezt, mely szerint egy implikáció igaz, amikor x is, y is hamis. A korai munkák közül sok elveszett, de például Galen [?] (Kr. u. 2. század) munkáiban vannak olyan részletek, melyek hivatkoznak az állításoknak mind a megengedő, mind a kizáró diszjunkciójára. Lásd Bocheński [?] kitűnő tanulmányát a logikának az ókortól a 20. századig tartó fejlődéséről.

Egy kétváltozós $f(x, y)$ függvényt valamilyen alkalmas $\circ$ műveleti jelet használva gyakran $x{\circ}y$ formában írunk. A 7.1. táblázat mutatja azt a tizenhat műveleti jelet, amit a kétváltozós Boole-függvények számára kiválasztottunk; például $\perp$ jelöli azt a függvényt, melynek az igazságtáblája 0000, $\wedge$ a műveleti jele a 0001 függvénynek, $\overline{\supset}$ a 0010-nek, és így tovább. Írhatjuk, hogy $x \perp y = 0$, $x \wedge y = xy$, $x \mathbin{\overline{\supset}} y = x \dot{-} y$, $x \llcorner y = x, \ldots, x \mathbin{\overline{\wedge}} y = \bar{x} \vee \bar{y}$, $x \top y = 1$.

Természetesen a 7.1. táblázatbeli műveletek nem mind egyformán fontosak. Például az első és az utolsó sorban lévők banálisak, mivel x és y értékétől függetlenül konstans az értékük. Négy közülük csak az x, vagy csak az y függvénye. $1 - x$ helyett pedig $\bar{x}$-et írunk x ***komplemense*** kifejezésére.

Azt a négy műveletet, melyeknek igazságtáblája egyetlen egyest tartalmaz, könnyű megadni az $\wedge$ művelettel: $x \wedge y$, $x \wedge \bar{y}$, $\bar{x} \wedge y$, $\bar{x} \wedge \bar{y}$, a három egyest tartalmazókat pedig a $\vee$ művelettel: $x \vee y$, $x \vee \bar{y}$, $\bar{x} \vee y$, $\bar{x} \vee \bar{y}$. A kiindulási $x \wedge y$ és $x \vee y$ függvények a gyakorlatban használhatóbbnak bizonyultak, mint komplemensük vagy félkomplemens párjaik, bár a NOR-nak és NAND-nak nevezett $x \mathbin{\overline{\vee}} y = \bar{x} \wedge \bar{y}$ és $x \mathbin{\overline{\wedge}} y = \bar{x} \vee \bar{y}$ műveletek is érdekesek, mert könnyű őket megvalósítani a tranzisztoros áramkörökben.

1913-ban Scheffer [41] megmutatta, hogy mind a 16 függvényt ki lehet fejezni már egyetlen művelet segítségével is, akár a $\overline{\vee}$, akár a $\overline{\wedge}$ műveletet választjuk (lásd a 4. gyakorlatot). A lényeget tekintve már Peirce is eljutott ugyanehhez az eredményhez 1880 körül, de a témáról szóló dolgozata [?, 4. kötet 12–20. §, 264. oldal] haláláig publikálatlan maradt. A 7.1. táblázatban feltüntettük, hogy a NAND és NOR műveleteket olykor $x \mid y$ és $x \downarrow y$ alakban írjuk; szokás ezeket a jeleket „Sheffer-vonásnak” és „Peirce-nyílnak” is nevezni. Manapság legjobb nem használni Sheffer függőleges vonalát a NAND jelölésére, mert az $x \mid y$ jelöli a bitenkénti $x \vee y$ műveletet a C-hez hasonló programozási nyelvekben.

A 7.1. táblázatban kettő kivételével már minden függvényt megvizsgáltunk. A kimaradt kettő az $x \equiv y$ és az $x \oplus y$, azaz az „ekvivalencia” és a „kizáró vagy”. Ezekkel kapcsolatosak az

$$x \equiv y = \bar{x} \oplus y = x \oplus \bar{y} = 1 \oplus x \oplus y\,, \tag{3}$$

$$x \oplus y = \bar{x} \equiv y = x \equiv \bar{y} = 0 \equiv x \equiv y \tag{4}$$

azonosságok. Mindkét művelet asszociatív (lásd a 6. gyakorlatot). Az ítéletlogikában az ekvivalencia fogalma fontosabb az épp ellentétes jelentésű kizáró vagy fogalmánál; amikor azonban teljes gépi szavakon bitenként végrehajtandó műveletekre gondolunk, a **??**. pontban látni fogjuk, hogy a helyzet éppen fordított: egy tipikus programban a kizáró vagy hasznosabbnak bizonyul az ekvivalenciánál. Annak fő oka, hogy az $x \oplus y$-nak jelentős alkalmazási területei vannak még egyetlen bit esetében is, az a tény, hogy

$$x \oplus y \;=\; (x + y) \mod 2\,. \tag{5}$$

Így tehát kételemű testben (lásd a 4.6. alfejezetben) az $x \oplus y$ és az $x \wedge y$ az összeadást és a szorzást jelentik, és $x \oplus y$ nyilván „tisztán” matematikai tulajdonságokkal is bír.

Alapvető azonosságok. Most vessünk egy pillantást az alapvető $\wedge$, $\vee$, $\oplus$ és $\bar{\ }$ műveletek közötti kapcsolatokra; a többi művelet ugyanis könnyen kifejezhető ennek a négynek a segítségével. A $\wedge$, $\vee$ és $\oplus$ műveletek asszociatívak és kommutatívak. A disztributivitás (1) és (2) törvényein túl még az

$$(x \oplus y) \wedge z \;=\; (x \wedge z) \oplus (y \wedge z) \tag{6}$$

disztributivitás, továbbá az

$$(x \wedge y) \vee x \;=\; (x \vee y) \wedge x \;=\; x \tag{7}$$

elnyelési törvények is érvényesek. A legegyszerűbb, de leghasznosabb azonosságok egyike az

$$x \oplus x \;=\; 0\,, \tag{8}$$

mivel maga után vonja többek között azt, hogy

$$(x \oplus y) \oplus x \;=\; y \text{ és } (x \oplus y) \oplus y \;=\; x\,, \tag{9}$$

ha felhasználjuk azt a nyilvánvaló tényt, hogy $x \oplus 0 = x$. Úgy is fogalmazhatunk, hogy ha ismerjük $x \oplus y$-t, továbbá x és y közül az egyiket, akkor a másikat könnyű meghatározni. És ne feledkezzünk el az egyszerű *komplementálás törvényéről* sem:

$$\bar{x} \;=\; x \oplus 1\,. \tag{10}$$

Egy további fontos azonosságpárt *De Morgan-törvényeknek* nevezünk Augustus De Morgan után. Õ mondta, hogy: „Egy aggregátum ellentettje megegyezik az aggregáltak ellentettjeinek kompozíciójával; egy kompozíció ellentettje pedig a komponáltak ellentettjeinek aggregátumával. Tehát (A, B)-nek és AB-nek ab és (a, b) alakú az ellentettje [9]." Modernebb jelölésekkel ezek épp azok a törvények, melyeket a 7.1. táblázatbeli NAND és NOR műveletekkel kapcsolatban az igazságtáblából olyan magától értetődően nyertünk, nevezetesen hogy

$$\overline{x \wedge y} \;=\; \bar{x} \vee \bar{y}\,, \tag{11}$$

$$\overline{x \vee y} \;=\; \bar{x} \wedge \bar{y}\,. \tag{12}$$

Egyébként Jevons ismerte a (12) azonosságot, de nem ismerte (11)-et: következetesen $\bar{A}B + \bar{B}A + \bar{A}\bar{B}$-t írt $\bar{A} + \bar{B}$ helyett AB komplemensére. Mégsem De Morgan volt az első angol, aki az említett törvényeket feltárta. Két skolasztikus filozófus, Ockham [?] és Burley [?] 14. század eleji írásaiban mindkét törvény megtalálható.

A De Morgan-törvényeket és néhány további azonosságot alkalmazva a $\wedge$, $\vee$ és $\oplus$ műveletek közül bármelyiket ki lehet fejezni a másik kettőt felhasználva:

$$x \wedge y = \overline{\bar{x} \vee \bar{y}} = x \oplus y \oplus (x \vee y)\,, \tag{13}$$

$$x \vee y = \overline{\bar{x} \wedge \bar{y}} = x \oplus y \oplus (x \wedge y)\,, \tag{14}$$

$$x \oplus y = (x \vee y) \wedge \overline{x \wedge y} = (x \wedge \bar{y}) \vee (\bar{x} \wedge y)\,. \tag{15}$$

A **??**. pont **??**. gyakorlata szerint az $x_1 \oplus x_2 \oplus \cdots \oplus x_n$ kiszámításához, ha csak a $\wedge$, $\vee$ és a $^-$ műveleteket lehet használni, legalább $4(n-1)$ lépés szükséges; így ez a három művelet nem igazán jó helyettesítője $\oplus$-nak.

n **változós függvények.** Egy az x, y és z Boole-változóktól függő, azaz háromváltozós $f(x, y, z)$ Boole-függvényt az $f(0,0,0)f(0,0,1)\ldots f(1,1,1)$ 8 bites igazságtáblával adhatunk meg; és általában is, minden n-változós $f(x_1, \ldots, x_n)$ Boole-függvényhez tartozik egy 2^n bites igazságtábla, mely rendre felsorolja az $f(0,\ldots,0,0)$, $f(0,\ldots,0,1)$, $f(0,\ldots,1,0)$, $\ldots$, $f(1,\ldots,1,1)$ függvényértékeket.

Ezeknek a függvényeknek a számára nem szükséges saját neveket és jelöléseket kitalálni, hiszen ki lehet fejezni őket a már megismert kétváltozós függvényekkel. Mint ahogy Zsegalkin [?] észrevette, ha $n > 0$, alkalmasan választott g és h függvények mellett

$$f(x_1, \ldots, x_n) \;=\; g(x_1, \ldots, x_{n-1}) \;\oplus\; h(x_1, \ldots, x_{n-1}) \wedge x_n\,, \tag{16}$$

ahol

$$\begin{aligned} g(x_1, \ldots, x_{n-1}) &= f(x_1, \ldots, x_{n-1}, 0)\,, \\ h(x_1, \ldots, x_{n-1}) &= f(x_1, \ldots, x_{n-1}, 0) \oplus f(x_1, \ldots, x_{n-1}, 1)\,. \end{aligned} \tag{17}$$

(A $\wedge$ művelet végrehajtása megállapodás szerint megelőzi a $\oplus$ műveletet, így (16) jobb oldalán nem kell zárójelek közé tenni a $h(x_1, \ldots, x_{n-1}) \wedge x_n$ részkifejezést.) Ha ezt az eljárást g-vel és h-val rekurzívan addig ismételjük, amíg 0-változós függvényeket nem kapunk, akkor egy olyan kifejezést nyerünk, amelyben csak $\oplus$ és $\wedge$ műveletek és egy 2^n konstansból álló sorozat szerepel. Ráadásul ezeket a konstansokat általában tovább lehet egyszerűsíteni, mert

$$x \wedge 0 = 0 \qquad \text{és} \qquad x \wedge 1 = x \oplus 0 = x\,. \tag{18}$$

Az asszociativitás és a disztributivitás törvényeinek alkalmazása után ott kötünk ki, hogy csak a 0 konstansra van szükségünk, ha $f(x_1, \ldots, x_n)$ azonosan 0, és csak az 1 konstansra, ha $f(0, \ldots, 0) = 1$.

Például

$$\begin{aligned} f(x,y,z) &= ((1 \oplus 0 \wedge x) \oplus (0 \oplus 1 \wedge x) \wedge y) \oplus ((0 \oplus 1 \wedge x) \oplus (1 \oplus 1 \wedge x) \wedge y) \wedge z \\ &= (1 \oplus x \wedge y) \;\oplus\; (x \oplus y \oplus x \wedge y) \wedge z \\ &= 1 \;\oplus\; x \wedge y \;\oplus\; x \wedge z \;\oplus\; y \wedge z \;\oplus\; x \wedge y \wedge z\,. \end{aligned}$$

És látjuk, hogy az (5) szabály miatt simán az

$$f(x,y,z) \;=\; (1 + xy + xz + yz + xyz) \mod 2 \tag{19}$$

polinommal fejezzük be a munkát, hiszen $x \wedge y = xy$. Vegyük észre, hogy ez a polinom lineáris minden változójában (foka ≤ 1). Hasonló számítással általában is megmutatható, hogy minden $f(x_1, \ldots, x_n)$ Boole-függvénynek egyetlen ilyen reprezentációja van; ezt *multilineáris reprezentációnak* nevezzük. A multilineáris reprezentáció az 1, x_1, x_2, x_1x_2, x_3, x_1x_3, x_2x_3, $x_1x_2x_3$, $\ldots$, $x_1x_2 \ldots x_n$, 2^n darab különböző lehetséges kifejezés közül nullának, egynek vagy többnek a modulo 2 összege.

Boole másképpen bontotta fel a Boole-függvényeket. Ez a felbontás a gyakorlatban felmerülő függvények esetében gyakran egyszerűbb. (16) helyett lényegében az

$$f(x_1, \ldots, x_n) \;=\; \big(g(x_1, \ldots, x_{n-1}) \wedge \bar{x}_n\big) \;\vee\; \big(h(x_1, \ldots, x_{n-1}) \wedge x_n\big) \tag{20}$$

összefüggést használta és ezt a „kifejtés törvényének” nevezte, melyben most egyszerűen a

$$\begin{aligned} g(x_1, \ldots, x_{n-1}) &= f(x_1, \ldots, x_{n-1}, 0)\,, \\ h(x_1, \ldots, x_{n-1}) &= f(x_1, \ldots, x_{n-1}, 1) \end{aligned} \tag{21}$$

egyenlőségeket használjuk (17) helyett. Boole eljárását újra meg újra megismételve, felhasználva az (1) disztributivitási szabályt és kiküszöbölve a konstansokat, nulla, egy vagy több *minterm* diszjunkcióját nyerjük, ahol minden egyes minterm egy olyan konjunkció, mint az $x_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge x_4 \wedge x_5$, amelyben jelen van minden változó vagy a változó komplemense. Vegyük észre, hogy egy teljes elemi konjunkció (röviden: minterm) egy olyan Boole-függvény, ami pontosan egy pontban igaz.

Például vizsgáljuk meg az

$$1100\,1001\,0000\,1111 \tag{22}$$

igazságtáblával adott, többé-kevésbé véletlen $f(w,x,y,z)$ függvényt. Ha ezt a függvényt kifejtjük Boole (20) törvényét ismételten alkalmazva, nyolc – az igazságtábla minden 1 értékéhez egy – minterm diszjunkcióját kapjuk:

$$\begin{aligned} f(w,x,y,z) = {} & (\bar{w} \wedge \bar{x} \wedge \bar{y} \wedge \bar{z}) \vee (\bar{w} \wedge \bar{x} \wedge \bar{y} \wedge z) \vee (\bar{w} \wedge x \wedge \bar{y} \wedge \bar{z}) \vee (\bar{w} \wedge x \wedge y \wedge z) \\ & \vee (w \wedge x \wedge \bar{y} \wedge \bar{z}) \vee (w \wedge x \wedge \bar{y} \wedge z) \vee (w \wedge x \wedge y \wedge \bar{z}) \vee (w \wedge x \wedge y \wedge z). \end{aligned} \tag{23}$$

defined $\sum_{k=1}^{0} a_k = 0$ and $\prod_{k=1}^{0} a_k = 1$ in Section 1.2.3.

Szokás mintermek diszjunkcióját *teljes diszjunktív normálformának* is nevezni. Minden Boole-függvényt ki lehet fejezni ilyen módon, és az eredmény egyértelmű, eltekintve természetesen a mintermek sorrendjétől. *Kukacoskodás:* Speciális eset, amikor $f(x_1,\ldots,x_n)$ azonosan nulla. A 0-ra tag nélküli üres diszjunkcióként, az 1-re pedig hasonlóan, üres konjunkcióként is tekinthetünk ugyanazon okok miatt, mint ami miatt a $\sum_{k=1}^{0} a_k = 0$ és a $\prod_{k=1}^{0} a_k = 1$ definíciókat az 1.2.3. pontban megadtuk.

Peirce [36] észrevette, hogy minden Boole-függvénynek van *teljes konjunktív normálformája* is, ami az $\bar{x}_1 \vee x_2 \vee \bar{x}_3 \vee \bar{x}_4 \vee x_5$ formulához hasonló teljes elemi diszjunkciót (röviden minklózok) konjunkciója. Egy minklóz csak egyetlen pontban 0; így egy ilyen konjunkció minden egyes minklóza egy olyan helyről ad számot, ahol az igazságtábla 0. Például a (22)-ben és (23)-ban megadott függvényünk teljes konjunktív normálformája

$$\begin{aligned} f(w,x,y,z) = {} & (w \vee x \vee \bar{y} \vee z) \wedge (w \vee x \vee \bar{y} \vee \bar{z}) \wedge (w \vee \bar{x} \vee y \vee \bar{z}) \wedge (w \vee \bar{x} \vee \bar{y} \vee z) \\ & \wedge (\bar{w} \vee x \vee y \vee z) \wedge (\bar{w} \vee x \vee y \vee \bar{z}) \wedge (\bar{w} \vee x \vee \bar{y} \vee z) \wedge (\bar{w} \vee x \vee \bar{y} \vee \bar{z}). \end{aligned} \tag{24}$$

Azonban az sem meglepő, hogy gyakran nem feltétlenül teljes mintermeket vagy minklózokat tartalmazó diszjunkciókkal és konjunkciókkal szeretnénk dolgozni. Ezért a következő terminológiát vezette be Bernays [?] munkájában: *diszjunktív normálformának* vagy „DNF”-nek szoktuk nevezni konjunkciók diszjunkcióját, azaz egy olyan

$$\bigvee_{j=1}^{m} \bigwedge_{k=1}^{s_j} u_{jk} \;=\; (u_{11} \wedge \cdots \wedge u_{1s_1}) \vee \cdots \vee (u_{m1} \wedge \cdots \wedge u_{ms_m}) \tag{25}$$

alakú kifejezést, ahol u_{jk} *literál*, azaz egy x_i változó vagy ennek komplemense. Hasonlóan pedig *konjunktív normálformának* vagy röviden „KNF”-nek nevezzük literálok diszjunkcióinak konjunkcióját, azaz egy

$$\bigwedge_{j=1}^{m} \bigvee_{k=1}^{s_j} u_{jk} \;=\; (u_{11} \vee \cdots \vee u_{1s_1}) \wedge \cdots \wedge (u_{m1} \vee \cdots \vee u_{ms_m}) \tag{26}$$

alakú kifejezést.

A mai számítógépek lapkáiba beépített rengeteg áramkört „programozható logikai tömbökből” (PLA-kból) állítják össze. Ezek – esetleg komplementált – bemenő jelek ÉS-einek VAGY-jai. Másképpen fogalmazva egy PLA tulajdonképpen egy vagy több diszjunktív normálformát számít ki. Az ilyen építőelemek gyorsak, általános célúak, és aránylag olcsók. Valójában már az 1950-es évek óta kiemelkedő szerepet játszanak a DNF-ek az elektrotechnikában, azóta, amióta a kapcsoló áramköröket megvalósították az olyan többé-kevésbé régimódi készülékekkel, mint a jelfogók és a vákuumcsövek. Az emberek régóta próbálják megtalálni a Boole-függvények különböző osztályai számára a legegyszerűbb DNF-eket, és arra számíthatunk, hogy továbbra is fontos marad a diszjunktív normálformák vizsgálata, hiszen a technológia is folyamatosan fejlődik.

Egy DNF tagjait gyakran *implikánsnak* hívjuk, mivel egy diszjunkció bármelyik tagjának igazsága maga után vonja (implikálja) az egész formula igazságát. Egy olyan formuláról, mint például az

$$f(x, y, z) \;=\; (x \wedge \bar{y} \wedge z) \vee (y \wedge z) \vee (\bar{x} \wedge y \wedge \bar{z}),$$

tudjuk, hogy f igaz, amikor $x \wedge \bar{y} \wedge z$ igaz, azaz amikor $(x, y, z) = (1, 0, 1)$. Vegyük észre ugyanakkor, hogy ebben a példában a rövidebb $x \wedge z$ tag szintén f implikánsa, még ha konkrétan nincs is leírva, hiszen az $y \wedge z$ második tag gondoskodik arról, hogy a függvény y értékétől függetlenül igaz legyen valahányszor $x = z = 1$. Az $\bar{x} \wedge y$ hasonlóan implikánsa függvényünknek, így az egyszerűbb

$$f(x, y, z) \;=\; (x \wedge z) \vee (y \wedge z) \vee (\bar{x} \wedge y) \tag{27}$$

formulával is dolgozhatunk. Ezen a ponton már nincs több lehetséges törlés az implikánsokban, mivel sem x, sem y, sem z, sem $\bar{x}$ nem elég erős feltétel ahhoz, hogy f igazságát maga után vonja.

Egy olyan implikánst, amelyiket nem lehet tovább bontani valamelyik literáljának eltávolításával anélkül, hogy túlságosan gyengévé ne tegyük, *prímimplikánsnak* nevezzük, követve Quine [38]-beli terminológiáját.

Talán legkönnyebben úgy lehet megérteni ezeket az alapvető fogalmakat, ha leegyszerűsítjük a jelölést és szemléletesebb nézőpontot választunk. $f(x_1, \ldots, x_n)$ helyett egyszerűen „$f(x)$"-et írhatunk, és x-re mint egy n hosszúságú $x_1 \ldots x_n$ vektorra vagy bináris füzérre tekinthetünk. Például a (22) függvény a

$$\{0000, 0001, 0100, 0111, 1100, 1101, 1110, 1111\} \tag{28}$$

halmazbeli sorozatokon igaz, és úgy gondolhatunk ezekre a sorozatokra, mint egy $2 \times 2 \times 2 \times 2$-es 4-dimenziós hiperkocka nyolc csúcspontjára. A (28)-beli nyolc pont megfelel azoknak a minterm implikánsoknak, amelyek a (23) teljes diszjunktív normálformában konkrétan megjelennek; bár ezeknek az implikánsoknak valójában egyike sem prím. Például (28) első két pontja a $000{*}$, az utolsó négy pontja az $11{*}{*}$ részkockát alkotja, amennyiben csillag karaktereket használunk a dzsóker jelölésére, ahogy a 6.5. alfejezetben tettük, amikor az adatbázis-lekérdezéseket tárgyaltuk. Így $\bar{w} \wedge \bar{x} \wedge \bar{y}$ és $w \wedge x$ is f implikánsai. Hasonlóan azt is észrevehetjük, hogy a $0{*}00$ részkocka a (28)-beli nyolc pont közül kettőt fed le és a $\bar{w} \wedge \bar{y} \wedge \bar{z}$ implikánst eredményezi.

Általában ilyen módon minden prímimplikáns megfelel egy olyan *maximális* részkockának, amelyik az f-et igazzá tevő pontok halmazán belül marad. (Egy részkocka abban az értelemben maximális, hogy nincs nagyobb olyan, ugyanezzel a tulajdonsággal rendelkező részkocka, amely őt tartalmazza; nem tudjuk kicserélni semelyik konkrét bitjét csillag karakterre. Egy maximális részkocka maximális számú csillag karaktert tartalmaz, ennélfogva minimális számú rögzített koordinátát a neki megfelelő implikánsban.) A (28)-beli nyolc pont maximális részkockái

$$000{*},\; 0*00,\; {*}100,\; {*}111,\; 11**, \tag{29}$$

tehát a (23)-beli $f(w, x, y, z)$ függvény prímimplikánsai

$$(\bar{w} \wedge \bar{x} \wedge \bar{y}) \vee (\bar{w} \wedge \bar{y} \wedge \bar{z}) \vee (x \wedge \bar{y} \wedge \bar{z}) \vee (x \wedge y \wedge z) \vee (w \wedge x). \tag{30}$$

Egy Boole-függvény *diszjunktív prímformája* az összes prímimplikánsának a diszjunkciója. A 30. gyakorlat egy olyan algoritmust tartalmaz, amely megkeresi az összes prímimplikánsát az olyan pontok listájával megadott függvénynek, ahol a függvény igaz.

A *prímklózt* is hasonló módon definiálhatjuk: ez egy olyan f által implikált klóz, amelynek nincs ugyanezzel a tulajdonsággal rendelkező részklóza. f *konjunktív prímformája* pedig az összes prímklózának a konjunkciója. (A 19. gyakorlatban példát adunk erre.)

Egyszerű esetekben egy függvény legrövidebb lehetséges diszjunktív normálformája a diszjunktív prímformája. De gyakran tudunk jobbat is csinálni, mivel az összes szükséges pontot képesek lehetünk csak néhány maximális részkockával lefedni. Például (27)-ben az $(y \wedge z)$ prímimplikáns felesleges. A (30) kifejezésben pedig nem szükséges egyszerre $(\bar{w} \wedge \bar{y} \wedge \bar{z})$ és $(x \wedge \bar{y} \wedge \bar{z})$; a többi tag megléte esetén az egyik is elegendő.

A 7.9. alfejezetben látni fogjuk, hogy a legjobb diszjunktív normálforma keresésének feladata sajnos NP-teljes, ezért általában elég nehéz. Elég kis problémákra sok hasznos gyorsítást dolgoztak ki, ezeket részletesen kifejti McCluskey [?] könyve. Újabb gondolatokért lásd Fišer és Hlavička [14] dolgozatát.

Van egy fontos speciális eset, amikor a legrövidebb DNF könnyen meghatározható. Egy Boole-függvényt *monotonnak* vagy másképp *pozitívnak* nevezünk, ha értéke nem fog változni 1-ről 0-ra, amikor változói közül bármelyik is 0-ról 1-re vált. Más szavakkal f akkor és csak akkor monoton, ha $f(x) \leq f(y)$, amennyiben $x \subseteq y$. Az $y = y_1 \ldots y_n$ bitfüzér az $x = x_1 \ldots x_n$ bitfüzért pontosan akkor tartalmazza vagy lesz vele egyenlő, ha $x_j \leq y_j$ minden j-re. Ezzel ekvivalens feltétel (lásd a 21. gyakorlatot), hogy az f függvény vagy konstans, vagy ki lehet fejezni csupán a $\wedge$ és $\vee$ műveletek segítségével, komplemensképzés nélkül.

Q tétel. *Egy monoton Boole-függvény legrövidebb diszjunktív normálformája a diszjunktív prímformája.*

Bizonyítás. [Quine, [39]] Legyen $f(x_1, \ldots, x_n)$ monoton és legyen $u_1 \wedge \cdots \wedge u_s$ egyike a prímimplikánsainak. Ekkor nem lehet mondjuk $u_1 = \bar{x}_i$, mert egyébként a monotonitás miatt a rövidebb $u_2 \wedge \cdots \wedge u_s$ szintén implikáns lenne. Tehát egyetlen prímimplikáns sem tartalmaz komplementált változót.

Most ha $u_1 \leftarrow \cdots \leftarrow u_s \leftarrow 1$, és minden más változó értéke 0, az f értéke 1 lesz, de f összes többi prímimplikánsa eltűnik. Mivel egy legrövidebb DNF minden implikánsa nyilván prím, így az $u_1 \wedge \cdots \wedge u_s$-nek benne kell lennie minden legrövidebb DNF-ben. ■

Q következmény. *Egy diszjunktív normálforma akkor és csak akkor lesz monoton Boole-függvény diszjunktív prímformája, ha nincs egyetlen komplementált változó sem benne, és egyetlen implikánsa sincs benne másikban.* ■

Kielégíthetőség. Egy Boole-függvényt *kielégíthetőnek* nevezünk, ha nem azonosan nulla, azaz ha van legalább egy implikánsa. A számítástudomány legismertebb megoldatlan problémája hatékony módszert találni arra, hogy eldöntsük, vajon egy adott Boole-függvény kielégíthető-e, vagy épp kielégíthetetlen. Pontosabban azt kérdezzük: van-e olyan algoritmus, ami megkap egy N hosszúságú Boole-formulát és ellenőrzi ennek kielégíthetőségét mindig legfeljebb $N^{O(1)}$ lépés végrehajtása után megadva a helyes választ?

Amikor erről a problémáról először hall az ember, kísértésbe eshet, hogy visszakérdezzen: „Hogyhogy? A számítástudománnyal foglalkozók még komolyan nem találták ki, hogyan oldjanak meg egy ilyen egyszerű feladatot?”

Nos, ha azt gondolja valaki, hogy a kielégíthetőség ellenőrzése egyszerű, kérjük, mondja el nekünk módszerét. Egyetértünk abban, hogy a probléma nem mindig nehéz. Ha például a formulánk csak 30 Boole-változót tartalmaz, 2^{30} – kb. milliárdnyi – esetet a nyers erő módszerével próbálgatva valóban elintézhető dolog. De rengeteg, a gyakorlatban előforduló - es meg megoldasra váró - problémát lehet mondjuk 100 változós Boole-függvényként formalizálni, hiszen a matematikai logika igen hathatós eszközöket biztosit fogalmaink leírására. Ezeknek a problémáknak a megoldásai azok az $x = x_1 \ldots x_{100}$ vektorok, melyekre $f(x) = 1$. Úgyhogy csodálatos eredmény lenne a kielégíthetőségi probléma valóban hatékony megoldása.

A kielégíthetőség ellenőrzése a következő értelmezés mellett nem kíván nagy ötletet: ha az $f(x_1, \ldots, x_n)$ függvényt találomra úgy választjuk, hogy mind a 2^n igazságtábla egyformán valószínű, akkor f majdnem biztosan kielégíthető, és (átlagban véve) kevesebb, mint 2 próbálkozás után találhatunk olyan x-et, melyre $f(x) = 1$. Hasonlóan, mint érmedobáláskor, míg fejet nem kapunk; ritkán kell sokáig várni. A turpisság természetesen az, hogy a gyakorlatban előforduló problémák igazságtáblái nem véletlenek.

Rendben van tehát, fogadjuk el, hogy a kielégíthetőség ellenőrzése általában nehéz feladatnak tűnik. Valójában a kielégíthetőségi probléma még akkor is nehéznek bizonyul, ha megpróbáljuk azzal a megszorítással egyszerűbbé tenni, hogy a vizsgált Boole-függvény legyen „3KNF formula”, azaz olyan konjunktív normálforma, amelynek minden klózában csak *három* literál van:

$$f(x_1, \ldots, x_n) = (t_1 \vee u_1 \vee v_1) \wedge (t_2 \vee u_2 \vee v_2) \wedge \cdots \wedge (t_m \vee u_m \vee v_m). \tag{31}$$

Itt minden t_j, u_j és v_j valamely k-ra vagy x_k, vagy $\bar{x}_k$. 3KNF formulák kielégíthetőségének eldöntési problémáját „3SAT”-nak nevezzük. A 39. gyakorlat megvilágítja, hogy ez valójában miért nem könnyebb, mint általában egy kielégíthetőségi probléma.

Sok példát fogunk meg látni komoly fejtörést okozó 3SAT problémára – különösen a 7.9. alfejezetben, ahol a kielégíthetőség ellenőrzését részletesen tárgyaljuk majd. A helyzet kissé mégis furcsa, hisz a formulának meglehetősen hosszúnak kell lennie ahhoz, hogy szükséges legyen a kielégíthetőségéről komolyabban elgondolkodni. Például a legrövidebb kielégíthetetlen 3KNF formula az $(x \vee x \vee x) \wedge (\bar{x} \vee \bar{x} \vee \bar{x})$; bár nyilván ezt nem kihívás észrevenni. Nem kerülünk mély vízbe, csak ha valamelyik klóz három literálja, mondjuk a t_j, u_j, v_j, három különböző változóhoz kötődik. Ebben az esetben minden klóz a lehetőségek közül pontosan $1/8$ részt kizár, mert (t_j, u_j, v_j) hét különböző kiértékelése őt igazzá teszi. Következésképpen minden ilyen, legfeljebb hét klózzal rendelkező 3KNF formula automatikusan kielégíthető, és változóinak véletlenszerűen értéket adva $\geq 1 - 7/8 = 1/8$ valószínűséggel leszünk sikeresek.

Tehát az érdeklődésre számot tartó legrövidebb 3KNF formula legalább nyolc klózt tartalmaz. Valóban, van a 8 klózzal rendelkező formulák között egy érdekes, ami a 6.5. alfejezetben vizsgált Rivest-féle asszociatív blokkrendszeren alapul:

$$\begin{gathered}(x_2 \vee x_3 \vee \bar{x}_4) \wedge (x_1 \vee x_3 \vee x_4) \wedge (\bar{x}_1 \vee x_2 \vee x_4) \wedge (\bar{x}_1 \vee \bar{x}_2 \vee x_3) \\ \wedge (\bar{x}_2 \vee \bar{x}_3 \vee x_4) \wedge (\bar{x}_1 \vee \bar{x}_3 \vee \bar{x}_4) \wedge (x_1 \vee \bar{x}_2 \vee \bar{x}_4) \wedge (x_1 \vee x_2 \vee \bar{x}_3)\ .\end{gathered} \tag{32}$$

Ezen nyolc klóz közül bármely hét kielégíthető, mégpedig pontosan kétféleképp, és közben három változó értékét határozza meg. Például az első hét miatt $x_1x_2x_3 = 001$. Ugyanakkor egyidejűleg mind a nyolcat nem lehet kielégíteni.

Egyszerű speciális esetek. A Boole-függvényeknek meghatározták két olyan fontos osztályát, amelyeken a kielégíthetőségi probléma elég könnyen megoldható. Akkor adódnak ezek a speciális esetek, amikor az ellenőrzés alatt álló konjunktív normálforma vagy kizárólag „Horn-klózokból”, vagy csak „Krom-klózokból” áll. Egy *Horn-klóz* literálok VAGY-ja, amelyben minden vagy majdnem minden literál komplementált – legfeljebb egy literál változó és nem pedig változó komplemense. Egy *Krom-klóz* pedig pontosan két literál VAGY-ja. Így például

$$\bar{x} \vee \bar{y}, \qquad w \vee \bar{y} \vee \bar{z}, \qquad \bar{u} \vee \bar{v} \vee \bar{w} \vee \bar{x} \vee \bar{y} \vee z \quad \text{és} \quad x$$

Horn-klózok;

$$x \vee x, \qquad \bar{x} \vee \bar{x}, \qquad \bar{x} \vee \bar{y}, \qquad x \vee \bar{y}, \qquad \bar{x} \vee y \quad \text{és} \quad x \vee y$$

pedig Krom-klózok, közülük csak az utolsó nem Horn-klóz is egyben. (Itt az első példa azért jó, mert $x \vee x = x$.) Vegyük észre, hogy egy Horn-klóz akárhány literált tartalmazhat, ha viszont Krom-klózokkal dolgozunk, 2SAT problémával van dolgunk. Mindkét esetben látni fogjuk, hogy a kielégíthetőséget lineáris időben, azaz N hosszúságú formula megadásakor csupán $O(N)$ elemi lépés végrehajtásával el lehet dönteni.

Először vizsgáljuk meg a Horn-klózokat. Miért is olyan könnyű kezelni ezeket? A fő oka az, hogy egy az $\bar{u} \vee \bar{v} \vee \bar{w} \vee \bar{x} \vee \bar{y} \vee z$-hez hasonló klóz átalakítható $\neg(u \wedge v \wedge w \wedge x \wedge y) \vee z$ formára, ami pedig nem más, mint

$$u \wedge v \wedge w \wedge x \wedge y \;\Rightarrow\; z.$$

Tehát ha u, v, w, x és y mind igazak, akkor z-nek is igaznak kell lennie. Emiatt a paraméteres Horn-klózokat választották a Prolognak nevezett programozási nyelv hátterében működő alapvető mechanizmusnak. Ráadásul könnyen és pontosan jellemezhető, hogy mely Boole-függvényeket lehet Horn-klózokkal kifejezni:

H tétel. *Az $f(x_1, \ldots, x_n)$ Boole-függvény pontosan akkor fejezhető ki Horn-klózok konjunkciójaként, ha x_j és y_j minden Boole-értékére teljesül, hogy*

$$\text{ha} f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n) = 1 \quad \text{akkor} \quad f(x_1 \wedge y_1, \ldots, x_n \wedge y_n) = 1\,. \tag{33}$$

Bizonyítás. [Horn [18, 7. lemma]] Ha $x_0 \vee \bar{x}_1 \vee \cdots \vee \bar{x}_k = 1$ és $y_0 \vee \bar{y}_1 \vee \cdots \vee \bar{y}_k = 1$, akkor

$$\begin{aligned}(x_0 \wedge y_0) &\vee \overline{x_1 \wedge y_1} \vee \cdots \vee \overline{x_k \wedge y_k}\\ &= (x_0 \vee \bar{x}_1 \vee \bar{y}_1 \vee \cdots \vee \bar{x}_k \vee \bar{y}_k) \wedge (y_0 \vee \bar{x}_1 \vee \bar{y}_1 \vee \cdots \vee \bar{x}_k \vee \bar{y}_k)\\ &\geq (x_0 \vee \bar{x}_1 \vee \cdots \vee \bar{x}_k) \wedge (y_0 \vee \bar{y}_1 \vee \cdots \vee \bar{y}_k) \;=\; 1\,.\end{aligned}$$

Hasonló (csak egyszerűbb) megfontolást alkalmazunk, amikor a negálatlan x_0 és y_0 literálok hiányoznak. Tehát Horn-klózok konjunkcióira (33) teljesül.

Fordítva, a (33) feltétel teljesülése esetén f minden prímklóza Horn-klóz (lásd a 44. gyakorlatot). ■

Ezek után mondjuk azt, hogy a *Horn-függvény* egy, a (33) feltételt teljesítő Boole-függvény, és nevezzük *definitnek*, ha teljesít még egy újabb, $f(1, \ldots, 1) = 1$ feltételt is.

Könnyű belátni, hogy Horn-klózok konjunkciója akkor és csak akkor lesz definit, ha minden klóznak van (*pontosan*) egy negálatlan literálja, mivel csak egy $\bar{x} \vee \bar{y}$-hoz hasonló, teljesen negatív klóz lesz hamis, ha minden változó igaz. A definit Horn-függvényekkel némileg egyszerűbb dolgozni, mint általában a Horn-függvényekkel, mert nyilván mindig kielégíthetők. A H tétel szerint ezeknek van egy legkisebb olyan x vektoruk, melyre $f(x) = 1$, mégpedig azoknak a vektoroknak a bitenkénti ÉS-je, melyek az összes klózt kielégítik. Egy definit Horn-függvény *magja* azoknak az x_j változóknak a halmaza, melyek igazak ebben az x minimális vektorban. Vegyük észre, hogy a magbeli változók igazak, valahányszor f igaz, és így lényegében egyszerűsíthetünk velük.

Sokféleképpen kerülhetnek definit Horn-függvények elénk, például játékok elemzésekor (lásd az 51. és 52. gyakorlatokat). Egy másik szép példa a fordítóprogramok készítése során merül fel. Vizsgáljuk meg egy programozási nyelv algebrai kifejezését generáló következő tipikus (bár leegyszerűsített) nyelvtant:

$$\begin{aligned}
&\langle\texttt{kifejezés}\rangle \to \langle\texttt{tag}\rangle \mid \langle\texttt{kifejezés}\rangle + \langle\texttt{tag}\rangle \mid \langle\texttt{kifejezés}\rangle - \langle\texttt{tag}\rangle\\
&\langle\texttt{tag}\rangle \to \langle\texttt{tényező}\rangle \mid -\langle\texttt{tényező}\rangle \mid \langle\texttt{tag}\rangle * \langle\texttt{tényező}\rangle \mid \langle\texttt{tag}\rangle \,/\, \langle\texttt{tényező}\rangle\\
&\langle\texttt{tényező}\rangle \to \langle\texttt{változó}\rangle \mid \langle\texttt{konstans}\rangle \mid (\langle\texttt{kifejezés}\rangle)\\
&\langle\texttt{változó}\rangle \to \langle\texttt{betű}\rangle \mid \langle\texttt{változó}\rangle\langle\texttt{betű}\rangle \mid \langle\texttt{változó}\rangle\langle\texttt{számjegy}\rangle\\
&\langle\texttt{betű}\rangle \to \texttt{a} \mid \texttt{b} \mid \texttt{c}\\
&\langle\texttt{konstans}\rangle \to \langle\texttt{számjegy}\rangle \mid \langle\texttt{konstans}\rangle\langle\texttt{számjegy}\rangle\\
&\langle\texttt{számjegy}\rangle \to 0 \mid 1
\end{aligned}\tag{34}$$

Például az `a/(-b0-10)+cc*cc` füzér megfelel a $\langle\texttt{kifejezés}\rangle$ szintaxisának és minden nyelvtani szabályt legalább egyszer felhasznál.

Tegyük fel, hogy azt akarjuk tudni, hogy mely karakterpárok jelenhetnek meg egymás mellett egy ilyen kifejezésben. Erre definit Horn-klózok adnak választ, hiszen a következőképpen tudjuk megfogalmazni a problémát: jelöljenek `Xx`, `xX` és `xy` Boole-állításokat, ahol `X` rendre a $\langle\texttt{kifejezés}\rangle, \langle\texttt{tag}\rangle, \ldots, \langle\texttt{számjegy}\rangle$ helyett írt $\{\texttt{E},\texttt{T},\texttt{F},\texttt{V},\texttt{L},\texttt{C},\texttt{D}\}$ szimbólumok közül valamelyik, és ahol `x` és `y` a $\{\texttt{+},\texttt{-},\texttt{*},\texttt{/},\texttt{(},\texttt{)},\texttt{a},\texttt{b},\texttt{c},\texttt{0},\texttt{1}\}$ halmaz elemei. Az `Xx` állítás azt jelenti, hogy „végződhet `X` az `x` karakterrel”, és hasonlóan `xX` azt jelenti, hogy „kezdődhet `X` az `x` karakterrel”, `xy` pedig azt jelenti, hogy „követheti közvetlenül az `x` karaktert az `y` karakter valamely kifejezésben”. ($7 \times 11 + 11 \times 7 + 11 \times 11 = 275$ állítás van összesen.) Ezután írhatjuk, hogy

$$\begin{array}{llllllllll}
\mathtt{xT} & \Rightarrow \mathtt{xE} & & \Rightarrow \mathtt{-T} & \mathtt{xC} & \Rightarrow \mathtt{xF} & \mathtt{Vx}\wedge\mathtt{yL} & \Rightarrow \mathtt{xy} & & \Rightarrow \mathtt{Lc}\\
\mathtt{Tx} & \Rightarrow \mathtt{Ex} & \mathtt{xF} & \Rightarrow \mathtt{-x} & \mathtt{Cx} & \Rightarrow \mathtt{Fx} & \mathtt{Vx}\wedge\mathtt{yD} & \Rightarrow \mathtt{xy} & \mathtt{xD} & \Rightarrow \mathtt{xC}\\
\mathtt{Ex} & \Rightarrow \mathtt{x+} & \mathtt{Tx} & \Rightarrow \mathtt{x*} & & \Rightarrow \mathtt{(F} & \mathtt{Dx} & \Rightarrow \mathtt{Vx} & \mathtt{Dx} & \Rightarrow \mathtt{Cx}\\
\mathtt{xT} & \Rightarrow \mathtt{+x} & \mathtt{xF} & \Rightarrow \mathtt{*x} & \mathtt{xE} & \Rightarrow \mathtt{(x} & & \Rightarrow \mathtt{aL} & \mathtt{Cx}\wedge\mathtt{yD} & \Rightarrow \mathtt{xy}\\
\mathtt{Ex} & \Rightarrow \mathtt{x-} & \mathtt{Tx} & \Rightarrow \mathtt{x/} & \mathtt{Ex} & \Rightarrow \mathtt{x)} & & \Rightarrow \mathtt{La} & & \Rightarrow \mathtt{0D}\\
\mathtt{xT} & \Rightarrow \mathtt{-x} & \mathtt{xF} & \Rightarrow \mathtt{/x} & & \Rightarrow \mathtt{F)} & & \Rightarrow \mathtt{bL} & & \Rightarrow \mathtt{D0}\\
\mathtt{xF} & \Rightarrow \mathtt{xT} & \mathtt{xV} & \Rightarrow \mathtt{xF} & \mathtt{xL} & \Rightarrow \mathtt{xV} & & \Rightarrow \mathtt{Lb} & & \Rightarrow \mathtt{1D}\\
\mathtt{Fx} & \Rightarrow \mathtt{Tx} & \mathtt{Vx} & \Rightarrow \mathtt{Fx} & \mathtt{Lx} & \Rightarrow \mathtt{Vx} & & \Rightarrow \mathtt{cL} & & \Rightarrow \mathtt{D1}
\end{array}\tag{35}$$

ahol `x` és `y` végigfut a tizenegy $\{\texttt{+}, \ldots, \texttt{1}\}$ terminális szimbólumon. Ez a sematikus felsorolás összesen $24 \times 11 + 3 \times 11 \times 11 + 13 \times 1 = 640$ definit Horn-klózt ad, amit formálisan úgy írhatunk le, hogy

$$\bigl(\overline{\mathtt{+T}} \vee \mathtt{+E}\bigr) \wedge \bigl(\overline{\mathtt{-T}} \vee \mathtt{-E}\bigr) \wedge \cdots \wedge \bigl(\overline{\mathtt{V+}} \vee \overline{\mathtt{0L}} \vee \mathtt{+0}\bigr) \wedge \cdots \wedge \bigl(\mathtt{D1}\bigr)$$

ha jobban szeretjük a Boole-algebra jelképes jelölésrendszeréét, mint (35)ben előforduló $\Rightarrow$-t.

Miért is csináltuk mindezt? Mert *ezen klózoknak a lényeges része, magja épp az ebben a speciális nyelvtanban igaz állítások halmaza*. Igazolhatjuk például, hogy `-E` igaz, ezért a `(-` szimbólumok előfordulhatnak egymás után valamely kifejezésben; de a `++` és `*-` szimbólumpárok nem (lásd a 46. gyakorlatot).

Ráadásul különösebb nehézség nélkül elő tudjuk állítani definit Horn-klózok tetszőlegesen adott halmazának a magját. Azokból az állításokból indulunk ki, amelyek a $\Rightarrow$ jobb oldalán egyedül állnak, miközben a bal oldal üres; a (35)-beli állítások között tizenhárom ilyen van. Mihelyt ezeknek az állításoknak az igazságát rögzítjük, máris találhatunk néhány olyan klózt, melyeknek a bal oldala igaz. Ezután ezek jobb oldala szintén a maghoz tartozik, és így folytatjuk tovább. Az egész eljárás meglehetősen hasonlít ahhoz, ahogy egy gát mögül a víz lezúdul, míg meg nem találja a saját medrét. Valóban, ha megfelelő adatszerkezetet választunk, ez a sodró folyamat meglehetősen gyors, csak $O(N+n)$ lépést kíván, ahol N a klózok összhosszát jelöli, n pedig a propozícionális változók számát. (Itt feltételeztük, hogy az összes klózban a fenti `x`-hez és `y`-hoz hasonló paramétereket konkrét terminális jelekre cseréltük, és nem rövidítettük meg. A tételbizonyítás kifinomultabb technikái is igénybe vehetők paraméteres klózokkal való munka esetén, de ezek kívül esnek a mostani vizsgálódásaink érdeklődési körén.)

C algoritmus *(definit Horn-klózok magjának meghatározására)*. Ítéletváltozók egy adott P halmaza és egy olyan C klózhalmaz esetén, melynek minden klóza

$$u_1 \wedge \cdots \wedge u_k \;\Rightarrow\; v \text{ alakú, ahol } k \geq 0 \text{ és } \{u_1, \ldots, u_k, v\} \subseteq P, \tag{36}$$

ez az algoritmus megkeresi az ítéletváltozók azon $Q \subseteq P$ halmazat, melyek szükségképpen mindannyiszor igazak, valahányszor a klózok mindegyike igaz.

A következő adatszerkezeteket használjuk egy c klózra, p állításra és h hipotézisre, ahol a „hipotézis” egy klóz bal oldalán előforduló állítás:

`KONKLÚZIÓ`(c) a c klóz jobb oldalán szereplő állítás;
`SZÁMLÁLÓ`(c) c még nem bizonyított hipotéziseinek száma;
`IGAZ`(p) 1, ha p igaz, egyébként 0;
`UTOLSÓ`(p) a legutolsó hipotézis, amelyikben p megjelenik;
`KLÓZ`(h) az a klóz, amelyikben h a bal oldalon megjelenik;
`ELŐZŐ`(h) a h állítást megelőző hipotézis.

Fenntartunk továbbá még egy S_0, S_1, $\ldots$, S_{s-1} vermet az igaznak gondolt, de még nem bizonyított állítások kezelésére..

C1. (Kezdőértékek beállítása.) Minden egyes p állításra legyen `UTOLSÓ`$(p) \leftarrow \Lambda$ és `IGAZ`$(p) \leftarrow 0$. Legyen továbbá $s \leftarrow 0$, és a verem pedig üres. Aztán minden (36) alakú c klóz esetén legyen `KONKLÚZIÓ`$(c) \leftarrow v$ és `SZÁMLÁLÓ`$(c) \leftarrow k$. Ha $k = 0$ és `IGAZ`$(v) = 0$, legyen `IGAZ`$(v) \leftarrow 1$, $S_s \leftarrow v$ és $s \leftarrow s+1$. Egyébként ha $1 \leq j \leq k$, hozzuk létre a h hipotézis rekordot és legyenek `KLÓZ`$(h) \leftarrow c$, `ELŐZŐ`$(h) \leftarrow$ `UTOLSÓ`(u_j), `UTOLSÓ`$(u_j) \leftarrow h$.

C2. (A p állítás előkészítése.) Ha $s = 0$, fejezzük be az algoritmust. A kívánt mag most az összes olyan állítást tartalmazza, melyre az `IGAZ` attribútum értéke 1.

Egyébként pedig legyenek $s \leftarrow s-1$, $p \leftarrow S_s$ és $h \leftarrow \texttt{UTOLSÓ}(p)$.

C3. (Kellenek a hipotézisek?) Ha $h = \Lambda$, menjünk vissza **C2**-re.

C4. (h jóváhagyása.) Legyenek $c \leftarrow \texttt{KLÓZ}(h)$ és $\texttt{SZÁMLÁLÓ}(c) \leftarrow \texttt{SZÁMLÁLÓ}(c) - 1$. Ha $\texttt{SZÁMLÁLÓ}(c)$ új értéke még nem nulla, a **C6** lépéssel folytassuk.

C5. ($\texttt{KONKLÚZIÓ}(c)$ levezetése.) Legyen $p \leftarrow \texttt{KONKLÚZIÓ}(c)$. Ha $\texttt{IGAZ}(p) = 0$, legyenek $\texttt{IGAZ}(p) \leftarrow 1$, $S_s \leftarrow p$, $s \leftarrow s+1$.

C6. (Ciklus h-ra.) Legyen $h \leftarrow \texttt{ELŐZŐ}(h)$, és menjünk vissza **C3**-ra. ∎

Vegyük észre, hogy az adatszerkezetek milyen zökkenőmentesen dolgoznak össze a számolás során, kikerülve a folytatáshoz szükséges bármiféle helykeresést. A C algoritmus sok szempontból hasonlít a 2.2.3.T (topologikus rendezés) algoritmushoz, ami első példánk volt hajdanán a 2. fejezetben a multilista adatszerkezetre; csakugyan a 2.2.3.T algoritmust úgy is tekinthetjük, mint a C algoritmus azon speciális esetét, amikor minden állítás pontosan egy klóz jobb oldalán jelenik meg. (Lásd a 47. gyakorlatot.)

A 48. gyakorlat bemutatja, hogy a C algoritmus egy kis módosítása a Horn-klózok kielégíthetőségi problémáját általánosan is megoldja. A téma további tárgyalását Dowling és Gallier [10] munkájában találhatjuk meg.

Most térjünk vissza a Krom-függvényekre és a 2SAT problémára. Újból van egy lineáris idejű algoritmusunk; de talán leginkább akkor értékelhetjük, ha először megint pillantást vetünk egy leegyszerűsített gyakorlati alkalmazásra. Tegyük fel, hogy hét komikus megállapodott abban, hogy egy háromnapos fesztivál során mindegyikőjük öt hotel közül kettőben egyestés fellépést tart, de más irányú kötelezettségei miatt mindenki csak két nap ér rá:

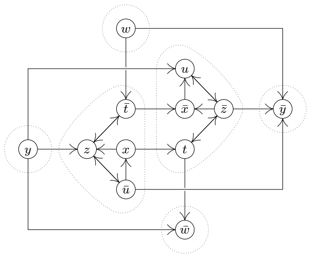
Tomlinnak az Aladdin és a Caesars hotelekben kellene dolgoznia az 1. és a 2. napon.
Unwinnak a Bellagio és az Excalibur hotelekben kellene dolgoznia az 1. és 2. napon.
Vegasnak a Desert és az Excalibur hotelekben kellene dolgoznia a 2. és 3. napon.
Williamsnek az Aladdin és a Desert hotelekben kellene dolgoznia az 1. és 3. napon.
Xienek a Caesars és az Excalibur hotelekben kellene dolgoznia az 1. és 3. napon.
Yankovicnak a Bellagio és a Desert hotelekben kellene dolgoznia a 2. és 3. napon.
Zanynek a Bellagio és a Caesars hotelekben kellene dolgoznia az 1. és 2. napon.
(37)

Be lehet őket osztani úgy, hogy minden adott napon minden adott hotelben pontosan 1 komikus lepjen fel?

A probléma megoldásához bevezethetünk hét Boole-változót: $\{t, u, v, w, x, y, z\}$, ahol t (például) azt jelenti, hogy Tomlin az Aladdin hotelben játszik az 1. napon és a Caesars hotelben a 2. napon, míg $\bar{t}$ azt jelenti, a szóban forgó hotelekben épp fordított sorrendben vannak előjegyezve ezek a napok. Azután azokat a megszorításokat adjuk meg, amelyek biztosítják, hogy két komikus ugyanabban a hotelben ugyanarra a napra ne legyen beosztva:

$$\begin{array}{llllllll}
\neg(t \wedge w) & [\mathrm{A1}] & \neg(y \wedge \bar{z}) & [\mathrm{B2}] & \neg(t \wedge z) & [\mathrm{C2}] & \neg(w \wedge y) & [\mathrm{D3}] \\
\neg(u \wedge z) & [\mathrm{B1}] & \neg(\bar{t} \wedge x) & [\mathrm{C1}] & \neg(v \wedge \bar{y}) & [\mathrm{D2}] & \neg(\bar{u} \wedge \bar{x}) & [\mathrm{E1}] \\
\neg(\bar{u} \wedge y) & [\mathrm{B2}] & \neg(\bar{t} \wedge \bar{z}) & [\mathrm{C1}] & \neg(\bar{v} \wedge w) & [\mathrm{D3}] & \neg(u \wedge \bar{v}) & [\mathrm{E2}] \\
\neg(\bar{u} \wedge \bar{z}) & [\mathrm{B2}] & \neg(x \wedge \bar{z}) & [\mathrm{C1}] & \neg(\bar{v} \wedge y) & [\mathrm{D3}] & \neg(v \wedge x) & [\mathrm{E3}]
\end{array} \qquad (38)$$

Ezeknek a megszorításoknak mindegyike nyilvánvalóan Krom-klóz; ki kell tehát elégítenünk



7.6. ábra. A (40) és (41)-beli sem v-t, sem $\bar{v}$-t nem tartalmazó implikációknak megfelelő irányított gráf. Az erős komponensekben a literálokhoz alkalmas értékeket hozzárendelve meg lehet oldani a bináris ütemezési problémát, ami a 2SAT probléma egy speciális esete.

a

$$\begin{aligned}&(\bar{t} \vee \bar{w}) \wedge (\bar{u} \vee \bar{z}) \wedge (u \vee \bar{y}) \wedge (u \vee z) \wedge (\bar{y} \vee z) \wedge (t \vee \bar{x}) \wedge (t \vee z) \wedge (\bar{x} \vee z)\\ \wedge&(\bar{t} \vee \bar{z}) \wedge (\bar{v} \vee y) \wedge (v \vee \bar{w}) \wedge (v \vee \bar{y}) \wedge (\bar{w} \vee \bar{y}) \wedge (u \vee x) \wedge (\bar{u} \vee v) \wedge (\bar{v} \vee \bar{x})\end{aligned} \tag{39}$$

formulát. Ráadásul a Krom-klózokat (a Horn-klózokhoz hasonlóan) implikációkként is fel lehet írni:

$$\begin{gathered}t \Rightarrow \bar{w},\;\; u \Rightarrow \bar{z},\;\; \bar{u} \Rightarrow \bar{y},\;\; \bar{u} \Rightarrow z,\;\; y \Rightarrow z,\;\; \bar{t} \Rightarrow \bar{x},\;\; \bar{t} \Rightarrow z,\;\; x \Rightarrow z,\\ t \Rightarrow \bar{z},\;\; v \Rightarrow y,\;\; \bar{v} \Rightarrow \bar{w},\;\; \bar{v} \Rightarrow \bar{y},\;\; w \Rightarrow \bar{y},\;\; \bar{u} \Rightarrow x,\;\; u \Rightarrow v,\;\; v \Rightarrow \bar{x}.\end{gathered} \tag{40}$$

Minden ilyen implikációnak van egy másik, „kontrapozíciós” formája:

$$\begin{gathered}w \Rightarrow \bar{t},\;\; z \Rightarrow \bar{u},\;\; y \Rightarrow u,\;\; \bar{z} \Rightarrow u,\;\; \bar{z} \Rightarrow \bar{y},\;\; x \Rightarrow t,\;\; \bar{z} \Rightarrow t,\;\; \bar{z} \Rightarrow \bar{x},\\ z \Rightarrow \bar{t},\;\; \bar{y} \Rightarrow \bar{v},\;\; w \Rightarrow v,\;\; y \Rightarrow v,\;\; y \Rightarrow \bar{w},\;\; \bar{x} \Rightarrow u,\;\; \bar{v} \Rightarrow \bar{u},\;\; x \Rightarrow \bar{v}.\end{gathered} \tag{41}$$

De hoppá – ó jaj – itt az ördögi kör:

$$u \Rightarrow \bar{z} \Rightarrow \bar{y} \Rightarrow \bar{v} \Rightarrow \bar{u} \Rightarrow z \Rightarrow \bar{t} \Rightarrow \bar{x} \Rightarrow u. \tag{42}$$

Ez a kör azt is kifejezi, hogy u és $\bar{u}$ azonos értékű kell legyen, így nincs mód rá, hogy a (37)-beli összes kikötést összeegyeztessük. A fesztivál szervezőinek újra kell tárgyalniuk a megállapodást a $\{t, u, v, x, y, z\}$ komikusok közül legalább eggyel, ha megvalósítható ütemezést akarnak elérni. (Lásd az 53. gyakorlatot.)

A szervezők például megpróbálhatják kihagyni az elképzelésből v-t. Ekkor a (38)-beli tizenhat feltétel közül öt kiesne, és a (40) és (41) implikációkból csak 22 maradna a 7.6. ábrán látható irányított gráfot eredményezve. Ez a gráf ugyan tartalmaz köröket, mint a $z \Rightarrow \bar{u} \Rightarrow x \Rightarrow z$ és a $t \Rightarrow \bar{z} \Rightarrow t$; de nincs olyan kör, amelyik egy változóval együtt a komplemensét is tartalmazza. Sőt még azt is láthatjuk a 7.6. ábrán, hogy a $tuwxyz = 110000$ értékek a (39)-beli v-t vagy $\bar{v}$-t nem tartalmazó klózok mindegyikét kielégítik. Ezek az értékek olyan ütemezést adnak, mely a (37)-beli hét eredeti kikötés közül hatot teljesít úgy, hogy az első nap (Tomlin, Unwin, Zany, Williams, Xie) kezd rendre az (Aladdin, Bellagio, Caesars, Desert, Excalibur) szállodákban.

Általánosan is, ha adott egy n Boole-változót tartalmazó és m Krom-klózból álló 2SAT probléma, irányított gráffal ugyanígy tudjuk ábrázolni. Egy ilyen gráfban $2n$ csúcs – minden lehetséges literálhoz egy – van, ezek az $\{x_1, \bar{x}_1, \ldots, x_n, \bar{x}_n\}$ csúcsok; és $2m$ él, minden $u \vee v$ klózhoz kettő: $\bar{u} \to v$ és $\bar{v} \to u$. Az u és v literálok akkor és csak akkor tartoznak ennek a gráfnak ugyanazon *erős komponenséhez*, ha u-ból v-be és v-ből u-ba is vezet irányított út. Például a 7.6. ábrán látható gráfban hat erős komponens van pontozott vonallal bejelölve. Egy erős komponens összes literáljának ugyanaz kell legyen a Boole-értéke a megfelelő 2SAT problémához tartozó bármelyik megoldásban.

K tétel. *Egy klózonként két-két literált tartalmazó konjunktív normálforma akkor és csak akkor elégíthető ki, ha a hozzá tartozó irányított gráf egyetlen erős komponense sem tartalmaz egyszerre egy változót és a komplemensét is.*

Bizonyítás. [Krom [24, 2.2. következmény]] Ha van x-ből $\bar{x}$-be és $\bar{x}$-ből x-be vezető út is, a formula kétségtelenül kielégíthetetlen.

Most azonban tegyük fel, hogy nincsenek ilyen utak. Bármelyik véges irányított gráfnak van legalább egy olyan erős komponense, vagyis „forrása”, amelybe egyetlen másik erős komponensbeli csúcsból induló él sem fut be. Jelöljük ezt S-sel. Továbbá a gráfunk mindig antiszimmetrikus a következő értelemben, ahogy a 7.6. ábrán is illusztráltuk: $u \to v$ akkor és csak akkor, ha $\bar{v} \to \bar{u}$. Így az S-beli literálok komplemensei egy másik $\overline{S} \neq S$ erős komponenst, azaz egy „nyelőt” alakítanak ki, amelyből más erős komponensbe nincs kivezető él. Emiatt az S-beli literálokhoz 0 értéket, az $\overline{S}$-beliekhez pedig 1 értéket rendelhetünk, azután távolítsuk el ezeket az irányított gráfból, majd ugyanígy folytassuk, míg minden literál értéket nem kap. Az eredményül kapott értékekre $u \leq v$, ha a gráfban $u \to v$ él; emiatt ezek az értékek kielégítik $\bar{u} \vee v$-t, amennyiben $\bar{u} \vee v$ a formula klóza. ∎

Tarjan [?] egy algoritmusának köszönhetően, mely lineáris időben megtalálja az erős komponenseket, a K tétel közvetlenül a 2SAT probléma hatékony megoldásához vezet. Lásd még Knuth [?] dolgozatát. Tarjan algoritmusát a **??**. pontban részletesen fogjuk tanulmányozni. Az 54. gyakorlat pedig azt mutatja meg, hogy a K tétel feltétele könnyen ellenőrizhető, amikor az algoritmus egy új erős komponenst tár fel. Továbbá az algoritmus először a „nyelőt” ismeri fel; így a Tarjan-algoritmussal mellesleg meg tudjuk határozni a kielégíthetőséget megalapozó értékeket is úgy, hogy egy erős komponens minden olyan literáljának, amely a komplemensét megelőzve fordul elő, 1-es értéket választunk.

Mediánok. Az $x \vee y$ vagy az $x \oplus y$ műveletekhez hasonló kétváltozós Boole-műveletekre összpontosítottunk eddig. Van azonban egy nevezetes, az x, y és z *mediánjának* nevezett *háromváltozós* művelet:

$$\langle xyz \rangle = (x \wedge y) \vee (y \wedge z) \vee (x \wedge z) = (x \vee y) \wedge (y \vee z) \wedge (x \vee z)\,. \tag{43}$$

Alighanem $\langle xyz \rangle$ a legfontosabb háromváltozós művelet a világon, mert olyan meghökkentő tulajdonságai vannak, amelyeket folyton újból és újból felfedeznek.

Először is könnyen beláthatjuk, hogy az $\langle xyz \rangle$ műveletet megadó formula bármely három x, y és z Boole-érték közül a többször előforduló értéket adja meg: $\langle 000 \rangle = \langle 001 \rangle = 0$ és $\langle 011 \rangle = \langle 111 \rangle = 1$. $\langle xyz \rangle$-t mégis „mediánnak” (középsőnek) nevezzük „majoritás” (többség) helyett, mert ha x, y és z tetszőleges *valós* számok és $\wedge$ és $\vee$ a min és a max műveleteket jelölik, akkor

$$\langle xyz \rangle = y, \text{ ha } x \leq y \leq z\,. \tag{44}$$

Másodszor pedig az alapvető $\wedge$ és $\vee$ kétváltozós műveletek a medián speciális esetei:

$$x \wedge y \;=\; \langle x0y\rangle \text{ és } x \vee y \;=\; \langle x1y\rangle\,. \tag{45}$$

Tehát így *bármelyik* monoton Boole-függvényt ki lehet fejezni kizárólag a háromváltozós medián művelet, továbbá a 0 és 1 konstansok segítségével. Valóban, ha egy csak a mediánt használó világban élnénk, megtehetnénk, hogy $\wedge$-vel jelöljük a hamis, és $\vee$-vel az igaz logikai értéket; ekkor $x \wedge y = \langle x{\wedge}y\rangle$ és $x \vee y = \langle x{\vee}y\rangle$ teljesen szabályos kifejezés lenne, sőt használhatnánk a $\langle{\wedge}xy\rangle$ és $\langle{\vee}xy\rangle$ lengyel jelölést is, ha ez előnyösebb lenne. Ugyanez az ötlet vonatkozik a kibővített valós számokra a $\wedge$ és $\vee$ min-max interpretációja mellett, ha a $\wedge = -\infty$ és a $\vee = +\infty$ konstansokkal képezzük a mediánokat.

Egy $f(x_1, x_2, \ldots, x_n)$ Boole-függvényt *önduálisnak* nevezünk, ha teljesül rá, hogy

$$\overline{f(x_1, x_2, \ldots, x_n)} \;=\; f(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n)\,. \tag{46}$$

Leírtuk már, hogy egy Boole-függvény akkor és csak akkor monoton, ha a $\wedge$ és $\vee$ műveletekkel ki lehet fejezni; a (11) és (12) De Morgan-törvények szerint így egy monoton formula akkor és csak akkor önduális, ha a $\wedge$ és $\vee$ szimbólumokat fel lehet benne cserélni a formula jelentésének változása nélkül. Ezért a (43)-ban definiált medián művelet monoton és önduális. Tulajdonképpen ez a legegyszerűbb ilyen tulajdonságú nemtriviális függvény, mivel a 7.1. táblázatban szereplő bináris műveletek egyike sem monoton és önduális egyszerre, kivéve a $\llcorner$ és R projekciókat.

Ráadásul *bármely*, konstans használata nélkül, csak a medián művelettel megadott kifejezés monoton és önduális. Például a $\langle w\langle xyz\rangle\langle w\langle uvw\rangle x\rangle\rangle$ függvény önduális, mert

$$\begin{aligned}\overline{\langle w\langle xyz\rangle\langle w\langle uvw\rangle x\rangle\rangle} \;&=\; \langle \bar{w}\,\overline{\langle xyz\rangle}\,\overline{\langle w\langle uvw\rangle x\rangle}\rangle\\ &=\; \langle \bar{w}\langle \bar{x}\bar{y}\bar{z}\rangle\langle \bar{w}\overline{\langle uvw\rangle}\bar{x}\rangle\rangle \;=\; \langle \bar{w}\langle \bar{x}\bar{y}\bar{z}\rangle\langle \bar{w}\langle \bar{u}\bar{v}\bar{w}\rangle\bar{x}\rangle\rangle\,.\end{aligned}$$

Emil Post, miközben a Ph.D. értekezésén [?] dolgozott, bebizonyította, hogy a fordított irányú állítás is igaz:

P tétel. *Minden $f(x_1, \ldots, x_n)$ monoton, önduális Boole-függvényt ki lehet fejezni csupán az $\langle xyz\rangle$ medián művelettel.*

Bizonyítás. [37] Vegyük észre először azt, hogy

$$\begin{aligned}&\langle x_1 y\langle x_2 y \ldots y\langle x_{s-1} y x_s\rangle \ldots\rangle\rangle\\ &\quad= ((x_1 \vee x_2 \vee \ldots \vee x_{s-1} \vee x_s) \wedge y) \vee (x_1 \wedge x_2 \wedge \ldots \wedge x_{s-1} \wedge x_s)\,.\end{aligned} \tag{47}$$

Ezt az ismételt mediánozást leíró formulát s-re vonatkozó indukcióval könnyű bizonyítani.

Most tegyük fel, hogy $f(x_1, \ldots, x_n)$ monoton, önduális és a diszjunktív prímformája

$$f(x_1, \ldots, x_n) \;=\; t_1 \vee \cdots \vee t_m, \qquad t_j = x_{j1} \wedge \cdots \wedge x_{js_j}\,,$$

ahol egyetlen t_j prímimplikáns sincs valamelyik másikban (Q következmény). Bármelyik két prímimplikánsban legalább egy közös literálnak kell lennie. Ugyanis ha mondjuk $t_1 = x \wedge y$ és $t_2 = u \wedge v \wedge w$, akkor azokban az esetekben, amikor $x = y = 1$ és $u = v = w = 0$, valamint amikor $x = y = 0$ és $u = v = w = 1$, f értéke 1, és ez az öndualitást cáfolja. Így ha valamelyik t_j egyetlen x változóból áll, akkor egyedüli prímimplikánsnak kell lennie –

ebben az esetben f a triviális $f(x_1,\dots,x_n) = x = \langle xxx\rangle$ függvény.

A g_0, g_1, …, g_m függvényeket definiáljuk mediánokkal a következőképpen:

$$\begin{aligned} &g_0(x_1,\dots,x_n) = x_1\,, \\ &g_j(x_1,\dots,x_n) = h(x_{j1},\dots,x_{js_j}; g_{j-1}(x_1,\dots,x_n))\,, \text{ ha } 1 \le j \le m, \end{aligned} \tag{48}$$

ahol $h(x_1,\dots,x_s;y)$ a (47) felső sorában szereplő függvényt jelöli. (47) és (48) felhasználásával j-re vonatkozó indukcióval be lehet bizonyítani, hogy $g_j(x_1,\dots,x_n) = 1$, valahányszor $t_1 \vee \dots \vee t_j = 1$, mert amint láttuk, bármely két primimplikáns tartalmaz közös literált, ezért $(x_{j1} \vee \dots \vee x_{js_j}) \wedge t_k = t_k$, ha $k < j$.

Végül $f(x_1,\dots,x_n)$ megegyezik a $g_m(x_1,\dots,x_n)$ függvénnyel, mert mindkettő monoton és önduális, és megmutattuk, hogy $f(x_1,\dots,x_n) \le g_m(x_1,\dots,x_n)$ a 0-k és 1-esek minden kombinációjára. Ez az egyenlőtlenség elegendő ahhoz, hogy megállapítsuk az egyenlőséget, hisz egy önduális függvény a 2^n lehetséges esetnek pontosan a felében 1. ■

A P tétel egyik következménye az, hogy öt elem mediánját ki tudjuk fejezni három elem mediánja segítségével, mert páratlan számú Boole-változó mediánja nyilván monoton és önduális Boole-függvény. Jelöljön $\langle x_1 \dots x_{2k-1}\rangle$ egy ilyen mediánt. Ekkor $\langle vwxyz\rangle$ diszjunktív prímformája

$$\begin{aligned} &(v \wedge w \wedge x) \vee (v \wedge w \wedge y) \vee (v \wedge w \wedge z) \vee (v \wedge x \wedge y) \vee (v \wedge x \wedge z) \\ \vee &(v \wedge y \wedge z) \vee (w \wedge x \wedge y) \vee (w \wedge x \wedge z) \vee (w \wedge y \wedge z) \vee (x \wedge y \wedge z)\,, \end{aligned}$$

így a P tétel bizonyításában szereplő konstrukció úgy fejezi ki $\langle vwxyz\rangle$-t mint egy nagy, 2046 darab háromváltozós medián műveletet tartalmazó $g_{10}(v,w,x,y,z)$ formulát. Természetesen ez a kifejezés nem a lehető legrövidebb; valójában

$$\langle vwxyz\rangle \;=\; \langle v\langle xyz\rangle\langle wx\langle wyz\rangle\rangle\rangle\,. \tag{49}$$

Lásd Miiller és Winder [31] dolgozatát.

Medián algebrák és medián gráfok. Korábban már megjegyeztük, hogy az $\langle xyz\rangle$ háromváltozós művelet hasznos, ha x, y és z egy rendezett halmaznak, például a valós számok halmazának elemei, a $\wedge$ és $\vee$ jeleket pedig minimum-képzésként és maximumképzésként vesszük figyelembe. Valójában az $\langle xyz\rangle$ művelet sokkal általánosabb körülmények között is hasznos szerepet játszik. A *medián algebra* egy olyan M halmaz, melyen egy olyan $\langle xyz\rangle$ háromváltozós művelet van definiálva, mely M elemeihez M elemeit rendeli és teljesíti a következő három axiómát:

$$\langle xxy\rangle = x \quad \text{többségi (majoritás) törvény);} \tag{50}$$

$$\langle xyz\rangle = \langle xzy\rangle = \langle yxz\rangle = \langle yzx\rangle = \langle zxy\rangle = \langle zyx\rangle \quad \text{(kommutativitás törvény);} \tag{51}$$

$$\langle xw\langle ywz\rangle\rangle = \langle\langle xwy\rangle wz\rangle \quad \text{(asszociativitás törvény).} \tag{52}$$

Boole-algebrák esetében például az (52) asszociativitás törvény teljesül, ha $w = 0$ és $w = 1$, hiszen $\wedge$ és $\vee$ asszociatív. A 75. és 76. gyakorlatokban bizonyítjuk, hogy ebből a három axiómából következik a mediánokra vonatkozó disztributivitás törvény, melynek egy rövid

$$\langle\langle xyz\rangle uv\rangle \;=\; \langle x\langle yuv\rangle\langle zuv\rangle\rangle \tag{53}$$

és egy szimmetrikusabb hosszú

$$\langle\langle xyz\rangle uv\rangle \;=\; \langle\langle xuv\rangle\langle yuv\rangle\langle zuv\rangle\rangle \tag{54}$$

alakja is van. Ennek a ténynek nem ismert egyszerű bizonyítása, de (53) és (54) egy speciális esetét, amikor $y = u$ és $z = v$, legalább ellenőrizhetjük:

$$\langle\langle xyz\rangle yz\rangle \;=\; \langle xyz\rangle\,, \tag{55}$$

mert mindkét oldal $\langle xy\langle zyz\rangle\rangle$. És valóban, az (52) asszociativitás törvény éppen (53) $y = u$ speciális esete. Továbbá (55) és (52) felhasználásával az $x = u$ esetet is ellenőrizhetjük: $\langle\langle uyz\rangle uv\rangle = \langle vu\langle yuz\rangle\rangle = \langle\langle vuy\rangle uz\rangle = \langle\langle yuv\rangle uz\rangle = \langle\langle\langle yuv\rangle uv\rangle uz\rangle = \langle\langle yuv\rangle u\langle vuz\rangle\rangle = \langle u\langle yuv\rangle\langle zuv\rangle\rangle$.

Az M medián algebrában egy $C \subseteq M$ halmaz *ideál*, amennyiben

$$\langle xyz\rangle \;\in\; C,\;\; \text{valahányszor } x \in C,\; y \in C \text{ és } z \in M\,. \tag{56}$$

Ha u és v M elemei, az $[u\,.\,.\,v]$ *intervallumot* a következőképpen definiálhatjuk:

$$[u\,.\,.\,v] \;=\; \{\langle xuv\rangle \mid x \in M\}\,. \tag{57}$$

Azt mondjuk, hogy „x az u és v között van”, ha $x \in [u\,.\,.\,v]$. Ezeknek a definícióknak az értelmében u és v maguk is az $[u\,.\,.\,v]$ intervallumhoz tartoznak.

M lemma. *Minden $[u\,.\,.\,v]$ intervallum ideál, és $x \in [u\,.\,.\,v] \iff x = \langle uxv\rangle$.*

Bizonyítás. Legyenek $\langle xuv\rangle$ és $\langle yuv\rangle$ az $[u\,.\,.\,v]$ elemei. Ekkor (51) és (53) alapján minden $z \in M$-re

$$\langle\langle xuv\rangle\langle yuv\rangle z\rangle \;=\; \langle\langle xyz\rangle uv\rangle \;\in\; [u\,.\,.\,v]\,,$$

ezért $[u\,.\,.\,v]$ ideál. Továbbá (51) és (53) miatt minden $\langle xuv\rangle \in [u\,.\,.\,v]$ elemre $\langle xuv\rangle = \langle u\langle xuv\rangle v\rangle$. ■

A mediánra vonatkozó törvények miatt az $[u\,.\,.\,v]$ intervallumok kellemes tulajdonságokkal rendelkeznek:

$$v \in [u\,.\,.\,u] \;\Longrightarrow\; u = v\,; \tag{58}$$

$$x \in [u\,.\,.\,v] \text{ és } y \in [u\,.\,.\,x] \;\Longrightarrow\; y \in [u\,.\,.\,v]\,; \tag{59}$$

$$x \in [u\,.\,.\,v] \text{ és } y \in [u\,.\,.\,z] \text{ és } y \in [v\,.\,.\,z] \;\Longrightarrow\; y \in [x\,.\,.\,z]\,. \tag{60}$$

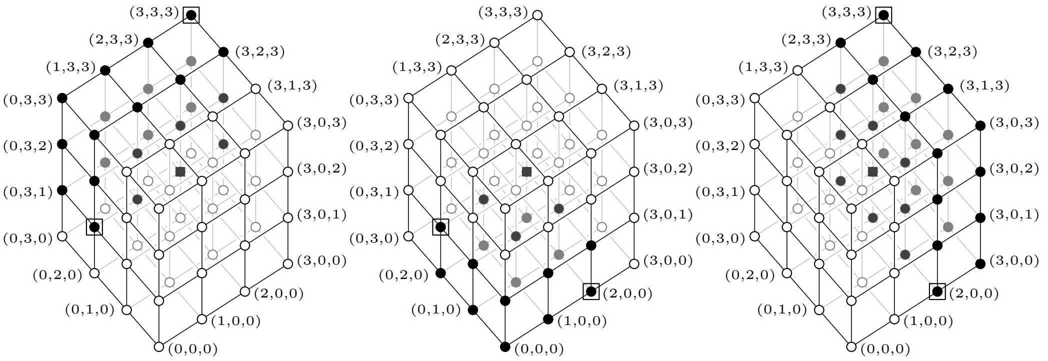
Ezzel ekvivalens megfogalmazásban: $[u\,.\,.\,u] = \{u\}$; ha $x \in [u\,.\,.\,v]$, akkor $[u\,.\,.\,x] \subseteq [u\,.\,.\,v]$; és $x \in [u\,.\,.\,v]$-ből az is következik, hogy minden z-re $[u\,.\,.\,z] \cap [v\,.\,.\,z] \subseteq [x\,.\,.\,z]$. (Lásd a 72. gyakorlatot.)

Most az M csúcshalmazon definiáljunk a következő élekkel egy gráfot:

$$u - v \quad\iff\quad u \neq v,\; \text{és } \langle xuv\rangle \in \{u, v\} \text{ minden } x \in M\text{-re}. \tag{61}$$

Más szavakkal u és v akkor és csak akkor szomszédosak, ha az $[u\,.\,.\,v]$ intervallum pontosan két pontot, az u-t és a v-t tartalmazza.

G tétel. *Ha M véges medián algebra, a (61) szerint definiált gráf összefüggő. Továbbá az*



7.7. ábra. Az $x = (0, 2, 1)$, $y = (3, 3, 3)$ és $z = (2, 0, 0)$ csúcsok közötti intervallumok egy $4 \times 4 \times 4$-es kockában.

x csúcs akkor és csak akkor tartozik az $[u\,..\,v]$ intervallumhoz, ha x az u-ból v-be vezető legrövidebb úton fekszik.

Bizonyítás. Ha M nem összefüggő, válasszuk u-t és v-t úgy, hogy ne vezessen út u-ból v-be, és az $[u\,..\,v]$ intervallum a lehető legkevesebb elemet tartalmazza. $x \in [u\,..\,v]$ különbözzön u-tól és v-től. Ekkor $\langle xuv \rangle = x \neq v$, így $v \notin [u\,..\,x]$; hasonlóan $u \notin [x\,..\,v]$. De (59) alapján $[u\,..\,x]$ és $[x\,..\,v]$ benne vannak $[u\,..\,v]$-ben. Így ezek szűkebb intervallumok, és út kell hogy vezessen u-ból x-be és x-ből v-be. Ez ellentmondás.

A tétel másik felét a 73. gyakorlatban bizonyítjuk. ■

Az intervallumokra vonatkozó definíciónkból $\langle xyz \rangle \in [x\,..\,y] \cap [x\,..\,z] \cap [y\,..\,z]$ következik, mert (55) szerint $\langle xyz \rangle = \langle \langle xyz \rangle xy \rangle = \langle \langle xyz \rangle xz \rangle = \langle \langle xyz \rangle yz \rangle$. A 74. gyakorlatban pedig a fordított irányt igazoljuk: ha $w \in [x\,..\,y] \cap [x\,..\,z] \cap [y\,..\,z]$, akkor $w = \langle xyz \rangle$. Másképp fogalmazva *az* $[x\,..\,y] \cap [x\,..\,z] \cap [y\,..\,z]$ *metszet mindig pontosan egy pontot tartalmaz*, amennyiben x, y és z M pontjai.

A 7.7. ábra ezt az elvet egy $4 \times 4 \times 4$-es kocka segítségével ábrázolja, ahol minden egyes x pontot (x_1, x_2, x_3) koordináták írnak le $(0 \leq x_1, x_2, x_3 < 4)$. Ennek a kockának a csúcsai medián algebrát alkotnak, mert $\langle xyz \rangle = (\langle x_1y_1z_1 \rangle, \langle x_2y_2z_2 \rangle, \langle x_3y_3z_3 \rangle)$; továbbá a 7.7. ábrán szereplő gráf élei a (61) definíciónak megfelelően azokat a csúcsokat kötik össze, melyek koordinátái megegyeznek egyetlen olyan koordináta kivételével, ahol a változás éppen ± 1. Három tipikus intervallum, az $[x\,..\,y]$, az $[x\,..\,z]$ és az $[y\,..\,z]$ intervallumok láthatók; az a három intervallum egyetlen közös pontja az $\langle xyz \rangle = (2, 2, 1)$ csúcs.

Eddig medián algebrából kiindulva definiáltunk bizonyos tulajdonságokkal rendelkező gráfot. De kiindulhatunk egy ilyen tulajdonságokkal bíró gráfból is, és felhasználhatjuk a gráfot, hogy medián algebrát definiáljunk. Ha u és v egy *tetszőleges* gráf csúcsai, definiáljuk az $[u\,..\,v]$ intervallumot az u és v közötti legrövidebb utakon fekvő pontok halmazával. Egy véges gráfot *medián gráfnak* nevezünk, ha pontosan egy csúcs van azon három intervallum $[x\,..\,y] \cap [x\,..\,z] \cap [y\,..\,z]$ metszetében, melyek három tetszőlegesen adott x, y és z csúcsot kötnek össze; ezt a csúcsot $\langle xyz \rangle$-vel jelöljük. A 75. gyakorlatban bizonyítjuk, hogy az így nyert háromváltozós művelet teljesíti a medián axiómákat.

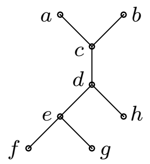
Ennek a definíciónak az értelmében medián gráfnak bizonyul sok fontos gráf. Például egy szabad fáról könnyen belátható, hogy medián gráf; egy másik egyszerű példa pedig az olyan gráf, mint az $n_1 \times n_2 \times \cdots \times n_m$ hipertégla. Medián gráfok Descartes-szorzatai is teljesítik az előírt feltételeket.

Medián címkék. Ha u és v egy medián algebra tetszőleges elemei, az $x \mapsto \langle xuv \rangle$ hozzárendeléssel megadott $f(x)$ függvény *homomorfizmus*; vagyis az (54) hosszú disztributivitás törvény miatt teljesül, hogy

$$f(\langle xyz \rangle) \;=\; \langle f(x) f(y) f(z) \rangle \,. \tag{62}$$

(57) szerint ez az $\langle xuv \rangle$ függvény egy adott x pontot „rávetít” az $[u \,.\,.\, v]$ intervallumra. És ez különösen érdekes abban az esetben, amikor $u — v$ a megfelelő gráf éle, mert ekkor $f(x)$ kétértékű, lényegében egy Boole-függvény.

Például vizsgáljuk az alább látható nyolc csúccsal és hét éllel rendelkező, tipikus szabad fát. Minden egyes x csúcsot rávetíthetünk az egyes $[u \,.\,.\, v]$ élintervallumokra úgy, hogy eldöntjük, x u-hoz vagy v-hez van-e közelebb:



$$\begin{array}{rccccccccc}
 & ac & bc & cd & de & ef & eg & dh & & \\
a \mapsto & a & c & c & d & e & e & d & & 0000000 \\
b \mapsto & c & b & c & d & e & e & d & & 1100000 \\
c \mapsto & c & c & c & d & e & e & d & & 1000000 \\
d \mapsto & c & c & d & d & e & e & d & & 1010000 \\
e \mapsto & c & c & d & e & e & e & d & & 1011000 \\
f \mapsto & c & c & d & e & f & e & d & & 1011100 \\
g \mapsto & c & c & d & e & e & g & d & & 1011010 \\
h \mapsto & c & c & d & d & e & e & h & & 1010001
\end{array} \tag{63}$$

A jobb oldalon a vetítéseket nullákra és egyesekre egyszerűsítettük, önkényesen eldöntve, hogy $a \mapsto 0000000$. Az előálló bitsorozatot a csúcsok *címkéinek* nevezzük, és azt írjuk például, hogy $l(b) = 1100000$. Mivel minden vetítés homomorfizmus, bármely három pont mediánját ki lehet számítani úgy, hogy egyszerűen meghatározzuk címkéi egyes komponenseinek a Boole-mediánját. Például ahhoz, hogy kiszámítsuk a $\langle bgh \rangle$ értéket, megkeressük $l(b) = 1100000$, $l(g) = 1011010$ és $l(h) = 1010001$ bitenkénti mediánját, ami $1010000 = l(d)$.

Amikor egy medián gráf éleire vetítünk, lehetséges, hogy azt tapasztaljuk, a bináris címkék két oszlopa azonos. Ilyen helyzet nem fordulhat elő egy szabad fával. De gondoljuk át, mi történne, ha (63)-ban a $g — h$ élt hozzáadnánk a fához: az eredménygráf medián gráf lenne, de az eg és dh oszlopok ($e \leftrightarrow d$ és $g \leftrightarrow h$ kivételével) azonossá válnának. Továbbá az új gh oszlop pedig azonos lenne a de oszloppal. Ilyen esetekben a redundáns komponenseket ki kellene törölni a címkékből; így a kibővített gráf csúcsainak a hét bites címkék helyett olyan hat bites címkéi lennének, mint $l(g) = 101101$ és $l(h) = 101001$.

Ilyen módon egy medián algebra elemei mindig reprezentálhatók címkékkel. Emiatt *bármelyik, Boole-algebrákban teljesülő azonosság igaz lesz minden medián algebrában is.* Ez a „nulla-egy elv” lehetővé teszi, hogy ellenőrizzük, vajon két, az $\langle xyz \rangle$ háromváltozós művelet felhasználásával felépített kifejezés az (50), az (51) és az (52) axiómák következményeként egyenlőnek tekinthető-e – bár ha n változós kifejezéseket tesztelünk ezzel a módszerrel, $2^{n-1} - 1$ esetet kell ellenőriznünk.

Például az asszociativitás $\langle xw \langle ywz \rangle \rangle = \langle \langle xwy \rangle wz \rangle$ törvénye azt sugallja, hogy bizonyára van mindkét oldalnak olyan szimmetrikus interpretációja, amelyik nem zavarodik bele az egymásba skatulyázott zárójelekbe. És valóban, van ilyen formula:

$$\langle xw\langle ywz\rangle\rangle \;=\; \langle\langle xwy\rangle wz\rangle \;=\; \langle xwywz\rangle\,, \tag{64}$$

ahol $\langle xwywz\rangle$ az $\{x,w,y,w,z\} = \{w,w,x,y,z\}$ ötelemű multihalmaz mediánját jelöli. Alkalmazva a nulla-egy elvet, továbbá figyelembe véve, hogy a medián ugyanaz a fogalom, mint Boole-algebrákban a majoritás, be tudjuk bizonyítani ezt a formulát. Hasonló módon bizonyíthatjuk (49)-et, és meg tudjuk mutatni, hogy a Post által (47)-ben használt függvény leegyszerűsíthető:

$$\langle x_1y\langle x_2y\ldots y\langle x_{s-1}yx_s\rangle\ldots\rangle\rangle \;=\; \langle x_1yx_2y\ldots yx_{s-1}yx_s\rangle\,. \tag{65}$$

Ez $2s-1$ elem mediánja, melyeknek közel fele y.

Egy gráf csúcsainak C halmazát *konvexnek* nevezzük, ha $[u\,.\,.\,v] \subseteq C$ minden olyan esetben, amikor $u \in C$ és $v \in C$. Másképp fogalmazva, amennyiben egy legrövidebb út végpontjai C-hez tartoznak, ezen út minden csúcsának szintén meg kell jelennie C-ben. (Következésképpen egy konvex halmaz megegyezik azzal, amit néhány oldallal ezelőtt „ideálnak” hívtunk; csak most az algebra nyelve helyett a geometria nyelvét használtuk.) $\{v_1,\ldots,v_m\}$ *konvex burka* az a legszűkebb konvex halmaz, amely a v_1, …, v_m csúcsok mindegyikét tartalmazza. A fenti elméleti eredményeink megmutatták, hogy minden $[u\,.\,.\,v]$ intervallum konvex; ennélfogva $[u\,.\,.\,v]$ az $\{u,v\}$ két pontból álló halmaz konvex burka. De valójában sokkal több igaz:

C tétel. *Egy medián gráfban $\{v_1,v_2,\ldots,v_m\}$ konvex burka a*

$$C \;=\; \bigl\{\langle v_1xv_2x\ldots xv_m\rangle \bigm| x \in M\bigr\} \tag{66}$$

halmaz. Továbbá x akkor és csak akkor van benne C-ben, ha $x = \langle v_1xv_2x\ldots xv_m\rangle$.

Bizonyítás. Világos, hogy $v_j \in C$, ha $1 \le j \le m$. C minden pontjának a konvex burokhoz kell tartoznia, mert az $x' = \langle v_2x\ldots xv_m\rangle$ pont (az m-re vonatkozó indukció szerint) a burokban van, és mert $\langle v_1x\ldots xv_m\rangle \in [v_1\,.\,.\,x']$. A nulla-egy elv biztosít, hogy

$$\langle x\langle v_1yv_2y\ldots yv_m\rangle\langle v_1zv_2z\ldots zv_m\rangle\rangle = \langle v_1\langle xyz\rangle v_2\langle xyz\rangle\ldots\langle xyz\rangle v_m\rangle\;; \tag{67}$$

ezért C konvex. Ebben a formulában ha $x = y$, akkor $\langle v_1xv_2x\ldots xv_m\rangle$ C-nek x-hez legközelebbi pontja, és $\langle v_1xv_2x\ldots xv_m\rangle \in [x\,.\,.\,z]$ minden $z \in C$-re. ■

C következmény. *A v_j címkéje legyen $v_{j1}\ldots v_{jt}$ $1 \le j \le m$-re. Ekkor $\{v_1,\ldots,v_m\}$ konvex burka azon $x \in M$ elemek halmaza, melyek $x_1\ldots x_t$ címkéje kielégíti az $x_j = c_j$ feltételt, valahányszor $v_{1j} = v_{2j} = \cdots = v_{mj} = c_j$.* ■

Például (63)-ban a $\{c,g,h\}$ konvex burka minden olyan elemet tartalmaz, amelynek a címkéje illeszkedik az 100 mintára, és ezek $\{c,d,e,g,h\}$.

Amikor egy medián gráf egy 4 hosszúságú u—x—v—y—u kört tartalmaz, az u—x és a v—y élek ekvivalensek abban az értelemben, hogy mind az $[u\,.\,.\,x]$-re vetítés, mind a $[v\,.\,.\,y]$-ra vetítés ugyanazt a címke koordinátát adja. A magyarázat erre az, hogy bármely olyan z-re, melyre $\langle zux\rangle = u$,

$$\begin{aligned} y = \langle uvy\rangle &= \langle\langle zux\rangle vy\rangle \\ &= \langle\langle zvy\rangle\langle uvy\rangle\langle xvy\rangle\rangle \\ &= \langle\langle zvy\rangle yv\rangle\;, \end{aligned}$$

ezért $\langle zvy \rangle = y$. Ehhez hasonlóan $\langle zux \rangle = x$ maga után vonja $\langle zvy \rangle = v$-t. Az $x — v$ és az $y — u$ élek pedig ugyanilyen okok miatt ekvivalensek. A 77. gyakorlatban többek között megmutatjuk, hogy két él akkor és csak akkor eredményez ekvivalens vetítést, ha be lehet bizonyítani ily módon ekvivalenciájukat 4 hosszúságú körökből nyert ekvivalencia-láncokon keresztül. Következésképpen az egyes csúcs-címkékben a bitek száma a 4 hosszúságú körökkel létrehozott élek ekvivalencia-osztályainak száma. Ezt követően a csúcsok redukált címkéit egyértelműen megállapíthatjuk, amint megadjuk a $00 \ldots 0$ címkéjű csúcsot.

Egy medián gráf csúcs-címkéjének megtalálására remek módszert talált ki Jha és Slutzki [20], majd Hagauer, Imrich és Klažar [17] tovább javította a módszert:

H algoritmus *(a medián címkékre)*. Adott G medián gráf és a forrás-csúcs esetén ez az algoritmus meghatározza a G 4 hosszúságú körei által definiált ekvivalencia-osztályokat, és kiszámolja minden egyes csúcs $l(v) = v_1 \ldots v_t$ címkéjét, ahol t az oszályok száma, továbbá $l(a) = 0 \ldots 0$.

H1. (Kezdőértékek beállítása.) Dolgozzuk fel előzetesen G-t úgy, hogy a-tól való távolságuk sorrendjében járjuk be az összes csúcsát. Egy $u — v$ él esetén azt mondjuk, hogy u a v ***közeli szomszédja***, ha a közelebb van u-hoz, mint v-hez, ellenkező esetben u ***távoli szomszéd***. Másképp, amire eljutunk v-hez, v közeli szomszédjait már felkerestük, de a távoli szomszédok még várakoznak erre. Rendezzük át az összes szomszédsági listát úgy, hogy először a közeli szomszédokat soroljuk fel. Kezdetben helyezzünk minden élt saját ekvivalencia-osztályába; egy a 2.3.3. algoritmushoz hasonló „uniókereső algoritmust” használunk majd az osztályok összefésülésére, amikor az algoritmus rájön, hogy ezek ekvivalensek.

H2. (Eljáráshívás.) Legyen $j \leftarrow 0$ és hívjuk meg az I eljárást az a paraméterrel. (Az I eljárást lentebb megadjuk. A j globális változót arra fogjuk használni, hogy létrehozzuk az $r_j — s_j$ élek elsődleges listáját, ahol $1 \leq j < n$ és n a csúcsok száma; minden $v \neq a$ csúcs esetén lesz egy listaelem, melyre $s_j = v$.)

H3. (Címkék meghatározása.) Sorszámozzuk meg az ekvivalencia-osztályokat 1-től t-ig. Aztán legyen $l(a)$ a t bites $0 \ldots 0$ sorozat. $j = 1, 2, \ldots, n-1$ sorrendben állítjuk elő az $l(s_j)$ sorozatot $l(r_j)$-ből úgy, hogy k bitet módosítunk benne 0-ról 1-re, ahol k az $r_j — s_j$ él ekvivalencia-osztályának sorszáma. ■

I eljárás *(r utódjainak feldolgozására)*. Ez az r paraméterrel és a j globális változóval dolgozó rekurzív eljárás végzi el a H algoritmus leglényegesebb feladatát az r csúcsból elérhető csúcsokat tartalmazó gráfon. A feldolgozás során az r csúcs kivételével fel fogunk jegyezni az elsődleges listára minden ilyen csúcsot, és az aktuális gráfból pedig el fogunk távolítani minden köztük futó élt. Minden egyes csúcs négy adatmezővel rendelkezik: `CSATOLÁS`, `JELÖLÉS`, `SZINTSZÁM`, `PÁR`, ezek kezdetben üresek.

I1. (s szerinti ciklus.) Válasszunk egy olyan s csúcsot, amelyikre $r — s$. Ha nincs ilyen csúcs, térjünk vissza az eljárásból.

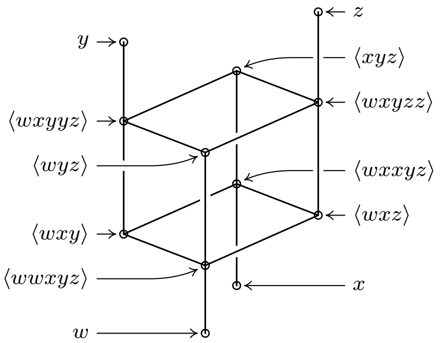
I2. (Rögzítsük az élt.) Legyen $j \leftarrow j + 1$, $r_j \leftarrow r$ és $s_j \leftarrow s$.

I3. (Kezdjük el a szélességi keresést.) (Most meg akarjuk keresni és ki akarjuk törölni az aktuális gráf összes olyan csúcsát, amelyik $r — s$-sel ekvivalens.) `JELÖLÉS(s)` $\leftarrow s$, `SZINTSZÁM(s)` $\leftarrow 1$, `CSATOLÁS(s)` $\leftarrow \Lambda$ és $v \leftarrow q \leftarrow s$.

I4. (Keressük meg v párját.) Keressük meg v azon u közeli szomszédját, melyre `JELÖLÉS(u)` $\neq s$. (Pontosan egy ilyen u csúcs van. Legyen `PÁR(v)` $\leftarrow u$.)

I5. ($u — v$ törlése.) Tegyük az $u — v$ és $r — s$ éleket ekvivalenssé ekvivalencia-osztályaik

7.2. táblázat.
NÉGY GENERÁTORON ALAPULÓ SZABAD MEDIÁN ALGEBRÁHOZ CÍMKÉK



j	r_j	s_j	$l(s_j)$
		w	0000000
1	w	$\langle wwxyz\rangle$	0000001
2	$\langle wwxyz\rangle$	$\langle wyz\rangle$	0010001
3	$\langle wyz\rangle$	$\langle wxyzz\rangle$	0010101
4	$\langle wxyzz\rangle$	$\langle xyz\rangle$	0010111
5	$\langle wxyzz\rangle$	z	1010101
6	$\langle wyz\rangle$	$\langle wxyyz\rangle$	0010011
7	$\langle wxyyz\rangle$	y	0110011
8	$\langle wwxyz\rangle$	$\langle wxz\rangle$	0000101
9	$\langle wxz\rangle$	$\langle wxxyz\rangle$	0000111
10	$\langle wxxyz\rangle$	x	0001111
11	$\langle wwxyz\rangle$	$\langle wxy\rangle$	0000011

egyesítésével. u-t és v-t távolítsuk el egymás szomszédsági listáiból.

I6. (v szomszédainak osztályozása.) v minden egyes u közeli szomszédjára lépjünk I7-re; v minden egyes u távoli szomszédjára lépjünk I8-ra. Aztán lépjünk I9-re.

I7. (Jegyezzünk fel egy lehetséges ekvivalenciát.) Ha SZINTSZÁM(u) $=$ s és SZINTSZÁM(u) $= 1$, tegyük az u—v élt ekvivalenssé az PÁR(u)—PÁR(v) éllel. Térjünk vissza I6-ra.

I8. (u szintszáma.) Ha JELÖLÉS(u) $= s$ és SZINTSZÁM(u) $= 1$, térjünk vissza I6-ra. Egyébként legyenek JELÖLÉS(u) $\leftarrow s$ és SZINTSZÁM(u) $\leftarrow 2$. Legyen w az u első szomszédja (ez közeli szomszéd lesz). Ha $w = v$, állítsuk vissza w-t u második közeli szomszédjának; de térjünk vissza I6-ra, ha u-nak csak egy közeli szomszédja van. Ha JELÖLÉS(w) $\neq$ s vagy SZINTSZÁM(w) $\neq$ 2, legyen SZINTSZÁM(u) $\leftarrow$ 1, CSATOLÁS(u) $\leftarrow \Lambda$, CSATOLÁS(q) $\leftarrow u$ és $q \leftarrow u$. Térjünk vissza I6-ra.

I9. (Folytassuk a szélességi keresést.) Legyen $v \leftarrow$ CSATOLÁS(v). Térjünk vissza I4-re, ha $v \neq \Lambda$.

I10. (Az s részgráf feldolgozása.) Hívjuk meg az I eljárást rekurzív módon az s paraméterrel. Aztán térjünk vissza I1-re. ■

Ezt az algoritmust és eljárást aránylag magas szintű adatszerkezetek nyelvén írtuk le; a további részletezés az olvasóra marad. Így például ahhoz, hogy az I5 lépésben az élek könnyedén törölhetők legyenek, a szomszédsági listáknak két irányban láncoltaknak kellene lenniük. Ugyanakkor az ekvivalencia-osztályok egyesítésére ebben a lépésben bármilyen alkalmas módszer használható.

A 77. gyakorlatban elmagyarázzuk az algoritmus által elvégzett munkát megalapozó elképzelést, a 78. gyakorlatban pedig igazoljuk, hogy az I4 lépésben minden egyes csúccsal legfeljebb $\lg n$ alkalommal találkozunk. A 79. gyakorlatban megmutatjuk továbbá, hogy egy medián gráfnak legfeljebb $O(n \lg n)$ éle van. Tehát ha figyelmen kívül hagyjuk a H3 lépésben a bitbeállítást, a H algoritmus teljes futási ideje $O(n(\lg n)^2)$.

Lehet, hogy az Olvasó szeretné a H algoritmust saját maga végigkövetni a 7.2. táblázatbeli medián gráfon, melynek csúcsai négy változó, aw, x, y és z, tizenkét monoton, önduális

Boole-függvényét reprezentálják. Minden ilyen, mind a négy változóval ténylegesen dolgozó függvény kifejezhető, (64)-hez hasonlóan, öt dolog mediánjaként. Az $a = w$ csúccsal kezdve az algoritmus kiszámolja az $r_j — s_j$ élek elsődleges listáját és a táblázatban látható bináris címkéket. (A feldolgozás tényleges sorrendje attól a sorrendtől függ, hogy a csúcsok a szomszédsági listában hogy jelennek meg. De a végső címkék bármely sorrend esetén az oszlopok sorrendjétől eltekintve megegyeznek.)

Vegyük észre, hogy az egyes $l(v)$ címkékben az 1-es bitek száma v-nek az a kezdő csúcstól való távolsága. Mivel bármely konkrét csúccsal kezdhettünk volna, a címkék egyértelműsége valójában azt jelenti, hogy *két csúcs közötti távolság azon bitpozíciók száma, amelyekben címkéik különböznek*.

A 7.2. táblázatbeli speciális medián gráfot voltaképpen egészen másképp is kezelhettük volna, a H algoritmus bármiféle használata nélkül, mert ebben az esetben a címkék lényegében ugyanazok, mint a megfelelő függvények *igazságtáblái*. Ez azért van így, mert a w, x, y és z egyszerű függvények igazságtáblái rendre $t(w) = 0000000011111111$, $t(x) = 0000111100001111$, $t(y) = 0011001100110011$ és $t(z) = 0101010101010101$. Ekkor $\langle wwxyz\rangle$ igazságtáblája a $\langle t(w)t(w)t(x)t(y)t(z)\rangle$ bitenkénti majoritás függvény, nevezetesen a 0000000101111111 füzér. Hasonló számítás adja az összes többi csúcs igazságtábláját.

Bármely önduális függvény igazságtáblájának második fele lényegében ugyanaz, mint az első fele, csak éppen az első fél komplemensének a fordítottja, így elhagyhatjuk. Továbbá igazságtábláinkban a legbaloldalibb bit mindig nulla, tehát végül a 7.2. táblázatbeli hét bites címkékkel fejeztük be ezt a gondolatmenetet. Az egyértelműség tulajdonsága pedig garantálja, hogy az oszlopok sorrendjétől eltekintve a H algoritmus ugyanezt az eredményt fogja adni, amikor ezen a speciális gráfon mutatjuk be a működését.

Ezen okoskodás szerint a 7.2. táblázatbeli gráf élei megfelelnek azoknak a függvénypároknak, melyeknek igazságtáblái majdnem megegyeznek. A szomszédos csúcsok között csak két, az igazságtábláikban szereplő eltérő bitnek az átváltásával mozgunk. Valójában egy csúcs foka a csúcs által reprezentált monoton önduális függvény diszjunktív prímformájában a prímimplikánsok pontos száma (lásd a 70. és a 84. gyakorlatokat).

***Medián halmazok.** Medián halmaz bináris vektorok olyan X halmaza, melyre $\{x, y, z\} \subseteq X$ esetén $\langle xyz\rangle \in X$, ahol a mediánokat koordinátánként számoljuk - úgy, ahogy azt a medián címkékkel tettük. Schaefer 1978-ban észrevette, hogy a medián halmazok a Horn-függvények H tételbeli jellemzésének elegáns gondolati ellenpontját szolgáltatják:

S tétel. *Egy $f(x_1, \ldots, x_n)$ Boole-függvény akkor és csak akkor fejezhető ki Krom-klózok konjunkciójaként, ha*

$$\begin{aligned} f(x_1,\ldots,x_n) = f(y_1,\ldots,y_n) = f(z_1,\ldots,z_n) = 1 \\ \textit{maga után vonja, hogy } f(\langle x_1y_1z_1\rangle,\ldots,\langle x_ny_nz_n\rangle) = 1 \end{aligned} \tag{68}$$

minden x_j, y_j és z_j Boole-értékre.

Bizonyítás. [?, Lemma 3.1B. lemma] Ha $x_1 \vee x_2 = y_1 \vee y_2 = z_1 \vee z_2 = 1$, és mondjuk $x_1 \le y_1 \le z_1$, akkor $\langle x_1y_1z_1\rangle \vee \langle x_2y_2z_2\rangle = y_1 \vee \langle x_2y_2z_2\rangle = 1$, mivel $y_1 = 0$ maga után vonja, hogy $x_2 = y_2 = 1$. Ezért (68) szükséges.

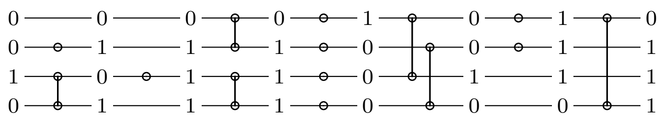
Fordítva, ha (68) teljesül, legyen $u_1 \vee \cdots \vee u_k$ f prímklóza, ahol minden u_j literál. Ekkor $1 \le j \le k$-ra az $u_1 \vee \cdots \vee u_{j-1} \vee u_{j+1} \vee \cdots \vee u_k$ klóz nem f klóza; így van egy $x^{(j)}$ vektor, melyre $f(x^{(j)}) = 1$, de $u_i^{(j)} = 0$ minden $i \ne j$-re. Ha $k \ge 3$, akkor az $\langle x^{(1)}, x^{(2)}x^{(3)}\rangle$

mediánban $u_i = 0$ minden $1 \le i \le k$-ra. Ez azonban lehetetlen, mert feltételezésünk szerint $u_1 \vee ... \vee u_k$ primklóza f-nek. Ezért $k \le 2$. ■

Így egy medián halmaz nem más, mint „2SAT előfordulások" – azaz valamely f 2KNF függvényt kielégítő pontok – halmaza.

Egy medián halmazt *redukáltnak* nevezünk, ha az $x = x_1 \dots x_t$ vektorai nem tartalmaznak redundáns komponenst. Másképp fogalmazva, egy redukált medián halmaz az egyes koordináta-pozíciókra legalább két olyan vektort tartalmaz, mondjuk a k pozícióra az $x^{(k)}$ és $y^{(k)}$ vektorokat, melyekre $x_k^{(k)} = 0$ és $y_k^{(k)} = 1$, de $x_i^{(k)} = y_i^{(k)}$, ha $i \ne k$. Láttuk, hogy egy medián gráf kielégíti ezt a feltételt. Valóban, a k koordináta megfelel az $u — v$ gráfbeli élnek, u és v címkéinek pedig választhatjuk $x^{(k)}$-t és $y^{(k)}$-t. Fordítva, bármely X redukált medián halmaz egy medián gráfot definiál, melyben X minden eleméhez tartozik egy csúcs, és X két vektorát pontosan akkor köti össze él, ha egy kivétellel minden megfelelő koordinátájuk egyenlő. Ezen csúcsok medián címkéinek meg kell egyeznie az X-beli eredeti vektorokkal, mert tudjuk, hogy a medián címkék lényegében egyértelműek.

Jellemezhetjük még a medián címkéket és a redukált medián halmazokat egy másik, az 5.3.4. pontban tanulmányozott *összehasonlító modulok* hálózatához visszatérő tanulságos módszerrel is. Ebben a pontban megfigyeltük, hogy az ilyen hálózatok hasznosak számok feledékeny rendezésére, és észrevettük az 5.3.4. tételben, hogy összehasonlító modulok hálózata akkor és csak akkor fogja rendezni a lehetséges $n!$ input permutációt, ha helyesen rendezi nulláknak és egyeseknek az összes, 2^n különböző kombinációját. Amikor egy összehasonlító modult két vízszintes vonalhoz kapcsolunk, melyek balról belépő x és y bemenettel rendelkeznek, ugyanezt a két kimenetet kapjuk a jobb oldalon, csak a felső vonalon $\min(x, y) = x \wedge y$-t, az alsó vonalon pedig $\max(x, y) = x \vee y$-t. Terjesszük ki kissé a fogalmunkat olyan *átalakító modulok* engedélyezésével, melyek a 0-t 1-re és 1-et 0-ra cserélik. Itt van például egy összehasonlító-átalakító hálózat (vagy röviden CI-net), ami a 0010 bináris értéket 0111-gyé alakítja:



. (69)

(Az egyedül álló pont átalakítót jelöl.) Valóban, ez a hálózat az alábbi átalakítást végez:

$$\begin{array}{llll} 0000 \mapsto 0110\,; & 0100 \mapsto 0111; & 1000 \mapsto 0111; & 1100 \mapsto 0110\,; \\ 0001 \mapsto 0111\,; & 0101 \mapsto 1111; & 1001 \mapsto 0101; & 1101 \mapsto 0111\,; \\ 0010 \mapsto 0111\,; & 0110 \mapsto 1111; & 1010 \mapsto 0101; & 1110 \mapsto 0111\,; \\ 0011 \mapsto 0110\,; & 0111 \mapsto 0111; & 1011 \mapsto 0111; & 1111 \mapsto 0110\,. \end{array} \tag{70}$$

Tegyük fel, hogy egy CI-net az $x = x_1 \dots x_t$ bitfüzért az $x'_1 \dots x'_t = f(x)$ bitfüzérré alakítja. Ez az f függvény, ami egy t-kockát saját magára képez, valójában egy *gráf homomorfizmus*. Másképp fogalmazva az eredmény kockában $f(x) — f(y)$, mindahányszor a t-kockában $x — y$: x egy bitjének megváltoztatása $f(x)$ pontosan egy bitjének megváltozását okozza mindig, mert a hálózatban minden modul így működik. Másfelől a CI-netek figyelemre méltó kapcsolatban vannak a medián címkékkel is:

F tétel. *t bites medián címkék bármely halmaza reprezentálható egy olyan $f(x)$ Boole-függvényt kiszámító CI-nettel, melyre $f(x) \in X$ minden $x_1 \dots x_t$ bitvektorra, és $f(x) = x$*

minden $x \in X$-re.

Bizonyítás. Feder [13]-beli 3.37-es lemmája; lásd még Wiedemann [?] Ph. D. értekezését. Vizsgáljuk a medián címkék i és j oszlopait ($1 \le i < j \le t$). Ha a címkék teljes halmazát átnézzük, bármelyik ilyen oszloppár a négy lehetséges $\{00, 01, 10, 11\}$ értékpár közül legalább hármat tartalmaz, mert a medián címkéknek nincs redundáns oszlopuk. Írjuk rendre azt, hogy $\bar{\jmath} \to i$, $j \to i$, $i \to j$ vagy $i \to \bar{\jmath}$, ha a 00, a 01, az 10 vagy éppen az 11 hiányzik ebből a két oszlopból; írhatjuk persze a megfelelő $\bar{\imath} \to j$, $\bar{\imath} \to \bar{\jmath}$, $\bar{\jmath} \to \bar{\imath}$ vagy $j \to \bar{\imath}$ ekvivalens relációkat az i helyett $\bar{\imath}$-t használva. Például a 7.2. táblázatbeli címkék az

$$\begin{array}{ll} 1 \to \bar{2}, 3, \bar{4}, 5, \bar{6}, 7 & 2, \bar{3}, 4, \bar{5}, 6, \bar{7} \to \bar{1}; \\ 2 \to 3, \bar{4}, \bar{5}, 6, 7 & \bar{3}, 4, 5, \bar{6}, \bar{7} \to \bar{2}; \\ 3 \to \bar{4}, 7 & 4, \bar{7} \to \bar{3}; \\ 4 \to 5, 6, 7 & \bar{5}, \bar{6}, \bar{7} \to \bar{4}; \\ 5 \to 7 & \bar{7} \to \bar{5}; \\ 6 \to 7 & \bar{7} \to \bar{6} \end{array} \tag{71}$$

relációkat adják. (A 3. és az 5. oszlopok között nem áll fenn reláció, mert mind a négy lehetőség előfordul ezekben az oszlopokban. De $3 \to \bar{4}$, mert a 3. és a 4. oszlopokban nem fordul elő a 11. A 7.2. táblázatban azok a csúcsok, amelyek címkéinek 3. oszlopa 1, pontosan azok, melyek közelebb vannak $\langle wyz \rangle$-hez, mint $\langle wwxyz \rangle$-hez; ezek a címkéik 4. oszlopában 0-át tartalmazó csúcsok konvex halmazt alkotnak, mert mind közelebb vannak $\langle wxxyz \rangle$-hez, mint x.)

Az $\{1, \bar{1}, 2, \bar{2}, \ldots, t, \bar{t}\}$ literálok közötti relációk nem tartalmaznak kört, így ezek mindig elrendezhetok topologikusan egy $u_1, u_2, \ldots, u_{2t}$ antiszimmetrikus sorozatba, ahol u_{2t+1-j} komplementuma u_j. lehetnek, ahol u_{2t+1-j} komplemense u_j. Például a (71)-beli relációknak az (71)-beli relációk az

$$1 \;\; \bar{7} \;\; 4 \;\; 2 \;\; \bar{3} \;\; \bar{5} \;\; \bar{6} \;\; 6 \;\; 5 \;\; 3 \;\; \bar{2} \;\; \bar{4} \;\; 7 \;\; \bar{1} \tag{72}$$

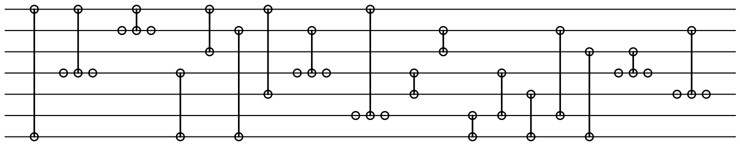
sorozat egy ilyen topologikus rendezése.

A t üres vonalból kiindulva most folytatjuk a hálózat építését úgy, hogy a topologikus sorozatban az u_k és u_{k+d} elemeket $k = 1, 2, \ldots, t - \lceil d/2 \rceil$-re egymás után megvizsgáljuk $d = 2t-2, 2t-3, \ldots, 1$ sorrendben. Ha $u_k \le u_{k+d}$ az i és j ($i < j$) oszlopok között fennálló reláció, a hálózat i és j vonalaihoz hozzáadunk egy új modult a következőképpen:

Ha $i \to j$ Ha $i \to \bar{\jmath}$ Ha $\bar{\imath} \to j$ Ha $\bar{\imath} \to \bar{\jmath}$

(73)

Például (71)-ből és (72)-ből először $1 \to 7$-et, aztán $1 \to \bar{4}$-et, aztán $1 \to \bar{2}$-t, aztán $\bar{7} \to \bar{4}$-et (azaz $4 \to 7$-et) stb. hajtjuk végre a következő hálózatot nyerve:



(74)

(Nézd meg az ábrát. Nincs működő modul amikor, mondjuk u_k $\bar{7}$ és u_{k+d} 3, mert a $\bar{3} \to 7$ reláció nem jelenik meg (71)-ben.)

A 89. gyakorlatban bebizonyítjuk, hogy a (73)-beli modulok minden egyes új egysége az előző egyenlőtlenségeket megőrzi és egy újat kikényszerít. Így ha x input vektor, $f(x)$ az összes egyenlőtlenséget kielégíti; így az S tétel szerint $f(x) \in X$. Fordítva, ha $x \in X$, x-et a hálózatban a modulok minden egysége változatlanul hagyja. ■

F következmény. *Az F tételben a medián címkékről tegyük fel, hogy a bitenkénti AND és OR műveletekre nézve zártak, azaz $x \mathbin{\&} y \in X$ és $x \mid y \in X$, ahányszor csak $x \in X$ és $y \in X$. Ekkor a koordinátáknak van olyan permutációja, mely mellett a címkék reprezentálhatók csak összehasonlító moduloknak a hálózatával.*

Bizonyítás. Az összes címke bitenkénti AND-je $0\ldots0$, és bitenkénti OR-ja $1\ldots1$. Így az oszlopok közötti lehetséges relációk csak $i \to j$ és $j \to i$. Az oszlopok topologikus rendezésével és átnevezésével biztosíthatjuk, hogy csak az $i \to j$ forduljon elő, ha $i < j$; és ebben az esetben a bizonyításbeli konstrukció soha nem használ átalakítót. ■

Egy G gráf csúcsait ezen csúcsok X részhalmazába képező f homomorfizmus *összehúzás*, ha $f(x) = x$ teljesül minden $x \in X$-re; X-et pedig G *összehúzójának* nevezzük, ha van ilyen f. A gráfelméletben ennek a fogalomnak a fontosságát először Hell [?] emelte ki. Az egyik eredmény például az, hogy az X-beli csúcsok közötti távolság – a legrövidebb úton fekvő élek száma – ugyanakkora marad akkor is, ha kizárólag az X-ben fekvő utakra szorítkozunk. (Lásd a 93. gyakorlatot.)

Az F tétel mutatja, hogy medián címkék minden t-dimenziós halmaza egy t-dimenziós hiperkocka összehúzása. Fordítva, a 94. gyakorlatban megmutatjuk, hogy a hiperkocka összehúzások mindig medián gráfok.

Küszöbfüggvények. Az $f(x_1, x_2, \ldots, x_n)$ Boole-függvények különösen fontos osztálya az, amikor f-et az

$$f(x_1, x_2, \ldots, x_n) \;=\; [w_1x_1 + w_2x_2 + \cdots + w_nx_n \geq t]\,, \tag{75}$$

formula definiálja, ahol a w_1, w_2, …, w_n konstansok egész szám „súlyok” és t egy egész „küszöbérték”. Fontosak például azok a küszöbfüggvények, amikor minden súly egységnyi:

$$x_1 \wedge x_2 \wedge \cdots \wedge x_n = [x_1 + x_2 + \cdots + x_n \geq n]\,; \tag{76}$$

$$x_1 \vee x_2 \vee \cdots \vee x_n = [x_1 + x_2 + \cdots + x_n \geq 1]\,; \tag{77}$$

$$\text{és} \qquad \langle x_1x_2\ldots x_{2t-1}\rangle = [x_1 + x_2 + \cdots + x_{2t-1} \geq t]\,, \tag{78}$$

ahol $\langle x_1x_2\ldots x_{2t-1}\rangle$ egy olyan multihalmaz medián (vagy majoritás) értékét jelenti, amelyik az $\{x_1, x_2, \ldots, x_{2t-1}\}$ tetszés szerinti páratlan sok Boole-értékből áll. Speciálisan az $x \wedge y$, $x \vee y$ és $\langle xyz\rangle$ alapleképezések mind küszöbfüggvények, és az

$$\bar{x} \;=\; [-x \geq 0] \tag{79}$$

is az.

Általánosabb súlyokkal olyan további érdekes függvényhez jutunk, mint a

$$\left[2^{n-1}x_1 + 2^{n-2}x_2 + \cdots + x_n \geq (t_1t_2\ldots t_n)_2\right], \tag{80}$$

ami pontosan akkor igaz, ha az $x_1x_2\ldots x_n$ bináris füzér lexikografikusan nagyobb vagy egyenlő, mint egy adott $t_1t_2\ldots t_n$ bináris füzér. Adva van w_1, w_2, …, w_n méretű objektumoknak egy n-elemű halmaza. Ezen objektumok egy részhalmaza pontosan akkor fér bele egy $t-1$ méretű hátizsákba, ha $f(x_1,x_2,\ldots,x_n)=0$, ahol $x_j=1$ reprezentálja a j objektumnak a részhalmazban való megjelenését. Az eredetileg McCullough és Pitts által [30]-ben javasolt egyszerű neuronmodell küszöbfüggvényekből felépülő neurális hálókról szóló publikációk ezreihez vezetett.

Bármelyik negatív w_j súlyt eltüntethetjük az $x_j \leftarrow \bar{x}_j$, $w_j \leftarrow -w_j$ és $t \leftarrow t+|w_j|$ beállításokkal. Így egy általános küszöbfüggvény olyan pozitív küszöbfüggvénnyé redukálható, amelyben minden súly nemnegatív. Továbbá bármely pozitív (110) küszöbfüggvény kifejezhető mint a páratlan medián/majoritás függvény egy speciális esete, mert

$$\langle 0^a 1^b x_1^{w_1} x_2^{w_2} \ldots x_n^{w_n}\rangle = [b + w_1x_1 + w_2x_2 + \cdots + w_nx_n \ge b+t]\,, \tag{81}$$

ahol x^m az x m darab másolatát jelenti, és ahol a és b az

$$a=\max(0,2t-1-w),\quad b=\max(0,w+1-2t),\quad w=w_1+w_2+\cdots+w_n \tag{82}$$

szabályokkal vannak definiálva. Például amikor minden súly 1,

$$\langle 0^{n-1}x_1\ldots x_n\rangle = x_1\wedge\cdots\wedge x_n \quad\text{és}\quad \langle 1^{n-1}x_1\ldots x_n\rangle = x_1\vee\cdots\vee x_n. \tag{83}$$

Amikor $n=2$, már láttuk ezeket a formulákat (45)-ben. Általában vagy a, vagy b nulla, és (81) bal oldala $2T-1$ elem mediánját határozza meg, ahol

$$T \;=\; b+t \;=\; \max(t, w_1+w_2+\cdots+w_n+1-t). \tag{84}$$

Nem változtatna ezen, ha előírnánk, hogy a is, és b is nullánál nagyobb legyen, mert a majoritás függvény nyilván kielégíti a

$$\langle 01x_1x_2\ldots x_{2t-1}\rangle \;=\; \langle x_1x_2\ldots x_{2t-1}\rangle \tag{85}$$

törlés törvényt.

(81) egyik fontos következménye, hogy minden pozitív küszöbfüggvény a

$$g(x_0,x_1,x_2,\ldots,x_n) \;=\; \langle x_0^{a+b}x_1^{w_1}x_2^{w_2}\ldots x_n^{w_n}\rangle \tag{86}$$

tiszta majoritás függvényből az $x_0=0$ vagy 1 beállítással származik. Másképp fogalmazva akkor és csak akkor ismerjük az összes n-változós küszöbfüggvényt, ha ismerjük az összes (konstanst nem tartalmazó) legfeljebb $n+1$ változós páratlan medián függvényt. Minden tiszta majoritás függvény monoton és önduális. Már vizsgáltuk a 25. oldalon található 7.2. táblázat s_j oszlopában a $\{w,x,y,z\}$ változók feletti tiszta majoritás függvényeket, nevezetesen a $\langle w\rangle$, $\langle wwxyz\rangle$, $\langle wyz\rangle$, $\langle wxyzz\rangle$, $\langle xyz\rangle$, $\langle z\rangle$, $\langle wxyyz\rangle$, $\langle y\rangle$, $\langle wxz\rangle$, $\langle wxxyz\rangle$, $\langle x\rangle$, $\langle wxy\rangle$ függvényeket. $w=0$ vagy 1 esetén megkapjuk az összes háromváltozós $f(x,y,z)$ pozitív küszöbfüggvényt:

$$\begin{gathered}\langle 0\rangle, \langle 1\rangle, \langle 00xyz\rangle, \langle 11xyz\rangle, \langle 0yz\rangle, \langle 1yz\rangle, \langle 0xyzz\rangle, \langle 1xyzz\rangle, \langle xyz\rangle, \langle z\rangle\,,\\ \langle 0xyyz\rangle, \langle 1xyyz\rangle, \langle y\rangle, \langle 0xz\rangle, \langle 1xz\rangle, \langle 0xxyz\rangle, \langle 1xxyz\rangle, \langle x\rangle, \langle 0xy\rangle, \langle 1xy\rangle\,.\end{gathered} \tag{87}$$

A 150 négyváltozós pozitív küszöbfüggvényt hasonló módon nyerjük az önduális majoritás függvényekből a 84. gyakorlat megoldásában.

Végtelen sok különböző $(w_1, w_2, \ldots, w_n)$ súlysorozat van, de bármely adott n értékre csak véges sok küszöbfüggvény. Ezért világos, hogy sok különböző súlysorozat ekvivalens. Például vizsgáljuk meg az

$$\langle x_1^2 x_2^3 x_3^5 x_4^7 x_5^{11} x_6^{13} \rangle$$

tiszta majoritás függvényt, melyben a prímszámokat súlyokként használjuk. A 2^6 esetet végigvizsgáló „nyers erő” módszer megmutatja, hogy

$$\langle x_1^2 x_2^3 x_3^5 x_4^7 x_5^{11} x_6^{13} \rangle = \langle x_1 x_2^2 x_3^2 x_4^3 x_5^4 x_6^5 \rangle ; \tag{88}$$

így ki tudjuk fejezni ugyanazt a függvényt lényegesen kisebb súlyokkal. Hasonlóan (80) speciális esete, az

$$[(x_1 x_2 \ldots x_{20})_2 \geq (01100100100001111110)_2] = \langle 1^{225028} x_1^{524288} x_2^{262144} \ldots x_{20} \rangle$$

küszöbfüggvény, egyszerűen

$$\langle 1^{323} x_1^{764} x_2^{323} x_3^{323} x_4^{118} x_5^{118} x_6^{87} x_7^{31} x_8^{31} x_9^{25} x_{10}^{6} x_{11}^{6} x_{12}^{6} x_{13}^{6} x_{14} x_{15} x_{16} x_{17} x_{18} x_{19} \rangle \tag{89}$$

lesz. A 103. gyakorlat tisztázza, hogyan kell megkeresni a minimális súlysorozatot lineáris programozást használva, a nyers erővel való hosszadalmas keresés igénybevétele nélkül.

Egy, az egyes küszöbfüggvényeket egyértelműen azonosító, gondos indexelési sémát talált ki Chow [?]. Egy adott $f(x_1, \ldots, x_n)$ Boole-függvény esetén legyen $N(f)$ azon $x = (x_1, \ldots, x_n)$ vektorok száma, melyre $f(x) = 1$, és legyen $\Sigma(f)$ ezen vektorok összege. Például ha $f(x_1, x_2) = x_1 \vee x_2$, akkor $N(f) = 3$ és $\Sigma(f) = (0, 1) + (1, 0) + (1, 1) = (2, 2)$.

T tétel. *Legyen az $f(x_1, \ldots, x_n)$ és $g(x_1, \ldots, x_n)$ Boole-függvényekre $N(f) = N(g)$ és $\Sigma(f) = \Sigma(g)$, ahol f küszöbfüggvény. Ekkor $f = g$.*

Bizonyítás. Tegyük fel, hogy pontosan k olyan $x^{(1)}, \ldots, x^{(k)}$ vektor van, amelyikre $f(x^{(j)}) = 1$ és $g(x^{(j)}) = 0$. Mivel $N(f) = N(g)$, pontosan k olyan $y^{(1)}, \ldots, y^{(k)}$ vektornak kell lennie, melyre $f(y^{(j)}) = 0$ és $g(y^{(j)}) = 1$. És mert $\Sigma(f) = \Sigma(g)$, $x^{(1)} + \cdots + x^{(k)} = y^{(1)} + \cdots + y^{(k)}$ kell legyen.

Most tegyük fel, hogy f a (110) küszöbfüggvény; ekkor $w \cdot x^{(j)} \geq t$ és $w \cdot y^{(j)} < t$, ha $1 \leq j \leq k$. De ha $f \neq g$, akkor $k > 0$ és $w \cdot (x^{(1)} + \cdots + x^{(k)}) \geq kt > w \cdot (y^{(1)} + \cdots + y^{(k)})$, ami ellentmondás. ∎

A küszöbfüggvényeknek sok különös tulajdonsága van, melyek közül a későbbi feladatokban kiderítünk néhányat. Klasszikus elméletüket Muroga [?] könyve jól összefoglalja.

Szimmetrikus Boole-függvények. Egy $f(x_1, \ldots, x_n)$ függvény *szimmetrikus*, ha az $\{1, \ldots, n\}$ minden $p(1) \ldots p(n)$ permutációjára $f(x_1, \ldots, x_n)$ egyenlő $f(x_{p(1)}, \ldots, x_{p(n)})$-nel. Amikor x_j 0 vagy 1, ez a feltétel azt jelenti, hogy f csak azoknak az egyeseknek a számától függ, amelyek az argumentumokban megjelennek, azaz a $\nu(x) = \nu(x_1, , ..., x_n)$ „oldalösszeg”-től. Az $S_{k_1, k_2, \ldots, k_r}(x_1, ..., x_n)$ jelölést általában olyan Boole-függvények megadására használják, melyek melyek akkor és csak akkor igazak, ha νx vagy k_1, vagy k_2, vagy $\cdots$ k_r. Például $S_{1,3,5}(v, w, x, y, z) = v \oplus w \oplus x \oplus y \oplus z$; $S_{3,4,5}(v, w, x, y, z) = \langle vwxyz \rangle$; $S_{4,5}(v, w, x, y, z) = \langle 00vwxyz \rangle$.

A szimmetria sok alkalmazása alapul az $S_k(x_1, \ldots, x_n)$ alapfüggvényeken, melyek csak akkor igazak, mikor $\nu x = k$. Például $S_3(x_1, x_2, x_3, x_4, x_5, x_6)$ akkor és csak akkor igaz, ha az $\{x_1, \ldots, x_6\}$ argumentumoknak pontosan a fele igaz és a másik fele hamis. Ilyen esetekben nyilván

$$S_k(x_1, \ldots, x_n) \;=\; S_{\geq k}(x_1, \ldots, x_n) \wedge \overline{S_{\geq k+1}(x_1, \ldots, x_n)}, \tag{90}$$

ahol $S_{\geq k}(x_1, \ldots, x_n)$ az $S_{k,k+1,\ldots,n}(x_1, \ldots, x_n)$ rövidítése. Az $S_{\geq k}(x_1, \ldots, x_n)$ függvények persze küszöbfüggvények, ahogy már meggondoltuk.

Bonyolultabb esetek küszöbfüggvények küszöbfüggvényeiként kezelhetők. Például

$$\begin{aligned} S_{2,3,6,8,9}(x_1, \ldots, x_{12}) \;&=\; \big[\nu x \geq 2 + 4\,[\nu x \geq 4] + 2\,[\nu x \geq 7] + 5\,[\nu x \geq 10]\big] \\ &=\; \big\langle 00x_1 \ldots x_{12} \langle 0^5 \bar{x}_1 \ldots \bar{x}_{12}\rangle^4 \langle 1\bar{x}_1 \ldots \bar{x}_{12}\rangle^2 \langle 1^7 \bar{x}_1 \ldots \bar{x}_{12}\rangle^5 \big\rangle, \end{aligned} \tag{91}$$

mert amikor $x_1 + \cdots + x_{12} = (0, 1, \ldots, 12)$, a legkülső 25 elemű többségi függvényben az egyesek száma rendre $(11, 12, 13, 14, 11, 12, 13, 12, 13, 14, 10, 11, 12)$. Általában is hasonló kétszintű séma működik (lásd Minnick [33]). Három- vagy többszintű sémákkal a küszöbölés műveletek számát még tovább redukálhatjuk. (Lásd a 113. gyakorlatot.)

Szimmetrikus Boole-függvények kiértékelésére ügyes trükkök egész sorát dolgozták ki. Például Muroga [?] Sasakinak tulajdonította formuláknak a következő említésre méltó sorozatát:

$$\begin{aligned} &x_0 \oplus x_1 \oplus \cdots \oplus x_{2m} = \langle \bar{x}_0 s_1 s_2 \ldots s_{2m}\rangle, \\ &\qquad\text{ahol}\quad s_j = \langle x_0 x_j x_{j+1} \ldots x_{j+m-1} \bar{x}_{j+m} \bar{x}_{j+m+1} \ldots \bar{x}_{j+2m-1}\rangle, \end{aligned} \tag{92}$$

ha $m > 0$, és ha x_{2m+k} ugyanaz, mint x_k minden $k \geq 1$-re. Speciálisan amikor $m = 1$ és $m = 2$, érvényesek az

$$x_0 \oplus x_1 \oplus x_2 = \langle \bar{x}_0 \langle x_0 x_1 \bar{x}_2\rangle \langle x_0 x_2 \bar{x}_1\rangle\rangle; \tag{93}$$

$$x_0 \oplus \cdots \oplus x_4 = \langle \bar{x}_0 \langle x_0 x_1 x_2 \bar{x}_3 \bar{x}_4\rangle \langle x_0 x_2 x_3 \bar{x}_4 \bar{x}_1\rangle \langle x_0 x_3 x_4 \bar{x}_1 \bar{x}_2\rangle \langle x_0 x_4 x_1 \bar{x}_2 \bar{x}_3\rangle\rangle \tag{94}$$

azonosságok. A jobb oldalak teljes mértékben szimmetrikusak, de nem nyilvánvalóan azok. (Lásd a 115. gyakorlatot.)

Kényszerítő függvények. Egy $f(x_1, \ldots, x_n)$ Boole-függvény *kényszerítő*, ha képesek vagyunk értékére változói közül legfeljebb egynek a vizsgálatával következtetni. Pontosabban f kényszerítő, ha $n = 0$, vagy ha van olyan j index, melyre $f(x)$ állandó értékű, amikor $x_j = 0$, vagy állandó értékű, amikor $x_j = 1$. Például $f(x, y, z) = (x \oplus z) \vee \bar{y}$ kényszerítő, mert mindig 1, amikor $y = 0$. (Amikor $y = 1$, nem tudjuk x és z vizsgálata nélkül f értékét; de fél cipó is jobb, mint ha nincs.) Ezek a Kauffman által [22]-ban bevezetett függvények sok alkalmazásban – különösen a kémiában és biológiában – fontosnak bizonyultak. A tulajdonságaik közül néhányat a 125–129. gyakorlatokban vizsgálunk.

Mennyiségi meggondolások. Már sok különböző fajta Boole-függvényt vizsgáltunk, így természetes megkérdezni: az egyes típusokból hány n-változós függvény létezik? A 7.3, 7.4 és 7.5. táblázatok választ adnak a kérdésre, legalábbis kis n értékekre.

A 7.3. táblázatban az összes függvényt felsoroltuk. Minden n-re 2^{2^n} lehetőség van, mert 2_{2^n} lehetséges igazságtábla van. Ezen függvények közül néhány önduális, néhány monoton; néhány monoton is, és önduális is, mint a P tételben. Néhány Horn-függvény, mint a H tételben, néhány Krom-függvény, mint az S tételben, és így tovább.

A 7.4. táblázatban pedig két függvényt azonosnak tekintünk, ha csak a változok nevében és komplementáltságában különböznek. Így amikor $n = 2$, csak 12 különböző eset merül fel, mert (például) $x \vee \bar{y}$ és $\bar{x} \vee y$ lényegében megegyeznek.

A 7.5. táblázat további lépést tesz: megengedi nekünk, hogy komplementáljuk az egyes változókat, sőt komplementáljuk az egész függvényt, lényegében megváltoztatásuk nélkül. Ebből a perspektívából nézve az (x, y, z) változók 256 lehetséges Boole-függvénye csak 14 különböző ekvivalencia-osztályba esik:

Jellemző	Osztályméret	Jellemző	Osztályméret
0	2	$x \wedge (y \oplus z)$	24
x	6	$x \oplus (y \wedge z)$	24
$x \wedge y$	24	$(x \wedge y) \vee (\bar{x} \wedge z)$	24
$x \oplus y$	6	$(x \vee y) \wedge (x \oplus z)$	48
$x \wedge y \wedge z$	16	$(x \oplus y) \vee (x \oplus z)$	8
$x \oplus y \oplus z$	2	$\langle xyz \rangle$	8
$x \wedge (y \vee z)$	48	$S_1(x, y, z)$	16

(95)

A **??**. pontban tanulmányozni fogjuk azokat a módszereket, amelyekkel meg lehet számlálni és ki lehet listázni a nem-ekvivalens kombinatorikus objektumokat.

7.3. táblázat.

n-VÁLTOZÓS BOOLE-FÜGGVÉNYEK

	n=0	n=1	n=2	n=3	n=4	n=5	n=6
tetszőleges	2	4	16	256	65,536	4,294,967,296	18,446,744,073,709,551,616
önduális	0	2	4	16	256	65,536	4,294,967,296
monoton	2	3	6	20	168	7,581	7,828,354
mindkettő	0	1	2	4	12	81	2,646
Horn	2	4	14	122	4,960	2,771,104	151,947,502,948
Krom	2	4	16	166	4,170	224,716	24,445,368
küszöb	2	4	14	104	1,882	94,572	15,028,134
szimmetrikus	2	4	8	16	32	64	128
kényszerítő	2	4	14	120	3,514	1,292,276	103,071,426,294

7.4. táblázat.

A VÁLTOZÓK PERMUTÁCIÓJA MELLETT KÜLÖNBÖZŐ BOOLE-FÜGGVÉNYEK

	n=0	n=1	n=2	n=3	n=4	n=5	n=6
tetszőleges	2	4	12	80	3,984	37,333,248	25,626,412,338,274,304
önduális	0	2	2	8	32	1,088	6,385,408
monoton	2	3	5	10	30	210	16,353
mindkettő	0	1	1	2	3	7	30
Horn	2	4	10	38	368	29,328	216,591,692
Krom	2	4	12	48	308	3,028	49,490
küszöb	2	4	10	34	178	1,720	590,440
kényszerítő	2	4	10	38	294	15,774	149,325,022

7.5. táblázat.
KIEGÉSZÍTÉS/PERMUTÁCIÓ MELLETT KÜLÖNBÖZŐ BOOLE-FÜGGVÉNYEK

	n=0	n=1	n=2	n=3	n=4	n=5	n=6
tetszőleges	1	2	4	14	222	616,126	200,253,952,527,184
önduális	0	1	1	3	7	83	109,950
küszöb	1	2	3	6	15	63	567
mindkettő	0	1	1	2	3	7	21
kényszerítő	1	2	3	6	22	402	1,228,158

GYAKORLATOK

1. [*15*] (Lewis Carroll.) Értelmezzük Subidu – a fejezet elején idézett – mondását. (*Útmutatás:* lásd a 7.1. táblázatot.)

2. [*17*] A távoli Pincus bolygó logikával foglalkozó lakói az 1 szimbólumot használják a „hamis" és a 0-t az „igaz" jelölésére. Azután például van egy bináris műveletük is, amit „or"-nak hívnak,

$$1 \text{ or } 1 = 1, \qquad 1 \text{ or } 0 = 0, \qquad 0 \text{ or } 1 = 0, \qquad 0 \text{ or } 0 = 0.$$

Ez a művelet a $\wedge$-t idézi fel bennünk. Mely műveleteket társítanánk ahhoz a 16 logikai művelethez, melyeket a pincusiak sorra „hamisság", „and", ..., „nand", „érvényesség" nevekkel illetnek (lásd a 7.1. táblázatot)?

3. [*13*] Tegyük fel, hogy a hamis logikai értéke -1, az igazé pedig +1 az eddigi 0 és 1 helyett. A 7.1. táblázat melyik $\circ$ operátora tartozna így az (a) $\max(x, y)$-hoz? (b) $\min(x, y)$-hoz? (c) $-x$-hez? (d) $x \cdot y$-hoz?

4. [*24*] (H. M. Sheffer) Ennek a gyakorlatnak az a célja, hogy megmutassuk, a 7.1. táblázat minden művelete kifejezhető NAND-del. (a) Találjunk a táblázat mind a 16 $\circ$ műveletére olyan formulát, ami ekvivalens $x \circ y$-nal és csak a $\overline{\wedge}$ műveletet használja. Legyen a formula a lehető legrövidebb. Például, az $\llcorner$ művelet esetén a formula egyszerűen „x", a $\overline{\llcorner}$ művelet esetén pedig „$x \,\overline{\wedge}\, x$". A formulákban a 0 és 1 konstansokat ne használjuk. (b) Találjunk ehhez hasonlóan 16 rövid formulát, ha megengedjük még a konstansokat is. Például az $x \,\overline{\llcorner}\, y$ így már az „$x \,\overline{\wedge}\, 1$" formulával is kifejezhető.

5. [*24*] Oldjuk meg a 4. gyakorlatot úgy, hogy válasszuk $\overline{\wedge}$ helyett az $\overline{\subset}$ alapműveletet.

6. [*21*] (E. Schröder.) (a) A 7.1. táblázat 16 művelete közül melyek asszociatívak – más szóval, melyekre igaz, hogy $x \circ (y \circ z) = (x \circ y) \circ z$? (b) Melyek tesznek eleget az $(x \circ y) \circ (y \circ z) = x \circ z$ azonosságnak?

7. [*20*] A 7.1. táblázat mely műveletei rendelkeznek azzal a tulajdonsággal, hogy $x \circ y = z$ akkor és csak akkor, ha $y \circ z = x$?

8. [*24*] A 16^2 $(\circ, \diamond)$ műveletpár közül melyek elégítik ki a bal oldali disztributivitás törvényét, vagyis melyekre igaz, hogy $x \circ (y \diamond z) = (x \circ y) \diamond (x \circ z)$?

9. [*16*] Igaz vagy hamis? (a) $(x \oplus y) \vee z = (x \vee z) \oplus (y \vee z)$; (b) $(w \oplus x \oplus y) \vee z = (w \vee z) \oplus (x \vee z) \oplus (y \vee z)$; (c) $(x \oplus y) \vee (y \oplus z) = (x \oplus z) \vee (y \oplus z)$.

10. [*17*] Mi a (22)-beli „véletlen" függvény multilineáris reprezentációja?

11. [*M25*] Van-e olyan intuitív módszer, mellyel megvizsgálhatjuk, hogy az $f(x_1, \ldots, x_n)$ multilineáris reprezentációja mikor tartalmazza mondjuk az $x_2 x_3 x_6 x_8$ tagot? (Lásd (19)-et.)

12. [*M23*] Egy Boole-függvény *egész együtthatós multilineáris reprezentációja* egy a (19)-hez hasonló reprezentációt terjeszt ki egész együtthatós $f(x_1,\ldots,x_n)$ polinommá. Ezt oly módon teszi, hogy mind a 2^n lehetséges, 0 és 1 értékeket tartalmazó $(x_1,\ldots,x_n)$ vektorra $f(x_1,\ldots,x_n)$ a helyes (0 vagy 1) értéket adja anélkül, hogy a 2-vel való osztás maradékát vennénk. Például a (19)-hez tartozó egész együtthatós multilineáris reprezentáció $1 - xy - xz - yz + 3xyz$.

a) Mi a (22) „véletlen” függvény egész együtthatós multilineáris reprezentációja?

b) Mekkorák lehetnek egy ilyen $f(x_1,\ldots,x_n)$ reprezentáció együtthatói?

c) Mutassuk meg, hogy minden egész együtthatós multilineáris reprezentációban $0 \le f(x_1,\ldots,$ $x_n) \le 1$, amennyiben $x_1, \ldots, x_n$ valós számok, és $0 \le x_1,\ldots,x_n \le 1$.

d) Hasonlóan lássuk be, ha $\{x_1,\ldots,x_n\} \subseteq \{0,1\}$ mellett $f(x_1,\ldots,x_n) \le g(x_1,\ldots,x_n)$, akkor $\{x_1,\ldots,x_n\} \subseteq [0\,.\,.\,1]$ mellett $f(x_1,\ldots,x_n) \le g(x_1,\ldots,x_n)$.

e) Ha f monoton, és $1 \le j \le n$-re $0 \le x_j \le y_j \le 1$, akkor bizonyítsuk be, hogy $f(x) \le f(y)$.

13. [*M20*] Tekintsünk egy n egységből álló rendszert, melyben egy adott egység vagy „működik”, vagy „nem működik”. Ha x_j reprezentálja azt az állapotot, amikor a „j-edik egység működik”, egy olyan Boole-függvény, mint az $x_1 \wedge (\bar{x}_2 \vee \bar{x}_3)$, azt az állítást fejezi ki, hogy az „1. egység működik, de a 2. vagy 3. nem”. $S_3(x_1,\ldots,x_n)$ pedig jelentse azt, hogy „pontosan 3 egység működik”.

Tegyük fel, hogy a többi egységtől függetlenül a j-edik egység p_j valószínűséggel működik. Mutassuk meg, hogy az $f(x_1,\ldots,x_n)$ Boole-függvény $F(p_1,\ldots,p_n)$ valószínűséggel igaz, ahol F a $p_1,\ldots,p_n$ változók polinomja.

14. [*M20*] A 13. gyakorlatban szereplő $F(p_1,\ldots,p_n)$ valószínűségi függvényt gyakran a rendszer *elérhetőségének* nevezzük. Keressük meg a maximális elérhetőségű önduális $f(x_1,x_2,x_3)$ függvényt, ha a (p_1,p_2,p_3) valószínűségek rendre a következők: (a) $(0.9,0.8,0.7)$; (b) $(0.8,0.6,0.4)$; (c) $(0.8,0.6,0.1)$.

15. [*M20*] Mutassuk meg, hogy amennyiben $f(x_1,\ldots,x_n)$ Boole-függvény, akkor van olyan $F(x)$ polinom, melyre $F(x)$ egész, ha x egész és $f(x_1,\ldots,x_n) = F\big((x_n\ldots x_1)_2\big) \mod 2$. *Útmutatás:* Fontoljuk meg, mennyi $\binom{x}{k} \mod 2$.

16. [*13*] Kicserélhetjük a $\vee$ műveletet a $\oplus$ műveletre egy teljes diszjunktív normálformában?

17. [*10*] De Morgan törvényei szerint egy a (25)-höz hasonló általános diszjunktív normálforma nem csak AND-ek OR-jaként, hanem NAND-ek NAND-jeként is felfogható:

$$\overline{\overline{(u_{11} \wedge \cdots \wedge u_{1s_1})} \wedge \cdots \wedge \overline{(u_{m1} \wedge \cdots \wedge u_{ms_m})}}.$$

A két felfogás egyenértékű.

Egy Quick nevű diák a következő formába írta át a kifejezést:

$$(u_{11} \,\overline{\wedge} \cdots \overline{\wedge}\, u_{1s_1}) \;\overline{\wedge} \cdots \overline{\wedge}\; (u_{m1} \,\overline{\wedge} \cdots \overline{\wedge}\, u_{ms_m}).$$

Jó ötlet volt ez?

18. [*20*] Legyen $u_1 \wedge \cdots \wedge u_s$ az f Boole-függvény diszjunktív normálformájában implikáns, és legyen $v_1 \vee \cdots \vee v_t$ ugyanannek a függvénynek a konjunktív normálformájában klóz. Bizonyítsuk be, hogy valamely i és j esetén $u_i = v_j$.

19. [*20*] Mi a (22) „véletlen” függvény konjunktív prímformája?

20. [*21*] Igaz vagy hamis a következő állítás? $f \wedge g$ minden prímimplikánsa felírható $f' \wedge g'$ alakban, ahol f' f prímimplikánsa, g' pedig g prímimplikánsa.

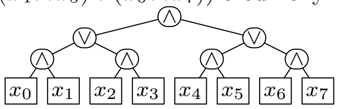
21. [*20*] Bizonyítsuk be, hogy egy nemkonstans Boole-függvény akkor és csak akkor monoton, ha ki lehet fejezni a $\wedge$ és a $\vee$ műveletekkel.

22. [*20*] Tegyük fel, hogy mint (16)-ban, $f(x_1,\ldots,x_n) = g(x_1,\ldots,x_{n-1}) \oplus h(x_1,\ldots,x_{n-1}) \wedge x_n$.

A g és h függvényekre vonatkozó milyen feltételek teljesülése szükséges és elegendő ahhoz, hogy f monoton legyen?

23. [*15*] Mi a $(v{\wedge}w{\wedge}x) \vee (v{\wedge}x{\wedge}z) \vee (x{\wedge}y{\wedge}z)$ konjunktív prímformája?

24. [*M20*] Vizsgáljuk az – itt $k = 3$ esetben ábrázolt – 2^k levéllel rendelkező teljes bináris fát. A gyökérben $\wedge$-t használva dolgozzunk szintről szintre váltakozva a $\wedge$ és a $\vee$ műveletekkel. Így például az $((x_0 \wedge x_1) \vee (x_2 \wedge x_3)) \wedge ((x_4 \wedge x_5) \vee (x_6 \wedge x_7))$ eredményre jutunk. Hány prímimplikánst tartalmaz az eredményfüggvény?



25. [*M21*] Hány prímimplikánsa van $(x_1{\vee}x_2) \wedge (x_2{\vee}x_3) \wedge \cdots \wedge (x_{n-1}{\vee}x_n)$-nek?

26. [*M23*] Legyen $\mathcal{F}$ ($\mathcal{G}$) egy monoton KNF (DNF) prímklózai (prímimplikánsai) indexhalmazainak családja:

$$f(x) = \bigwedge_{I\in\mathcal{F}} \bigvee_{i\in I} x_i; \qquad\qquad g(x) = \bigvee_{J\in\mathcal{G}} \bigwedge_{j\in J} x_j.$$

Adjunk meg olyan x-et, melyre $f(x) \neq g(x)$, amennyiben a következő feltételek valamelyike teljesül:

a) Van olyan $I \in \mathcal{F}$ és $J \in \mathcal{G}$, hogy $I \cap J = \emptyset$.
b) $\bigcup_{I\in\mathcal{F}} I \neq \bigcup_{J\in\mathcal{G}} J$.
c) Van olyan $I \in \mathcal{F}$, hogy $|I| > |\mathcal{G}|$, vagy van olyan $J \in \mathcal{G}$, hogy $|J| > |\mathcal{F}|$.
d) $\sum_{I\in\mathcal{F}} 2^{n-|I|} + \sum_{J\in\mathcal{G}} 2^{n-|J|} < 2^n$, ahol $n = \bigl|\bigcup_{I\in\mathcal{F}} I\bigr|$.

27. [*M31*] Az előző gyakorlatot folytatva vizsgáljuk a következő $\mathrm{X}(\mathcal{F},\mathcal{G})$ algoritmust, mely vagy egy olyan x vektorral tér vissza, melyre $f(x) \neq g(x)$, vagy Λ-val, ha $f = g$:

X1. (A szükséges feltételek ellenőrzése.) Térjünk vissza egy megfelelő x értékkel, ha a 26. gyakorlatban megadott (a), (b), (c) vagy (d) teljesülnek.

X2. (Készen vagyunk?) Ha $|\mathcal{F}||\mathcal{G}| \leq \infty$, térjünk vissza Λ-val.

X3. (Rekurzió.) A legjobb k index meghatározásához számítsuk ki a következő redukált családokat:

$$\mathcal{F}_1 = \{I \mid I \in \mathcal{F}, k \notin I\}, \qquad\qquad \mathcal{F}_0 = \mathcal{F}_1 \cup \{I \mid k \notin I,\ I \cup \{k\} \in \mathcal{F}\};$$
$$\mathcal{G}_0 = \{J \mid J \in \mathcal{G}, k \notin J\}, \qquad\qquad \mathcal{G}_1 = \mathcal{G}_0 \cup \{J \mid k \notin J,\ J \cup \{k\} \in \mathcal{G}\}.$$

Töröljük az $\mathcal{F}_0$ vagy $\mathcal{G}_1$ olyan elemeit, melyek ugyanazon család egy másik elemét már tartalmazzák. A k indexet úgy kellene megválasztani, hogy a $\rho = \min\bigl(|\mathcal{F}_1|/|\mathcal{F}|, |\mathcal{G}_\prime|/|\mathcal{G}|\bigr)$ hányados a lehetséges legkisebb legyen. Ha $\mathrm{X}(\mathcal{F}_0, \mathcal{G}_0)$ tér vissza az x vektorral, térjünk vissza ezzel a vektorral úgy, hogy kibővítjük az $x_k = 0$-val. Ha pedig $\mathrm{X}(\mathcal{F}_1, \mathcal{G}_1)$ tér vissza az x vektorral, térjünk vissza ezzel a vektorral úgy, hogy az $x_k = 1$-gyel bővítjük ki. Egyébként térjünk vissza Λ-val. ∎

Ha $N = |\mathcal{F}| + |\mathcal{G}|$, bizonyítsuk be, hogy az X1 lépés legfeljebb $N^{O(\lg N)^2}$ alkalommal hajtódik végre. *Útmutatás:* Mutassuk meg, hogy az X3 lépésben $\rho \leq 1 - 1/\lg N$ mindig teljesül.

28. [*21*] (W. V. Quine, 1952.) Ha $f(x_1,\ldots,x_n)$ a p_1, …, p_q prímimplikánsokkal rendelkező valamely Boole-függvény, legyen $g(y_1,\ldots,y_q) = \bigwedge_{f(x)=1} \bigvee\{y_j \mid p_j(x) = 1\}$. Például a (22) „véletlen" függvény a (28)-ban felsorolt nyolc pontban igaz, és a (29) és (30) képletek által meghatározott öt prímimplikánssal rendelkezik. Így $g(y_1,\ldots,y_5)$ ebben az esetben

$$\begin{aligned}(y_1{\vee}y_2) \wedge (y_1) \wedge (y_2{\vee}y_3) \wedge (y_4) \wedge (y_3{\vee}y_5) \wedge (y_5) \wedge (y_5) \wedge (y_4{\vee}y_5)&\\ = (y_1{\wedge}y_2{\wedge}y_4{\wedge}y_5) \vee (y_1{\wedge}y_3{\wedge}y_4{\wedge}y_5).&\end{aligned}$$

Bizonyítsuk be, hogy az f-et kifejező minden legrövidebb DNF-hez hozzárendelhető a monoton g függvény egy prímimplikánsa.

29. [*22*] (A következő néhány gyakorlatot Boole-függvények implikánsaival dolgozó olyan algoritmusok tárgyalására szánjuk, amelyek az n-kocka pontjait – $x_1 \ldots x_n$ bitfüzérek helyett – n bites $(b_{n-1} \ldots b_1 b_0)_2$ számokkal reprezentálják.) Legyen adva egy j bitpozíció és a $v_0 < v_1 < \cdots < v_{m-1}$ n bites értékek. Fejtsük ki, hogyan lehet megtalálni növekvő k mellett az összes olyan (k, k') párt, amelyre $0 \le k < k' < m$ és $v_{k'} = v_k \oplus 2^j$. A megtervezett eljárás futási ideje $O(m)$ kellene legyen, ha az n bites szavakon bitenként végzett műveletek konstans idejűek.

30. [*27*] Könyvünk kiemeli, hogy egy Boole-függvény implikánsait azon pontok V halmazában, melyekre a függvény igaz, részkockáknak tekinthetjük, például a 01∗0∗ részkockának. Egy részkockát az $a = (a_{n-1} \ldots a_0)_2$ és $b = (b_{n-1} \ldots b_0)_2$ bináris számokból álló párként írhatunk le, ahol a a csillag karakterek pozícióit tartja nyilván, b pedig a nem ∗ pozíciókon szereplő biteket. Például az $a = (00101)_2$ és $b = (01000)_2$ számok a $c =$ 01∗0∗ részkockát reprezentálják. $a\&b = 0$ mindig teljesül.

Valahányszor $a_j = 0$, definiálhatjuk a részkocka „j-társát”, mégpedig úgy, hogy b-t kicseréljük $b \oplus 2^j$-re. Például 01∗0∗-nak három társa van, nevezetesen a 4-társ 11∗0∗, a 3-társ 00∗0∗ és az 1-társ 01∗1∗. Minden $c \subseteq V$ részkockához kijelölhetünk egy $(t_{n-1} \ldots t_0)_2$ jelzőértéket, ahol $t_j = 1$ akkor és csak akkor, ha c j-társa definiált és V-ben van. c akkor és csak akkor határoz meg maximális részkockát (prímimplikánst), ha jelzőértéke nulla.

Használjuk fel ezeket a fogalmakat egy olyan algoritmus megtervezésére, ami megkeresi egy adott, $v_0 < v_1 < \cdots < v_{m-1}$ n-bites számokkal reprezentált V halmaz összes maximális (a, b) részkockáját.

31. [*28*] A 30. gyakorlatbeli algoritmusnak szüksége van azon pontok teljes listájára, ahol egy Boole-függvény igaz, és ez a lista bizony elég hosszú is lehet. Ezért előnyben részesíthetjük a részkockákkal való közvetlen munkát, egyáltalán nem térve át az explicit n-esek szintjére, hacsak nem nélkülözhetetlen. Az ilyen magasabb-szintű módszerek kulcsa a c és c' részkockák közötti *konszenzus* fogalma, amit $c \sqcup c'$-vel jelölünk, és a legnagyobb olyan c'' részkockával definiálunk, amelyre

$$c'' \subseteq c \cup c', \qquad c'' \not\subseteq c \quad \text{és} \quad c'' \not\subseteq c' .$$

Ilyen c'' nincs mindig. Például ha $c =$ 000∗ és $c' =$ ∗111, a $c \cup c'$-ban szereplő minden részkocka vagy c-ben, vagy c'-ben benne van.

a) Bizonyítsuk be, hogy a konszenzust, ha egyáltalán létezik, ki lehet számítani komponensenként úgy, hogy az egyes koordináta-pozíciókban a következő formulákat használjuk:

$$x \sqcup x = x \sqcup * = * \sqcup x = x \quad \text{és} \quad x \sqcup \bar{x} = * \sqcup * = * \qquad x = 0\text{-ra és } x = 1\text{-re}.$$

Továbbá $c \sqcup c'$ akkor és csak akkor létezik, ha az $x \sqcup \bar{x} = *$ szabályt pontosan egy komponensben használtuk.

b) Egy k csillag karaktert tartalmazó részkockát k-kockának nevezünk. Mutassuk meg, hogy ha c egy k-kocka, c' pedig egy k'-kocka, továbbá létezik a $c'' = c \sqcup c'$ konszenzus, akkor c'' egy k''-kocka, ahol $1 \le k'' \le \min(k, k') + 1$.

c) Ha C és C' részkocka-családok, legyen

$$C \sqcup C' \;=\; \{\, c \sqcup c' \mid c \in C,\, c' \in C',\, \text{és létezik } c \sqcup c' \,\}.$$

Magyarázzuk meg, miért működik megfelelően a következő algoritmus.

E algoritmus (*maximális részkocka keresésére*). Ha egy n-kocka részkockáinak adott egy C családja, az algoritmus $V = \bigcup_{c \in C} c$ maximális részkockáit eredményezi anélkül, hogy magát a V halmazt ténylegesen meghatározná.

E1. (Kezdőértékek beállítása.) Legyen $j \leftarrow 0$. Töröljük C minden olyan c részkockáját, amelyik egy másikban benne van.

E2. (Készen vagyunk?) (Ebben a lépésben minden V-beli j-kocka benne van C valamely elemében, és C nem tartalmaz olyan k-kockát, melyre $k < j$.) Ha C üres, az algoritmus megáll.

E3. (Vegyük a konszenzusokat.) Legyen $C' \leftarrow C \sqcup C$. Távolítsuk el C'-ből az összes olyan k-kocka részkockát, melyre $k \leq j$. Közben írjuk ki azokat a $c \in C$ j-kockákat, melyekre $c \sqcup C$ nem ad C'-beli $(j+1)$-kockát.

E4. (Továbblépés.) Legyen $C \leftarrow C \cup C'$, de töröljük az összes j-kockát ebből az unióból. Aztán töröljük az olyan $c \in C$ részkockákat, amelyek valamely másikban benne vannak. Legyen $j \leftarrow j + 1$, és folytassuk E2-vel. ■

(Lásd a **??**. gyakorlatot, ahol bemutatjuk ezeknek a számításoknak egy lehetséges hatékony módját.)

32. [*M29*] Legyenek $c_1, \ldots, c_m$ egy n-kocka részkockái.

a) Bizonyítsuk be, hogy $c_1 \cup \cdots \cup c_m$ legfeljebb egy olyan maximális c részkockát tartalmaz, amelyik nincs benne egyetlen $j \in \{1, \ldots, m\}$-re sem $c_1 \cup \cdots \cup c_{j-1} \cup c_{j+1} \cup \cdots \cup c_m$-ben. (Ha c létezik, c-t $c_1, \ldots, c_m$ *általánosított konszenzusának* nevezzük, hisz a 31. gyakorlat jelölései szerint $c = c_1 \sqcup c_2$, ha $m = 2$.)

b) Keressük meg a részkockáknak azt az m elemű halmazát, melyre $\{c_1, \ldots, c_m\}$ mind a $2^m - 1$ nemüres részhalmazának van általánosított konszenzusa.

c) Bizonyítsuk be, hogy egy m implikánssal rendelkező DNF-nek legfeljebb $2^m - 1$ prímimplikánsa van.

d) Keressünk m implikánssal és $2^m - 1$ prímimplikánssal rendelkező DNF-et.

33. [*M21*] Legyen $f(x_1, \ldots, x_n)$ a $\binom{2^n}{m}$ olyan Boole-függvény egyike, amelyik pontosan m pontban igaz. Ha f-et véletlenül választjuk, mi a valószínűsége, hogy $x_1 \wedge \cdots \wedge x_k$ (a) f implikánsa? (b) f prímimplikánsa? (A (b) kérdésre egy összeg legyen a válasz; a $k = n$ esetben pedig adjuk meg az összeget zárt formában is.)

34. [*F37*] Folytatva a 33. gyakorlatot, jelölje $c(m, n)$ az implikánsok és $p(m, n)$ a prímimplikánsok átlagos számát.

a) Ha $0 \leq m \leq 2^n/n$, mutassuk meg, hogy $m \leq c(m, n) \leq \frac{3}{2}m + O(m/n)$ és $p(m, n) \geq me^{-1} + O(m/n)$; ezért ebben az értéktartományban $p(m, n) = \Theta(c(m, n))$.

b) Most legyen $2^n/n \leq m \leq (1 - \epsilon)2^n$, ahol ϵ rögzített pozitív konstans. Definiáljuk a t és az α_{mn} számokat az

$$n^{-4/3} \;\leq\; \left(\frac{m}{2^n}\right)^{2^t} \;=\; \alpha_{mn} \;<\; n^{-2/3}, \qquad (t \text{ egész})$$

relációkkal. Fejezzük ki $c(m, n)$ és $p(m, n)$ aszimptotikus értékeit n, t és α_{mn} függvényében. (*Segítség:* Mutassuk meg, hogy csaknem az összes implikánsnak éppen $n - t$ vagy $n - t - 1$ literálja van.)

c) Becsüljük meg a $c(m, n)/p(m, n)$ hányadost, amikor $m = 2^{n-1}$ és $n = \lfloor (\ln t - \ln\ln t)2^{2^t} \rfloor$, t egész.

d) Bizonyítsuk be, hogy $c(m, n)/p(m, n) = O(\log\log n / \log\log\log n)$, amikor $m \leq (1 - \epsilon)2^n$.

35. [*M25*] Egy DNF *ortogonális*, ha implikánsai diszjunkt részkockáknak felelnek meg. Az ortogonális diszjunktív normálformák különösen hasznosak, amikor a 13. gyakorlat megbízhatósági polinomját számoljuk, vagy becsüljük. Egy függvény teljes diszjunktív normálformája nyilvánvalóan ortogonális, mert részkockái egyetlen pontból állnak. De gyakran találkozunk lényegesen kevesebb implikánst tartalmazó ortogonális DNF-fel, különösen amikor a függvény monoton. Például az $(x_1{\wedge}x_2) \vee (x_2{\wedge}x_3) \vee (x_3{\wedge}x_4)$ függvény nyolc pontban igaz, és ortogonális DNF-je

$$(x_1{\wedge}x_2) \vee (\bar{x}_1{\wedge}x_2{\wedge}x_3) \vee (\bar{x}_2{\wedge}x_3{\wedge}x_4).$$

Másképp fogalmazva az egymást részben átfedő $11{*}{*}$, ${*}11{*}$, ${*}{*}11$ részkockák felválthatók az $11{*}{*}$, $011{*}$, ${*}011$ diszjunkt részkockákkal. A részkockákra a 30. gyakorlatbeli bináris jelölést használva ezen részkockák csillag karakterjeinek kódjai 0011, 0001, 1000 és bitkódjai 1100, 0110, 0011.

A $B_1, \ldots, B_p$ bitkódok listájával – miközben a csillag karakterek kódjai rendre $\bar{B}_1, \ldots, \bar{B}_p$ – minden monoton függvény definiálható. Egy adott ilyen lista mellett minden olyan $1 \le j < k$-ra, melyre $\nu(B_j \& \bar{B}_k) = 1$, jelölje S_k a B_k „árnyékát",egymást követő 1-esek = consecutive 1's azaz $B_j \& \bar{B}_k$ bitenkénti OR-ját:

$$S_k = \beta_{1k} | \cdots | \beta_{(k-1)k}, \quad \beta_{jk} = \big((B_j \& \bar{B}_k) \oplus ((B_j \& \bar{B}_k) - 1)\big) \dot{-} ((B_j \& \bar{B}_k) - 1).$$

Például amikor a bitkódok $(B_1, B_2, B_3) = (1100, 0110, 0011)$, az $(S_1, S_2, S_3) = (0000, 1000, 0100)$ árnyékkódokat kapjuk.

a) Mutassuk meg, hogy az $A'_j = \bar{B}_j - S_j$ csillagkarakter-kódok és a B_j bitkódok azokat a részkockákat definiálják, amelyek éppen az $A_j = \bar{B}_j$ csillagkarakter-kódokkal rendelkező részkockák által lefedett pontokat fedik le.

b) Bitkódok egy $B_1, \ldots, B_p$ listáját *kifejtésnek* nevezzük, ha egyik $1 \le j < k \le p$-re sem lesz $B_j \& S_k$ nulla. Például $(1100, 0110, 0011)$ kifejtés; de ha átrendezzük ezeket a bitkódokat az $(1100, 0011, 0110)$ sorrendbe, a kifejtésre vonatkozó feltétel nem teljesül, amikor $j = 1$ és $k = 2$, jóllehet $S_3 = 1001$. Bizonyítsuk be, hogy (a)-ban a részkockák akkor és csak akkor diszjunktak, ha a bitkódok listája kifejtés.

c) Amikor egy monoton Boole-függvényt így reprezentálunk, a B-k között – a Q tételnek megfelelően – minden prímimplikáns megjelenik. De néha további implikánsokat kell hozzáadnunk, ha azt akarjuk, hogy a részkockák diszjunktak legyenek. Például az 1100 és 0011 bitkódok esetén nincs kifejtés. Mutassuk meg, hogy még egy bitkód hozzáadása után ennek az $(x_1{\wedge}x_2) \vee (x_3{\wedge}x_4)$ függvénynek mégis van kifejtése. Mi lesz az eredményül kapott ortogonális DNF?

d) Permutáljuk úgy az $\{11000, 01100, 00110, 00011, 11010\}$ bitkódokat, hogy kifejtést nyerjünk.

e) Adjunk két bitkódot az $\{110000, 011000, 001100, 000110, 000011\}$ halmazhoz olyan sorrendben, hogy kifejtést nyerjünk.

36. [*M21*] Folytatva a 35. gyakorlatot, legyen f egy monoton és nem azonosan 1 függvény. Mutassuk meg, hogy bitvektoroknak a

$$B = \{\, x \mid f(x) = 1 \text{ és } f(x') = 0 \,\}, \qquad x' = x \& (x{-}1)$$

halmaza, amikor lexikografikusan csökkenő sorrendben listázzuk, kifejtés. (Az x' vektort az x-ből a legjobboldalibb 1 kinullázásával nyerjük.) Az $(1100, 1011, 0111, 0011)$ listából például ez a módszer az $(x_1{\wedge}x_2) \vee (x_3{\wedge}x_4)$ ortogonális DNF-jét állítja elő.

37. [*M31*] Keressünk $(x_1{\wedge}x_2) \vee (x_3{\wedge}x_4) \vee \cdots \vee (x_{2n-1}{\wedge}x_{2n})$-hez $2^n - 1$ implikánst tartalmazó kifejthető DNF-et, és bizonyítsuk be, hogy ehhez a függvényhez nincs kevesebb implikánst tartalmazó ortogonális DNF.

38. [*05*] Vajon nehéz *diszjunktív* normálformában megadott függvények kielégíthetőségét tesztelni?

39. [*25*] Legyen $f(x_1, \ldots, x_n)$ N belső csúccsal és $N - 1$ levéllel rendelkező, kiterjesztett bináris fával reprezentált Boole-formula. A leveleket egy-egy x_k változóval, a belső csúcsokat a 7.1. táblázatbeli tizenhat bináris művelet közül eggyel-eggyel címkézzük. A műveleteket lentől felfelé alkalmazva a gyökér értékeként $f(x_1, \ldots, x_n)$-t kapjuk.

Derítsük ki, hogyan konstruáljunk egy pontosan $4N+1$ klózt tartalmazó $F(x_1, \ldots, x_n, y_1, \ldots, y_N)$ 3KNF formulát úgy, hogy $f(x_1, \ldots, x_n) = \exists y_1 \ldots \exists y_N F(x_1, \ldots, x_n, y_1, \ldots, y_N)$. (Ekképpen f akkor és csak akkor elégíthető ki, ha F is.)

40. [*23*] Adott G irányítatlan gráfban a $\{p_{uv} \mid u \neq v\} \cup \{q_{uvw} \mid u \neq v,\ u \neq w,\ v \neq w,\ u \not\!\!- w\}$ Boole-változókon, ahol u, v és w G csúcsait jelölik, konstruáljuk meg a következő klózokat:

$$A = \bigwedge\{(p_{uv} \vee p_{vu}) \wedge (\bar{p}_{uv} \vee \bar{p}_{vu}) \mid u \neq v\};$$
$$B = \bigwedge\{(\bar{p}_{uv} \vee \bar{p}_{vw} \vee p_{uw}) \mid u \neq v,\ u \neq w,\ v \neq w\};$$
$$C = \bigwedge\{(\bar{q}_{uvw} \vee p_{uv}) \wedge (\bar{q}_{uvw} \vee p_{vw}) \wedge (q_{uvw} \vee \bar{p}_{uv} \vee \bar{p}_{vw}) \mid u \neq v,\ u \neq w,\ v \neq w,\ u \not\!\!- w\};$$
$$D = \bigwedge\{\big(\bigvee_{v \notin \{u,w\}} (q_{uvw} \vee q_{wvu})\big) \mid u \neq w,\ u \not\!\!- w\}.$$

Bizonyítsuk be, hogy az $A \wedge B \wedge C \wedge D$ formula akkor és csak akkor elégíthető ki, ha G-ben van Hamilton-út. *Útmutatás:* Gondoljunk p_{uv}-re mint az „$u < v$" állításra.

41. [*20*] (A skatulya elv.) San Serriffe szigetén m galamb és n galambdúc van. Keressük meg azt a konjunktív normálformát, amelyik akkor és csak akkor elégíthető ki, ha minden galamb legalább egy galambdúc egyedüli lakója.

42. [*20*] Keressünk olyan rövid és kielégíthetetlen KNF-et, ami nem teljesen triviális, jóllehet kizárólag olyan Horn-klózokból áll, melyek egyúttal Krom-klózok is.

43. [*20*] Van-e hatékony módszer arra, hogy eldöntsük, kielégíthető-e egy olyan konjunktív normálforma, amelyik kizárólag Horn-klózokból és/vagy Krom-klózokból (esetleg vegyesen mindkettőből) áll.

44. [*M23*] Egészítsük ki a H tétel bizonyítását a (33) implikációk vizsgálatával.

45. [*M20*] (a) Mutassuk meg, hogy az n-változós Horn-függvényeknek pontosan a fele definit. (b) Mutassuk meg azt is, hogy több olyan n-változós Horn-függvény van, mint n-változós monoton függvény (kivéve, ha $n = 0$).

46. [*20*] A 11×11 különböző `xy` karakterpár közül melyek azok, amelyekben a karakterek a (34) környezetfüggetlen nyelvtan szerint előfordulhatnak egymás után?

47. [*20*] Ha adott $j \prec k$ relációknak egy olyan sorozata, mint a (topologikus rendezés) 2.2.3.T algoritmusában, vizsgáljuk meg az

$$x_{j_1} \wedge \cdots \wedge x_{j_t} \Rightarrow x_k, \qquad 1 \leq k \leq n$$

klózokat, ahol $\{j_1, \ldots, j_t\}$ azon elemek halmaza, melyekre $j_i \prec k$. Vessük össze ezeken a klózokon a C algoritmus viselkedését a 2.2.3.T algoritmus viselkedésével.

48. [*20*] Milyen jó módszer segítségével lehetne ellenőrizni, hogy Horn-klózok valamely halmaza kielégíthető-e?

49. [*22*] Mutassuk meg, hogy ha egy KNF-ben $f(x_1, \ldots, x_n)$ és $g(x_1, \ldots, x_n)$ Horn-klózok, akkor könnyen lehet ellenőrizni, vajon teljesül-e minden $x_1, \ldots, x_n$-re $f(x_1, \ldots, x_n) \leq g(x_1, \ldots, x_n)$.

50. [*HM42*] n változó esetén $(n+2)2^{n-1}$ lehetséges Horn-klóz van. Ismétlést is megengedve válasszunk ki közülük véletlenül $c \cdot 2^n$ klózt $(c > 0)$. Legyen $P_n(c)$ annak a valószínűsége, hogy a kiválasztott klózok egyidejűleg kielégíthetők. Bizonyítsuk be, hogy

$$\lim_{n \to \infty} P_n(c) \;=\; 1 - (1-e^{-c})(1-e^{-2c})(1-e^{-4c})(1-e^{-8c}) \ldots .$$

51. [*22*] Számos kétszemélyes játék definiálható irányított gráf segítségével, ahol az egyes csúcsok a játék egyes pozícióit reprezentálják. Két játékos van, Alice és Bob, akik egy konkrét csúcsból indulva, felváltva, egy-egy lépésben egy-egy éllel építik az irányított utat. Mielőtt a játék elkeződik, minden csúcsot vagy A-val (jelentése: Alice nyer), vagy B-vel (jelentése: Bob nyer), vagy C-vel (jelentése: a cica nyer) jelölünk, vagy pedig jelöletlen marad a csúcs.

Ha az út egy A-val vagy B-vel jelölt v csúcsba ér, az illető játékos nyer. A játék nyertes nélkül fejeződik be, ha v-t az illető játékos már korábban is elérte. Ha v egy C-vel jelölt csúcs, az éppen aktív játékosnak lehetősége van, hogy elfogadja a döntetlent, vagy pedig egy innen kiinduló élt válasszon az út folytatásához, majd a másik játékos lesz aktív. (Ha v egy nulla kimenő fokszámú jelöletlen csúcs, az aktív játékos veszít.)

A gráf csúcsaihoz rendeljük hozzá az $A^+(v)$, $A^-(v)$, $B^+(v)$ és $B^-(v)$ ítéletváltozókat. Tisztázzuk, hogyan kell megkonstruálni definit Horn-klózoknak olyan halmazát, hogy $A^+(v)$ akkor és csak akkor legyen a magban, ha Alice ki tudja harcolni a győzelmet a v-ben kezdődő úton, ha ő kezd; $B^+(v)$ és $B^-(v)$ hasonló jelentéssel bír, mint $A^+(v)$ és $A^-(v)$, csak a szerep fordul.

52. [*25*] (*Boole-játékok.*) Egy $f(x_1,\ldots,x_n)$ Boole-függvény az úgynevezett „két lépést előre, egy lépést hátra" játékhoz vezethet a következő módon: van két játékos, 0 és 1, akik rendre értékeket rendelnek az x_j változókhoz; az y játékos azt próbálja meg elérni, hogy $f(x_1,\ldots,x_n)$ y legyen. Kezdetben nincs a változókhoz érték rendelve, és az m pozíciójelző nulla. A játékosok felváltva lépnek, és az aktuális aktív játékos vagy úgy dönt, hogy legyen $m \leftarrow m+2$ (ha $m+2 \le n$), vagy pedig úgy, hogy legyen $m \leftarrow m-1$ (ha $m-1 \ge 1$), aztán pedig legyen

$$\begin{cases} x_m \leftarrow 0 \text{ vagy } 1, & \text{ha } x_m\text{-hez nem volt korábban érték rendelve;} \\ x_m \leftarrow \bar{x}_m, & \text{ha } x_m\text{-hez már volt korábban érték rendelve.} \end{cases}$$

A játéknak vége, mihelyt minden változónak értéke van; ekkor $f(x_1,\ldots,x_n)$ a győztes. Döntetlenül végződik a játék, ha ugyanazt az állapotot (beleértve m értékét is) a játékosok másodjára érik el. Vegyük észre, hogy minden lépés során legfeljebb négyféle módosítás lehetséges.

Tanulmányozzuk a játékot a következő négy esetben, ha $2 \le n \le 9$:

a) $f(x_1,\ldots,x_n) = [x_1\ldots x_n < x_n\ldots x_1]$ (lexikografikus sorrend szerint);
b) $f(x_1,\ldots,x_n) = x_1 \oplus \cdots \oplus x_n$;
c) $f(x_1,\ldots,x_n) = [x_1\ldots x_n$ nem tartalmaz két egymást követő 1-est$]$;
d) $f(x_1,\ldots,x_n) = [(x_1\ldots x_n)_2$ prím$]$.

53. [*23*] Mutassuk meg, hogy a (37) megvalósíthatatlan humorfesztivál programbeosztása már akkor is elkészíthető, ha csak (a) Tomlin; (b) Unwin; (c) Vegas; (d) Xie; (e) Yankovic vagy (f) Zany szerződése változik.

54. [*20*] Legyen $S = \{u_1, u_2, \ldots, u_k\}$ egy 2KNF formulához tartozó (a 7.6. ábrán láthatóhoz hasonló) irányított gráf valamely erős komponensében a literálok halmaza. Mutassuk meg, hogy S akkor és csak akkor tartalmaz egy változót és komplemensét is, ha $u_j = \bar{u}_1$ valamely $2 \le j \le k$-ra.

55. [*30*] Nevezzük $f(x_1,\ldots,x_n)$-t *átnevezett Horn-függvénynek*, ha vannak olyan $y_1,\ldots,y_n$ Boole-konstansok, melyek mellett $f(x_1 \oplus y_1,\ldots,x_n \oplus y_n)$ Horn-függvény.

a) Egy KNF-ben megadott $f(x_1,\ldots,x_n)$ esetén tisztázzuk, hogyan konstruálható meg 2KNF-ben egy olyan $g(y_1,\ldots,y_n)$, melyre $g(y_1,\ldots,y_n)$=1 akkor és csak akkor, amennyiben $f(x_1 \oplus y_1,\ldots,x_n \oplus y_n)$ klózai Horn-klózok.
b) Tervezzünk algoritmust, amely $O(m)$ lépésben eldönti, vajon a változók valamely részhalmazának komplementálásával Horn-klózokká lehet-e alakítani egy adott m hosszúságú KNF klózait.

56. [*20*] Egy $f(x_1,x_2,\ldots,x_n)$ Boole-függvényre vonatkozó kielégíthetőségi problémát a következő kérdésként is megfogalmazhatjuk: vajon a

$$\exists x_1\, \exists x_2 \ldots \exists x_n\, f(x_1,x_2,\ldots,x_n)$$

kvantált formula igaz-e. A „$\exists x_j\,\alpha$” azt jelenti, hogy „van olyan x_j Boole-érték, hogy α teljesül”.

Egy sokkal általánosabb kiértékelési probléma keletkezik, amikor egy vagy több $\exists x_j$ egzisztenciális kvantort $\forall x_j$ univerzális kvantorra cserélünk, ahol „$\forall x_j\,\alpha$” azt jelenti, hogy „minden x_j Boole-értékre α teljesül.”

A nyolc kvantált $\exists x\,\exists y\,\exists z\,f(x,y,z)$, $\exists x\,\exists y\,\forall z\,f(x,y,z)$, $\ldots$, $\forall x\,\forall y\,\forall z\,f(x,y,z)$ formula közül melyek igazak, amikor $f(x,y,z)=(x\vee y)\wedge(\bar{x}\vee z)\wedge(y\vee\bar{z})$?

57. [*30*] (Aspvall, Plass és Tarjan [?].) Folytatva az 56. gyakorlatot, tervezzünk algoritmust, amely lineáris időben eldönti, vajon egy adott teljesen kvantált $f(x_1,\ldots,x_n)$ formula igaz-e, amikor f 2KNF formula (Krom-klózok konjunkciója).

58. [*37*] Folytatva az 57. gyakorlatot, tervezzünk hatékony algoritmust, ami eldönti, vajon Horn-klózok adott teljesen kvantált konjunkciója igaz-e.

59. [*M20*] (Pehoushek és Fraer, [?].) Mutassuk meg, hogy ha $f(x_1,x_2,\ldots,x_n)$ igazságtáblája pontosan k helyen 1, akkor a teljesen kvantált $Qx_1\,Qx_2\,\ldots Qx_n\,f(x_1,x_2,\ldots,x_n)$ formulák közül pontosan k igaz, ahol Q vagy $\exists$, vagy $\forall$.

60. [*12*] A következő kifejezések közül melyik szolgáltatja a (43)-ban definiált $\langle xyz\rangle$ mediánt? (a) $(x\wedge y)\oplus(y\wedge z)\oplus(x\wedge z)$. (b) $(x\vee y)\oplus(y\vee z)\oplus(x\vee z)$. (c) $(x\oplus y)\wedge(y\oplus z)\wedge(x\oplus z)$. (d) $(x\equiv y)\oplus(y\equiv z)\oplus(x\equiv z)$. (e) $(x\overline{\wedge}y)\wedge(y\overline{\wedge}z)\wedge(x\overline{\wedge}z)$. (f) $(x\overline{\wedge}y)\vee(y\overline{\wedge}z)\vee(x\overline{\wedge}z)$.

61. [*13*] Igaz-e vagy hamis a következő állítás? A $w\circ\langle xyz\rangle=\langle(w\circ x)(w\circ y)(w\circ z)\rangle$ disztributivitás törvény a 7.1. táblázat bármelyik $\circ$ kétváltozós Boole-művelete esetén érvényes.

62. [*25*] (Schensted.) Bizonyítsuk be, hogy

$$f(x_1,\ldots,x_n)=\big\langle f(x_1,x_1,x_3,x_4,\ldots,x_n)f(x_1,x_2,x_2,x_4,\ldots,x_n)f(x_3,x_2,x_3,x_4,\ldots,x_n)\big\rangle,$$

ha $f(x_1,\ldots,x_n)$ monoton Boole-függvény, és $n\ge 3$.

63. [*20*] A (49) egyenlőség megmutatja, hogyan kell kiszámítani öt elem mediánját háromváltozós medián segítségével. Megfordítva, ki tudjuk vajon $\langle xyz\rangle$-t is számolni öt elem mediánjára vonatkozó eljárás segítségével?

64. [*23*] (Akers.) (a) Bizonyítsuk be, hogy egy $f(x_1,\ldots,x_n)$ Boole-függvény akkor és csak akkor monoton és önduális, ha kielégíti a következő feltételt:

$$\text{minden } x=x_1\ldots x_n\text{-re és } y=y_1\ldots y_n\text{-re van olyan } k,\text{ hogy } f(x)=x_k \text{ és } f(y)=y_k.$$

(b) Tegyük fel, hogy f néhány érték esetén nincs definiálva, de az előbbi feltétel mindig teljesül, amikor $f(x)$ is, $f(y)$ is definiált. Mutassuk, meg, hogy van olyan monoton és önduális g Boole-függvény, hogy $g(x)=f(x)$, amikor $f(x)$ definiált.

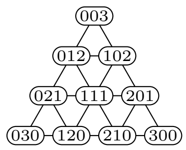
65. [*M21*] $\{1,2,\ldots,n\}$ bármely X részhalmazához hozzárendelhetünk az $x_j=[j\in X]$ szabállyal egy $x=x_1x_2\ldots x_n$ bináris vektort. És ilyen részhalmazok bármely $\mathcal{F}$ családjához pedig az $f(x)=[X\in\mathcal{F}]$ szabállyal hozzárendelhetünk egy n-változós $f(x)=f(x_1,x_2,\ldots,x_n)$ Boole-függvényt. Így a részhalmazok családjairól szóló minden állításnak egy Boole-függvényekről szóló állítás felel meg, és viszont.

Egy $\mathcal{F}$ család *egymást metsző*, ha $X\cap Y\ne\emptyset$, amikor $X,Y\in\mathcal{F}$. Egy olyan egymást metsző családot, amely elveszíti ezt a tulajdonságot, amikor megpróbálunk hozzáadni egy másik részhalmazt, *maximálisnak* nevezünk. Bizonyítsuk be, hogy $\mathcal{F}$ akkor és csak akkor maximális egymást metsző család, ha a megfelelő f Boole-függvény monoton és önduális.

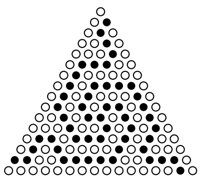
66. [*M25*] $\{1,\ldots,n\}$ *klikkje kvórumoknak* nevezett részhalmazok következő tulajdonságokkal rendelkező $\mathcal{C}$ családja: minden $Q\in\mathcal{C}$ és $Q'\in\mathcal{C}$ esetén (i) $Q\cap Q'\ne\emptyset$; (ii) $Q\subseteq Q'$ maga után vonja $Q=Q'$-t. A $\mathcal{C}$ klikk *dominálja* a $\mathcal{C}'$ klikket, ha $\mathcal{C}\ne\mathcal{C}'$, és ha minden $Q'\in\mathcal{C}'$-hez van olyan $Q\in\mathcal{C}$, hogy $Q\subseteq Q'$. Például az $\{\{1,2\},\{2,3\}\}$ klikket dominálja $\{\{1,2\},\{1,3\},\{2,3\}\}$, és $\{\{2\}\}$ is. (A klikkeket Lamport, illetve Garcia-Molina és Barbara vezették be [27] és [?] klasszikus dolgozataikban. Ezek a dolgozatok számos alkalmazást tartalmaznak elosztott rendszerek protokoljaival kapcsolatban, felölelve a kölcsönös kizárás, az adat többszörözés és a névkiszolgálók témáit is. Ezekben az alkalmazásokban $\mathcal{C}$ bármelyik olyan klikknél előnyösebb, mint amelyet dominál.)

Bizonyítsuk be, hogy $\mathcal{C}$ akkor és csak akkor nemdominált klikk, ha kvórumjai éppen valamely monoton önduális $f(x_1,\ldots,x_n)$ Boole-függvény prímimplikánsaiban szereplő változóknak az indexhalmazai. (Tehát a 7.2. táblázat $\{1,2,3,4\}$ nemdominált klikkjeit szemlélteti.)

67. [*M30*] (Milnor és Schensted.) Egy n-ed rendű háromszögrács $(n+2)(n+1)/2$ pontot tartalmaz, ha olyan nemnegatív xyz „baricentrikus koordinátákkal" rendelkezik, melyekre $x+y+z=n$ teljesül. Két pont szomszédos, ha egymástól pontosan két koordináta-pozícióban ±1-gyel különböznek. Egy pont a háromszögrács x oldalán fekszik, ha az x koordinátája nulla, y oldalán, ha az y koordinátája nulla, z oldalán, ha a z koordinátája nulla; így minden oldal $n+1$ pontot tartalmaz. Ha $n>0$, egy pont akkor és csak akkor fekszik két különböző oldalon is, ha a három sarokpozíció valamelyikét foglalja el.



Pontok olyan összefüggő halmazát, amely a rács minden oldaláról legalább egy pontot tartalmaz, „Y"-nak nevezzük. Tegyük fel, hogy a háromszögrács minden csúcsában egy fehér vagy egy fekete golyó van. Az alábbi ábrán látható 52 fekete golyó például egy (némileg csavarodó) Y:



Ha bármelyik golyót ezek közül kicseréljük feketéről fehérre, az előbbi helyett egy fehér Y-t nyerünk. Ha gyorsan átgondoljuk, intuitíven is világos, hogy bármely elrendezés esetén a fekete golyók akkor és csak akkor alkotnak Y-t, ha a fehér golyók nem.

Egy-egy golyó színét Boole-értékkel reprezentálhatjuk: 0-val a fehéret, 1-gyel a feketét. Legyen $Y(t)=1$ akkor és csak akkor, ha fekete Y-unk van, ahol t egy az összes Boole-értéket tartalmazó háromszögrács. Ez az Y függvény nyilvánvalóan monoton; és az előző bekezdésben megfogalmazott intuitív állítás ekvivalens azzal a megállapítással, hogy Y önduális is. A gyakorlat célja a medián algebrák eszközeit használva precízen bebizonyítani az állítást.

Adott $a,b,c\ge0$ mellett legyen t_{abc} az a rész-háromszögrács, mely az összes olyan xyz koordinátájú pontot tartalmazza, melyre $x\ge a$, $y\ge b$, $z\ge c$. Például t_{001} a z oldalon (alsó soron) fekvők kivételével az összes többi pontot jelenti. Vegyük észre, hogy ha $a+b+c=n$, akkor t_{abc} az abc koordinátával rendelkező egyetlen pontból áll; és általában pedig t_{abc} egy $n-a-b-c$ -ed rendű háromszögrács.

a) Bizonyítsuk be, hogy ha $n>0$, akkor $Y(t)=\langle Y(t_{100})Y(t_{010})Y(t_{001})\rangle$.

b) Ha $n>0$, legyen t^* a

$$t^*_{xyz}=\langle t_{(x+1)yz}t_{x(y+1)z}t_{xy(z+1)}\rangle, \qquad \text{ha } x+y+z=n-1$$

szabállyal definiált $n-1$ -ed rendű háromszögrács. Bizonyítsuk be, hogy $Y(t)=Y(t^*)$. (Másképp fogalmazva t^* minden kis golyó-háromszöget összetömörít a golyók színeire vonatkozó mediánozással. Az eljárás ismétlése golyók egy egész *piramisát* definiálja, ahol a felső golyó akkor és csak akkor fekete, ha fekete Y van alul. Jó szórakozás ezt a tömörítő elvet a fenti csavart Y-ra alkalmazni.)

68. [*46*] Az előző gyakorlatban bemutatott „éppen csak hogy Y" konfigurációban 52 fekete golyó van. Egy ilyen konfigurációban mi a fekete golyók lehetséges legnagyobb száma? (Azaz hány változó lehet az $Y(t)$ függvény egy prímimplikánsában?)

69. [*M26*] (Schensted.) A 67. gyakorlat az Y függvényt mediánok segítségével fejezi ki. Megfordítva, legyen $f(x_1, \ldots, x_n)$ egy $m+1$ prímimplikánssal, mondjuk a $p_0, p_1, \ldots, p_m$ prímimplikánsokkal rendelkező monoton és önduális Boole-függvény. Bizonyítsuk be, hogy $f(x_1, \ldots, x_n) = Y(T)$, ahol T egy $m-1$-ed rendű olyan háromszögrács, amelyben T_{abc} közös változója p_a-nak és p_{a+b+1}-nek, ha $a+b+c = m-1$. Például amikor $f(w,x,y,z) = \langle xwywz\rangle$, akkor $m=3$, és

$$f(w,x,y,z) = (w \wedge x) \vee (w \wedge y) \vee (w \wedge z) \vee (x \wedge y \wedge z) = Y\left(\begin{smallmatrix} & & w & & \\ & w & & w & \\ x & & y & & z \end{smallmatrix}\right).$$

70. [*M20*] (Meyerowitz, 1989.) Adott monoton és önduális $f(x) = f(x_1, \ldots, x_n)$ Boole-függvény mellett válasszunk egy $x_{j_1} \wedge \cdots \wedge x_{j_s}$ prímimplikánst, és legyen

$$g(x) = \bigl(f(x) \wedge [x \neq t]\bigr) \vee [x = \bar{t}],$$

ahol $t = t_1 \ldots t_n$ olyan bitvektor, mely a $\{j_1, \ldots, j_s\}$ pozíciókban 1. Bizonyítsuk be, hogy ekkor $g(x)$ is monoton és önduális. (Vegyük észre, hogy a t és $\bar{t}$ pontok kivételével $g(x)$ megegyezik $f(x)$-szel.)

71. [*M21*] A medián algebrákra vonatkozó (50), (51) és (52) axiómák ismeretében bizonyítsuk be, hogy az (54) hosszú disztributivitás törvény az (53) rövidebb törvény következménye.

72. [*M22*] Vezessük le az (58), (59) és (60) tulajdonságokat a mediánra vonatkozó (50)–(53) törvényekből.

73. [*M32*] (Avann.) Egy olyan M medián algebra esetén, mely intervallumait (57), és melyhez tartozó medián gráfot (61) definiálja, jelölje $d(u,v)$ az u-nak v-től való távolságát. „$[uxv]$" jelentse, hogy „x egy az u-ból v-be vezető legrövidebb úton fekszik".

a) Bizonyítsuk be, hogy $[uxv]$ akkor és csak akkor teljesül, ha $d(u,v) = d(u,x) + d(x,v)$.

b) Tegyük fel, hogy $x \in [u\,..\,v]$ és $u \in [x\,..\,y]$, ahol $x \neq u$, és y — v a gráf egy éle. Mutassuk meg, hogy x — u is él.

c) Ha $x \in [u\,..\,v]$, bizonyítsuk be $d(u,v)$-re vonatkozó indukcióval, hogy $[uxv]$.

d) Megfordítva, bizonyítsuk be, hogy $d(u,v)$ maga után vonja, hogy $x \in [u\,..\,v]$.

74. [*M21*] Mutassuk meg, hogy egy medián algebrában $w = \langle xyz\rangle$, amikor az (57) definíciónak megfelelően $w \in [x\,..\,y]$, $w \in [x\,..\,z]$ és $w \in [y\,..\,z]$.

75. [*M36*] (Sholander, 1954.) Tegyük fel, hogy M egy ponthalmaz az „x az u és a v között fekszik" $[uxv]$-vel jelölt relációval, mely a következő három axiómát teljesíti:

i) Ha $[uvu]$, akkor $u = v$.

ii) Ha $[uxv]$ és $[xyu]$, akkor $[vyu]$.

iii) Adott x, y és z esetén pontosan egy $w = \langle xyz\rangle$ pont teljesíti, hogy $[xwy]$, $[xwz]$ és $[ywz]$.

A gyakorlat célja bebizonyítani, hogy M medián algebra.

a) Bizonyítsuk be az $\langle xxy\rangle = x$ majoritás törvényt, azaz (50)-t.

b) Bizonyítsuk be az $\langle xyz\rangle = \langle xzy\rangle = \cdots = \langle zyx\rangle$ kommutativitás törvényt, azaz (51)-et.

c) Bizonyítsuk be, hogy $[uxv]$ akkor és csak akkor, ha $x = \langle uxv\rangle$.

d) Bizonyítsuk be, hogy $[xyv]$, ha $[uxy]$ és $[uyv]$.

e) Bizonyítsuk be, hogy $[xyz]$, ha $[uxv]$, $[uyz]$ és $[vyz]$. *Segítség:* Konstruáljuk meg a $w = \langle yuv\rangle$, $p = \langle wux\rangle$, $q = \langle wvx\rangle$, $r = \langle pxz\rangle$, $s = \langle qxz\rangle$ és $t = \langle rsz\rangle$ pontokat.

f) Végül vezessük le az (53) rövid disztributivitás törvényt: $\bigl\langle\langle xyz\rangle uv\bigr\rangle = \bigl\langle x\langle yuv\rangle\langle zuv\rangle\bigr\rangle$.

76. [*M33*] Származtassuk most a 75. gyakorlatbeli „közöttlevőség” relációra vonatkozó (i), (ii) és (iii) axiómákat úgy, hogy az (50), (51) és (52) medián axiómákból induljunk ki, az $[uxv]$-t pedig az „$x = \langle uxv \rangle$” rövidítésének tekintsük. Ne használjuk az (53) disztributivitás törvényt. *Segítség:* Lásd a 74. gyakorlatot.

77. [*M28*] Legyen G az $r — s$ élt tartalmazó medián gráf. Egy $u — v$ él esetén u-t akkor és csak akkor nevezzük v *közeli szomszédjának*, ha u-hoz r közelebb van, mint v-hez. Osszuk szét a csúcsokat „bal” és „jobb” csúcsokra, ahol a bal csúcsok közelebb vannak r-hez, mint s-hez, és a jobb csúcsok pedig közelebb vannak s-hez, mint r-hez. Egy v jobb csúcs *szintszáma* a bal csúcsok v-től való legkisebb távolsága. Ehhez hasonlóan, egy u bal csúcs $1 - d$ szintszámú, ha d a jobb csúcsok u-tól való legkisebb távolsága. Ezért u szintszáma nulla, ha valamelyik jobb csúccsal szomszédos, egyébként szintszáma negatív. Az r csúcs nyilván 0 szintszámú, s pedig 1 szintszámú.

a) Mutassuk meg, hogy minden 1 szintszámú csúcs a 0 szintszámú csúcsok közül pontosan eggyel szomszédos.
b) Mutassuk meg, hogy a jobb csúcsok halmaza konvex.
c) Mutassuk meg, hogy az 1 szintszámú csúcsok halmaza konvex.
d) Bizonyítsuk be, hogy az I eljárás I3-I9 lépései helyesen jelölnek meg minden 1 és 2 szintszámú csúcsot.
e) Bizonyítsuk be, hogy a H algoritmus helyes.

78. [*M26*] Bizonyítsuk be, hogy a gráfnak legalább 2^k csúcsa van, ha a H algoritmus végrehajtása közben a v csúcsot az I4 lépés során k-szor vizsgáljuk. *Segítség:* k féleképpen indíthatunk v-ből a-ba vezető legrövidebb utat; így $l(v)$-ben legalább k darab 1-es van.

79. [*M27*] (Graham.) Egy *hiperkocka részgráfja* olyan gráf, melynek v csúcsait címkézhetjük $l(v)$ bitfüzérekkel úgy, hogy $u — v$ akkor és csak akkor, ha $l(u)$ és $l(v)$ pontosan egy bitpozícióban különböznek. (Minden címke ugyanolyan hosszú.)

a) Egy hiperkocka n csúcsú részgráfjának definiálására az egyik lehetőség az, hogy minden $0 \le v < n$-re megadjuk $l(v)$-t, v bináris reprezentációját. Mutassuk meg, hogy ennek a részgráfnak pontosan $f(n) = \sum_{k=0}^{n-1} \nu(k)$ éle van, ahol $\nu(k)$ az oldalösszeg-függvény.
b) Bizonyítsuk be, hogy $f(n) \le n\lceil \lg n \rceil/2$.
c) Bizonyítsuk be, hogy egy hiperkocka egyetlen n csúcsú részgráfja sem tartalmaz $f(n)$-nél több élt.

80. [*M27*] *Parciális kockának* nevezzük egy hiperkocka „izometrikus” (távolság-megőrző) részgráfját, azaz egy olyan részgráfot, melyben a csúcsok közötti távolság ugyanakkora, mint a teljes gráfban. Egy parciális kocka csúcsait ezért címkézhetjük úgy, hogy az u és v közötti távolság az $l(u)$ és $l(v)$ közötti „Hamming-távolság”, azaz $\nu(l(u) \oplus l(v))$. A H algoritmus megmutatja, hogy minden medián gráf parciális kocka.

a) Keressük meg a négydimenziós kocka egy nem parciális kocka részgráfját.
b) Adjunk olyan parciális kockára példát, amelyik nem medián gráf.

81. [*16*] Vajon minden medián gráf páros?

82. [*25*] (*Fokozatos változtatások* a rendszerszolgáltatásban.) Vizsgáljuk a következő problémát: egy G gráfban adott $(v_0, v_1, \ldots, v_t)$ csúcs-sorozathoz keressük meg azt az $(u_0, u_1, \ldots, u_t)$ sorozatot, melyre $u_0 = v_0$, és a

$$\big(d(u_0,u_1) + d(u_1,u_2) + \cdots + d(u_{t-1},u_t)\big) \ + \ \big(d(u_1,v_1) + d(u_2,v_2) + \cdots + d(u_t,v_t)\big)$$

összeg a lehető legkisebb, ahol $d(u,v)$ az u és v közötti távolság. (Minden v_k-ra egy az abban a csúcsban felmerülő erőforrás-igényként tekinthetünk; amint a sorozatban az igény intézendővé válik, a kiszolgáló u_k-hoz fordul.) Bizonyítsuk be, hogy ha G medián gráf, optimális megoldást kapunk $0 < k < t$-re az $u_k = \langle u_{k-1} v_k v_{k+1} \rangle$ és az $u_t = v_t$ választással.

83. [*28*] Általánosítva a 82. gyakorlatot, keressünk hatékony módszert most arra, hogy egy medián gráfban – adott pozitív ρ súly mellett – hogyan minimalizáljuk a

$$\big(d(u_0,u_1)+d(u_1,u_2)+\cdots+d(u_{t-1},u_t)\big) \ + \ \rho\big(d(u_1,v_1)+d(u_2,v_2)+\cdots+d(u_t,v_t)\big)$$

összeget.

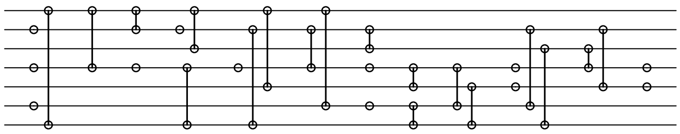
84. [*30*] Írjunk programot, mely megkeresi az összes monoton és önduális ötváltozós Boole-függvényt. Mik lesznek a megfelelő medián gráf élei? (A 7.2. táblázat a négyváltozós esetet szemlélteti.)

85. [*M22*] Az S tétel szerint minden 2KNF formula egy-egy medián halmazt határoz meg; ezért minden olyan antiszimmetrikus irányított gráf, mint a 7.6. ábrán látható, medián halmaz. Ezek közül az irányított gráfok közül pontosan melyek felelnek meg a *redukált* medián halmazoknak?

86. [*15*] Ha v, w, x, y és z az X medián halmaz elemei, $\langle vwxyz \rangle$, azaz a komponensenként számított ötváltozós mediánjuk, vajon eleme-e mindig X-nek?

87. [*24*] A (63) szabad fára melyik CI-net adja az F tétel bizonyítását?

88. [*M21*] Párhuzamos számítással a (74) hálózatot az alábbi hálózattá tömöríthetjük úgy, hogy az egyes modulok a lehető legkorábbi időpontban működjenek:



Bizonyítsuk be, hogy bár az F tétel bizonyításában konstruált hálózat csak $\Omega(t^2)$ modult tartalmazhat, mégis várakoznia mindig legfeljebb $O(t \log t)$ szakasznyit kell.

89. [*24*] Amikor a (73) konstrukció a moduloknak egy új csoportját csatolja azért, hogy valamely u és v literálokra érvényesítse az $u \to v$ feltétel teljesülését, bizonyítsuk be, hogy közben megőrzi az összes előzőekben érvényesített $u' \to v'$ feltételt.

90. [*21*] Konstruáljunk CI-netet az $x_1 \ldots x_t$ input- és az $y_1 \ldots y_t$ outputbitekkel, ahol $y_1 = \cdots = y_{t-1} = 0$ és $y_t = x_1 \oplus \cdots \oplus x_t$. Próbáljuk meg elérni, hogy csak $O(\log t)$ várakozó szakasz legyen.

91. [*46*] Kiszámíthatjuk-e az egyes t dimenziós medián gráfok címkéinek behúzó leképezését olyan CI-nettel, amiben csak $O(\log t)$ várakozó szakasz van? (Ezt a kérdést a rendezés hasonló problémájára vonatkozó aszimptotikusan optimális hálózatok létezése motiválta; lásd Ajtai, Komlós és Szemerédi [1] dolgozatát.)

92. [*46*] Kevesebb modullal tud-e rendezni egy CI-net n Boole-inputot, mint egy „tiszta” – átalakítót nem tartalmazó – rendező hálózat?

93. [*M20*] Bizonyítsuk be, hogy egy G gráf minden X behúzója G távolság-megőrző részgráfja. (Másképp fogalmazva X-ben a távolságok ugyanazok, mint G-ben; lásd a 80. gyakorlatot.)

94. [*M21*] Bizonyítsuk be, hogy egy hiperkocka minden X behúzója medián címkék halmaza, ha eltekintünk azoktól a koordinátáktól, melyek minden $x \in X$-re konstansok.

95. [*M25*] Igaz vagy hamis a következő állítás? Egy összehasonlító-átalakító hálózat által eredményezett outputok halmaza – miközben az input végigfut az összes lehetséges bitfüzéren – mindig medián halmaz.

96. [*HM25*] Ahelyett, hogy ragaszkodnánk ahhoz, hogy (110)-ben a w_1, w_2, $\ldots$, w_n és t konstansok egészek legyenek, engedjük meg, hogy a valós számok közül tetszőlegesen választhassuk ki őket. Megnövekszik-e vajon ekkor a küszöbfüggvények száma?

97. [*10*] Milyen medián/majoritás függvények adódnak (81)-ben, ha $n = 2$, $w_1 = w_2 = 1$ és $t = -1$, 0, 1, 2, 3 vagy 4?

98. [*M23*] Bizonyítsuk be, hogy bármely önduális küszöbfüggvény kifejezhető

$$f(x_1, x_2, \ldots, x_n) = [v_1 y_1 + \cdots + v_n y_n > 0]$$

formában, ahol minden y_j vagy x_j, vagy $\bar{x}_j$. Például $2x_1 + 3x_2 + 5x_3 + 7x_4 + 11x_5 + 13x_6 \geq 21$ akkor és csak akkor, ha $2x_1 + 3x_2 + 5x_3 - 7\bar{x}_4 + 11x_5 - 13\bar{x}_6 > 0$.

99. [*20*] (Mezei, 1961.) Bizonyítsuk be, hogy

$$\big\langle \langle x_1 \ldots x_{2s-1} \rangle y_1 \ldots y_{2t-2} \big\rangle = \langle x_1 \ldots x_{2s-1} y_1^s \ldots y_{2t-2}^s \rangle.$$

100. [*20*] Igaz vagy hamis a következő állítás? Ha $f(x_1, \ldots, x_n)$ küszöbfüggvény, akkor az $f(x_1, \ldots, x_n) \wedge x_{n+1}$ és az $f(x_1, \ldots, x_n) \vee x_{n+1}$ függvények is azok.

101. [*M23*] Az $F_n(x_1, \ldots, x_n)$ Fibonacci-küszöbfüggvényt $n \geq 3$ esetben az $\langle x_1^{F_1} x_2^{F_2} \ldots x_{n-1}^{F_{n-1}} x_n^{F_{n-2}} \rangle$ formulával definiálhatjuk. Például $F_7(x_1, \ldots, x_7) = \langle x_1 x_2 x_3^2 x_4^3 x_5^5 x_6^8 x_7^5 \rangle$.

a) Adjuk meg $F_n(x_1, \ldots, x_n)$ prímimplikánsait.
b) Keressük meg $F_n(x_1, \ldots, x_n)$ ortogonális DNF-jét (lásd a 35. gyakorlatot).
c) Fejezzük ki $F_n(x_1, \ldots, x_n)$-t az Y függvény segítségével (lásd a 67. és 69. gyakorlatokat).

102. [*M21*] Egy Boole-függvény *öndualizálását* az

$$\begin{aligned} \hat{f}(x_0, x_1, \ldots, x_n) &= (x_0 \wedge f(x_1, \ldots, x_n)) \vee (\bar{x}_0 \wedge \overline{f(\bar{x}_1, \ldots, \bar{x}_n)}) \\ &= (\bar{x}_0 \vee f(x_1, \ldots, x_n)) \wedge (x_0 \vee \overline{f(\bar{x}_1, \ldots, \bar{x}_n)}). \end{aligned}$$

formulával definiáljuk.

a) Bizonyítsuk be, hogy tetszőleges $f(x_1, \ldots, x_n)$ Boole-függvény esetén $\hat{f}$ önduális.
b) Bizonyítsuk be, hogy $\hat{f}$ akkor és csak akkor küszöbfüggvény, ha f is küszöbfüggvény.

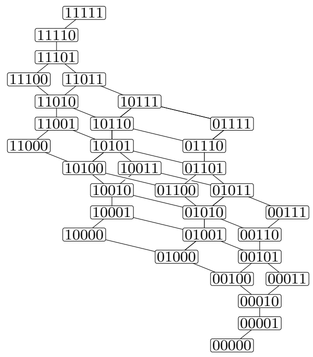
103. [*HM25*] Tisztázzuk, hogy hogyan használjuk fel a lineáris programozást annak ellenőrzésére, vajon egy monoton, önduális Boole-függvény küszöbfüggvény-e, vagy sem. Továbbá ha küszöbfüggvény, derítsük ki, hogyan minimalizáljuk az $\langle x_1^{w_1} \ldots x_n^{w_n} \rangle$ majoritás függvényként megadott reprezentációjának méretét.

104. [*25*] Alkalmazzuk a 103. gyakorlat módszerét arra, hogy megkeressük a következő küszöbfüggvények mint majoritás függvények legrövidebb reprezentációit: (a) $\langle x_1^2 x_2^3 x_3^5 x_4^7 x_5^{11} x_6^{13} x_7^{17} x_8^{19} \rangle$; (b) minden $0 \leq t \leq 16$-re $[(x_1 x_2 x_3 x_4)_2 \geq t]$ (17 eset); (c) $\langle x_1^{29} x_2^{25} x_3^{19} x_4^{15} x_5^{12} x_6^8 x_7^8 x_8^3 x_9^3 x_{10} \rangle$.

105. [*M25*] Mutassuk meg, hogy a 101. gyakorlatbeli Fibonacci-küszöbfüggvénynek nincs rövidebb majoritás függvény reprezentációja, mint amit a definiálására használtunk.

106. [*M25*] A háromváltozós $\langle x\bar{y}\bar{z} \rangle$ medián művelet eredménye akkor és csak akkor igaz, ha $x \geq y + z$.

a) Ezt általánosítva mutassuk meg, hogy az $(x_1 x_2 \ldots x_n)_2 \geq (y_1 y_2 \ldots y_n)_2 + z$ feltételt $2^{n+1} - 1$ Boole-változó mediánozásával ellenőrizhetjük.
b) Bizonyítsuk be, hogy $2^{n+1} - 1$-nél kevesebb változó mediánozása nem lesz elegendő ennek a problémának a megoldására.



7.8. ábra. Bináris majorizációs háló 5 hosszúságú füzérekre. (Lásd a 109. gyakorlatot.)

107. [*17*] Számoljuk ki $N(f)$-et és $\Sigma(f)$-et a 7.1. táblázat 16 függvényére. (Lásd a T tételt.)

108. [*M21*] Legyen $g(x_0, x_1, \ldots, x_n)$ önduális függvény. Így a T tétel jelölését használva $N(g) = 2^n$. Fejezzük ki $N(f)$-et és $\Sigma(f)$-et $\Sigma(g)$ segítségével, amikor $f(x_1, \ldots, x_n)$ éppen (a) $g(0, x_1, \ldots, x_n)$; (b) $g(1, x_1, \ldots, x_n)$.

109. [*M25*] Az $\alpha = a_1 \ldots a_n$ bináris füzér a $\beta = b_1 \ldots b_n$ bináris füzért *majorizálja*, ha minden $k \geq 0$-ra $a_1 + \cdots + a_k \geq b_1 + \cdots + b_k$. Jelölve $\alpha \succeq \beta$ vagy $\beta \preceq \alpha$.

a) Legyen $\bar{\alpha} = \bar{a}_1 \ldots \bar{a}_n$. Mutassuk meg, hogy $\alpha \succeq \beta$ akkor és csak akkor, ha $\bar{\beta} \succeq \bar{\alpha}$.
b) Mutassuk meg, hogy bármely két n hosszúságú bináris füzérnek $\alpha \wedge \beta$ a legnagyobb alsó korlátja, azaz $\alpha \succeq \gamma$ és $\beta \succeq \gamma$ akkor és csak akkor, ha $\alpha \wedge \beta \succeq \gamma$. Magyarázzuk meg, hogyan számoljuk ki $\alpha \wedge \beta$-t adott α és β esetén.
c) Hasonlóan az előbbi gyakorlathoz, magyarázzuk meg, hogyan számoljuk ki az $\alpha \vee \beta$ legkisebb felső korlátot, azaz amikor $\gamma \succeq \alpha$ és $\gamma \succeq \beta$ akkor és csak akkor, ha $\gamma \succeq \alpha \vee \beta$.
d) Igaz vagy hamis a következő két állítás? $\alpha \wedge (\beta \vee \gamma) = (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$; $\alpha \vee (\beta \wedge \gamma) = (\alpha \vee \beta) \wedge (\alpha \vee \gamma)$.
e) Mondjuk azt, hogy α *lefedi* β-t, ha $\alpha \succeq \beta$ és $\alpha \neq \beta$, továbbá ha $\alpha \succeq \gamma \succeq \beta$ maga után vonja, hogy vagy $\gamma = \alpha$, vagy $\gamma = \beta$. Példaként a 7.8. ábra szemlélteti az 5 hosszúságú bináris füzérek közötti lefedés relációt. Keressünk egyszerű módszert arra, hogyan írjuk le azokat a füzéreket, amelyeket egy adott bináris füzér lefed.
f) Mutassuk meg, hogy egy adott α füzérből $0 \ldots 0$-ba vezető minden olyan $\alpha = \alpha_0, \alpha_1, \ldots, \alpha_r = 0 \ldots 0$ út ugyanolyan $r = r(\alpha)$ hosszúságú, ahol minden $1 \leq j \leq r$-re α_{j-1} lefedi α_j-t.
g) Legyen $m(\alpha)$ azon β bináris füzérek száma, melyekre $\beta \succeq \alpha$. Bizonyítsuk be, hogy $m(1\alpha) = m(\alpha)$ és $m(0\alpha) = m(\alpha) + m(\alpha')$, ahol α'-t úgy nyerjük, hogy α-ban legbaloldalibb 1-est (ha egyáltalán van ilyen) 0-ra cseréljük.
h) Hány n hosszúságú α füzérre teljesül, hogy $\bar{\alpha} \succeq \alpha$?

110. [*M23*] Egy Boole-függvényt *regulárisnak* nevezünk, ha $x \preceq y$ esetén $f(x) \leq f(y)$ minden x és y-ra, ahol $\preceq$ a 109. feladatbeli majorálás reláció. Igazoljuk vagy cáfoljuk a következő állításokat:

a) Minden reguláris függvény monoton.
b) Ha f küszöb függvény (), amelyre $w_1 \geq w_2 \geq \cdots \geq w_n$, akkor f reguláris.

c) Ha f olyan, mint (b)-ben és $\Sigma(f) = (s_1, \ldots, s_n)$, akkor $s_1 \geq s_2 \geq \cdots \geq s_n$.

d) Ha f egy küszöb függvény (), ahol $s_1 \geq s_2 \geq \cdots \geq s_n$, akkor $w_1 \geq w_2 \geq \cdots \geq w_n$.

111. [*M36*] Egy $(p_1, \ldots, p_n)$ működési valószínűségekkel rendelkező rendszer *optimális klikkje* egy olyan klikk, ami az összes n-változós monoton önduális függvények egy maximális elérhetőségű monoton önduális függvényének felel meg. (Lásd a 14. és a 66. gyakorlatokat)

a) Igazoljuk, hogy ha $1 \geq p_1 \geq \cdots \geq p_n \geq \frac{1}{2}$, akkor legalább egy maximális elérhetőségű önduális függvény reguláris függvény.

b) Azonkívül, egy f reguláris önduális függvénynek az optimalitását elegendő ellenőrizni a bináris majorizáló hálónak azokban az y pontjaiban, amelyekben $f(y) = 1$, de $f(x) = 0$ minden az y-al lefedett x-re.

c) Milyen klikk optimális, ha néhány valószínűség $< \frac{1}{2}$?

112. [*M37*] (J. Håstad.) Legyen $M(f)$ az $f(x_1, x_2, \ldots, x_m)$ Boole-függvény egy reprezentációja egész együtthatós multilineáris polinom alakban (lásd 12. gyakorlat). Rendezzük ebben a polinomban a kitevőket figyelembe vevő $\alpha_0 = 00\ldots0$, $\alpha_1 = 10\ldots0$, $\ldots$, $\alpha_{2^m-1} = 11\ldots1$ Chase sorozat felhasználásával a termeket. A Chase sorozatnak amit a 7.2.1.3–(35)-ben lévő A_{n0}, $A_{(n-1)1}$, $\ldots$, A_{0n} sorozatok konkatenálásával kaptunk érdekes tulajdonsága van. α_j egybeesik α_{j+1}-el ha a következő cserék valamelyikét elvégezzük: $0 \to 1$ vagy $01 \to 10$ vagy $001 \to 100$ vagy $10 \to 01$ vagy $100 \to 001$.

Például Chase sorozat

$$0000, 1000, 0010, 0001, 0100, 1100, 1010, 1001, 0011, 0101, 0110, 1110, 1101, 1011, 0111, 1111$$

ha $m = 4$. a megfelelő termek 1, x_1, x_3, x_4, x_2, x_1x_2, $\ldots$, $x_2x_3x_4$, $x_1x_2x_3x_4$; így mondjuk az $((x_1 \oplus \bar{x}_2) \wedge x_3) \vee (x_1 \wedge \bar{x}_3 \wedge x_4)$-nek egész együtthatós multilineáris reprezentációja

$$x_3 - x_1x_3 + x_1x_4 - x_2x_3 + 2x_1x_2x_3 - x_1x_3x_4$$

ha a termeket ebben a sorrendben tekintjük. Legyen most

$$F(f) \;=\; [\text{a legjelentősebb együtthatója } M(f)\text{-nek pozitív}].$$

Például, az $((x_1 \oplus \bar{x}_2) \wedge x_3) \vee (x_1 \wedge \bar{x}_3 \wedge x_4)$ legjelentősebb együtthatója (az utolsó) nemzéró term a Chase rendezés szerint $-x_1x_3x_4$, ezért ebben az esetben $F(f) = 0$.

a) Határozzuk meg $F(f)$-et az 1. táblázat mind a 16 függvényére.

b) Mutassuk meg, hogy $F(f)$ küszöbfüggvénye az f igazságtáblájának $\{f_{0\ldots00}, f_{0\ldots01}, \ldots, f_{1\ldots11}\}$, $n = 2^m$ bemenetére. Írjuk le $m = 2$ esetben ezeket a függvényeket.

c) Bizonyítsuk, hogy ha m nagy, akkor F bármely küszöb reprezentációjában minden súly nagyon nagy. Ezek abszolút értéke meg kell hogy haladja a

$$\frac{3^{\binom{m}{3}}7^{\binom{m}{4}}15^{\binom{m}{5}}\ldots(2^{m-1}-1)^{\binom{m}{m}}}{n}\bigl(1 - O(n)\bigr) \;=\; 2^{mn/2-n-2(3/2)^m/\ln 2+O((5/4)^m)}.$$

Segítség: Tekintsük az igazságtábla bemenetek diszkrét Fourier transzformáltjait.

113. [*24*] Mutassuk meg, hogy a következő három küszöb művelet elegendő a (91)-beli $S_{2,3,6,8,9}(x_1, \ldots, x_{12})$ függvény kiértékeléséhez:

$$\begin{aligned} g_1(x_1, \ldots, x_{12}) &= [\nu x \geq 6] = \langle 1 x_1 \ldots x_{12} \rangle; \\ g_2(x_1, \ldots, x_{12}) &= [\nu x - 6g_1 \geq 2] = \langle 1^3 x_1 \ldots x_{12} \bar{g}_1^6 \rangle; \\ g_3(x_1, \ldots, x_{12}) &= [-2\nu x + 13g_1 + 7g_2 \geq 1] = \langle 0^5 \bar{x}_1^2 \ldots \bar{x}_{12}^2 g_1^{13} g_2^7 \rangle. \end{aligned}$$

Adjunk meg négy küszöb műveletet az $S_{1,3,5,8}(x_1,\ldots,x_{12})$ kiértékeléséhez.

114. [*20*] (D. A. Huffman.) Mi az $S_{3,6}(x,x,x,x,y,y,z)$ függvény?

115. [*M22*] Magyarázzuk el, hogy a (92) miért számítja ki pontosan az $x_0\oplus x_1\oplus\cdots\oplus x_{2m}$ paritásfüggvényt.

116. [*HM28*] (B. Dunham és R. Fridshal, 1957.) A szimmetrikus függvényeket tekintve bizonyítható, hogy az n-változós Boole-függvényeknek sok prímimplikánsuk lehet.

a) Tegyük fel hogy $0\le j\le k\le n$. Mely $f(x_1,\ldots,x_n)$ szimmetrikus függvényekre lesz az $x_1\wedge\cdots\wedge x_j\wedge\bar{x}_{j+1}\wedge\cdots\wedge\bar{x}_k$ term prímimplikáns?
b) Hány prímimplikánsa van az $S_{3,4,5,6}(x_1,\ldots,x_9)$ függvénynek?
c) Legyen $\hat{b}(n)$ az összes n-változós szimmetrikus függvény prímimplikánsainak maximális száma. Keressünk $\hat{b}(n)$-re egy rekurzív formulát és számítsuk ki $\hat{b}(n)$-et.
d) Bizonyítsuk, hogy $\hat{b}(n)=\Theta(3^n/n)$.
e) Mutassuk meg, hogy vannak olyan $f(x_1,\ldots,x_n)$ szimmetrikus függvények, ahol az f és a $\bar{f}$ prímimplikánsainak száma $\Theta(2^{3n/2}/n)$.

117. [*M26*] Egy diszjunktív normál formát *irredundánsnak* nevezünk, ha egyik implikánsa sem implikál egy másikat. Legyen $b^*(n)$ az összes n-változós Boole-függvény irredundáns DNF-jeiben lévő prímimplikánsok számának maximuma. Keressünk egy egyszerű formulát $b^*(n)$-re és határozzuk meg ennek aszimptotikus értékét.

118. [*29*] Hány $f(x_1,x_2,x_3,x_4)$ Boole-függvénynek van pontosan m primimplikánsa, ha $m=0$, $1,\ldots$?

119. [*M48*] Folytatva az előző gyakorlatokat, legyen $b(n)$ egy n-változós Boole-függvény prímimplikánsai számának maximuma. Világos, hogy $\hat{b}(n)\le b(n)<b^*(n)$; de mi a $b(n)$ aszimptotikus értéke?

120. [*23*] Mi a legrövidebb DNF alakja az (a) $x_1\oplus x_2\oplus\cdots\oplus x_n$ és a (b) $S_{0,1,3,4,6,7}(x_1,\ldots,x_7)$ szimmetrikus függvényeknek. (c) Bizonyítsuk be, hogy minden n-változós Boole-függvény leírható legfeljebb 2^{n-1} primimplikánst tartalmazó DNF-el.

121. [*M23*] Az $\langle 1(x_1\oplus x_2)y_1y_2y_3\rangle$ függvény parciálisan szimmetrikus, mivel szimmetrikus $\{x_1,x_2\}$-re és $\{y_1,y_2,y_3\}$-re, de nem mind az öt $\{x_1,x_2,y_1,y_2,y_3\}$ változóra.

a) Pontosan mennyi $f(x_1,\ldots,x_m,y_1,\ldots,y_n)$ Boole-függvény szimmetrikus $\{x_1,\ldots,x_m\}$-re és $\{y_1,\ldots,y_n\}$-re?
b) E függvények közül mennyi monoton?
c) E függvények közül mennyi önduális?
d) E függvények közül mennyi monoton és önduális?

122. [*M25*] Folytatva a 110-es és a 121-es gyakorlatokat, megtaláljuk az összes olyan $f(x_1,x_2,x_3,$ $y_1,y_2,y_3,y_4,y_5,y_6)$ Boole-függvényt, amely szimmetrikus $\{x_1,x_2,x_3\}$-ra, szimmetrikus $\{y_1,y_2,\ldots,y_6\}$-ra, önduális, és reguláris. Ezek közül melyek küszöb függvények?

123. [*46*] Határozzuk meg azoknak a tíz változós, önduális függvényeknek a pontos számát, amelyek egyben küszöb függvények is.

124. [*20*] Keressük meg azokat a négyváltozós Boole-függvényeket, amelyek az **??**. táblázat alapszabályai szerint ekvivalensek 767 másik függvénnyel.

125. [*18*] A 95-ben lévő függvényosztályok közül melyek irányítók?

126. [*23*] (a) Mutassa meg, hogy egy Boole-függvény akkor és csak akkor irányító, ha prímimplikánsai és prímklózai rendelkeznek bizonyos egyszerű tulajdonsággal. (b) Mutassa meg, hogy egy

Boole-függvény akkor és csak akkor irányító, ha a Chow paraméterei $N(f)$ és $\Sigma(f)$ rendelkeznek bizonyos egyszerű tulajdonsággal (lásd T tétel). (c) Definiálja a

$$\vee(f) = \bigvee\{x \mid f(x) = 1\} \qquad \text{és} \qquad \wedge(f) = \bigwedge\{x \mid f(x) = 1\};$$

Boole-vektorokat hasonlóan a $\Sigma(f)$ egész vektorhoz. Mutassa meg, hogy lehetséges eldönteni csak a négy $\vee(f)$, $\vee(\bar{f})$, $\wedge(f)$, és $\wedge(\bar{f})$ vektor megadásával, hogy az f irányító-e vagy nem.

127. [*M25*] Mely irányító függvények (a) önduálisak? (b) definit Horn függvények?

128. [*20*] Keresse meg azt az $f(x_1, \ldots, x_n)$ nem irányító függvényt, amely pontosan két pontban igaz.

129. [*M25*] Hány darab n-változós irányító függvény létezik?

130. [*M21*] A 3. táblázat szerint a négy változós Boole-függvények között 168 monoton függvény van. Azonban ezek közül néhány, mint az $x \wedge y$-hoz hasonlók, csak három, vagy kevesebb változótól függnek.

a) Hány 4-változós monoton Boole-függvény tartalmazza? minden változóját?
b) E függvények közül hány olyan van, amelyek permutációra különbözőek lesznek, mint a **??**. táblázatban?

131. [*HM42*] A **??**. táblázat alapján világos, hogy sokkal több Horn-függvény van, mint Krom függvény. Mi a közelítő szám, amikor $n \to \infty$?

132. [*F30*] A $g(x) = g(x_1, \ldots, x_n)$ függvényt *affin* függvénynek hívjuk, ha felírható $y_0 \oplus (x_1 \wedge y_1) \oplus \cdots \oplus (x_n \wedge y_n) = (y_0 + x \cdot y) \mod 2$ alakban, bizonyos $y_0, y_1, \ldots, y_n$ Boole konstansokkal.

a) Adott egy $f(x)$ tetszőleges Boole-függvény, mutassuk meg, hogy bizonyos affin függvények megegyeznek $f(x)$-el $2^{n-1} + 2^{n/2-1}$ vagy több x pontban. Segítség: Legyen $s(y) = \sum_x (-1)^{f(x)+x\cdot y}$, és mutassuk meg, hogy $\sum_y s(y)s(y \oplus z) = 2^{2n}[z = 0\ldots0]$ minden z vektorra.
b) Az $f(x)$ Boole-függvényt *bent* függvénynek hívjuk, ha nincs olyan affin függvény, amelyik legfeljebb $2^{n-1} + 2^{n/2-1}$ pontban megegyezne vele. Igazoljuk, hogy

$$(x_1 \wedge x_2) \oplus (x_3 \wedge x_4) \oplus \cdots \oplus (x_{n-1} \wedge x_n) \oplus h(x_2, x_4, \ldots, x_n)$$

bent függvény, ha n páros és $h(y_1, y_2, \ldots, y_{n/2})$ tetszőleges.
c) Igazoljuk, hogy $f(x)$ akkor és csak akkor bent függvény, ha

$$\sum_x \big(f(x) \oplus f(x \oplus y)\big) = 2^{n-1} \qquad \text{for all } y \neq 0\ldots0.$$

d) Reprezentáljuk az $f(x_1, \ldots, x_n)$ bent függvényt egy mod 2 multilineáris polinommal, mint (19)-ben. Mutassuk meg, hogy ez sohasem tartalmaz olyan $x_1 \ldots x_r$ termeket, ahol $r > n/2 > 1$.

133. [*20*] (Mark A. Smith , 1990.) Tegyük fel, hogy n független érme feldobásával állítunk elő n véletlen bitet, ahol a k-adik érme p_k valószínűséggel eredményez 1-et. Válasszuk meg $(p_1, \ldots, p_n)$-t úgy, hogy $f(x_1, \ldots, x_n) = 1$ valószínűsége $(t_0 t_1 \ldots t_{2^n-1})_2/(2^{2^n} - 1)$ legyen, ahol $t_0 t_1 \ldots t_{2^n-1}$ az f Boole-függvény igazságtáblája. (Igy n egymásutáni véletlen érme 2^n-bit pontossággal képes generálni egy valószínűséget)

A 7.1.1. pont gyakorlatainak megoldása

1. (C. Sartena megoldása.) Subidu mondását $x \Rightarrow y$ alakú implikációkkal írhatjuk le, ahol az alany rendre y-t, x-et, x-et, y-t, y-t, x-et jelenti. (Más megoldás is lehetséges.)

2. A pincusi $x \circ y$-hoz tartozó földi művelet az $\overline{\bar{x} \circ \bar{y}}$. Az igazságtábláját emiatt úgy kapjuk meg, hogy a $\circ$ igazságtábla komplemensét megfordítjuk. Így a válaszok sorrendben $\top$, $\vee$, $\subset$, $\llcorner$, $\supset$, R, $\equiv$, $\wedge$, $\bar\wedge$, $\oplus$, $\overline{\mathsf{R}}$, $\bar\supset$, $\overline{\llcorner}$, $\bar\subset$, $\bar\vee$, $\perp$. (Bármely a 7.1. táblázat 16 műveletével kapcsolatos azonosság maga után von egy duális azonosságot, melyet a megfelelő pincusi műveletek behelyettesítésével nyerünk. Például De Morgan (11) és (12) törvényei egymás duálisai, mint ahogy az $\equiv$ és a $\oplus$ műveletekhez kötődő (3) és (4) azonosságok is. Ebben az értelemben az $\equiv$ éppen olyan hasznosnak tekinthető, mint duálisa, az $\oplus$.)

3. (a) $\vee$; (b) $\wedge$; (c) $\overline{\llcorner}$; (d) $\equiv$. (Valójában sok formula jobban működik, ha -1-et használunk az igazság és $+1$-et a hamisság kifejezésére, bár ez a jelölés szentségtörésnek tűnhet. Ilyenkor az $x \cdot y$ a $\oplus$ műveletnek felel meg. Vegyük észre, hogy $\langle xyz \rangle = \operatorname{sign}(x+y+z)$, bármelyik jelölést használjuk is.)

4. [41] (a) Kezdjük a $\llcorner$ és R igazságtáblákkal, ezután bitenként számítsuk ki az $\alpha \bar\wedge \beta$ igazságtábláját az α és a β igazságtáblák minden már ismert párjából úgy, hogy az eredményeket az egyes formulák hossza szerinti sorrendben generáljuk, és leírjuk a legrövidebb formulát, ami az adott 4-bites táblához vezet:

$\perp$: $(x \bar\wedge (x \bar\wedge x)) \bar\wedge (x \bar\wedge (x \bar\wedge x))$
$\wedge$: $(x \bar\wedge y) \bar\wedge (x \bar\wedge y)$
$\bar\supset$: $(x \bar\wedge (x \bar\wedge y)) \bar\wedge (x \bar\wedge (x \bar\wedge y))$
$\llcorner$: x
$\bar\subset$: $(y \bar\wedge (x \bar\wedge x)) \bar\wedge (y \bar\wedge (x \bar\wedge x))$
R: y
$\oplus$: $(y \bar\wedge (x \bar\wedge x)) \bar\wedge (x \bar\wedge (x \bar\wedge y))$
$\vee$: $(y \bar\wedge y) \bar\wedge (x \bar\wedge x)$

$\bar\vee$: $(x \bar\wedge (x \bar\wedge x)) \bar\wedge ((y \bar\wedge y) \bar\wedge (x \bar\wedge x))$
$\equiv$: $(x \bar\wedge y) \bar\wedge ((y \bar\wedge y) \bar\wedge (x \bar\wedge x))$
$\overline{\mathsf{R}}$: $y \bar\wedge y$
$\subset$: $y \bar\wedge (x \bar\wedge x)$
$\overline{\llcorner}$: $x \bar\wedge x$
$\supset$: $x \bar\wedge (x \bar\wedge y)$
$\bar\wedge$: $x \bar\wedge y$
$\top$: $x \bar\wedge (x \bar\wedge x)$

(b) Ebben az esetben négy táblázattal kezdjük: $\perp$, $\top$, $\llcorner$, R, és amennyiben azonos hosszúságú formulák között kell döntenünk, azt választjuk, amelyikben kevesebb változó fordul elő:

$\perp$: 0
$\wedge$: $(x \bar\wedge y) \bar\wedge 1$
$\bar\supset$: $((y \bar\wedge 1) \bar\wedge x) \bar\wedge 1$
$\llcorner$: x
$\bar\subset$: $(y \bar\wedge (x \bar\wedge 1)) \bar\wedge 1$
R: y
$\oplus$: $(y \bar\wedge (x \bar\wedge 1)) \bar\wedge ((y \bar\wedge 1) \bar\wedge x)$
$\vee$: $(y \bar\wedge 1) \bar\wedge (x \bar\wedge 1)$

$\bar\vee$: $1 \bar\wedge ((y \bar\wedge 1) \bar\wedge (x \bar\wedge 1))$
$\equiv$: $(x \bar\wedge y) \bar\wedge ((y \bar\wedge 1) \bar\wedge (x \bar\wedge 1))$
$\overline{\mathsf{R}}$: $y \bar\wedge 1$
$\subset$: $y \bar\wedge (x \bar\wedge 1)$
$\overline{\llcorner}$: $x \bar\wedge 1$
$\supset$: $(y \bar\wedge 1) \bar\wedge x$
$\bar\wedge$: $x \bar\wedge y$
$\top$: 1

5. (a) $\perp$: $x \bar\subset x$; $\wedge$: $(x \bar\subset y) \bar\subset y$; $\bar\supset$: $y \bar\subset x$; $\llcorner$: x; $\bar\subset$: $x \bar\subset y$; R: y; a további 10-et nem lehet kifejezni. (b) Konstansokat is használva ugyanakkor mind a 16 kifejezhető:

$\bot$: 0	$\overline{\vee}$: $y \,\overline{\subset}\, (x \,\overline{\subset}\, 1)$
$\wedge$: $(y \,\overline{\subset}\, 1) \,\overline{\subset}\, x$	$\equiv$: $(y \,\overline{\subset}\, x) \,\overline{\subset}\, ((x \,\overline{\subset}\, y) \,\overline{\subset}\, 1)$
$\overline{\supset}$: $y \,\overline{\subset}\, x$	$\overline{\mathsf{R}}$: $y \,\overline{\subset}\, 1$
$\llcorner$: x	$\subset$: $(x \,\overline{\subset}\, y) \,\overline{\subset}\, 1$
$\overline{\subset}$: $x \,\overline{\subset}\, y$	$\overline{\llcorner}$: $x \,\overline{\subset}\, 1$
R: y	$\supset$: $(y \,\overline{\subset}\, x) \,\overline{\subset}\, 1$
$\oplus$: $((y \,\overline{\subset}\, x) \,\overline{\subset}\, ((x \,\overline{\subset}\, y) \,\overline{\subset}\, 1)) \,\overline{\subset}\, 1$	$\overline{\wedge}$: $((y \,\overline{\subset}\, 1) \,\overline{\subset}\, x) \,\overline{\subset}\, 1$
$\vee$: $(y \,\overline{\subset}\, (x \,\overline{\subset}\, 1)) \,\overline{\subset}\, 1$	$\top$: 1

(Lásd Bernstein cikkét [5].)

6. (a) $\bot, \wedge, \llcorner, \mathsf{R}, \oplus, \vee, \equiv, \top$. (b) $\bot, \llcorner, \mathsf{R}, \oplus, \equiv, \top$. (Vegyük észre, hogy ezen műveletek mindegyike asszociatív. Valóban, a megadott azonosságból következik az általános asszociativitás törvény: először azt kapjuk, hogy (i) $(x{\circ}y){\circ}((z{\circ}y){\circ}w) = ((x{\circ}z){\circ}(z{\circ}y)){\circ}((z{\circ}y){\circ}w) = (x{\circ}z){\circ}w$, és hasonlóan (ii) $(x{\circ}(y{\circ}z)){\circ}(y{\circ}w) = x{\circ}(z{\circ}w)$. Továbbá (iii) $(x{\circ}y){\circ}(z{\circ}w) = (x{\circ}y){\circ}((z{\circ}y){\circ}(y{\circ}w)) = (x{\circ}z){\circ}(y{\circ}w)$ (i) alapján. Így $(x \circ z) \circ w = (x \circ z) \circ ((z \circ z) \circ w) = (x \circ (z \circ z)) \circ (z \circ w) = x \circ (z \circ w)$ (i), (iii) és (ii) alapján. Az $\{x_1, \ldots, x_n\}$ által generált szabad rendszernek pontosan $n + 2^n n^2$ különböző eleme van, egész pontosan $\{x_j \mid 1 \le j \le n\}$ és $\{x_i \circ x_{j_1} \circ \cdots \circ x_{j_r} \circ x_k \mid r \ge 0$ és $1 \le i, k \le n$ és $1 \le j_1 < \cdots < j_r \le n\}$.)

7. Az előzőekhez hasonlóan keressük az $y \circ (x \circ y) = x$ azonosságot. Ez csak a $\oplus$ és $\equiv$ műveletek esetén teljesül. (Jevons [?] könyvében leírta $\oplus$ ezen tulajdonságát, de nem vizsgálta részletesen a témát. Az ilyen természetű, „tapogatásnak” nevezett általános rendszerekkel a ??. pontban bővebben foglalkozunk.)

8. $(\{\bot, \wedge, \overline{\subset}\}, S_0)$, $(\{\top, \vee, \supset\}, S_1)$, $(\{\llcorner, \overline{\llcorner}\}, S_0 \cap S_1)$, $(\{\oplus, \equiv, \overline{\mathsf{R}}\}, S_2)$, $(\{\overline{\supset}, \overline{\vee}\}, S_0 \cap S_2)$, $(\{\subset, \overline{\wedge}\}, S_1 \cap S_2)$ és (R, bármelyik), ahol $S_0 = \{\diamond \mid 0 \diamond 0 = 0\}$, $S_1 = \{\diamond \mid 1 \diamond 1 = 1\}$ és $S_2 = \{\diamond \mid \bar{x}{\diamond}\bar{y} = \overline{x{\diamond}y}\} = \{\llcorner, \mathsf{R}, \overline{\llcorner}, \overline{\mathsf{R}}\}$. Vagyis a 256 párból 92 bal-disztributív. (Ezzel és a 6. gyakorlat problémáival először Schröder foglakozott, a halála után megjelent [?] könyvben. A probléma megoldását lényegében úgy fejezte ki, hogy leírta, a ($\circ$,$\diamond$) műveletek $(pqrs, wxyz)$ igazságtábláinak az alábbi egyenlőséget kell kielégíteniük: $((pq \vee rs) \wedge \bar{z}) \vee ((\bar{p}\bar{q} \vee \bar{r}\bar{s}) \wedge w) \vee ((p\bar{q} \vee r\bar{s}) \wedge ((w \equiv z) \vee (x \equiv y))) = 0$.)

9. (a) Hamis, $(x \oplus y) \vee z = (x \vee z) \oplus (y \vee z) \oplus z$. (b) Igaz, mert az azonosság nyilvánvalóan fennáll $z = 0$ és $z = 1$ esetén is. (c) Igaz, továbbá $(x \oplus y) \vee (y \oplus z) = 1 - [x = y = z]$.

10. A (16) felbontás első lépése a $g = 10100011$ és a $h = 10100011 \oplus 10010011 = 00110000$ igazságtáblákkal rendelkező függvényeket adja. Hasonlóan folytatva $1 + y + xz + w + wy + wx + wxz$ (modulo 2) adódik.

11. A kijelölt tag akkor és csak akkor jelenik meg, ha $f(x_1, \ldots, x_n)$ páratlan sokszor igaz, amikor $x_1 = x_4 = x_5 = x_7 = x_9 = x_{10} = \cdots = 0$. ($2^k$ olyan eset van, amikor k kivételével a többi változó értékét zérusnak rögzítjük.) Másképp fogalmazva a multilineáris reprezentáció kifejezhető olyan sokatmondó jelölés segítségével, mint $n = 3$ esetén a következő:

$$f(x, y, z) = (f_{000} + f_{00*}z + f_{0*0}y + f_{0**}yz + f_{*00}x + f_{*0*}xz + f_{**0}xy + f_{***}xyz) \mod 2,$$

ahol $f_{**0} = f(1, 1, 0) \oplus f(1, 0, 0) \oplus f(0, 1, 0) \oplus f(0, 0, 0)$ stb.

12. (a) (23)-ban helyettesítsük $\bar{w}$-t $1 - w$-vel, majd folytassuk így tovább. Végül az $1 - y - xz + 2xyz - w + wy + wx + wxz - 2wxyz$ kifejezést nyerjük. (Néhány szerző ezt „Zsegalkin-polinomnak” nevezi, bár maga Zsegalkin mindig modulo 2 dolgozott. További megnevezések az irodalomban: „elérhetőségi polinom”, „megbízhatósági polinom”, „karakterisztikus polinom”.)

(b) Egy n változós függvényhez tartozó együtthatók abszolút értéke legfeljebb 2^{n-1} (és indukcióval belátható, hogy tényleg ez a maximum.) Például az $x_1 \oplus \cdots \oplus x_n$ kifejezés egész számok feletti egész együtthatós multilineáris reprezentációja $e_1 - 2e_2 + 4e_3 - \cdots + (-2)^{n-1}e_n$, ahol e_k az $\{x_1, \ldots, x_n\}$ változók k-adik elemi szimmetrikus függvénye. Az előző megoldásban szereplő formula az egész számok felett

$$f(x,y,z) \;=\; f_{000} + f_{00*}z + f_{0*0}y + f_{0**}yz + f_{*00}x + f_{*0*}xz + f_{**0}xy + f_{***}xyz,$$

ahol $f_{**0} = f(1,1,0) - f(1,0,0) - f(0,1,0) + f(0,0,0)$, és így tovább. Ez a kiterjesztés az Hadamard-transzformációHadamard, Jacques Salomon (1865–1963) burkolt formája, lásd a 4.6.4. pontban (38)-at.

(c,d) Polinomunk $x_1(1-x_2)(1-x_3)x_4$-hez hasonló mintermek összege. $0 \le x_1, \ldots, x_n \le 1$ esetén minden minterm nemnegatív, és az összes minterm összege 1.

(e) $\partial f/\partial x_j = h(x) - g(x)$, ahol (d) szerint $h(x) \ge g(x)$. (Lásd a 21. gyakorlatot.) F valójában éppen az egész együtthatós multilineáris reprezentáció (lásd a 12. gyakorlatot).

13. Valójában Fpontosan az egész multilineáris reprezentáció (lásd a **??**. gyakorlatot).

14. Legyen $r_j = p_j/(1-p_j)$. Elvárásunkat figyelembe véve $f(0,0,0) = 0$ és $f(1,1,1) = 1 \Leftrightarrow r_1r_2r_3 > 1$, $f(0,0,1) = 0$ és $f(1,1,0) = 1 \Leftrightarrow r_1r_2 > r_3$, $f(0,1,0) = 0$ és $f(1,0,1) = 1 \Leftrightarrow r_1r_3 > r_2$, $f(0,1,1) = 0$ és $f(1,0,0) = 1 \Leftrightarrow r_1 > r_2r_3$. Tehát (a) $\langle x_1x_2x_3\rangle$; (b) x_1; (c) $\bar{x}_3$.

15. Az 1.2.6. pont 10. gyakorlata szerint $\binom{x}{k} \bmod 2 = [x\&k = k]$. Ennélfogva például amikor $x = (x_n \ldots x_1)_2$, akkor $\binom{x}{11} \equiv x_4 \wedge x_2 \wedge x_1$ (modulo 2), és ilyen módon kaphatunk meg minden tagot egy, a (19)-hez hasonló multilineáris reprezentációban. Sőt, nem szükséges modulo 2 vennünk a tagokat, mert az $\binom{x}{11}\binom{15-x}{4}$ interpolációs polinom pontosan az $x_4 \wedge \bar{x}_3 \wedge x_2 \wedge x_1$ formulát fejezi ki.

16. Igen, sőt még a $+$ műveletre is, mert a különböző mintermek egyidejűleg nem lehetnek igazak. (De nem tudjuk ezt megtenni a (25) általános diszjunktív normálformában. Lásd a 35. gyakorlatot.)

17. A $\overline{\wedge}$ bináris művelet nem asszociatív, ezért egy $x \,\overline{\wedge}\, y \,\overline{\wedge}\, z$-hez hasonló kifejezést *háromváltozós* műveletként kell interpretálni. Quick jelölése kitűnő, bár ha valaki a NAND-re n változós műveletként gondol, vegye körültekintően figyelembe, hogy *egyetlen* x változó NAND-je $\bar{x}$.

18. Ellenkező esetben ugyanis legyen $u_1 \leftarrow \cdots \leftarrow u_s \leftarrow 1$ és $v_1 \leftarrow \cdots \leftarrow v_t \leftarrow 0$, ami miatt f egyszerre kellene, hogy igaz és hamis legyen. (És ha egy DNF-fel kapcsolatban átgondoljuk a (2) disztributivitási törvény ismételt alkalmazását egészen addig, amíg KNF formulává nem válik, arra jövünk rá, hogy a megfordított állítás is igaz: a $v_1 \vee \cdots \vee v_t$ diszjunkció akkor és csak akkor adódik f-ből,vagy ha f minden implikánsával van közös literálja; ha f minden prímimplikánsával van közös literálja; vagy ha f valamely DNF-jének minden implikánsával van közös literálja.)

19. A 0010, 0011, 0101, 0110, 1000, 1001, 1010 és 1011 pontok által meghatározott maximális részkockák 0$*$10, 0101, $*$01$*$ és 10$**$, így a megoldás $(w\vee\bar{y}\vee z) \wedge (w\vee\bar{x}\vee y\vee\bar{z}) \wedge (x\vee\bar{y}) \wedge (\bar{w}\vee x)$. (Ez a KNF egyúttal a legrövidebb is.)

20. Igaz. A megfelelő maximális részkocka benne van az f' által és g' által meghatározott maximális részkockában és ezek metszete pedig nem lehet nagyobb. (Ez a megfigyelés Samsonnak és Millsnek köszönhető, akiknek [?] cikkére majd a 31. megoldásban is hivatkozunk.)

21. A (20)-as Boole-törvény alapján belátjuk, hogy egy n változós f függvény akkor és csak akkor monoton, ha az $(n-1)$ változós g és h projekciói monotonok, és teljesül, hogy $g \le h$. Ezért

$$f = (g \wedge \bar{x}_n) \vee (h \wedge x_n) \;=\; (g \wedge \bar{x}_n) \vee (g \wedge x_n) \vee (h \wedge x_n) \;=\; g \vee (h \wedge x_n),$$

így komplementálás nélkül tudunk dolgozni. A 0 és 1 konstans eltűnik, kivéve, ha a függvény azonosan konstans. Megfordítva pedig, a $\wedge$ és $\vee$ segítségével felépített bármely kifejezés nyilván monoton.

Megjegyzés a terminológiával kapcsolatban: Ha meg akarjuk őrizni a klasszikus matematika nyelvét, tulajdonképpen azt kellene mondanunk, hogy „monoton nem-csökkenő”, ahelyett, hogy egyszerűen azt mondjuk, „monoton”, mert egy valós változó csökkenő függvényét is monotonnak nevezzük. (Lásd például a 3.3.2. pontbeli „teszt futtatást”.) De a „nem-csökkenő” szó elég hosszú; ezért a Boole-függvényekkel foglalkozó kutatók csaknem egyöntetűen úgy döntöttek, elfogadják, hogy ilyen szövegkörnyezetben a „monoton” automatikusan magában foglalja, hogy nem-csökkenő. Hasonlóan, a „pozitív függvény” matematikai fogalommal rendszerint olyan függvényre hivatkozunk, amelyiknek az értéke nagyobb, mint nulla; de a „pozitív Boole-függvényről” író szerzők azokra a függvényre hivatkoznak így, amelyeket mi monotonnak nevezünk. Mivel egy monoton függvény megőrzi a rendezést, néhány szerző az „izoton” kifejezést használja; de ezt a szót már használják a fizikusok, vegyészek és zenetudósok is.

Egy az $\bar{x} \vee y$-hoz hasonló Boole-függvényt, amelyik monotonná válik, ha bizonyos változóit komplementáljuk, *unate*-nek hívunk. A Q tétel nyilván unate függvényekre vonatkozik.

22. Mind g, mind $g \oplus h$ monoton kell legyen, és $g(x) \wedge h(x) = 0$ kell teljesüljön.

23. $x \wedge (v \vee y) \wedge (v \vee z) \wedge (w \vee z)$. (A Q következmény monoton függvények *konjunktív* prímformáira is vonatkozik. Emiatt bármelyik ilyen probléma megoldásához csak a (2) disztributivitás törvényének alkalmazására van szükség addig, ameddig $\wedge$ már nem fordul elő $\vee$ belsejében, majd el kell távolítani minden olyan klózt, amelyik egy másik összes változóját tartalmazza.)

24. k-ra vonatkozó indukció szerint egy a gyökerében $\vee$-t tartalmazó hasonló fa $2_{2\lceil k/2\rceil -1}$ darab $2_{\lfloor k/2\rfloor}$ hosszú prímimplikánst tartalmazó formulát ad, míg a $\wedge$ gyökerű fa $4_{2\lfloor k/2\rfloor -1}$ darab $2_{\lceil k/2\rceil}$ hosszú prímimplikánst. Ha például $k = 6$, a $\wedge$ gyökerű fa esetében a $4^7 = 2^{14}$ különböző prímimplikáns a következő alakú:

$$x_{(0t_0 0t_{00} 0t_{000})_2} \wedge x_{(0t_0 0t_{00} 1t_{001})_2} \wedge x_{(0t_0 1t_{01} 0t_{010})_2} \wedge x_{(0t_0 1t_{01} 1t_{011})_2} \\ \wedge x_{(1t_1 0t_{10} 0t_{100})_2} \wedge x_{(1t_1 0t_{10} 1t_{101})_2} \wedge x_{(1t_1 1t_{11} 0t_{110})_2} \wedge x_{(1t_1 1t_{11} 1t_{111})_2},$$

ahol a t vagy 0, vagy 1. (Ilyen Boole-függvényekkel kapcsolatos további információkért lásd Knuth és Moore [23], továbbá Gurvich és Khachiyan [16] cikkeit.)

25. Jelölje a_n a választ. Ekkor $a_2 = a_3 = 2$, $a_4 = 3$, és $n > 4$-re $a_n = a_{n-2} + a_{n-3}$, mert $n > 4$ esetén a prímimplikánsok vagy $p_{n-2} \wedge x_{n-1}$, vagy $p_{n-3} \wedge x_{n-2} \wedge x_n$ alakúak, ahol p_k egy a k-változós esetben előálló prímimplikánst jelöl. (Ezek a prímimplikánsok a P_n útgráf csúcsainak minimális lefedései, és a 35. gyakorlat értelmében „kifejthetők”, amikor lexikografikus sorrendben vannak listázva. Ekkor $a_n = (7P_n + 10P_{n+1} + P_{n+2})/23$, ahol P_n a **??**. gyakorlat Perrin-száma.)

26. (a) Legyen $x_j = [j \in J]$. Ekkor $f(x) = 0$ és $g(x) = 1$. (Ezt a 18. gyakorlatból tudjuk.)

(b) Tegyük fel például, hogy $k \in J \in \mathcal{G}$, de $k \notin \bigcup_{I \in \mathcal{F}} I$, és hogy az (a) feltétel vizsgálatát elszalasztottuk. Legyen $x_j = [j \in J \text{ és } j \neq k]$. Ekkor $f(x) = 1$, és mert minden $J' \in \mathcal{G}$ $(J' \neq J)$ tartalmaz egy $\notin J$ elemet, ezért $g(x) = 0$.

(c) Tegyük fel megint, hogy az (a) feltétel ellenőrzését elszalasztottuk. Ha mondjuk $|J| > |\mathcal{F}|$, legyen $x_j = [j$ $I \cap J$ legkisebb eleme valamely $I \in \mathcal{F}$-re]. Ekkor $f(x) = 1$ és $g(x) = 0$.

(d) Most tegyük fel, hogy $\bigcup_{I \in \mathcal{F}} I = \bigcup_{J \in \mathcal{G}} J$. Minden egyes $J \in \mathcal{G}$ $2_{n-|J|}$ olyan vektort jelez, ahol $f(x) = 0$, $J \in \mathcal{G}$ pedig hasonlóan $2_{n-|J|}$ olyan vektort, ahol $g(x) = 1$. Ha az s összeg kisebb, mint 2^n, számolhatjuk az $s = s_0 + s_1$-et, ahol s_0 azt jelenti, hogy $x_n = 0$ esetén mennyi járult hozzá az s-hez. Ha $s_0 < 2^{n-1}$, legyen $x_n \leftarrow 0$, egyébként pedig $s_1 < 2^{n-1}$, így legyen $x_n \leftarrow 1$. Aztán legyen $n \leftarrow n - 1$. Végül minden x_j ismert lesz, és ekkor $f(x) = 1$, $g(x) = 0$.

27. Legyen $m = \min\bigl(\{|I| \mid I \in \mathcal{F}\} \cup \{|J| \mid J \in \mathcal{G}\}\bigr)$ a legrövidebb prímklóz vagy prímimplikáns hossza. Ekkor $N \cdot 2^{n-m} \geq \sum_{I \in \mathcal{F}} 2_{n-|I|} + \sum_{J \in \mathcal{G}} 2_{n-|J|} \geq 2^n$, így $m \leq \lg N$. Ha mondjuk $|I| = m$, valamely k index meg kell jelenjen a $J \in \mathcal{G}$ elemek közül legalább $1/m$-ben, mert minden J metszi I-t. Ez az észrevétel azt bizonyítja, amit a gyakorlat „segítségében” javasoltunk.

Most legyen $A(0) = A(1) = 1$, és $v > 1$-re $A(v) = 1 + A(v-1) + A(\lfloor \rho v \rfloor)$. Ekkor $A(|\mathcal{F}||\mathcal{G}|)$ a rekurzív hívások számának (X1 végrehajtásai számának) felső korlátja. Ha $B(v) = A(v)+1$, akkor $v > 1$-re $B(v) = B(v-1)+B(\lfloor \rho v \rfloor)$, ezért $v > k$-ra $B(v) \le B(v-k)+kB(\lfloor \rho v \rfloor)$. $k = v - \lfloor \rho v \rfloor$ azt mutatja, hogy $B(v) \le ((1-\rho)v+2)B(\lfloor \rho v \rfloor)$. Ezért $B(v) = O(((1-\rho)v+2)^t)$, amikor $\rho^t v \le 1$, azaz amikor $t \ge \ln v/\ln(1/\rho) = \Theta((\lg v)(\lg N))$. Következésképpen $A(|\mathcal{F}||\mathcal{G}|) \le \mathcal{A}(\mathcal{N}^{\in}/\triangle) = \mathcal{N}_{\mathcal{O}(\lg \mathcal{N})^{\in}}$.

A gyakorlatban az algoritmus sokkal gyorsabban fog futni, mint ahogy a most kinyert pesszimista korlátok mutatják. Mivel egy függvény prímklózai duáljának prímimplikánsai, ez a probléma lényegében ugyanaz, mint annak ellenőrzése, hogy egy adott DNF egy másik duálja-e. Továbbá ha $f(x) = 0$-val kezdünk, és ismételten keressük azon minimális x-eket, ahol $f(x) = g(\bar{x}) = 0$, f-et addig „növelhetjük”, amíg g duáljához nem jutunk.

Az itt bemutatott ötlet Fredmantól és Khachiyantól származik, akik javításokat is kidolgoztak a [15] publikációban a futási idő $N^{O(\lg N/\lg\lg N)}$-re csökkentésére. Polinom idejű algoritmus nem ismert, de azért nem valószínű, hogy a probléma NP-teljes, mert meg tudjuk oldani kevesebb, mint exponenciális időben.

28. Az eredmény nyilvánvaló mihelyt megértjük, de a jelölések és a terminológia zavarba hozóak. Ezért gondoljunk végig egy konkrét példát: ha mondjuk $y_1 = y_4 = y_6 = 1$ és a többi y_k zérus, a g függvény akkor és csak akkor igaz, ha a p_1, p_4 és p_6 prímimplikánsok lefedik az összes olyan pontot, ahol f igaz. Ekképpen láthatjuk, hogy kölcsönösen egyértelmű kapcsolat van g prímimplikánsai és f csak a p_j prímimplikánsokat tartalmazó DNF-jei között. A leképezésben g prímimplikánsai megfelelnek azoknak a „nem redundáns” DNF-eknek, amelyekben nem lehet p_j-t figyelmen kívül hagyni.

Cutler és Muroga ennek az elvnek számos tökéletesítését tárgyalja a [8] cikkben.

29. (Az 5.19. gyakorlatban hasonló eljárásokat vizsgáltunk.)

- **B1.** (Kezdőértékek beállítása.) Legyen $k \leftarrow k' \leftarrow 0$.
- **B2.** (Keressünk egy nullát.) Ha kell, növeljük k-t, amíg nem lesz vagy $k = m$ (vége), vagy $v_k \& 2^j = 0$.
- **B3.** (Állítsunk elő egy $k' > k$-t.) Ha $k' \le k$, legyen $k' \leftarrow k+1$.
- **B4.** (Próbálkozzunk k'-vel.) Ha kell, növeljük k'-t, amíg nem lesz vagy $k' = m$ (vége), vagy $v_{k'} \ge v_k + 2^j$.
- **B5.** (Ugorjunk túl egy hibás párost.) Ha $v_k \oplus v_{k'} \ge 2^{j+1}$, legyen $k \leftarrow k'$, és térjünk vissza B2-re.
- **B6.** (Rögzítsünk egy párosítást.) Ha $v_{k'} = v_k + 2^j$, (k, k') egy eredménypár.
- **B7.** (Próbálkozzunk k-val.) Legyen $k \leftarrow k+1$, és térjünk vissza B2-re. ■

(A B3 és B5 lépések elhagyhatók, bár ajánljuk őket.)

30. A következő algoritmus változó hosszúságú rendezett listákat kezel egy olyan S verem segítségével, amelynek a mérete sohasem haladja meg a $(2m+n)$-et. Amikor a verem teteje $S_t = s$, a felső lista az $S_s < S_{s+1} < \cdots < S_{t-1}$ rendezett halmaz. A jelző biteket egy másik, az S-sel (kezdőértékek beállítását követően) megegyező méretű T veremben kezeljük.

- **P1.** (Kezdőértékek beállítása.) Legyen $0 \le k < m$-re $T_k \leftarrow 0$. Ekkor $0 \le j < n$-re alkalmazzuk a 29. gyakorlat j-társ pásztázó algoritmusát, és minden (k, k') megtalált párra legyenek $T_k \leftarrow T_k + 2^j$, $T_{k'} \leftarrow T_{k'} + 2^j$. Aztán legyen $s \leftarrow t \leftarrow 0$, és ismételjük a következőket, amíg $s = m$ nem lesz: ha $T_s = 0$, kiírjuk a $(0, v_s)$ részkockát, és legyen $s \leftarrow s+1$; egyébként pedig legyen $S_t \leftarrow v_s$, $T_t \leftarrow T_s$, $t \leftarrow t+1$, $s \leftarrow s+1$. Végül legyen $A \leftarrow 0$ és $S_t \leftarrow 0$.
- **P2.** (Próbálkozzunk A-val.) (Ebben a részben az S verem részkockák $\nu(A)+1$ számú listáját tartalmazza. Mégpedig ha $A = 2^{e_1} + \cdots + 2^{e_r}$ miközben $e_1 > \cdots > e_r \ge 0$, a verem az összes olyan $(a, b) \subseteq V$ részkockának a b értékeit tartalmazza, ahol az a értékek rendre 0, 2^{e_1}, $2^{e_1} + 2^{e_2}$, …, A, eltekintve attól, hogy azok a részkockák, amelyek jelei nullák, nem jelennek meg. Esetleg az utolsót kivéve, ezek a listák nemüresek. Most A-t a következő lehetséges értékre fogjuk növelni.) Legyen $j \leftarrow 0$. Ha $S_t = t$ (azaz ha a felső lista üres),

ha szükséges, növeljük j-t, amíg nem lesz $j \geq n$ vagy $A\&2^j \neq 0$. Aztán amíg $j < n$ és $A\&2^j \neq 0$, legyen $t \leftarrow S_t - 1$, $A \leftarrow A - 2^j$ és $j \leftarrow j + 1$. Fejezzük be az algoritmust, ha $j \geq n$; egyébként pedig legyen $A \leftarrow A + 2^j$. **P3.** (Hozzuk létre az A listát.) Legyenek $r \leftarrow t$, $s \leftarrow S_t$, és alkalmazzuk a 29. gyakorlat j-társ pásztázó algoritmusát az $r - s$ számú $S_s < \cdots < S_{r-1}$ értékekre. Minden (k, k') megtalált pár esetén, legyen $x \leftarrow (T_k\&T_{k'}) - 2^j$; és ha $x = 0$, írjuk ki az (A, S_k) részkockát mint eredményt, egyébként legyen $t \leftarrow t + 1$, $S_t \leftarrow S_k$, $T_t \leftarrow x$. Végül legyen $t \leftarrow t + 1$, $S_t \leftarrow r + 1$, és térjünk vissza a P2 lépésre. ■

Ez az algoritmus részben Morreale [34] ötletén alapul. A futási idő lényegében (a P1 lépés miatt) mn-nel és a V-beli részkockák számával arányos. Ha $m \leq 2^n(1 - \epsilon)$, és ha az m méretű V-t véletlenül választjuk, a 34. gyakorlatban megmutatjuk, hogy a részkockák átlagos száma legfeljebb $O(\lg\lg n/\lg\lg\lg n)$-szorosa a maximális részkockák átlagos számának. Így a legtöbb esetben az átlagos futási idő közel arányos az előállított eredmény-részkockák átlagos mennyiségével. Másrészt pedig a 32. és 116. gyakorlatokban megmutatjuk, hogy az előállított output nagy mennyiségű lehet.

31. (a) Legyenek $c = c_{n-1} \ldots c_0$, $c' = c'_{n-1} \ldots c'_0$, $c'' = c''_{n-1} \ldots c''_0$. Ekkor kell, hogy legyen olyan j, hogy $c_j \neq *$ és $c_j \neq c''_j$; ellenkező esetben $c'' \subseteq c$ lenne. Ehhez hasonlóan kell, hogy legyen olyan k, hogy $c'_k \neq *$ és $c'_k \neq c''_k$. Ha $j \neq k$, lenne olyan $x_{n-1} \ldots x_0 \in c''$ pont, ami sem c-ben, sem c'-ben nincs benne, mert $x_j = \bar{c}_j$ és $x_k = \bar{c}'_k$. Ezért $j = k$, és j értéke egyértelműen meg van határozva. Továbbá könnyű belátni, hogy $c'_j = \bar{c}_j$. És ha $i \neq j$, akkor vagy $c_i = *$, vagy $c_i = c''_i$, továbbá vagy $c'_i = *$, vagy $c'_i = c''_i$.

(b) Ez az állítás (a) nyilvánvaló következménye.

(c) Először bebizonyítjuk, hogy az E2 lépésben zárójelbe tett megállapítás igaz, valahányszor ez a lépés sorra kerül. $j = 0$ esetben az állítás nyilvánvalóan igaz. Egyébként legyen $c \subseteq V$ j-kocka, és tegyük fel, hogy $c = c_0 \cup c_1$, ahol c_0 és c_1 $(j-1)$-kockák. Az E2 lépés előző végrehajtása során viszont azt kaptuk, hogy $c_0 \subseteq c'_0 \in C$ és $c_1 \subseteq c'_1 \in C$ valamely c'_0-ra és c'_1-re; ezért vagy $c \subseteq c'_0 \sqcup c'_1$, vagy $c \subseteq c'_0$, vagy $c \subseteq c'_1$. Mindegyik esetben c benne van C valamelyik elemében.

Bebizonyítjuk másrészt, hogy az E3 lépésben kapott eredmények éppen a V-beli maximális j-kockák. Legyen $c \subseteq V$ k-kocka. Ha c maximális, amikor $j = k$-val érünk el az E3 lépéshez, akkor c C-beli lesz, és ez lesz az eredmény. Ha c nem maximális, amikor az E3 lépést elérjük, akkor pedig van valamely $c'' \in C$ részkockában benne levő $c' \subseteq V$ k-kocka társa. Mivel $c \not\subseteq c''$, a $c \sqcup c''$ konszenzus C' $(j+1)$-kockája, és c nem lesz output.

Hivatkozások: A konszenzus fogalmát először Blake definiálta [?] Ph.D. értekezésében, lásd [?]. A fogalmat Samson és Mills egymástól függetlenül újból kitalálta ([?]). A műveletet néha *rezolválásnak* nevezik, amióta Robinson általánosabb formában (de inkább csak a klózokra, mint az implikánsokra vonatkozóan) – mint a tételbizonyításhoz használt „rezolúciós elvének” alapját – használta ([40]). Az E algoritmus Ewingnek, Rothnak és Wagnernek tulajdonítható ([12]).

32. (a) Cseréljük ki a 31. gyakorlatban megadott $\sqcup$ definíciót az $A = \{0, 1, *, \bullet\}$ négyelemű szimbólumhalmazon értelmezett következő asszociatív és kommutatív műveletre: minden $a \in A$-ra és $x \in \{0, 1\}$-re

$$* \sqcup a = a \sqcup * = a, \qquad \bullet \sqcup a = a \sqcup \bullet = x \sqcup \bar{x} = \bullet \qquad \text{és} \qquad x \sqcup x = x.$$

Legyenek $h(0) = 0$, $h(1) = 1$, $h(*) = *$ és $h(\bullet) = *$. Ekkor $c = h(c_1 \sqcup \cdots \sqcup c_m)$ – komponensenként számolva – akkor és csak akkor általánosított konszenzus, ha ez a részkocka benne van $c_1 \cup \cdots \cup c_m$-ben. (Lásd Tison [?] dolgozatát.)

(b) Legyen például $c_j = *^{j-1}1*^{m-j}1^{j-1}0*^{m-j}$. (Az utolsó komponens felesleges. Sloan, Szörényi és Turán [?] írásában jellemezte az összes megoldást.)

(c) (a) szerint minden prímimplikáns egyértelműen megfelel a vele „találkozó” implikánsok részhalmazának (Chandra és Markowsky, [7]).

(d) Mint (b)-ben például az $(y_1 \wedge \bar{x}_1) \vee (y_2 \wedge x_1 \wedge \bar{x}_2) \vee \cdots \vee (y_m \wedge x_1 \wedge \cdots \wedge x_{m-1} \wedge \bar{x}_m)$ (Laborde, [26]).

33. (a) $\binom{2^n-2^{n-k}}{m-2^{n-k}}/\binom{2^n}{m}$.

(b) Ki kell zárnunk azokat az eseteket, amikor $x_1\wedge\cdots\wedge x_{j-1}\wedge\bar{x}_j\wedge x_{j+1}\wedge\cdots\wedge x_k$ is implikáns. A logikai szita elve alapján

$$\sum_l \binom{k}{l}(-1)^l\binom{2^n-(l+1)2^{n-k}}{m-(l+1)2^{n-k}}\Big/\binom{2^n}{m}$$

a válasz; ami $\binom{2^n-n-1}{m-1}/\binom{2^n}{m}$-re egyszerűsíthető, amikor $k=n$.

34. (a) $c(m,n)=\sum c_j(m,n)$, ahol $c_j(m,n)=2^{n-j}\binom{n}{j}\binom{2^n-2^j}{m-2^j}/\binom{2^n}{m}$ az $n-j$ literált tartalmazó implikánsok átlagos száma (a 30. gyakorlatban megadott terminológia szerint a j dimenziós részkockák átlagos száma). Világos, hogy $c_0(m,n)=m$, és

$$c_1(m,n)=\frac{nm(m-1)}{2(2^n-1)}\le\frac{mn}{2}\Big(\frac{m}{2^n}\Big)\le\frac{1}{2}m;$$

hasonlóan $c_j(m,n)\le m/(2^j j!n^{2^j-1-j})$. $p(m,n)=\sum_j p_j(m,n)$, ahol

$$\begin{aligned}p_0(m,n)=2^n\binom{2^n-n-1}{m-1}\Big/\binom{2^n}{m}&=m\frac{(2^n-n-1)^{\underline{m-1}}}{(2^n-1)^{\underline{m-1}}}\ge m\frac{(2^n-n-m)^{m-1}}{(2^n-m)^{m-1}}\\&\ge m\Big(1-\frac{n}{2^n-m}\Big)^m\ge m\Big(1-\frac{n}{2^n-2^n/n}\Big)^{2^n/n}=m\exp\Big(\frac{2^n}{n}\ln\Big(1-\frac{n^2}{2^n(n-1)}\Big)\Big).\end{aligned}$$

(b) Vegyük észre, hogy $t=\lfloor\lg\lg n-\lg\lg(2^n/m)+\lg(4/3)\rfloor\le\lg\lg n+O(1)$ elég kicsi. Újra meg újra felhasználjuk, hogy $\binom{2^n-j\cdot 2^t}{m-j\cdot 2^t}/\binom{2^n}{m}<\alpha_{mn}^j$, és valóban, amikor j nem túl nagy,

$$\binom{2^n-j\cdot 2^t}{m-j\cdot 2^t}\Big/\binom{2^n}{m}\;=\;\alpha_{mn}^j(1+O(j^2 2^{2t}/m))$$

rendkívül jó közelítés. Hogy megalapozzuk a gyakorlat „útmutatásában" bizonyítani javasolt állítást, figyeljük meg, hogy $\sum_{j<t}c_j(m,n)/c_t(m,n)=O(tc_{t-1}(m,n)/c_t(m,n))=O(t^2/(n\sqrt{\alpha_{mn}}))=O((\lg\lg n)^2/n^{1/3})$, továbbá $c_{t+j}(m,n)/c_t(m,n)=O((n/(2t))^j\alpha_{mn}^{2^j-1})$. Következésképpen $c(m,n)/c_t(m,n)\approx 1+\frac{1}{2}\binom{n-t}{t+1}\alpha_{mn}$, ahol a második kifejezés dominál, amikor α_{mn} nagy értékű. Továbbá

$$\sum_l\binom{n-t}{l}(-1)^l\alpha_{mn}^l\Big(1+O\Big(\frac{l^2 2^{2t}}{m}\Big)\Big)\;=\;(1-\alpha_{mn})^{n-t}+O(n^2\alpha_{mn}(1+\alpha_{mn})^n 2^{2t}/m)$$

exponenciálisan kicsi hibatagot tartalmaz, mert $(1+\alpha_{mn})^n=O(e^{n^{1/3}})\ll m$. Így $p(m,n)/c_t(m,n)$ aszimptotikusan $e^{-n\alpha_{mn}}+\frac{1}{2}\binom{n-t}{t+1}\alpha_{mn}e^{-n\alpha_{mn}^2}$.

(c) $\alpha_{mn}=2^{-2^t}\approx n^{-1}\ln(t/\ln t)$, így $c(m,n)/c_t(m,n)=1+O(t^{-1}\lg t)$, $p(m,n)/c_t(m,n)=t^{-1}\ln t+\frac{1}{2}t^{-1}\ln t+O(t^{-1}\lg\lg t)$. Ebben az esetben arra következtethetünk, hogy

$$\frac{c(m,n)}{p(m,n)}\;=\;\frac{2}{3}\frac{\lg\lg n}{\lg\lg\lg n}\Big(1+O\Big(\frac{\lg\lg\lg\lg n}{\lg\lg\lg n}\Big)\Big).$$

(d) Ha $n\alpha_{mn}\le\ln t-\ln\ln t$, akkor $p(m,n)/c(m,n)\ge p_t(m,n)/c(m,n)\ge t^{-1}\ln t+O(t^{-1}\lg t)^2$. Másrészt, ha $n\alpha_{mn}\ge\ln t-\ln\ln t$, akkor $p(m,n)/c(m,n)\ge p_{t+1}(m,n)/c(m,n)\ge\frac{1}{2}t^{-1}\ln t+O(t^{-1}\lg\lg t)$.

(A $c(m,n)$ és $p(m,n)$ átlagokat, továbbá $c(m,n)$ szórásnégyzetét először Mileto és Putzolu tanulmányozta a [32] dolgozatban. Az olyan véletlen Boole-függvények implikánsaival, prímimplikánsaival és redundancia mentes DNF-jeivel kapcsolatos részletekbe menő aszimptotikus információk, amikor minden $f(x_1,\ldots,x_n)$ érték a többitől függetlenül $p(n)$ valószínűséggel 1, Weber [?] munkájából származnak.)

35. (a) A koordináták átrendezésével elérhetjük, hogy a p-edik részkocka $0^k 1^u *^v$, azaz $B_p = 0^k 1^u 0^v$ és $S_p = 1^k 0^{u+v}$. Ekkor p-re vonatkozó indukció szerint $*^k 1^u *^v$ minden pontja lefedett, mert $1 \leq j \leq k$-ra $*^{j-1} 1 *^{k-j} 1^u *^v$ minden pontja lefedett.

(b) A j-edik és k-adik részkockák minden olyan koordináta-pozícióban különböznek, ahol $B_j \& S_k$ nem nulla. Másrészt ha $B_j \& S_k$ nulla, a k részkocka $\bar{S}_k$ pontja – (a) szerint – egy előző részkockában fekszik, mert $\bar{S}_k \supseteq B_j$.

(c) Az 1100, $1\underline{0}11$, $\underline{0}011$ listából az $(x_1 \wedge x_2) \vee (x_1 \wedge \bar{x}_2 \wedge x_3 \wedge x_4) \vee (\bar{x}_1 \wedge x_3 \wedge x_4)$ ortogonális DNF-et nyerjük. (Az S_k bitjei vannak aláhúzva.)

(d) Nyolc megoldás van. Például $(01100, 0\underline{0}110, 00\underline{0}11, 11\underline{0}1\underline{0}, 11\underline{000})$.

(e) $(001100, 011\underline{0}00, 00\underline{0}110, 11\underline{00}10, 11\underline{0}0\underline{0}0, \underline{0}1\underline{00}11, 0\underline{000}11)$ szimmetrikus megoldás. És sokkal több lehetőség is van, például az $\{110000, 011000, 001100, 000110, 000011, 110010, 011010\}$ bitkódok 42 permutációja kifejtés.

(Ball és Provan [4] publikációban vezette be monoton Boole-függvények esetén a kifejtés fogalmát, és sok fontos alkalmazást is tárgyaltak.)

36. Ha $j < k$, valamely α, β, γ füzérekre $B_j = \alpha 1 \beta$ és $B_k = \alpha 0 \gamma$. Készítsük el az $x_0 = \alpha 1 \gamma$, $x_1 = x_0'$, …, $x_l = x_{l-1}'$ sorozatot, ahol $x_l = \alpha 0 0^{|\gamma|}$. Ekkor $f(x_0) = 1$, mivel $x_0 \supseteq B_k$, de $f(x_l) = 0$ mivel $x_l \subseteq B_j'$. Így azon x_i füzér, melyre $f(x_i) = 1$ és $f(x_{i+1}) = \cdots = f(x_l) = 0$, B-ben van, megelőzi B_k-t és igazolja, hogy $B_j \& S_k \supseteq 0^{|\alpha|} 1 0^{|\beta|}$.

(Ez a konstrukció és a 35. gyakorlat részei Boros, Crama, Ekin, Hammer, Ibaraki és Kogan [6] cikkének köszönhetők.)

37. A $(000011$, $0011\underline{0}1$, $00110\underline{0}$, $11\underline{0}1\underline{0}1$, $11\underline{0}10\underline{0}$, $110\underline{00}1$, $110\underline{0}0\underline{0})$ kifejtés sorrend az n-re vonatkozó általános jegyeket is kiemeli. Vannak ugyanakkor az $(110{*}{*}{*}$, $1110{*}{*}$, ${*}{*}110{*}$, ${*}{*}1110$, $0{*}{*}{*}11$, $10{*}{*}11$, $111111)$ ciklikusan szimmetrikushoz hasonló érdekes megoldások is, melyek nem a kiterjesztésen alapszanak.

Az alsó korlát meghatározásához rendeljünk minden x ponthoz egy $w_x = -\prod_{j=1}^{n}(x_{2j-1} + x_{2j} - 3x_{2j-1}x_{2j})$ súlyt, és vegyük észre, hogy egy részkockában szereplő összes x feletti w_x összeg 0 vagy ± 1. (Elegendő ezt a furcsa tényt az $n = 1$ esetben előálló kilenc lehetséges részkockára igazolni.) Most válasszunk diszjunkt részkockáknak egy halmazát, ami $F = \{x \mid f(x) = 1\}$-et részekre osztja. Ekkor

$$\sum_{C \text{ választott}} 1 \;\geq\; \sum_{C \text{ választott}} \sum_{x \in C} w_x \;=\; \sum_{x \in F} w_x \sum_{C \text{ választott}} [x \in C] \;=\; \sum_{x \in F} w_x.$$

$\binom{n}{k} 2^{n-k}$ olyan x vektor van, amelyben pontosan k darab $x_{2j-1}x_{2j} = 1$ pár van, és a súly nem nulla. Ezért $\sum_{x \in F} w_x = \sum_{k>0} \binom{n}{k} 2^{n-k} (-1)^{k-1} = 2^n - (2-1)^n$. (Lásd Ball és Nemhauser [3] munkáját.)

38. Egyáltalán nem. Egy DNF akkor és csak akkor kielégíthető, ha van legalább egy implikánsa. Egy DNF-fel kapcsolatban azt a problémát nehéz eldönteni, vajon *tautológia-e* (mindig igaz-e), vagy sem.

39. Rendeljük preorder sorrendben az egyes belső csúcsokhoz az $y_1, \ldots, y_N$ változókat, azaz a fa minden egyes csúcsa F pontosan egy változójának felel meg. Minden egyes olyan y belső csúcshoz, melynek gyermekei (l, r) és címkéje a $\circ$ kétváltozós művelet, készítsünk négy $c_{00} \wedge c_{01} \wedge c_{10} \wedge c_{11}$ 3KNF klózt, ahol

$$c_{pq} = (y^{\overline{p \circ q} N} \vee l^{pN} \vee r^{qN}),$$

és N komplemens-képzést jelöl (azaz $x^{0N} = x$ és $x^{1N} = \bar{x}$). Ezek a klózok tulajdonképpen azt állítják, hogy $y = l \circ r$. Például ha a $\circ$ művelet éppen $\wedge$, a négy klóz $(\bar{y} \vee l \vee r) \wedge (\bar{y} \vee l \vee \bar{r}) \wedge (\bar{y} \vee \bar{l} \vee r) \wedge (y \vee \bar{l} \vee \bar{r})$. Végül adjunk meg még egy klózt, az $(y_1 \vee y_1 \vee y_1)$-t, hogy $F = 1$ legyen.

Minden magasabb szám előállítható hármasok egyszerű összeillesztésével.

Tekintsük azt a ténynégyest, hogy A eladja B-t C-nek D áron.
Ez két tény összetettje:
először is A egy bizonyos ügyletet bonyolít le C-vel, amit E-vel jelölhetünk,
másodszor, ez az E ügylet a B eladása D összegért.

— CHARLES S. PEIRCE, *A Guess at the Riddle* (1887) [?]

40. Ha követjük az „útmutatást”, A azt jelenti, hogy „$u < v \oplus v < u$”, B pedig azt, hogy „$u < v \wedge v < w \Rightarrow u < w$”. Ekkor $A \wedge B$ azt jelenti, hogy a csúcsoknak van $u_1 < u_2 < \cdots < u_n$ lineáris rendezése. ($n!$ féleképpen elégíthető ki $A \wedge B$.) C azt jelenti, hogy q_{uvw} és $u < v < w$ ekvivalensek, ezért D azt jelenti, hogy u és w a rendezés szerint nem követik egymást, ha $u \not— w$. Tehát $A \wedge B \wedge C \wedge D$ akkor és csak akkor elégíthető ki, ha van olyan lineáris rendezés, mely szerint a gráfban egymással nem szomszédos csúcsok nem követik egymást (azaz a rendezés szerint egymást követő csúcsok a gráfban szomszédosak).

41. 0. megoldás: Az „$[m \leq n]$” egy ilyen formula, de ez nem felel meg a gyakorlat szellemének.

1. megoldás: Jelentse x_{jk} azt, hogy a j-edik galamb a k-adik dúcot lakja. Ekkor a klózok a következők: minden $1 \leq j \leq m$-re $(x_{j1} \vee \cdots \vee x_{jn})$ és minden $1 \leq i < j \leq m$-re és $1 \leq k \leq n$-re $(\bar{x}_{ik} \vee \bar{x}_{jk})$. (Lásd Cook és Reckhow, [?]; Haken, [?].)

2. megoldás: Tegyük fel, hogy $n = 2^t$, és lakjon a j-edik galamb az $(x_{j1} \ldots x_{jt})_2$ dúcban. $1 \leq i < j \leq m$-re az $\big((x_{i1} \oplus x_{j1}) \vee \cdots \vee (x_{it} \oplus x_{jt})\big)$ klózok berakhatók az $(y_{ij1} \vee \cdots \vee y_{ijt})$ alakú KNF-be, a $(\bar{y}_{ijk} \vee x_{ik} \vee x_{jk}) \wedge (y_{ijk} \vee x_{ik} \vee \bar{x}_{jk}) \wedge (y_{ijk} \vee \bar{x}_{ik} \vee x_{jk}) \wedge (\bar{y}_{ijk} \vee \bar{x}_{ik} \vee \bar{x}_{jk})$ kiegészítő klózok bevezetésével, mint ahogy a 39. gyakorlatban tettük. Ennek a KNF-nek a teljes mérete $\Theta(m^2 \lg n)$, szemben az 1. megoldásbeli $\Theta(m^2 n)$-val. Ha n nem 2 hatvány, akkor $O(m \lg n)$ darab további $O(\lg n)$ méretű klóz fogja kizárni a nem megfelelő értékeket.

42. $(\bar{x} \vee y) \wedge (\bar{z} \vee x) \wedge (\bar{y} \vee \bar{z}) \wedge (z \vee z)$.

43. Valószínűleg nincs, mert minden 3SAT problémát át lehet alakítani ilyen alakúvá. Például az $(x_1 \vee x_2 \vee \bar{x}_3)$ klózt helyettesíthetjük $(x_1 \vee \bar{y} \vee \bar{x}_3) \wedge (\bar{y} \vee \bar{x}_2) \wedge (y \vee x_2)$-vel, ahol y új változó (ekvivalens $\bar{x}_2$-vel).

44. Tegyük fel, hogy $f(x) = f(y) = 1$ maga után vonja $f(x\&y) = 1$-et, és azt is, hogy mondjuk $c = x_1 \vee x_2 \vee \bar{x}_3 \vee \bar{x}_4$ f prímklóza. Ekkor $c' = \bar{x}_1 \vee x_2 \vee \bar{x}_3 \vee \bar{x}_4$ *nem* klóza f-nek, ellenkező esetben $c \wedge c' = x_2 \vee \bar{x}_3 \vee \bar{x}_4$ is klóza lenne, cáfolva a prímséget. Így van olyan y vektor, melyre $f(y) = 1$ és $y_1 = 1$, $y_2 = 0$, $y_3 = y_4 = 1$. Hasonlóan van olyan z, melyre $f(z) = 1$ és $z_1 = 0$, $z_2 = 1$, $z_3 = z_4 = 1$. De ekkor $f(y\&z) = 1$, és így c nem klóza f-nek. Ugyanez az érvelés működik minden, különböző számú literált tartalmazó c klózra, feltéve, hogy legalább két literál nem komplementált benne.

45. (a) Egy $f(x_1, \ldots, x_n)$ Horn-függvény akkor és csak akkor indefinit, ha nem egyenlő a $g(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) \vee (x_1 \wedge \cdots \wedge x_n)$ definit Horn-függvénnyel. Ezért $f \leftrightarrow g$ kölcsönösen egyértelmű leképezés az indefinit és definit Horn-függvények között. (b) Ha f monoton, komplemense, $\bar{f}$, vagy azonosan 1, vagy indefinit Horn-függvény.

46. A C algoritmus 88 `xy` párt helyez a magba: amikor `x` = `a`, `b`, `c`, `0` vagy `1`, a következő `y` karakter bármi lehet, kivéve `(`. Amikor `x` = `(`, `*`, `/`, `+`, `-`, akkor `y` = `(`, `a`, `b`, `c`, `0`, `1` és ha `x` = `(`, `+` vagy `-`, akkor `y` = `-`. Végül a szabályos `x` = `)` karakterrel kezdődő párok `)+`, `)-`, `)*`, `)/`, `))`.

47. Az a sorrend, amelyben a C algoritmus a magba rakja a csúcsokat, topologikus rendezés, mivel minden k-t megelőzőt az előtt állítunk, mielőtt az algoritmus a `TRUTH`$(x_k) \leftarrow 1$ értéket beállítaná. A 2.2.3. algoritmus ugyanakkor sort használ verem helyett, ezért a rendezés, amit előállít, többnyire különbözik a C algoritmus által létrehozottól.

48. Legyen $\perp$ egy új változó, és cseréljünk ki minden indefinit Horn-klózt definitre úgy, hogy ezt az új változót hozzátesszük OR-ral. (Például a „$\bar{w} \vee \bar{y}$”-ből „$\bar{w} \vee \bar{y} \vee \perp$”, azaz „$w \wedge y \Rightarrow \perp$” lesz, a definit Horn-klózok változatlanok maradnak.) Aztán alkalmazzuk a C algoritmust. Az eredeti klózok akkor és csak akkor kielégíthetetlenek, ha $\perp$ az új klózok magjában van. Az algoritmust ezért be lehet fejezni, mihelyt TRUTH($\perp$) $\leftarrow 1$.

(Quick kitalált egy másik megoldást: a C algoritmust alkalmazhatjuk a 45. gyakorlat (a) megoldásában megkonstruált g függvényre is, mert f akkor és csak akkor kielégíthetetlen, ha minden x_j változó g magjában van. Az f olyan indefinit klózaiból, mint a $\bar{w} \vee \bar{y}$, a g függvény olyan különböző $(\bar{w} \vee \bar{y} \vee z) \wedge (\bar{w} \vee \bar{y} \vee x) \wedge (\bar{w} \vee \bar{y} \vee v) \wedge (\bar{w} \vee \bar{y} \vee u) \wedge \cdots$ klózai lesznek, melyekben a változók közül egy nincs az eredeti klózban. Ezért Quick első ránézésre elegánsnak tűnő javaslata a klózok számát $\Omega(n)$-szeresére növeli.)

49. $f \le g$ akkor és csak akkor, ha $f \wedge \bar{g}$ kielégíthetetlen, $f \wedge \bar{g}$ pedig akkor és csak akkor kielégíthetetlen, ha $f \wedge \bar{c}$ kielégíthetetlen g minden c klózára. De $\bar{c}$ literálok AND-je, így alkalmazhatjuk a 48. gyakorlatot. (További részleteket azzal kapcsolatban, hogyan lehet hatékonyan ellenőrizni, g vajon f „átnevezése”-e, azaz meghatározni, vajon vannak-e olyan $(y_1, \ldots, y_n)$ konstansok, hogy $f(x_1, \ldots, x_n) = g(x_1 \oplus y_1, \ldots, x_n \oplus y_n)$ lásd Kleine Büning és Lettmann [?] könyvét.)

50. Lásd Istrate [19] cikkét.

51. Ha a v csúcs A-val jelölt, vezessük be az $\Rightarrow A^+(v)$ és $\Rightarrow B^-(v)$ klózokat, ha pedig B-vel jelölt, az $\Rightarrow A^-(v)$ és $\Rightarrow B^+(v)$ klózokat. Egyébként legyen v-nek k kiinduló $v \to u_1, \ldots, v \to u_k$ éle. Vezessük be az $A^-(u_j) \Rightarrow B^+(v)$ és $B^-(u_j) \Rightarrow A^+(v)$ klózokat minden $1 \le j \le k$-re. Ha v nincs C-vel megjelölve, vezessük be az $A^+(u_1) \wedge \cdots \wedge A^+(u_k) \Rightarrow B^-(v)$ és $B^+(u_1) \wedge \cdots \wedge B^+(u_k) \Rightarrow A^-(v)$ klózokat. Minden kényszerítő stratégia ezeknek a klózoknak a következménye. A 2.2.3–28. gyakorlat és megoldása további információkat nyújt.

Vegyük észre, hogy a C algoritmus emiatt elvileg annak a kérdésnek az eldöntésére is használható, hogy a sakkban a világos figurákkal lépő játékos kikényszerítheti-e a győzelmet, eltekintve attól a bosszantó körülménytől, hogy a megfelelő irányított gráf mérete nagyobb, mint a létező világegyetemé.

52. A legjobb játék mellett az eredmények (lásd az 51. gyakorlatot):

n	(a)	(b)	(c)	(d)
2	0 nyer	második játékos nyer	1 nyer	második játékos nyer
3	0 nyer	kezdő játékos nyer	kezdő játékos nyer	kezdő játékos nyer
4	kezdő játékos nyer	kezdő játékos nyer	kezdő játékos nyer	kezdő játékos nyer
5	második játékos nyer	döntetlen	döntetlen	1 veszít, ha ő kezd
6	második játékos nyer	második játékos nyer	1 veszít, ha ő kezd	1 veszít, ha ő kezd
7	1 veszít, ha ő kezd	második játékos nyer	1 veszít, ha ő kezd	1 veszít, ha ő kezd
8	döntetlen	döntetlen	döntetlen	1 veszít, ha ő kezd
9	döntetlen	döntetlen	döntetlen	1 veszít, ha ő kezd

(„1 veszít, ha ő kezd” azt jelenti, hogy ha a 0 játékos kezd, a játszma döntetlen, egyébként 0 győzni tud.) *Megjegyzések:* (a)-ban az 1 játékosnak van egy kis hátránya, mert amikor $x_1 \ldots x_n$ tükörszó, $f(x) = 0$. Ez a kis különbség még akkor is befolyásolja az eredményt, amikor $n = 7$. Bár az 1 játékos számára jobbnak tűnne, hogy a tábla bal felén kizárja a 0-ákat, kiderül, hogy amikor $n = 4$, az első lépés $*1**$ kell legyen; az alternatíva, $*0**$, döntetlent eredményez. A (b) játék lényegében a játékosok közötti verseny azt észrevenni, hogy ki tudja az utolsó $*$-ot törölni. A (c) játékban $x_1 \ldots x_n$ véletlen választása mellett $F_{n+2}/2^n = \Theta((\phi/2)^n)$ valószínűséggel lesz $f(x) = 1$. A (d) játékban ez a valószínűség lassabban közelíti meg a nullát, mint $\Theta(1/\lg n)$. Az 1 játékos jobb (c)-ben, mint (d)-ben, amikor $n = 2$, 5, 8 és 9; de nem rosszabb a többi esetben sem.

53. (a) A 3. napra kellene változtatni az 1. vagy a 2. napot. (b, f) Több lehetőség van. Például a 2. nap 3. napra való cseréje. (c) Ezt az esetet illusztrálja a 7.6. ábra. Cseréljük ki a Desert vagy az Excalibur hotelt az Aladdinra. (e) Cseréljük ki a Bellagio vagy a Desert hotelt az Aladdinra.

Williams pedig, aki a (42) körben nem jelenik meg, nem tehet az ütközésekről.

54. Ha x és $\bar{x}$ S-ben vannak, akkor $u \in S \iff \bar{u} \in S$, mert az x-ből $\bar{x}$-be, az $\bar{x}$-ből x-be, az x-ből u-ba és az u-ból x-be vezető utak létezése maga után vonja az $\bar{u}$-ból $\bar{x}$-be és az $\bar{x}$-ből $\bar{u}$-ba, ezért az u-ból $\bar{u}$-ba és az $\bar{u}$-ból u-ba vezető utak létezését.

55. (a) Egy olyan klóz, mint az $x_1 \vee \bar{x}_2 \vee x_3 \vee \bar{x}_4$ sikeres átnevezésének szükséges és elegendő feltétele $(y_1 \vee \bar{y}_2) \wedge (y_1 \vee y_3) \wedge (y_1 \vee \bar{y}_4) \wedge (\bar{y}_2 \vee y_3) \wedge (\bar{y}_2 \vee \bar{y}_4) \wedge (y_3 \vee \bar{y}_4)$. Az $\{y_1, \ldots, y_n\}$ változók feletti $\binom{k}{2}$ 2 hosszúságú klózból álló halmaz kapcsolatban van egy az $\{x_1, \ldots, x_n\}$ feletti k hosszúságú klózzal. (Lásd Lewis cikkét [28]).

(b) Egy $\{x_1, \ldots, x_n\}$ feletti $k > 3$ hosszúságú klóz az új $\{t_2, \ldots, t_{k-2}\}$ változók bevezetésével – a fenti $\binom{k}{2}$ klóz helyett – $3(k-2)$ 2 hosszúságú klózzá alakítható. Az $x_1 \vee x_2 \vee x_3 \vee x_4 \vee x_5$ klóz esetén ezt illusztráljuk:

$$(y_1 \vee y_2) \wedge (y_1 \vee t_2) \wedge (y_2 \vee t_2) \wedge (\bar{t}_2 \vee y_3) \wedge (\bar{t}_2 \vee t_3) \wedge (y_3 \vee t_3) \wedge (\bar{t}_3 \vee y_4) \wedge (\bar{t}_3 \vee y_5) \wedge (y_4 \vee y_5).$$

Általában is az $x_1 \vee \cdots \vee x_k$-ból származó klózok az $1 < j < k$-ra rendre $(\bar{t}_{j-1} \vee y_j) \wedge (\bar{t}_{j-1} \vee t_j) \wedge (y_j \vee t_j)$ lesznek, de t_1-et $\bar{y}_1$-gyel és t_{k-1}-et y_k-val helyettesítjük. Ha x_j helyett $\bar{x}_j$ van, cseréljük y_j-t $\bar{y}_j$-re. Minden klózra tegyük meg ezt, a különböző klózok esetén különböző t_j segédváltozókat használva. Az eredmény egy $< 3m$ hosszúságú 2KNF formula, ami akkor és csak akkor elégíthető ki, ha lehetséges Horn-átnevezés. Most pedig alkalmazzuk a K tételt.

(Lásd Aspvall [?] cikkét. Kleine Büning és Lettmann [?] könyvében leírt egyik következmény, az 5.24. tétel úgy szól, hogy bármely kielégíthető 2KNF formulát át lehet nevezni Horn-klózokká. Vegyük észre, hogy ugyanazon függvény két KNF-je különböző eredményt adhat, például $(x \vee y \vee z) \wedge (\bar{x} \vee \bar{y} \vee \bar{z}) \wedge (\bar{x} \vee z) \wedge (\bar{y} \vee z)$ Horn-függvény, de a klózok ebben a reprezentációban komplementálással nem alakíthatók át Horn-formára.)

56. A gyakorlatbeli $f(x, y, z)$-hoz az itt látható (a 7.6. ábrával analóg) irányított gráf tartozik, és még egyszerűsíteni is lehet $y \wedge (\bar{x} \vee z)$-re. Minden csúcs erős komponens. Így a formula az $\exists\exists\exists$, $\exists\exists\forall$, $\forall\exists\exists$; kvantorokkal igaz; és a további $\forall\exists\forall$, (akármi)$\forall$(akármi) esetekben hamis. Általában is a nyolc lehetőséget elrendezhetjük egy kocka csúcsaiban úgy, hogy minden $\exists$-ről $\forall$-re váltással a formula egyre nagyobb valószínűséggel válik hamissá.

$$\begin{tikzcd} x \arrow[r] & z \arrow[r] & y \\ \bar{y} \arrow[u] \arrow[r] & \bar{z} \arrow[r] & \bar{x} \arrow[u] \end{tikzcd}$$

57.

Felépítve az irányított gráfot, a K tételhez hasonlóan be tudjuk bizonyítani, hogy a kvantált formula akkor és csak akkor teljesül, ha (i) nincs olyan erős komponens, amelyik egy x-szel együtt $\bar{x}$-et is tartalmazza; (ii) nincs univerzálisan kvantált x változóból induló, másik univerzálisan kvantált y változóba vagy $\bar{y}$ komplemensébe vezető út; (iii) nincs olyan univerzálisan kvantált x változót tartalmazó erős komponens, amelyik egy olyan egzisztenciálisan kvantált v változót vagy annak $\bar{v}$ komplemensét is tartalmazza, melyekre „$\exists v$" „$\forall x$" bal oldalán jelenik meg. Ez a három feltétel nyilván szükséges, és könnyen tesztelhető, miközben az erős komponenseket keressük.

Hogy megmutassuk, a feltételek elegendőek, vegyük először észre, hogy ha S egy csak egzisztenciális literálokkal rendelkező erős komponens, az (i) feltétel teljesülése megengedi, hogy minden literált azonos értékűvé tegyünk, mint ahogy azt a K tételben tettük. Egyébként S-nek pontosan egy univerzális literálja van: $u_j = x_j$ vagy $u_j = \bar{x}_j$. S-ben az összes többi literál egzisztenciális, és x_j jobb oldalán van, ezért ezeket u_j-vel tehetjük egyenlővé. Továbbá az összes S-be vezető út ilyen esetben tisztán egzisztenciális erős komponensekből indul, melyek értékét 0-ra lehet állítani, mert az ilyen erős komponensek komplemensei szintén S-be vezetnek, ugyanis ha v és $\bar{v}$ maga után vonja u_j-t, akkor $\bar{u}_j$ maga után vonja $\bar{v}$-t és v-t.

Lásd Aspvall, Plass és Tarján cikkét [2]. Krom [25] írásában bebizonyította, hogy az elsőrendű predikátum-kalkulusban a hasonló probléma – ahol az egyszerű Boole-változók helyét paraméteres predikátumok foglalják el, és a kvantifikáció a paraméterek felett zajlik – általánosan megoldhatatlan.

58. Hasonlóan a 48. gyakorlathoz, a „$\perp$” bevezetése és a bal oldalon „$\forall\perp$” elhelyezése után feltehetjük, hogy minden klóz definit. Legyenek x_0, x_1, ..., x_m ($\perp$-ot x_0 jelöli) az univerzális változók és y_1, ..., y_n az egzisztenciális változók. Jelentse „$u \prec v$” azt, hogy a kvantorok listájában az u változó a v változó bal oldalán jelenik meg. Ha $y_k \prec x_j$, távolítsuk el $\bar{x}_j$-t azokból a klózokból, amelyeknek nem komplementált literálja y_k. Minden $0 \le j \le m$-re az $(x_0) \wedge \cdots \wedge (x_{j-1}) \wedge (x_{j+1}) \wedge \cdots \wedge (x_m) \wedge \bigwedge\{(y_k) \mid y_k \prec x_j \text{ és } y_k \in C_0\}$ kiegészítő klózok hozzáfűzése után, legyen C_j a Horn-klózok magja. (Másképp fogalmazva C_j azt mondja meg, mire következtethetünk, amikor x_j kivételével minden x-ről feltesszük, hogy igaz.) Azt állítjuk, hogy az adott formula akkor és csak akkor igaz, ha minden $0 \le j \le m$-re $x_j \notin C_j$.

Hogy bebizonyítsuk, amit akarunk, jegyezzük meg először, hogy a formula biztosan hamis, ha valamely j-re $x_j \in C_j$. (Legyen $y_k \leftarrow 1$, amikor $y_k \in C_0$, $y_k \prec x_j$ és $x_i = 1$, ha $i \ne j$.) Különben mindegyik y_k-t megválaszthatjuk úgy, hogy a formulát igazzá tegye: ha $y_k \notin C_0$, legyen $y_k \leftarrow 0$, egyébként pedig legyen $y_k \leftarrow \bigwedge\{x_j \mid y_k \notin C_j\}$. Vegyük észre, hogy y_k x_j-től csak akkor függ, amikor $x_j \prec y_k$. A nem komplemens x_j literállal rendelkező minden c klóz igaz: ha $x_j = 0$, valamely $\bar{y}_k$ megjelenik abban a c-ben, melyre $y_k \notin C_j$, mert $x_j \notin C_j$; ezért $y_k = 0$. És minden a nem komplemens y_k literált tartalmazó c klóz is igaz: ha $y_k = 0$, akkor vagy $y_k \notin C_0$, ebben az esetben valamely c-beli $\bar{y}_l$ olyan, hogy $\notin C_0$, ezért $y_l = 0$; vagy pedig valamely j-re $y_k \in C_0 \setminus C_j$, és ebben az esetben valamely $x_j = 0$, és vagy $\bar{x}_j$ lesz benne c-ben, vagy valamely olyan $\bar{y}_l$ jelenik meg c-ben, amely $y_l \notin C_j$, és így $y_l = 0$.

(Ez a megoldás Dahlheimernek köszönhető. Lásd Karpinski, Kleine Büning és Schmitt [21]; Kleine Büning, Subramani és Zhao [**?**].)

59. n-re vonatkozó indukcióval: Tegyük fel, hogy $f(0, x_2, \ldots, x_n)$ az y_1, ..., $y_{2^{n-1}}$ kvantált formulákhoz vezet, miközben $f(1, x_2, \ldots, x_n)$ pedig – ehhez hasonlóan – a z_1, ..., $z_{2^{n-1}}$ formulákhoz. Ekkor $\exists x_1 f(x_1, x_2, \ldots, x_n)$ az $y_1 \vee z_1$, ...,$y_{2^{n-1}} \vee z_{2^{n-1}}$ formulákhoz, $\forall x_1 f(x_1, x_2, \ldots, x_n)$ pedig az $y_1 \wedge z_1$, ..., $y_{2^{n-1}} \wedge z_{2^{n-1}}$ formulákhoz vezet. Most használjuk fel azt a tényt, hogy $(y \vee z) + (y \wedge z) = y + z$. (Lásd Pehoushek előadását [**?**].)

60. (a) és (b). De (c) mindig 0; (d) mindig 1; (e) $\overline{\langle xyz \rangle}$; (f) $\bar{x} \vee \bar{y} \vee \bar{z}$.

61. Igaz – és ez csakugyan magától értetődően így van, ha $w = 0$, és ha $w = 1$.

62. Mivel $\{x_1, x_2, x_3\} \subseteq \{0, 1\}$, a szimmetria miatt feltehetjük, hogy x_1 egyenlő x_2-vel. Ekkor csak annyit feltételezve, hogy f az első három változójában monoton, vagy $f(x_1, x_1, x_3, x_4, \ldots, x_n) = f(x_1, x_1, x_1, x_4, \ldots, x_n)$, vagy $f(x_1, x_1, x_3, x_4, \ldots, x_n) = f(x_3, x_1, x_3, x_4, \ldots, x_n)$.

63. $\langle xyz \rangle = \langle xxyyz \rangle$. *Megjegyzés:* Post tulajdonképpen azt is bebizonyította, hogy *bármelyik* nemtriviális monoton önduális függvényhez egyetlen eljárás elég lesz, hogy mindet kiszámolhassuk. (n-re vonatkozó indukcióval belátható, hogy egy ilyen n-paraméteres eljárást legalább egyféleképpen meg tudunk hívni úgy, hogy $\langle xyz \rangle$-t eredményezze.)

64. [*FOCS* **3** (1962), 149–157.] (a) Ha f monoton és önduális, a P tétel szerint $f(x) = x_k$ vagy $f(x) = \langle f_1(x) f_2(x) f_3(x) \rangle$. A feltétel ezért vagy rögtön, vagy pedig indukcióval bizonyíthatóan teljesül. Megfordítva, ha a feltétel teljesül, az maga után vonja, hogy f monoton (amikor x és y csak egyetlenegy bitben különböznek) és önduális (amikor minden bitben különböznek).

(b) Csak azt kell bizonyítani, hogy f-et a feltétel megsértése nélkül lehet egy új pontban definiálni. Legyen x a lexikografikusan legkisebb olyan pont, ahol $f(x)$ definiálatlan. Ha $f(\bar{x})$ definiált, legyen $f(x) = \overline{f(\bar{x})}$. Egyébként ha $f(x') = 1$ valamely $x' \subseteq x$-re, legyen $f(x) = 1$; különben legyen $f(x) = 0$. Ezután a feltétel továbbra is teljesül.

65. Ha $\mathcal{F}$ maximális egymást metsző család, akkor (i) ha $X \in \mathcal{F} \implies \overline{X} \notin \mathcal{F}$, ahol $\overline{X}$ az $\{1, 2, \ldots, n\} \setminus X$ komplementer halmazt jelöli; (ii) ha $X \in \mathcal{F}$ és $X \subseteq Y \implies Y \in \mathcal{F}$, mert $\mathcal{F} \cup \{Y\}$

is egymást metsző család; és (iii) $X \notin \mathcal{F} \implies \overline{X} \in \mathcal{F}$, mert $\mathcal{F} \cup \{X\}$-nek tartalmaznia kell egy $Y \subseteq \overline{X}$ elemet. Megfordítva nehézség nélkül be lehet bizonyítani, hogy bármely $\mathcal{F}$ család, amelyik kielégíti (i)-t és (ii)-t, egymást metsző, és maximális is, ha (iii)-t is kielégíti.

Csattanó: A Boole-függvények nyelvén mind a három állítás egyszerű: (i) $f(x) = 1 \implies f(\bar{x}) = 0$; (ii) $x \subseteq y \implies f(x) \le f(y)$; (iii) $f(x) = 0 \implies f(\bar{x}) = 1$.

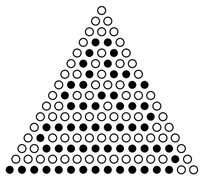
66. (Ibaraki és Kameda, [**?**]) Minden olyan kvórumcsalád, melyre $Q \subseteq Q'$ maga után vonja, hogy $Q = Q'$, kapcsolatba hozható valamely f monoton Boole-függvény prímimplikánsaival. A további $Q \cap Q' \neq \emptyset$ feltétel pedig az $f(\bar{x}) \le \overline{f(x)}$ relációval hozható kapcsolatba, mert $f(\bar{x}) = f(x) = 1$ akkor és csak akkor, ha x is, $\bar{x}$ is igazzá teszi a prímimplikánsokat.

Ha a $\mathcal{C}$ és $\mathcal{C}'$ klikkekhez hozzárendelünk ilyen f és f' függvényeket, akkor $\mathcal{C}$ akkor és csak akkor dominálja $\mathcal{C}'$-t, ha minden x-re $f \neq f'$ és $f'(x) \le f(x)$. Ekkor f' nem önduális, mert van olyan x, hogy $f'(\bar{x}) = 0$, $f(\bar{x}) = 1$; és $f(x) = 0$, ezért $f'(x) = 0$.

Megfordítva, ha f' nem önduális, van olyan y, melyre $f'(y) = f'(\bar{y}) = 0$. Ha $y = 0\ldots0$, a $\mathcal{C}'$ klikk üres, és minden más klikk dominálja. Különben pedig legyen $f(x) = f'(x) \vee [x \supseteq y]$. Ekkor f monoton, és $f(\bar{x}) \le \overline{f(x)}$ minden x-re; tehát egy olyan klikkel hozható kapcsolatba, amely dominálja $\mathcal{C}'$-t.

67. (a) Indukcióval, ha $Y(t_{100}) = Y(t_{010}) = 1$, 1-esek Y-ját nyerjük, mert a t_{100}-beli és t_{010}-beli Y-ok vagy egymást metszők, vagy egymás mellett levők. Hasonlóan, ha $Y(t_{100}) = Y(t_{010}) = 0$, akkor nincs 1-esek Y-ja, mert épp 0-ák Y-ja van.

(b) Ez a formula (a)-ból következik, és tény, hogy $(t_{abc})_{def} = t_{(a+d)(b+e)(c+f)} = (t_{def})_{abc}$. (Ennek, a 62. és a 69. gyakorlatoknak az eredményeit Schensted fejtette ki egy Martin Gardnernek 1979-ben írt 28 oldalas levelében. Milnor 1957-ben írt Gardnernek egy ide kapcsolódó, „Háromszögnek” nevezett játékról.)



68. Amikor $n = 15$, a szerző legjobb próbálkozása eddig 59 fekete golyó: ($1 \le n \le 10$ esetben a válaszok rendre 2, 3, 4, 6, 8, 11, 14, 18, 23, 27. Ezeknek a függvényeknek a prímimplikánsait elég kis ZDD-kkel reprezentálhatjuk, lásd a 7.1.4. pontban.)

69. A P tétel bizonyítása szerint csak azt kell megmutatnunk, hogy $Y(T) \le f(x)$. Egy T-beli Y azt jelenti, hogy legalább egy változó van minden p_j-ben. Ezért $f(\bar{x}_1, \ldots, \bar{x}_n) = 0$ és $f(x_1, \ldots, x_n) = 1$.

70. Ha f önduális, g öndualitása tetszőleges t-re nyilvánvaló: $\overline{g(\bar{x})} = \big(\overline{f(\bar{x})} \vee [\bar{x} = t]\big) \wedge [\bar{x} \neq \bar{t}] = \big(f(x) \vee [x = \bar{t}]\big) \wedge [x \neq t] = \big(f(x) \wedge [x \neq t]\big) \vee \big([x = \bar{t}] \wedge [x \neq t]\big) = g(x)$.

Legyenek $x = x_1 \ldots x_{j-1} 0 x_{j+1} \ldots x_n$ és $y = x_1 \ldots x_{j-1} 1 x_{j+1} \ldots x_n$; a monotonitáshoz be kell bizonyítani, hogy $g(x) \le g(y)$. Ha $x = t$ vagy $y = t$, akkor $g(x) = 0$; ha $x = \bar{t}$ vagy $y = \bar{t}$, akkor $g(y) = 1$; egyébként $g(x) = f(x) \le f(y) = g(y)$. (J. Combinatorics 16 (1995), 491–501; ettől függetlenül Bioch és Ibaraki is közölte a [**?**] cikkben.)

71. $\langle\langle xyz\rangle uv\rangle = \langle\langle\langle xyz\rangle uv\rangle uv\rangle = \langle\langle\langle yuv\rangle x\langle zuv\rangle\rangle v\rangle = \langle\langle yuv\rangle\langle xuv\rangle\langle\langle zuv\rangle uv\rangle\rangle = \langle\langle xuv\rangle\langle yuv\rangle\langle zuv\rangle\rangle$.

72. (58) bizonyításához $v = \langle uvu\rangle = u$. (59) bizonyításához $\langle uyv\rangle = \langle vu\langle xuy\rangle\rangle = \langle\langle vux\rangle uy\rangle = \langle xuy\rangle = y$. (60) bizonyításához $\langle xyz\rangle = \langle\langle xuv\rangle yz\rangle = \langle x\langle uyz\rangle\langle vyz\rangle\rangle = \langle xyy\rangle = y$.

73. (a) Ha $d(u,v) = d(u,x) + d(x,v)$, egy $u — \cdots — x — \cdots — v$ alakú legrövidebb utat nyilvánvalóan nyerünk. Megfordítva, ha $[uxv]$, legyen $u — \cdots — x — \cdots — v$ legrövidebb út, melyben l lépést tettünk meg x-ig, majd innen m lépést v-ig. Ekkor $d(u,v) = l + m \ge d(u,x) + d(x,v) \ge d(u,v)$.

(b) Minden z-re $\langle zxu\rangle = \big\langle z\langle vux\rangle\langle yux\rangle\big\rangle = \big\langle\langle zvy\rangle ux\big\rangle \in \big\{\langle yux\rangle, \langle vux\rangle\big\} = \{u, x\}$.

(c) Feltehetjük, hogy $d(x,u) \ge d(x,v) > 0$. Legyen $u — \cdots — y — v$ legrövidebb út, és legyen $w = \langle xuy\rangle$. Ekkor $\langle vxw\rangle = \big\langle v\langle vux\rangle\langle wux\rangle\big\rangle = \big\langle\langle vvw\rangle ux\big\rangle = \langle vux\rangle = x$, így $x \in [w \,..\, v]$. Továbbá

$[uwy]$, mert $d(u,y) < d(u,v)$ és $w \in [u\,.\,.\,y]$. Ha $w \neq u$, akkor $d(w,v) < d(u,v)$; ezért $[wxv]$, így $[uxv]$. Ha $w = u$, akkor (b) szerint $x \text{---} u$. De $d(x,u) \geq d(x,v)$; ezért $x \text{---} v$ és $[uxv]$.

(d) Legyen $y = \langle uxv \rangle$. Mivel $y \in [u\,.\,.\,x]$, így (a) és (b) szerint $d(u,x) = d(u,y) + d(y,x)$. Hasonlóan $d(u,v) = d(u,y) + d(y,v)$ és $d(x,v) = d(x,y) + d(y,v)$. De ez a három egyenlőség $d(u,v) = d(u,x) + d(x,v)$-vel együtt $d(x,y) = 0$-t adja. (Proc. Amer. Math. Soc. 12 (1961), 407–414.)

74. Rendre (55), (55), újból (55), majd (52), (51), (53) és (50) felhasználásával $w = \langle yxw \rangle = \langle yx\langle zxw \rangle \rangle = \langle yx\langle zx\langle yzw \rangle \rangle \rangle = \langle \langle yxz \rangle x \langle yzw \rangle \rangle = \langle x\langle xyz \rangle \langle wyz \rangle \rangle = \langle \langle xxw \rangle yz \rangle = \langle xyz \rangle$.

75. (a) Ha $w = \langle xxy \rangle$, akkor (iii) szerint $[xwx]$, ezért (i) szerint $w = x$.

(b) Az (iii) axióma és az (a) rész szerint $[xxy]$ mindig igaz. (ii)-ben legyen $x = y$, így levonhatjuk a következtetést: $[uxv] \iff [vxu]$. Emiatt $\langle xyz \rangle$ (iii)-ben megadott definíciója tökéletesen szimmetrikus x-ben, y-ban és z-ben.

(c) $\langle uxv \rangle$ (iii)-beli definíciója alapján $x = \langle uxv \rangle$ akkor és csak akkor, ha $[uxx]$, $[uxv]$ és $[xxv]$. De tudjuk, hogy $[uxx]$ és $[xxv]$ mindig igaz.

(d) Ebben és a következő lépésekben megkonstruáljuk M néhány kisegítő pontját, és aztán a C algoritmust használjuk, hogy levezessük a „közöttlevőség” reláció minden ismert következményét. (Az axiómák az alkalmas Horn-klóz alakban vannak megadva.) Itt például $z = \langle xyv \rangle$-t határozzuk meg úgy, hogy tudjuk $[uxy]$-t, $[uyv]$-t, $[xzy]$-t, $[xzv]$-t és $[yzv]$-t. Így pedig $z = \langle uyv \rangle = y$.

(e) A javasolt konstrukció többek között maga után vonja $[utv]$-t, $[utz]$-t, $[vtz]$-t, $[uwv]$-t, $[uwz]$-t, $[vwz]$-t; ezért $t = w$. (Itt hasznos lehet egy számítógépes program.) Az $[rws]$, $[rwz]$, $[swz]$ hipotézisek hozzáadásával, ahogy kívántuk, $[xyz]$ is teljesül; és az is kiderül, hogy $r = p$ és $s = q$.

(f) Legyenek $r = \langle yuv \rangle$, $s = \langle zuv \rangle$, $t = \langle xyz \rangle$, $p = \langle xrs \rangle$, $q = \langle tuv \rangle$; ekkor viszont $[pqp]$ következik. (Proc. Amer. Math. Soc. 5 (1954), 801–807. A „közöttlevőség” relációra vonatkozó axiómák kezdeti vizsgálatáról lásd Huntington és Kline [?] cikkét.)

76. Az (i) axióma nyilván teljesül, és az (ii) axióma pedig a kommutativitásból és (52)-ből következik. A 74. gyakorlat megoldása levezeti az $\langle xyz \rangle = \langle x\langle xyz \rangle \langle wyz \rangle \rangle$ azonosságból (iii)-t, így csak a következő formulát kell ellenőrizni: $\langle x\langle xyz \rangle \langle wyz \rangle \rangle = \langle \langle yxz \rangle x \langle wyz \rangle \rangle = \langle \langle \langle yxz \rangle xz \rangle x \langle wyz \rangle \rangle = \langle \langle yxz \rangle x \langle zx\langle wyz \rangle \rangle \rangle = \langle x\langle xyz \rangle \langle z\langle xyz \rangle w \rangle \rangle = \langle \langle x\langle xyz \rangle z \rangle \langle xyz \rangle w \rangle = \langle \langle xyz \rangle \langle xyz \rangle w \rangle$.

Megjegyzések: Birkhoff és Kiss [?] dolgozatukban a medián algebra kezelése során eredetileg az (50) és (51) törvényeket, továbbá az (53) rövid disztributivitás törvényt feltételezték. Arra a tényre, hogy az (52) asszociativitás tulajdonképpen maga után vonja a disztributivitást, egészen addig nem jöttek rá, amíg sok évvel később Kolibiar és Marcisová a [?] munkában Sholander axiómáival be nem bizonyította, mint ahogy mi is tesszük ebben a gyakorlatban. Az (53) törvény (50)–(52)-ből való mechanikus levezetését 2005-ben találta meg Veroff és McCune az Otter tételbizonyító program egy bővített verzióját használva.

77. (a) Az $r \text{---} s$-hez tartozó címkék egy koordinátájában tegyük fel, hogy $l(r)$ 0 és $l(s)$ 1; ekkor a bal csúcsoknak ez a koordinátája 0. Ha $u \text{---} v \text{---} u'$ olyan, hogy u és u' a bal oldalon vannak, de v a jobb oldalon, $\langle uu'v \rangle$ a bal oldalon fekszik. De $[u\,.\,.\,v] \cap [u'\,.\,.\,v] = \{v\}$ kivéve, ha $u = u'$.

(b) A C következmény alapján ez az állítás nyilvánvaló.

(c) Tegyük fel, hogy $u \text{---} v$ és $u' \text{---} v'$ olyan élek, ahol u és u' a bal oldalon, v és v' pedig a jobb oldalon vannak. Legyen $v = v_0 \text{---} \cdots \text{---} v_k = v'$ legrövidebb út, és legyen $u_0 = u$, $u_k = u'$. (b) szerint minden v_j csúcs a jobb oldalon fekszik. Az $u_1 = \langle u_0 v_1 u_k \rangle$ bal csúcs u_0 és v_1 közös szomszédja kell legyen, mert a távolság $d(u_0, v_1) = 2$. (Nem lehet $u_1 = u_0$, mert ez maga után vonná egy v-ből az u bal csúcson keresztül v'-be vezető legrövidebb út létezését.) Ezért v_1 szintszáma 1; és ugyanezen indokok miatt ilyenek v_2, …, v_{k-1} is. (Nebeský, [?]; Mulder, [?].)

(d) Ezek a lépések minden 1 szintszámú v csúcsot megvizsgálnak az s-től való $d(v,s)$ távolságuk sorrendjében. Ha egy ilyen v-nek van még meg nem vizsgált u távoli szomszédja, u szintszáma 1 vagy 2 kell legyen. Ha a szintszám 1, u-nak legalább két közeli szomszédja lesz, mégpedig v és a jövőbeli `PÁR(`u`)`. Az I8 lépés u egy olyan w közeli szomszédjával kapcsolatban dönt, melyre $w \neq v$.

Mivel $d(w,v)=2$, (c) szerint az $x=\langle svw\rangle$ csúcs szintszáma 1. Ha w szintszáma 0, akkor $x=v$; így u szintszáma 1. Egyébként $d(x,s)<d(v,s)$, és w szintszámát helyesen állapítottuk meg, amikor x-et vizsgáltuk. Ha w szintszáma 1, u egy v-ből w-be vezető legrövidebb úton fekszik; ha pedig w szintszáma 2, w egy u-ból s-be vezető legrövidebb úton van. (c) szerint u és w mindkét esetben azonos szintszámmal rendelkezik.

(e) Az algoritmus eltávolítja az $r — s$ éllel ekvivalens összes élt (a) és (d) szerint. Ezeknek az eltávolítása után a gráf nyilván nem marad összefüggő; a két rész, ami marad, (b) alapján konvex, így összefüggő és tulajdonképpen egy-egy medián gráf. A két rész közötti összes releváns relációt feljegyzi az I7 lépés, mert minden négy hosszúságú kört, ami eltűnik, itt ellenőrzünk. A csúcsok száma szerinti indukcióval bizonyítható, hogy a részek helyesen címkézettek.

78. Minden alkalommal, amikor az I4 lépésben v megjelenik, egy u_j szomszédját elveszíti. A címkében pedig minden $v — u_j$ élnek különböző koordináta felel meg, ezért feltehetjük, hogy $l(v)$ valamely α bináris füzérre $\alpha 1^k$ alakú. Az u_1, u_2, …, u_k csúcsokra vonatkozó címkék ekkor $\alpha 01^{k-1}$, $\alpha 101^{k-2}$, …, $\alpha 1^{k-1}0$. Komponensenkénti mediánozással be tudjuk bizonyítani, hogy az összes – 2^k különböző – $\alpha\beta$ alakú címke felbukkan a gráf valamely csúcsában, mert $\big\langle(\alpha\beta)(\alpha\beta')(0\ldots0)\big\rangle$ az $\alpha(\beta\&\beta')$ bitfüzér.

79. (a) Ha $l(v)=k$, pontosan $\nu(k)$ kisebb csúcs alkotja v szomszédjait.

(b) Minden $0\le j<\lceil\lg n\rceil$-re a j-edik bitpozícióban legfeljebb $\lfloor n/2\rfloor$ 1-es van.

(c) Tegyük fel, hogy pontosan k csúcsnak van 0-val kezdődő címkéje. Legfeljebb $\min(k,n-k)$ él hozható kapcsolatba ezekkel a bitpozíciókkal, és legfeljebb $f(k)+f(n-k)$ további él van. De

$$f(n)=\max_{0\le k\le n}\big(\min(k,n-k)+f(k)+f(n-k)\big),$$

mert a $g(m,n)=f(m+n)-m-f(m)-f(n)$ függvény kielégíti a

$$g(2m+a,2n+b)=ab+g(m+a,n)+g(m,n+b),\qquad \text{ha } 0\le a,b\le 1$$

rekurzív egyenlőséget. Indukcióval következik, hogy $g(m,m)=g(m,m+1)=0$, és hogy $g(m,n)\ge 0$, amikor $m\le n$. (Annals of the New York Academy of Sciences 175 (1970), 170–186; Knuth, [?].)

80. (a) (Imrich megoldása.) A 0000, 0001, 0010, 0011, 0100, 0110, 0111, 1100, 1101, 1110, 1111 csúcscímkékkel rendelkező gráfot nem lehet lényegesen másképp címkézni; de 0001 és 1101 távolsága 4, és nem 2.

(b) A C_{2m} kör parciális kocka, mert csúcsainak a címkéi lehetnek $l(k)=1^k0^{m-k}$, $l(m+k)=0^k1^{m-k}$, ahol $0\le k<m$. De $l(0)$, $l(m-1)$ és $l(m+1)$ bitenkénti mediánja $01^{m-2}0$; és valóban ezeknek a csúcsoknak nincs a körben mediánja, ha $m>2$.

81. Igen. Minden medián gráf egy hipergráf páros részgráfja.

82. Az általános eset arra az egyszerű esetre redukálhatjuk, amikor G-nek csak két csúcsa van: $\{0,1\}$; mert komponensenként dolgozhatunk a medián címkéken, és mert $d(u,v)$ az $l(u)$ és $l(v)$ közötti Hamming-távolság.

Az egyszerű esetben a megadott szabály szerint $u_k\leftarrow v_k$, kivéve ha $u_{k-1}=v_{k-1}=v_{k+1}\ne v_k$, és ez azonnal bizonyítja az optimalitást. (Emellett lehetnek további optimális megoldások is, például ha $v_0v_1v_2v_3=0110$, akkor $u_0u_1u_2u_3=0000$.)

(Ezt a problémát az önszervező adatszerkezetek tanulmányozása motiválta. Chung, Graham és Saks [?] könyvükben bebizonyították, hogy a medián gráfok az *egyedüli* gráfok, melyekre u_k-t mint $(v_0,v_1,\ldots,v_{k+1})$ függvényét mindig megválaszthatjuk optimálisan, függetlenül a $(v_0,v_1,\ldots,v_{k+1})$ részsorozatbeli értékektől. A [?] dolgozatukban a szerzők azokat az eseteket is mind jellemezték, ahol elegendő véges sok lépésnyi előretekintés.)

83. Most is elég, ha az egyszerű, két csúcsból álló esetet vizsgáljuk. Ebben az esetben az optimális megoldásban sose lesz $u_{k-1} \neq u_k$ kivéve, amikor $u_{k-1} = v_{k-1} \neq v_k = u_k$. Ezért csak azt kell eldöntenünk, hogy $v_0 v_1 \ldots v_t$-ben az egymást követő 0-ák vagy 1-esek mely „futamai” idézhetik elő az $u_0 u_1 \ldots u_t$-beli megfelelő „futamokat”.

Tegyük fel, hogy $v_{k-1} v_k \ldots v_{k+r} = 01^r 0$ és $u_{k-1} = 0$. Ha $u_{k-1} u_k \ldots u_{k+r} = 01^r 0$, akkor az $u_{k-1} u_k \ldots u_{k+r} = 00\ldots0$-ra vonatkozó $r\rho$ költséget a 2 költséggel hasonlítjuk össze; így a utóbbit kell választani, ha $\rho < 2/r$, és az előbbit, ha $\rho > 2/r$. Ez a vezérelv mediánokkal is kifejezhető, amennyiben azt mondjuk, hogy legyen $u_k = \langle u_{k-1} \ldots u_{k-1} v_k \ldots v_{k+r} \rangle$, amikor $2/(r+1) \le \rho < 2/r$, $r \ge 0$ és u_{k-1}-nek r előfordulása van. (Általános medián gráfban ez a $(2r+1)$ operandussal dolgozó medián helyes eredményt ad, mert érvényes medián címkéket hoz létre; lásd a 86. gyakorlatot.)

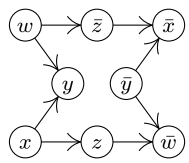
De amikor a befejezéshez közel kerülünk, ezt a szabályt meg kell változtatnunk, mert ez végül $j > t$-re is kéri a v_j értékeket. A végjáték elmés. Ha $v_{k-1} v_k \ldots v_t = 01^r$ és $u_{k-1} = 0$ (ahol $r = t + 1 - k$), az $u_{k-1} u_k \ldots u_t = 00\ldots0$ választás most csak akkor jobb, ha $\rho < 1/r$. Például ha $2/4 < \rho < 2/3$, $v_0 v_1 = 01$ és $t = 1$, akkor az $u_0 u_1 = 00$-át kell választani; de ha $v_0 v_1 v_2 = 011$ és $t = 2$, akkor az $u_0 u_1 u_2 = 011$-et. Egy lehetséges megoldás az, hogy legyen $v_{t+j} \leftarrow v_t$, ha $1 \le j \le \lceil r/2 \rceil$, és $v_{t+j} \leftarrow v_0$, ha $\lceil r/2 \rceil < j \le r$.

84. 81 ilyen függvény van, melyek mindegyike páratlan számú elem mediánjaként reprezentálható. Hétféle csúcs fordul elő:

Típus	Jellemző csúcs	Esetek	Szomszédok	Fokszám
1	$\langle z\rangle$	5	$\langle vwxyzzz\rangle$	1
2	$\langle vwxyzzz\rangle$	5	$\langle z\rangle, \langle wxyzz\rangle$	5
3	$\langle wxyzz\rangle$	20	$\langle vwxyzzz\rangle, \langle vwxxyyzzz\rangle$	4
4	$\langle vwxxyyzzz\rangle$	30	$\langle xyz\rangle, \langle wxyzz\rangle, \langle vwxyyzz\rangle$	5
5	$\langle vwxyyzz\rangle$	10	$\langle vwxxyyzzz\rangle, \langle vwxyz\rangle$	7
6	$\langle vwxyz\rangle$	1	$\langle vwxyyzz\rangle$	10
7	$\langle xyz\rangle$	10	$\langle vwxxyyzzz\rangle$	3

(Neumann és Morgenstern sorolták fel ezt a hét típust [?] könyvükben az – általuk egyszerű játékoknak nevezett – nyerő koalíciók rendszereinél felmerülő ekvivalenciaprobléma tanulmányozásával kapcsolatban. A hatváltozós függvényekhez tartozó gráf, melynek 30 különböző típusú 2646 csúcsa van, Meyerowitznak a 70. gyakorlatban hivatkozott dolgozatában jelenik meg. Ezek közül a típusok közül csak 21 reprezentálható mint páratlan számú operandus egyszerű mediánja; például egy az $\langle\langle abd\rangle\langle ace\rangle\langle bcf\rangle\rangle$-hez hasonló csúcsnak nincs ilyen reprezentációja. n változó esetén legyen a megfelelő gráfnak M_n csúcsa. Erdős és Hindman [?] cikkükben megmutatták, hogy $\lg M_n$ aszimptotikusan egyenlő $\binom{n-1}{\lfloor n/2 \rfloor}$-vel. Kleitman [?] munkájában pedig azt mutatta meg, hogy a gráfban a különböző projekciós függvényekhez tartozó csúcsok (mint x és y) mindig a legtávolabb vannak egymástól.

85. Minden erős komponens tartalmaz magában álló csúcsot; különben két koordináta mindig egyenlő vagy komplemens lenne. Így az irányított gráf körmentes.



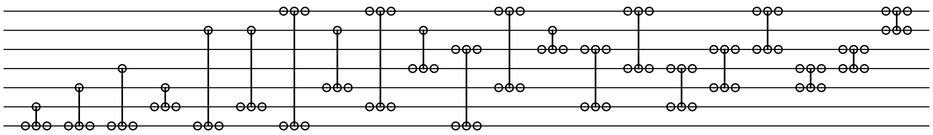
Ráadásul nem vezethet út egy csúcsból a komplemensébe, különben egy koordináta konstans lenne.

Ha ez a két feltétel teljesül, be tudjuk bizonyítani, hogy nincs redundáns x csúcs azzal, hogy minden olyan csúcshoz 0-át rendelünk, amelyik megelőzi x-et vagy $\bar x$-et, 1-et rendelünk ahhoz, amelyik követi, és az összes többi csúcsnak pedig valami alkalmas értéket adunk.

(Következésképpen teljesen más módszert nyerünk arra, hogy egy medián gráfot reprezentáljunk. Például az itt látható gráf a $\{0000, 0001, 0010, 0011, 0111, 1010\}$ címkékkel rendelkező medián gráfnak felel meg.)

86. Igen. A P tétel szerint *bármely* monoton és önduális függvény X elemeit X-be képezi.

87. Most a $7\,6\,5\,4\,3\,2\,1\,\bar1\,\bar2\,\bar3\,\bar4\,\bar5\,\bar6\,\bar7$ topologikus rendezés lép (72) helyébe, majd az alábbi hálózatot kapjuk:

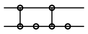


(Az azonos vonalon egymást követő átalakítók természetesen semlegesíthetik egymást.)

88. d egy adott értéke ($2\lceil t/d\rceil$ egységre) várakozó legfeljebb $6\lceil t/d\rceil$ szakaszban játszik szerepet.

89. Először tegyük fel, hogy az új feltétel $i \to j$, miközben a régi $i' \to j'$ volt, ahol $i < j$, $i' < j'$, és nincsenek komplemens literálok. Az új modul az $x_1 \ldots x_t$ bitvektort az $y_1 \ldots y_t$ bitvektorrá alakítja, ahol $y_i = x_i \wedge x_j$, $y_j = x_i \vee x_j$, egyébként pedig $y_k = x_k$. Ekkor $y_{i'} \le y_{j'}$, ha $\{i', j'\} \cap \{i, j\} = \emptyset$. És akkor sincs probléma, ha $i = i'$, mivel $y_{i'} = y_i \le x_i = x_{i'} \le x_{j'} = y_{j'}$. De az $i = j'$ eset bonyolultabb: az $i' \to i$ és $i \to j$ relációk maguk után vonják $i' \to j$-t is; és ezt a relációt az *előző* modulok juttatták érvényre, hisz a modulokat az $u_1 \ldots u_{2t}$ topologikus rendezés szerinti csökkenő d távolság sorrendjében csatoltuk egymáshoz. Következésképpen $y_{i'} = x_{i'} \le x_j$ és $y_{i'} \le x_{j'} = x_i$, ezért $y_{i'} \le x_i \wedge x_j = y_i = y_{j'}$. Hasonló a bizonyítás, amikor $j = i'$ vagy $j = j'$.

Végül, ha komplemens literálok is előfordulnak, a konstrukció az általános esetet ügyesen komplemens mentes esetté redukálja a bitek át-, illetve visszafordításával.

90. Amikor $t = 2$,  végzi a munkát. Az általános eset ebből az építőelemből t-nek $\lceil t/2\rceil$-vé redukálásával rekurzív módon következik. (A CI-netek és más, általánosabb hálózatok tanulmányozását Mayr és Subramanian [**?**] munkájukkal indították el.)

91. A válasz nem ismert még speciális esetben sem, amikor a medián gráf ($t+1$ csúcsú) szabad fa, vagy monoton esetben, amikor disztributív háló, mint az F következményben. Az utóbbi esetben az átalakító szükségtelen lehet.

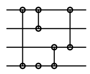
92.

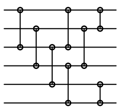
93. Legyen $d_X(u,v)$ az u és v közötti olyan legrövidebb úton a csúcsok száma, amikor az út teljesen X-en belül vezet. Világos, hogy ekkor $d_X(u,v) \ge d_G(u,v)$. És ha $u = u_0 — u_1 — \cdots — u_k = v$ egy legrövidebb út G-ben, az $u = f(u_0) — f(u_1) — \cdots — f(u_k) = v$ út X-ben fekszik, amikor f G-nek egy X-be való behúzása; ezért $d_X(u,v) \le d_G(u,v)$.

94. Ha f a t kocka X-be való behúzása, akkor két különböző koordináta-pozíció nem lehet minden $x \in X$ esetén mindig azonos értékű vagy ennek komplemense értékű, kivéve ha konstans. Ha mondjuk X minden eleme $00{*}\ldots{*}$ vagy $11{*}\ldots{*}$ alakú, nem lenne út ezen különböző típusú csúcsok között, ami cáfolja azt a tényt, hogy X távolság-megőrző részgráf (ezért összefüggő).

Adott $x, y, z \in X$ esetén jelölje a t kockában a mediánjukat $w = \langle xyz\rangle$. Ekkor $f(w) \in [x\,..\,y] \cap [x\,..\,z] \cap [y\,..\,z]$, mert (például) $f(w)$ X-ben az x-ből y-ba vezető egyik legrövidebb úton fekszik. Így $f(w) = w$, és ezzel bebizonyítottuk, hogy $w \in X$. (Ez az eredmény és a lényegesen nehezebb megfordítottja Bandeltnek tulajdonítható, [**?**].)

95. Hamis (jóllehet a szerző mást remélt); a jobb oldalon látható hálózat hatása $0001 \mapsto 0000$, $0010 \mapsto 0011$, $1101 \mapsto 0110$, de egyáltalán nem $\mapsto 0010$.





(A lehetséges outputok halmazát úgy tűnik, nem könnyű jellemezni, sőt ha átalakítót nem használunk, még akkor sem. Például a bal oldalon látható – Feder által konstruált – tiszta összehasonlító hálózat hatása $000000 \mapsto 000000$, $010101 \mapsto 010101$, és $101010 \mapsto 011001$, de egyáltalán nem $\mapsto 010001$. Lásd még az 5.3.4. pontbeli 50. és 52. gyakorlatokat.)

96. Nem. Ha f a $w = (w_1, \ldots, w_n)$ és t valós paraméterekkel rendelkező küszöbfüggvény, legyen $\max\{w \cdot x \mid f(x) = 0\} = t - \epsilon$. Ekkor $\epsilon > 0$, és a következő 2^n egyenlőtlenség meghatározza

f-et: $w \cdot x - t \geq 0$, amikor $f(x) = 1$, $t - w \cdot x - \epsilon \geq 0$, amikor $f(x) = 0$. Ha A egy $M \times N$-es egész számokból álló mátrix, melyre az $Av \geq (0, \ldots, 0)^T$ lineáris egyenlőtlenség-rendszernek olyan $v = (v_1, \ldots, v_N)^T$ valós megoldása van, hogy $v_N > 0$, akkor van ilyen egész megoldása is. (A bizonyítás N-re vonatkozó indukcióval történik.) Így feltehetjük, hogy $w_1, \ldots, w_n$, t és ϵ egészek.

(A Hadamard-egyenlőtlenséget (lásd 4.6.1. (25)) használó hasonló elemzés bebizonyítja, hogy legfeljebb $(n+1)^{(n+1)/2}/2^n$ nagyságú egész súlyok elegendőek lesznek; lásd Muroga, Toda és Takasu [?] dolgozatát. Ráadásul a 112. gyakorlat megmutatja, hogy közel ilyen nagy súlyok olykor szükségesek is.)

97. $\langle 11111x_1x_2\rangle$, $\langle 111x_1x_2\rangle$, $\langle 1x_1x_2\rangle$, $\langle 0x_1x_2\rangle$, $\langle 000x_1x_2\rangle$, $\langle 00000x_1x_2\rangle$.

98. Feltehetjük, hogy $f(x_1, \ldots, x_n) = \langle y_1^{w_1} \ldots y_n^{w_n}\rangle$, ahol w_j-k pozitív egész súlyok, és $w_1 + \cdots + w_n$ páratlan. Legyen δ az n szabadon változó előjelet tartalmazó 2^n lehetséges $\pm w_1 \pm \cdots \pm w_n$ összeg minimális pozitív értéke. Számozzuk át az összes alsó indexet úgy, hogy $w_1 + \cdots + w_k - w_{k+1} - \cdots - w_n = \delta$ legyen. Ekkor $w_1y_1 + \cdots + w_ny_n > \frac{1}{2}(w_1 + \cdots + w_n) \iff w_1(y_1 - \frac{1}{2}) + \cdots + w_n(y_n - \frac{1}{2}) > 0 \iff w_1(y_1 - \frac{1}{2}) + \cdots + w_n(y_n - \frac{1}{2}) > -\delta/2 \iff w_1y_1 + \cdots + w_ny_n > \frac{1}{2}(w_1 + \cdots + w_n - (w_1 + \cdots + w_k - w_{k+1} - \cdots - w_n)) = w_{k+1} + \cdots + w_n \iff w_1y_1 + \cdots + w_ky_k - w_{k+1}\bar{y}_{k+1} - \cdots - w_n\bar{y}_n > 0$.

99. $[x_1 + \cdots + x_{2s-1} + s(y_1 + \cdots + y_{2t-2}) \geq st] = [\lfloor (x_1 + \cdots + x_{2s-1})/s \rfloor + y_1 + \cdots + y_{2t-2} \geq t]$; és $\lfloor (x_1 + \cdots + x_{2s-1})/s \rfloor = [x_1 + \cdots + x_{2s-1} \geq s]$.

(Például $\langle\langle xyz\rangle uv\rangle = \langle xyzu^2v^2\rangle$, ami az (53) és (54) egyenlőségek szerint megegyezik az $\langle x\langle yuv\rangle\langle zuv\rangle\rangle$ és $\langle\langle xuv\rangle\langle yuv\rangle\langle zuv\rangle\rangle$ értékekkel. *Hivatkozás:* Elgot, [11])

100. Az előző gyakorlat és (45) miatt igaz.

101. (a) $n = 7$ esetben a prímimplikánsok $x_7 \wedge x_6$, $x_6 \wedge x_5$, $x_7 \wedge x_5 \wedge x_4$, $x_6 \wedge x_4 \wedge x_3$, $x_7 \wedge x_5 \wedge x_3 \wedge x_2$, $x_6 \wedge x_4 \wedge x_2 \wedge x_1$ és $x_7 \wedge x_5 \wedge x_3 \wedge x_1$. Az általános esetben pedig hasonló séma szerint n prímimplikánst adhatunk meg. (Ugyanis vagy $x_n = x_{n-1}$, vagy $x_n = \bar{x}_{n-1}$. Az első esetben $x_n \wedge x_{n-1}$ nyilvánvalóan prímimplikáns. A második esetben $F_n(x_1, \ldots, x_{n-1}, \bar{x}_{n-1}) = F_{n-1}(x_1, \ldots, x_{n-1})$; ezért az utóbbinak a prímimplikánsát használjuk, és beszúrjuk x_n-t, amikor x_{n-1} nem jelenik meg.)

(b) Az $n = 7$-re vonatkozó (0000011, $000011\underline{0}$, $00011\underline{0}1$, $0011\underline{0}1\underline{0}$, $011\underline{0}1\underline{0}1$, $11\underline{0}1\underline{0}1\underline{0}$, $1\underline{0}1\underline{0}1\underline{0}1$) mintakifejtés minden n esetén működik.

(c) Az $n = 7$ esetbeli különböző lehetőségek közül kettő megvilágítja az általános esetet is:

$$F_7(x_1, \ldots, x_7) = Y\begin{pmatrix} x_6 \\ x_7\ x_5 \\ x_6\ x_6\ x_4 \\ x_7\ x_5\ x_7\ x_3 \\ x_6\ x_6\ x_4\ x_6\ x_2 \\ x_7\ x_5\ x_7\ x_3\ x_7\ x_1 \end{pmatrix} = Y\begin{pmatrix} x_6 \\ x_7\ x_5 \\ x_6\ x_6\ x_4 \\ x_7\ x_5\ x_5\ x_3 \\ x_6\ x_6\ x_4\ x_4\ x_2 \\ x_7\ x_5\ x_5\ x_3\ x_3\ x_1 \end{pmatrix}.$$

(A Fibonacci-küszöbfüggvényeket Muroga vezette be, aki a 105. gyakorlatbeli optimális eredményt is megtalálta; lásd Muroga cikkét [?].)

102. (a) $\hat{f}(\bar{x}_0, \bar{x}_1, \ldots, \bar{x}_n)$ (1) és (2) szerint $\hat{f}(x_0, x_1, \ldots, x_n)$ komplemense.

(b) Ha f-et a (110) képlet adja meg, $\hat{f}$ éppen $[(w+1-2t)x_0 + w_1x_1 + \cdots + w_nx_n \geq w+1-t]$, ahol $w = w_1 + \cdots + w_n$. Megfordítva, ha $\hat{f}$ küszöbfüggvény, akkor pedig $f(x_1, \ldots, x_n) = \hat{f}(1, x_1, \ldots, x_n)$ is az. (Goto és Takahasi, [?].)

103. (Lásd Minnick [33] dolgozatát.) A $w_1 + \cdots + w_n$ összeget akarjuk minimalizálni azzal a kikötéssel, hogy $w_j \geq 0$ minden $1 \leq j \leq n$-re, és $(2e_1-1)w_1 + \cdots + (2e_n-1)w_n \geq 1$ minden $x_1^{e_1} \wedge \cdots \wedge x_n^{e_n}$ prímimplikánsra. Például ha $n = 6$, az $x_2 \wedge x_5 \wedge x_6$ prímimplikáns a $-w_1 + w_2 - w_3 - w_4 + w_5 + w_6 \geq 1$ korlátozáshoz vezetne. Ha a minimum $+\infty$, az adott függvény nem küszöbfüggvény. (A 84. gyakorlat megoldása egy ilyen eset legegyszerűbb példái egyikét adja.) Egyébként pedig ha a $(w_1, \ldots, w_n)$ megoldás csak egész számokból áll, ez a kívánt méretet minimalizálja. Amikor nem csak egész számokból álló megoldás adódik, további kikötéseket kell hozzáadnunk, amíg a legjobb megoldást – mint a következő gyakorlat (c) részében – meg nem találjuk.

104. Először is szükségünk van egy adott $\langle x_1^{w_1} \dots x_n^{w_n}\rangle$ majoritás függvény $x_1^{e_1} \wedge \cdots \wedge x_n^{e_n}$ prímimplikánsait generáló algoritmusra, amikor $w_1 \geq \cdots \geq w_n$ és $w_1 + \cdots + w_n$ páratlan:

K1. (Kezdőértékek beállítása.) Legyen $t \leftarrow 0$. Aztán a $j = n$, $n-1$, …, 1 sorrendben legyenek $a_j \leftarrow t$, $t \leftarrow t + w_j$, $e_j \leftarrow 0$. Végül legyen $t \leftarrow (t+1)/2$, $s_1 \leftarrow 0$ és $l \leftarrow 0$.

K2. (Az l szintre lépünk.) Legyen $l \leftarrow l+1$, $e_l \leftarrow 1$, $s_{l+1} \leftarrow s_l + w_l$.

K3. (Küszöb alatt vagyunk?) Ha $s_{l+1} < t$, térjünk vissza K2-re.

K4. (Vizsgáljunk meg egy prímimplikánst.) Vizsgáljuk meg az $(e_1, \dots, e_n)$ kitevőket.

K5. (Csökkentés.) Legyen $e_l \leftarrow 0$. Ekkor ha $s_l + a_l \geq t$, legyen $s_{l+1} \leftarrow s_l$ és térjünk vissza K2-re.

K6. (Visszalépés.) Legyen $l \leftarrow l-1$. Befejezzük, ha $l = 0$. Egyébként ha $e_l = 1$, akkor térjünk vissza K5-re, különben ismételjük meg ezt a lépést.

(a) $\langle x_1 x_2^2 x_3^3 x_4^5 x_5^6 x_6^8 x_7^{10} x_8^{12}\rangle$ (21 prímimplikáns).

(b) $\langle x_0^{16-2t} x_1^8 x_2^4 x_3^2 x_4\rangle$ esetében az optimális súlyok $0 \leq t \leq 8$-re $w_0w_1w_2w_3w_4 = 10000$, 31111, 21110, 32211, 11100, 23211, 12110, 13111, 01000; a további esetek ezek duáljai.

(c) Itt az optimális $(w_1, \dots, w_{10})$ súlyok $(29, 25, 19, 15, 12, 8, 8, 3, 3, 0)/2$; így megtudjuk, hogy x_{10} nem releváns, és törtszám súlyokkal kell foglalkoznunk. A $w_8 \geq 2$ korlátozás a $(15, 13, 10, 8, 6, 4, 4, 2, 1, 0)$ egész súlyokat adja, aminek optimálisnak kell lennie, mert összegük 2-vel haladja meg az előző összeget. (A 175 428 kilencváltozós önduális küszöbfüggvény közül csak kettőnek vannak nemegész, a $w_1 + \cdots + w_n$ összeget minimalizáló súlyai; a másik $\langle x_1^{17} x_2^{15} x_3^{11} x_4^9 x_5^7 x_6^5 x_7^4 x_8^2 x_9\rangle$. A minimális reprezentációban a legnagyobb w_1 az $\langle x_1^{42} x_2^{22} x_3^{18} x_4^{15} x_5^{13} x_6^{10} x_7^8 x_8^4 x_9^3\rangle$ medián függvényben fordul elő; a legnagyobb $w_1 + \cdots + w_9$ pedig egyedül az $\langle x_1^{34} x_2^{32} x_3^{28} x_4^{27} x_5^{24} x_6^{20} x_7^{18} x_8^{15} x_9^{11}\rangle$-ben, ami egyúttal a legnagyobb w_9-re is példa. Lásd Muroga, Tsuboi és Baugh [?] dolgozatát.)

105. Amikor $n = 7$, a 103. gyakorlatban generált egyenlőtlenségek a következők: $w_7 + w_6 - w_5 - w_4 - w_3 - w_2 - w_1 \geq 1$, $-w_7 + w_6 + w_5 - w_4 - w_3 - w_2 - w_1 \geq 1$, $w_7 - w_6 + w_5 + w_4 - w_3 - w_2 - w_1 \geq 1$, $-w_7 + w_6 - w_5 + w_4 + w_3 - w_2 - w_1 \geq 1$, $w_7 - w_6 + w_5 - w_4 + w_3 + w_2 - w_1 \geq 1$, $-w_7 + w_6 - w_5 + w_4 - w_3 + w_2 + w_1 \geq 1$, $w_7 - w_6 + w_5 - w_4 + w_3 - w_2 + w_1 \geq 1$. Szorozzuk meg ezeket rendre az 1, 1, 2, 3, 5, 8, 5 számokkal, hogy $w_1 + \cdots + w_7 \geq 1+1+2+3+5+8+5$ kapjunk. Ugyanez az ötlet minden $n \geq 3$-ra működik.

106. (a) $\langle x_1^{2^{n-1}} x_2^{2^{n-2}} \dots x_n\, \bar y_1^{2^{n-1}} \bar y_2^{2^{n-2}} \dots \bar y_n \bar z\rangle$. (A 99. gyakorlat szerint n háromváltozós mediánt is végrehajthatunk: $\langle\langle \dots \langle x_n \bar y_n \bar z\rangle \dots x_2 \bar y_2\rangle x_1 \bar y_1\rangle$.) (b) Ha $\langle x_1^{u_1} x_2^{u_2} \dots x_n^{u_n} \bar y_1^{v_1} \bar y_2^{v_2} \dots \bar y_n^{v_n} \bar z^{w}\rangle$ oldja meg a problémát, $2^{n+1} - 1$ alapegyenlőtlenség kell, hogy teljesüljön; például amikor $n = 2$, akkor: $u_1 + u_2 - v_1 + v_2 - w \geq 1$, $u_1 + u_2 - v_1 - v_2 + w \geq 1$, $u_1 - u_2 + v_1 - v_2 - w \geq 1$, $u_1 - u_2 - v_1 + v_2 + w \geq 1$, $-u_1 + u_2 + v_1 + v_2 - w \geq 1$, $-u_1 + u_2 + v_1 - v_2 + w \geq 1$, $-u_1 - u_2 + v_1 + v_2 + w \geq 1$. Adjuk össze ezeket, hogy az $u_1 + u_2 + \cdots + u_n + v_1 + v_2 + \cdots + v_n + w \geq 2^{n+1} - 1$ eredményhez jussunk.

107.

f	$N(f)$	$\Sigma(f)$	f	$N(f)$	$\Sigma(f)$	f	$N(f)$	$\Sigma(f)$	f	$N(f)$	$\Sigma(f)$
$\perp$	0	$(0,0)$	$\bar\subset$	1	$(0,1)$	$\bar\vee$	1	$(0,0)$	$\bar{\mathsf{L}}$	2	$(0,1)$
$\wedge$	1	$(1,1)$	R	2	$(1,2)$	$\equiv$	2	$(1,1)$	$\supset$	3	$(1,2)$
$\bar\supset$	1	$(1,0)$	$\oplus$	2	$(1,1)$	$\bar{\mathsf{R}}$	2	$(1,0)$	$\bar\wedge$	3	$(1,1)$
L	2	$(2,1)$	$\vee$	3	$(2,2)$	$\subset$	3	$(2,1)$	$\top$	4	$(2,2)$

Figyeljük meg, hogy $\oplus$ és $\equiv$ ugyanazokkal az $N(f)$ és $\Sigma(f)$ paraméterekkel rendelkezik, és csak ezek olyan bináris műveletek, melyek nem küszöbfüggvények.

108. Ha $\Sigma(g) = (s_0, s_1, \dots, s_n)$, g értéke s_0 olyan esetben 1, amikor $x_0 = 1$, és $2^n - s_0$ olyan esetben, amikor $x_0 = 0$. Továbbá $\Sigma(f_0) + \Sigma(f_1) = (s_1, \ldots, s_n)$, és

$$\begin{aligned}\Sigma(f_0) &= \sum_{x_1=0}^{1} \cdots \sum_{x_n=0}^{1} (\bar{x}_1, \ldots, \bar{x}_n) g(0, \bar{x}_1, \ldots, \bar{x}_n) \\ &= \sum_{x_1=0}^{1} \cdots \sum_{x_n=0}^{1} \big((1, \ldots, 1) - (x_1, \ldots, x_n)\big)\big(1 - g(1, x_1, \ldots, x_n)\big) \\ &= (2^{n-1} - s_0, \ldots, 2^{n-1} - s_0) + \Sigma(f_1).\end{aligned}$$

Így $n > 0$ esetén a válaszok a következők: (a) $N(f_0) = 2^n - s_0$, $\Sigma(f_0) = \frac{1}{2}(s_1 - s_0 + 2^{n-1}, \ldots, s_n - s_0 + 2^{n-1})$; (b) $N(f_1) = s_0$, $\Sigma(f_1) = \frac{1}{2}(s_1 + s_0 - 2^{n-1}, \ldots, s_n + s_0 - 2^{n-1})$. (Ezzel ekvivalens eredményekről beszélt Goto a MIT-en tartott előadásaiban 1963-ban.)

109. (a) $a_1 + \cdots + a_k \geq b_1 + \cdots + b_k$ akkor és csak akkor, ha $k - a_1 - \cdots - a_k \leq k - b_1 - \cdots - b_k$.

(b) Legyen $\alpha^+ = (a_1, a_1{+}a_2, \ldots, a_1{+}\cdots{+}a_n)$. Ekkor az α^+-ból és β^+-ból komponensenkénti minimumszámítással nyert $(c_1, \ldots, c_n)$ vektor éppen $(\alpha \wedge \beta)^+$. (Világos, hogy $c_j = c_{j-1} + a_j$ vagy b_j.)

(c) Folytassuk – mint (b)-ben – de komponensenkénti *maximumszámítással*; vagy vegyük az $\overline{\bar{\alpha} \wedge \bar{\beta}}$ formulát.

(d) Igaz, mert max és min teljesíti a disztributivitási törvényeket. (Valóban, egy disztributív vegyes-alapszámú majorizációs hálót nyerünk, így az összes olyan $a_1 \ldots a_n$ n-est tartalmazó halmazból, melyre minden $1 \leq j \leq n$ esetén $0 \leq a_j < m_j$.)

(e) $\alpha 1$ lefedi $\alpha 0$-t, $\alpha 10\beta$ pedig lefedi $\alpha 01\beta$-t. (Ez a jellemzés Winder [?] cikkéből származik, de Winder nem bizonyította a háló tulajdonságot. A hálót gyakran $M(n)$-nek nevezik; lásd Lindström [?] és Stanley [?] dolgozatait.)

(f) (e) miatt $r(\alpha) = na_1 + (n-1)a_2 + \cdots + a_n$.

(g) $0\beta \succeq 0\alpha$ akkor és csak akkor, ha $\beta \succeq \alpha$ és $1\beta \succeq 0\alpha$ akkor és csak akkor, ha $1\beta \succeq 10\ldots0 \vee 0\alpha = 1\alpha'$.

(h) Azaz, hány $a_1 \ldots a_n$ bír azzal a tulajdonsággal, hogy $a_1 \ldots a_k$ nem tartalmaz több 1-est, mint 0-át. A válasz $\binom{n}{\lfloor n/2 \rfloor}$; lásd például a 2.2.1. pont 4. vagy a 7.2.1.6. alpont 42.(a) gyakorlatokat.

110. (a) Ha $x \subseteq y$, akkor $x \preceq y$, ezért $f(x) \leq f(y)$; QED.

(b) Nem; A küszöb függvény nem szükségszerűen monoton (lásd). De meg *lehet* mutatni hogy f reguláris ha azt is megköveteljük, hogy $w_n \geq 0$: Amikor $f(x) = 1$ és y fedi x-et még az is igaz, hogy $w \cdot y \geq w \cdot x$.

(c) Valahányszor $f(x) = 1$ és $x_j < x_{j+1}$, akkor lesz $f(y) = 1$, ha y fedi x-et amikor $x_j \leftrightarrow x_{j+1}$; ennélfogva $s_j \geq s_{j+1}$. (Ez az érvelés megállja a helyét, akkor is ha $w_n < 0$.)

(d) Nem; Tekintsük például $\langle x_1 x_2^2 x_3^2 \rangle$-t, ami megegyezik $\langle x_1 x_2 x_3 \rangle$-al. Ellenpéldák keletkezhetnek akkor is ha a súlyok minimalizálják $w_1 + \cdots + w_n$-et, mivel a 103. gyakorlatbeli lineáris programnak nem mindig egyetlen megoldása van. Egy ilyen esetet találtak Muroga, Tsuboi, és Baugh, ami $\rangle x_1^{17} x_2^9 x_3^8 x_4^6 x_5^7 x_6^5 x_7^3 x_8^2 x_9^2 \langle$, ez egy olyan függvény, ami szimmetrikus x_4-re és x_5-re. Azonban, ha $s_j > s_{j+1}$ a (c) miatt $w_j > w_{j+1}$ kell hogy legyen.

111. (a) Keressen egy optimális önduális f függvényt, ugyanúgy mint a 14. gyakorlatban. Probléma esetén legyen $f(x_1, \ldots, x_n) = x_1$. Ekkor $f(x_1, \ldots, x_n) = [r_1^{x_1} \ldots r_n^{x_n} \geq \sqrt{r_1 \ldots r_n}]$, kivéve, ha „$\geq$" $x_1 = 0$ esetén „$>$" lesz. Ez a függvény reguláris, ha $r_1 \geq \cdots \geq r_n \geq 1$.

(b) Legyen g az (a)-ban előállított reguláris, önduális függvény. Ha f egy adott reguláris, önduális függvény, akkor igazolni fogjuk, hogy mivel mindkét függvény önduális, amennyiben minden x vektorra $f(x) \leq g(x)$ következik az $f = g$.

Tegyük fel, hogy $f(x) = 1$ és legyen a minimális olyan $y \preceq x$, amelyre $f(y) = 1$. Ha igazoltuk hogy $g(y) = 1$, akkor nyilván $g(x) = 1$ is fennáll. Lásd Makino[?] és Kameda[?] cikkét.

Például $n = 5$ esetén mindössze hét önduális reguláris Boole-függvény van, amiket a 8. ábrán látható következő minimális elemek generálnak: 10000; 01111, 10001; 01110, 10010; 01101, 10011, 10100; 01100; 01011, 11000; 00111. Így egy optimális klikk mindössze néhány függvényérték megvizsgálásával megtalálható.

(c) Tegyük fel, hogy $1 > p_1 \geq \cdots \geq p_r \geq \frac{1}{2} > p_{r+1} \geq \cdots \geq p_n > 0$. Legyen $f_k(x_1, \ldots, x_n)$ a k-adik önduális függvény és $F_k(x_1, \ldots, x_n)$ ennek egész együtthatós multilineáris reprezentációja. Keressük a $G(p_1, \ldots, p_n) = \max_k F_k(p_1, \ldots, p_n)$ optimális elérhetőséget. Ha $p_1 \leq p_1'$,..., $p_n \leq p_n'$, akkor a 12. gyakorlat (e) pontja szerint $F_k(p_1, \ldots, p_n) \leq F_k(p_1', \ldots, p_n')$; ennek megfelelően $G(p_1, \ldots, p_n) \leq G(p_1', \ldots, p_n')$.

Emiatt ha $0 < r < n$, akkor azt kapjuk hogy $G(p_1, \ldots, p_n) \leq G(p_1, \ldots, p_r, \frac{1}{2}, \ldots, \frac{1}{2})$. Az utóbbi $F(p_1, \ldots, p_r, \frac{1}{2}, \ldots, \frac{1}{2})$ az (a)-ban kialakított f függvény. Ez a függvény nem függ $(x_{r+1}, \ldots, x_n)$-től, így az optimumot adja.

$r = 0$ esetén a probléma mélyebbnek tűnik. Rendelkezünk a $G(p_1, \ldots, p_n) \leq G(p_1, \ldots, p_1)$-vel, így levonhatjuk azt a következtetést, hogy az optimális klikk $f(x_1, \ldots, x_n) = x_1$, amennyiben meg tudjuk mutatni hogy valahányszor $p < \frac{1}{2}$ az $F_k(p, \ldots, p) \leq p$ minden k-ra. Általában $F_k(p \ldots, p) = \sum_m c_m p^m (1-p)^{n-m}$, ahol c_m az olyan x vektorok száma, amelyekre $f_k(x) = 1$ és $\nu x = m$. A 70. gyakorlat alapján $c_m + c_{n-m} = \binom{n}{m}$, minden k-ra. Az Erdős-Radó tétel miatt (7.2.1.3–|erdos-korado| gyakorlat) $c_m \leq \binom{n-1}{m-1}$ bármely m halmazból álló egymást metsző családra , ahol $m \leq n/2$. Az eredmény ebből már adódik.

Lásd Amir[?] és Wool [?] cikkét.

112. (a) A meghatározó termek sorrendben: 0, $+xy$, $-xy$, $+x$, $-xy$, $+y$, $-2xy$, $-xy$, $+xy$, $+2xy$, $-y$, $+xy$, $-x$, $+xy$, $-xy$, 1; Így $F(f) = 1$, ha f az $\wedge$, $\bar{\vee}$, $\equiv$, $\subset$, $\supset$, (b) A 01101 kitevőnek megfelelő együttható, mondjuk f_{0**0*} a 12. válasz jelölése szerint, lineáris kombinációja a $\lceil -2^{k-1} \rceil \leq f_{0**0*} \leq \lceil 2^{k-1} \rceil$ intervallumba eső igazságtábla bemeneteknek, ahol k a csillagok száma. Így a meghatározó együttható akkor és csak akkor pozitív, ha az kevert alapszám

$$\begin{bmatrix} f_{**\ldots*}, & f_{0*\ldots*}, & \ldots, & f_{*0\ldots0}, & f_{00\ldots0} \\ 2^m{+}1, & 2^{m-1}{+}1, & \ldots, & 2^1{+}1, & 2^0{+}1 \end{bmatrix}$$

pozitív, ahol az f-ek fordított Chase sorrendben vannak és a $2^k + 1$ alapszám egy k csillagot tartalmazó f-nek felel meg. Például, ha $m = 2$ az $F(f) = 1$ akkor és csak akkor, ha az összeg $18f_{**} + 6f_{0*} + 2f_{*0} + f_{00} = 18(f_{11} - f_{01} - f_{10} + f_{00}) + 6(f_{01} - f_{00}) + 2(f_{10} - f_{00}) + f_{00} = 18f_{11} - 12f_{01} - 16f_{10} + 11f_{00}$ pozitív; így a küszöb függvény felírható $\langle f_{11}^{18} \bar{f}_{01}^{12} \bar{f}_{10}^{16} f_{00}^{11} \rangle$.

(Ebben a speciális esetben a legegyszerűbb $\langle f_{11} f_{11} \bar{f}_{01} \bar{f}_{10} f_{00} \rangle$ kifejezés érvényes. Azonban a (c) részben látni fogjuk, hogy ha m nagy nem lehet sokat tenni.)

(c) Tegyük fel, hogy $F(f) = [\sum_\alpha v_\alpha (f_\alpha - \frac{1}{2}) > 0]$, ahol az összegzést a 2^m m hosszúságú α bináris sorozatra értjük, ahol minden v_α egész értékű súly. Definiáljuk a

$$w_\alpha = \sum_\beta (-1)^{\nu(\alpha \dot{-} \beta)} v_\beta \qquad \text{and} \qquad F_\alpha = \sum_\beta (-1)^{\nu(\alpha \dot{-} \beta)} f_\beta - 2^{m-1}\,[\alpha = 00\ldots0];$$

úgy, hogy például $w_{01} = -v_{00} + v_{01} - v_{10} + v_{11}$ és $F_{11} = f_{00} - f_{01} - f_{10} + f_{11}$. Meg lehet mutatni, hogy $F_{1^k 0^l} = 2^l f_{*^k 0^l}$, amennyiben $F_\alpha = 0$, amikor $\nu(\alpha) > k > 0$. Ezért az F_α transzformált igaz együtthatói meghatározzák a multilineáris ábrázolásban a meghatározó együttható jelét. Azonkívül megkaptuk, hogy $F(f) = [\sum_\alpha w_\alpha F_\alpha > 0]$.

A bizonyítás alapötlete olyan f tesztfüggvény választása, amelyikből le tudjuk vezetni az w_α transzformált súlyok tulajdonságait. Például, ha $f(x_1, \ldots, x_m) = x_1 \oplus \cdots \oplus x_k$, akkor $F_\alpha = 0$ minden α-ra, kivéve az $F_{1^k 0^{m-k}} = (-1)^{k-1} 2^{m-1}$-et. Az $x_1 \oplus \cdots \oplus x_k$ multilineáris reprezentációjának meghatározó termje $\lceil (-2)^{k-1} \rceil x_1 \ldots x_k$. Emiatt arra a következtetésre jutunk, hogy $w_{1^k 0^{m-k}} > 0$, és hasonlóan, hogy $w_\alpha > 0$ for all α. Általában, ha m-ről $m+1$-re változik, de az f nem függ az x_{m+1}-től, akkor $F_{\alpha 0} = 2F_\alpha$ and $F_{\alpha 1} = 0$.

Az $x_2 \oplus \cdots \oplus x_m \oplus x_1\bar{x}_2 \ldots \bar{x}_m$ teszt függvény igazolja hogy

$$w_{1^m} > (2^{m-1}-1)w_{01^{m-1}} + \sum_{k=1}^{m-1} w_{1^k01^{m-1-k}} + \text{kisebb tagok},$$

ahol a kisebb tagok csak w_α-t jelentik $\nu(\alpha) \le m-2$ esetben. Speciálisan, $w_{11} > w_{01} + w_{10} + w_{00}$. Az $x_1 \oplus \cdots \oplus x_{m-1} \oplus \bar{x}_1 \ldots \bar{x}_{m-2} @ (x_{m-1} \oplus \bar{x}_m)$ teszt függvény mutatja, hogy

$$w_{1^{m-2}01} > (2^{m-2}-1)w_{1^{m-2}10} + \sum_{k=0}^{m-3} (w_{1^k01^{m-3-k}10} + w_{1^k01^{m-3-k}01}) + \text{kisebb tagok},$$

ahol a kisebb tagokra ezúttal $\nu(\alpha) \le m-3$. speciálisan $w_{101} > w_{110} + w_{010} + w_{001}$. Az indexek permutálásával hasonló egyenlőtlenségekhez jutunk

$$w_{\alpha_j} \;>\; (2^{\nu(\alpha_j)-1} - 1)w_{\alpha_{j-1}} \qquad \text{for } 0 < j < 2^m,$$

mivel a w-k gyorsan növekedni kezdenek. Azt kapjuk, hogy $v_\alpha = \sum_\beta (-1)^{\nu(\beta \dot{-} \alpha)} w_\beta / n$ és ezért $|v_\alpha| = w_{11\ldots1}/n + O(w_{11\ldots1}/n^2)$. [*SIAM J. Discrete Math.* **7** (1994), 484–492. Ennek az eredménynek egy fontos általánosítását találták Alon[**?**] és Vũ. [**?**]]

113. A megadott g_3 az $S_{2,3,6,8,9}$, mivel a megadott g_2 az $S_{2,3,4,5,8,9,10,11,12}$.

A nehezebb $S_{1,3,5,8}$ függvényre, legyen $g_1 = [\nu x \ge 6]$; $g_2 = [\nu x \ge 3]$; $g_3 = [\nu x - 5g_1 - 2g_2 \ge 2] = S_{2,4,5,9,10,11,12}$; $g_4 = [2\nu x - 15g_1 - 9g_3 \ge 1] = S_{1,3,5,8}$. Lásd M. A. Fischler[**?**] és Tannenbaum[**?**].

114. $[4x+2y+z \in \{3,6\}] = (\bar{x} \wedge y \wedge z) \vee (x \wedge y \wedge \bar{z})$. Hasonlóan, *tetszőleges* n-változós Boole-függvény egy $2^n - 1$-változós szimmetrikus függvény speciális esete. Lásd Kautz[**?**] cikkét.

115. Mindkét esetben önduális, ezért feltételezhetjük hogy $x_0 = 0$. Ekkor

$$s_j = [x_j + \cdots + x_{j+m-1} > x_{j+m} + \cdots + x_{j+2m-1}].$$

Ha $x_1 + \cdots + x_{2m}$ páratlan, akkor $s_j = \bar{s}_{j+m}$; és így $s_1 + \cdots + s_{2m} = m$ és az eredmény 1. De, ha $x_1 + \cdots + x_{2m}$ páros, akkor az $x_j + \cdots + x_{j+m-1} - x_{j+m} - \cdots - x_{j+2m-1}$ különbség nulla lesz legalább egy $j \le m$-re; ami miatt $s_j = s_{j+m} = 0$, így $s_1 + \cdots + s_{2m} < m$ lesz.

116. (a) Ez akkor és csak akkor implikáns, ha $f(x) = 1$ valahányszor $j \le \nu x \le n-k+j$. Ez akkor és csak akkor prímimplikáns, ha $f(x) = 0$ valahányszor $\nu x = j-1$ vagy $\nu x = n-k+j+1$.

(b) Tekintsük a $v = v_0v_1 \ldots v_n$ sorozatot, amelyre $f(x) = v_{\nu x}$. Az (a) miatt $\binom{a+b+c}{a,b,c}$ olyan prímimplikáns létezik, ahol $v = 0^a1^{b+1}0^c$. A szóbanforgó esetben $a = b = c = 3$, tehát 1680 prímimplikáns létezik.

(c) Egy általános szimmetrikus függvényre összeadjuk a v-ben lévő 1-esek szerinti prímimplikánsokat. Világos hogy, ha $a < c-1$, akkor több van $v = 0^{a+1}1^{b+1}0^{c-1}$-re, mint $v = 0^a1^{b+1}0^c$-re. Így a maximum elérése esetén v-ben nincs két egymásutáni 0.

Legyen $\hat{b}(m,n)$ a lehetséges prímimplikánsok maximális száma, ha $v_m = 1$ és $v_j = 0$ amikor $m < j \le n$. Ekkor amennyiben $m \le \frac{1}{2}n$ azt kapjuk, hogy

$$\begin{aligned}\hat{b}(m,n) &= \max_{0 \le k \le m} \left(\binom{n}{k, m-k, n-m} + \hat{b}(k-2,n) \right) \\ &= \binom{n}{\lceil m/2 \rceil, \lfloor m/2 \rfloor, n-m} + \hat{b}(\lceil m/2 \rceil - 2, n),\end{aligned}$$

ahol $\hat{b}(-2,n) = \hat{b}(-1,n) = 0$. És a teljes maximum:

$$\hat{b}(n) \;=\; \binom{n}{n_0, n_1, n_2} + \hat{b}(n_1 - 2, n) + \hat{b}(n_2 - 2, n), \qquad n_j = \left\lfloor \frac{n+j}{3} \right\rfloor.$$

Speciálisan azt kapjuk, hogy a $v = 1101111011$-vel elérhető maximum $\hat{b}(9) = 1698$.

(d) Stirling közelítéssel, $\hat{b}(n) = 3^{n+3/2}/(2\pi n) + O(3^n/n^2)$.

(e) Ebben az esetben az alkalmas rekurzió $m < \lceil n/2 \rceil$-re:

$$\tilde{b}(m,n) = \max_{0\le k\le m}\left(\binom{n}{k, m-k, n-m} + \binom{n}{k-1, 0, n-k+1} + \tilde{b}(k-2,n)\right)$$
$$= \binom{n}{\lceil m/2\rceil, \lfloor m/2\rfloor, n-m} + \binom{n}{\lceil m/2\rceil - 1} + \tilde{b}(\lceil m/2\rceil - 2, n)$$

és $\tilde{b}(n) = \tilde{b}(\lceil n/2\rceil - 1, n)$ maximalizálja a $\min\bigl(\text{prmimpliknsok}(f), \text{prmimpliknsok}(\bar{f})\bigr)$. Azt kapjuk, hogy $(\tilde{b}(1), \tilde{b}(2), \dots) = (1, 1, 4, 5, 21, 31, 113, 177, 766, 1271, 4687, 7999, 34412, \dots)$; például, $\tilde{b}(9) = 766$ megfelel az $S_{0,2,3,4,8}(x_1, \dots, x_9)$-nek. Közelítőleg, $\tilde{b}(n) = 2^{(3n+3+(n \bmod 2))/2}/(2\pi n) + O(2^{3n/2}/n^2)$.

Hivatkozások: Summaries, Summer Inst. for Symbolic Logic (Dept. of Math., Cornell Univ., 1957), 211–212; B. Dunham[?] és Fridshal[?] Vikulin[?], ami 1960-ban végzett munkákról számol be; Igarashi[?]

117. Az n-kocka olyan részkockáinak maximális száma, amelyek közül egyik sem tartalmazza a másikat, megkapható, ha tekintjük az összes $\lfloor n/3\rfloor$ dimenziós részkockát. (Ugyanez elérhető, ha az összes $\lfloor (n+1)/3\rfloor$ dimenziós részkockát tekintjük. Például, ha $n = 2$, akkor választhatjuk akár a $\{0{*}, 1{*}, {*}0, {*}1\}$-t, akár a $\{00, 01, 10, 11\}$-t.) Ennek megfelelően $b^*(n) = \binom{n}{\lfloor n/3\rfloor} 2^{n-\lfloor n/3\rfloor} = 3^{n+1}/\sqrt{4\pi n} + O(3^n/n^{3/2})$. Lásd Vikulin [?] cikkét az előző válaszból, továbbá Chandra [7] és Markowsky [29], valamint Metropolis [?] és Rota [?] cikkét.

118. Két függvényt ekvivalensnek tekintünk, ha az egyik a másikból a változóik komplementálásával és/vagy permutálásával megkapható, de a függvényérték komplementálása nélkül. Az ilyen függvények prímimplikánsainak száma nyilván ugyanannyi. Ezt az ekvivalencia relációt később a 125-ös válaszban tanulmányozzuk. Egy, a 30. gyakorlaton alapuló számítógépes program a következő eredményt adja:

m	Osztályok	Függvények	m	Osztályok	Függvények	m	Osztályok	Függvények
0	1	1	5	87	17472	10	7	632
1	5	81	6	70	12696	11	1	96
2	18	1324	7	43	7408	12	2	24
3	46	6608	8	24	3346	13	1	16
4	87	14536	9	10	1296	14	0	0

Itt a megfelelő statisztikákat látjuk az ötváltozós függvényekre:

m	Osztályok	Függvényeks	m	Osztályok	Függvények	m	Osztályok	Függvények
0	1	1	11	186447	666555696	22	338	608240
1	6	243	12	165460	590192224	23	130	197440
2	37	14516	13	129381	459299440	24	71	75720
3	244	318520	14	91026	319496560	25	37	28800
4	1527	3319580	15	57612	199792832	26	15	10560
5	6997	19627904	16	33590	113183894	27	6	2880
6	23434	73795768	17	17948	58653984	28	4	1040
7	57048	190814016	18	8880	27429320	29	2	640
8	105207	362973410	19	3986	11597760	30	2	48
9	152763	538238660	20	1795	4548568	31	2	64
10	183441	652555480	21	720	1633472	32	1	16

119. Több szerző igazolta, hogy $b(n) = \hat{b}(n)$; Gadzhiev[?] bizonyította, hogy $n \le 6$-ra az egyenlőség teljesül.

120. (a) Itt minden primimplikáns minterm, mivel az n-kockának nincsenek azonos paritású szomszédos pontjai. Ezért a teljes diszjunktív normálforma az egyetlen megfelelő DNF. (b) Itt minden prímimplikáns két szomszédos pontot fed le. Ide kell tartoznia a $\nu x = 1$ and $\nu x = 6$ pontok lefedéséhez a 14 darab $0^j * 0^{6-j}$ és $1^j * 1^{6-j}$ részkockának, ahol $0 \leq j \leq 6$. A többi $\binom{7}{3} + \binom{7}{4} = 70$ pontot le lehet fedni 35 jól megválasztott prímimplikánssal (lásd, például a 6.5–|perm-prefixes| gyakorlatot, vagy a 7.2.1.6 pontbeli „karácsonyfa mintát”). Ezért a legrövidebb DNF hossza 49. [Egy nyilvánvaló, de félrevezető S. B. Yablonsky publikációjában [**?**] az az állítás, hogy 70 prímimplikáms szükséges.]

(c) Az $(x_1, \ldots, x_{n-1})$-nek 2^{n-1}-féle megválasztásának mindegyikéhez legfejebb egy implikáns szükséges, ami azt mutatja meg, hogy a függvény hogyan viselkedik az x_n vonatkozásában.

[Majdnem minden n-változós Boole-függvénynek van legrövidebb DNF-je, ami aszimptotikusan $\Theta(2^n/(\log n \log\log n))$ prímimplikánsból áll. Lásd R. G. Nigmatullin[**?**], V. V. Glagolev,[**?**] A. D. Korshunov,[**?**] N. Pippenger,[**?**]

121. (a) Legyen adva $x = x_1 \ldots x_m$ and $y = y_1 \ldots y_n$. Mivel f a $(\nu x, \nu y)$ függvénye, összesen $2^{(m+1)(n+1)}$ lehetőség van.

(b) Ebben az esetben $\nu x \leq \nu x'$ és $\nu y \leq \nu y'$ implikálja, hogy $f(x,y) \leq f(x', y')$. Minden ilyen függvény megfelel az $a_0 = (-\frac{1}{2}, n+\frac{1}{2})$-ból az $a_{m+n+2} = (m+\frac{1}{2}, -\frac{1}{2})$-ba vezető cikkcakkos útnak, ahol $a_j = a_{j-1} + (1,0)$ or $a_j = a_{j-1} - (0,1)$ for $1 \leq j \leq m+n+2$; az $f(x,y) = 1$ akkor és csak akkor, ha a $(\nu x, \nu y)$ pont az út felett helyezkedik el. Így a lehetőségek száma az ilyen utak száma, nevezetesen $\binom{m+n+2}{m+1}$.

(c) Komplementáláskor x és y cserélődik νx ről $m - \nu x$-re és νy-ről $n - \nu y$-ra. Tehát, ha m is és n is párosak nincsenek ilyen függvények; egyébként $2^{(m+1)(n+1)/2}$ létezik.

(d) A (b) út kell hogy az $a_j + a_{m+n+2-j} = (m,n)$-t teljesítse $0 \leq j \leq m+n+2$-re. Ezért létezik $\binom{\lceil m/2\rceil + \lceil n/2\rceil}{\lceil m/2\rceil}[m$ páratlan vagy n páratlan$]$ ilyen függvény. Például, az a tíz eset, amikor $m = 3$ és $n = 6$. EZ ITT EGY ÁBRA

122. Egy ilyen függvény akkor és csak akkor reguláris a baloldalon lévő x-ekre és a jobboldalon lévő y-okra, ha a cikkcakkos út nem tartalmazza az (x,y) és az $(x+2,y)$ pontokat $0 < y < n$ esetén. Ugyancsak akkor és csak akkor reguláris az x-ek baloldalán lévő y-ra, ha a cikkcakkos út nem tartalmazza az $(x, y+2)$ és (x,y) pontokat, amikor $0 < x < m$. Ez akkor és csak akkor egy küszöb függvény, ha létezik egy egyenes vonal az $(m/2, n/2)$ ponton keresztül, úgy hogy az (s,t) akkor és csak akkor van a vonal felett, ha $0 \leq s \leq m$ és $0 \leq t \leq n$-re (s,t) az út felett van. Így az előző válaszban illusztrált 5 és 8 esetek nem regulárisak. Az 1, 2, 3, 7, 9, és 10 esetek küszöb függvények. A maradék reguláris nem-küszöb függvényeket a következőkép lehet kifejezni: $((x_1 \vee x_2 \vee x_3) \wedge < x_1x_2x_3y_1y_2y_3y_4y_5y_6\ ) \vee (x_1 \wedge x_2 \wedge x_3)$ (4. eset); $< 00x_1x_2x_3y_1y_2y_3y_4y_5y_6\ \vee (< x_1x_2x_3 \wedge < 11x_1x_2x_3y_1y_2y_3y_4y_5y_6\ )$ (6. eset).

123. Az önduális *reguláris* függvényeket kis n-ekre viszonylag könnyű kilistázni, de a számuk gyorsan növekszik. $n = 9$ esetén a számuk már 319,124, amit Muroga, Tsuboi, and Baugh talált meg 1967-ben. Ha $n = 10$, akkor a számuk 1,214,554,343 (lásd a 7.1.4–|reg-enum|gyakorlatot). Az 5.táblázatban $n \leq 6$-ra a megfelelő számok megtalálhatók, mivel $n < 9$re az összes ilyen függvény küszöb függvény; számuk 135 ha $n = 7$, és 2470 ha $n = 8$.

A küszöb feltételek tesztelését tetszőleges ilyen függvényre gyorsan elvégezhetjük a 103. gyakorlatbeli módszer finomításával, mivel a megszorítások csak azokra a *minimális* x vektorokra szükségesek (tekintettel a majoritásra) amelyekre $f(x) = 1$.

Az n-változós küszöbfüggvények θ_n számára fennáll, hogy $\lg\theta_n = n^2 - O(n^2/\log n)$; lásd Yu. A.Zuev [**?**], *Matematicheskie Voprosy Kibernetiki* **5** (1994), 5–61.

124. Az 5. táblázatban felsorolt 222 ekvivalencia osztályban 24 osztály mérete $2^{n+1}n! = 768$. Ennek megfelelően a problémára $24 \times 768 = 18432$ válasz létezik. Ezek közül egy a $(w \wedge (x \vee (y \wedge z))) \oplus z$ függvény.

125. 0; x; $x \wedge y$; $x \wedge y \wedge z$; $x \wedge (y \vee z)$; $x \wedge (y \oplus z)$. (Ezek a függvények $x \wedge f(y,z)$ alakúak, ahol f befutja a kétváltozós függvények ekvivalencia osztályait a változóik permutálására és/vagy komplementálására nézve, de *nem* a függvényértékekére. Általában jelentse $f \simeq g$, hogy f ekvivalens g-vel ebben a gyengébb értelemben, de $f \cong g$-t írunk, ha az 5. táblázat értelmében ekvivalensek. Tehát $x \wedge f \cong x \wedge g$ akkor és csak akkor, ha $f \simeq g$, feltéve hogy f és g nem függnek az x változótól. Ezután könnyű belátni, hogy $(x \wedge f) \simeq (\bar{x} \vee \bar{g})$ lehetetlen. De, ha $(x \wedge f) \simeq (x \wedge g)$, akkor az $f \simeq g$ bebizonyításához megmutatjuk hogy, ha σ az $\{x_0, \ldots, x_n\}$-re egy kiválasztott permutáció és ha $x = x_1 \ldots x_n$, akkor az $x_0 \wedge f(x) = (x_0\sigma) \wedge g(x\sigma)$ identitásnak következménye az $f(x) = g(x\sigma\tau)$. Itt a τ a $x_0 \leftrightarrow x_0\sigma$ cseréket végzi el. Az 5. táblázat alsó sora az $\simeq$ szerinti ekvivalencia osztályokat sorolja fel, de ha n-et 1-el növeljük 4-változós függvények esetén, akkor már 402 ilyen osztályt kapunk.)

126. (a) A függvény akkor és csak akkor irányító, ha van egy legfeljebb egy literált tartalmazó prímimplikánsa, vagy egy legfeljebb egy literált tartalmazó prímklóza.

(b) A függvény akkor és csak akkor irányító, ha a $\Sigma(f)$ legalább egy komponense egyenlő 0, 2^{n-1}, $N(f)$, vagy $N(f) - 2^{n-1}$. [Lásd I. , H. , és K. , *IEEE Signal Processing Letters* **11** (2004), 289–292, 6. állítás]

(c) Ha, mondjuk $\vee(f) = y_1 \ldots y_n$ $y_j = 0$-ra, akkor $f(x) = 0$ amikor $x_j = 1$. Ennélfogva az f akkor és cak akkor irányító, ha nem áll fenn, hogy $\vee(f) = \vee(\bar{f}) = 1 \ldots 1$ és $\wedge(f) = \wedge(\bar{f}) = 0 \ldots 0$. Ezzel a teszttel sok függvényre, amelynek értékét csak néhány pontban ismerjük, bizonyíthatjuk hogy nem irányító.

127. (a) Mivel egy $f(x_1, \ldots, x_n)$ önduális függvény pontosan 2^{n-1} pontban igaz, egyúttal irányító az x_j-re akkor és csak akkor, ha $f(x_1, \ldots, x_n) = x_j$.

(b) Egy definit Horn függvény nyilván irányító, ha (i) tartalmaz valamilyen egyetlen literálból álló klózt, vagy (ii) valamely literál minden klózban előfordul. Egyébként nem irányító. Ekkor $f(0, \ldots, 0) = f(1, \ldots, 1) = 1$, mivel (i) nem áll fenn; és ha x_j egy tetszőleges változó, van olyan C_0 klóz, amely nem tartalmazza $\bar{x}_j$-t és olyan C_1 klóz, amely nem tartalmazza x_j-t, mivel (ii) nem áll fenn. Megfelelő értéket választva a többi változónak elérhetjük, hogy $C_0 \wedge C_1$ hamis legyen akkor is ha $x_j = 0$ és akkor is ha $x_j = 1$.

128. Például, $(x_1 \wedge \cdots \wedge x_n) \vee (\bar{x}_1 \wedge \cdots \wedge \bar{x}_n)$.

129. $\sum_{k=1}^{n} (-1)^{k+1} \binom{n}{k} 2^{2^{n-k}+k+1} - 2(n-1) - 4(n \mod 2) = n2^{2^{n-1}+2} + O(n^2 2^{2^{n-2}})$. [Lásd W. Just, I. Shmulevich , és J. Konvalina, *Physica* **D197** (2004), 211–221.]

130. (a) Ha a_n az n vagy annál kevesebb változótól függő függvények száma és b_n a pontosan n változótól függő függvények száma, akkor $a_n = \sum_k \binom{n}{k} b_k$. Ugyanígy $b_n = \sum_k (-1)^{n-k} \binom{n}{k} a_k$. (Ezt a szabályt, amely C. E. Shannon nevéhez fűződik, [?] a 3. táblázat minden sorára alkalmazzák, *kivéve* a szimmetrikus függvényeket.) Ebben az esetben a keresett válasz $168 - 4 \cdot 20 + 6 \cdot 6 - 4 \cdot 3 + 2 = 114$.

(b) Ha van a'_n darab lényegesen különböző n vagy annál kevesebb változótól függő és b'_n darab pontosan n változótól függő függvény, akkor $a'_n = \sum_{k=0}^{n} b'_k$. Ennek megfelelően $b'_n = a'_n - a'_{n-1}$ és a válasz ebben az esetben $30 - 10 = 20$.

131. Legyenek $h(n)$ Horn függvények és $k(n)$ Krom függvények. Az világos, hogy $\lg h(n) \ge \binom{n}{\lfloor n/2 \rfloor}$ and $\lg k(n) \ge \binom{n}{2}$. V. B. Alekseyev[?] [*Diskretnaĭa Matematika* **1** (1989), 129–136] bizonyította, hogy $\lg h(n) = \binom{n}{\lfloor n/2 \rfloor}(1 + O(n^{-1/4} \log n))$. B. Bollobás, G. Brightwell , és I. Leader [*Israel J. Math.* **133** (2003), 45–60] bizonyították, hogy $\lg k(n) \sim \frac{1}{2}n^2$.

132. (a) A segítség igaz, mivel $\sum_y s(y)s(y \oplus z) = \sum_{w,x,y} (-1)^{f(w)+w \cdot y + f(x) + x \cdot (y+z)} = 2^n \sum_{w,x} (-1)^{f(w)+f(x)+x \cdot z} [x = w]$. Tegyük fel most, hogy $f(x) = g(x)$ az x-nek $2^{n-1} + k$ különböző értékére. Ekkor $f(x) = g(x) \oplus 1$ az x-nek $2^{n-1} - k$ különböző értékére. De, ha $|k| < 2^{n/2-1}$ az összes g affin függvényre, akkor azt kapjuk, hogy $|s(y)| < 2^{n/2}$ minden y-ra, ami $z = 0$ esetben ellentmond a segítségnek.

(b) Legyen $y = y_1 \ldots y_n$ adott, ekkor pontosan $2^{n/2}((y_1 y_2 + y_3 y_4 + \cdots + y_{n-1} y_n + 1 +$

$h(y_1, y_3, \ldots, y_{n-1})\big) \mod 2\big)$ megoldás létezik $f(x) = x \cdot y \mod 2$-re, ha $x_{2k} = y_{2k-1}$, amikor $1 \le k \le n/2$. Ugyanakkor $2^{n/2-1}$ megoldás létezik az $(x_2, x_4, \ldots, x_n)$ lehetséges $2^{n/2} - 1$-féle értékének mindegyikére. Ezért összesen $2^{n-1} \pm 2^{n/2-1}$ megoldás létezik. (Ez tulajdonképpen azt igazolja, hogy $\big(g(x_1, x_3, \ldots, x_{2n-1}) \cdot (x_2, x_4, \ldots, x_{2n}) + h(x_2, x_4, \ldots, x_{2n})\big) \mod 2$ bent függvény, valahányszor $g(x_1, x_3, \ldots, x_{2n-1})$ egy permutációja az összes $2^{n/2}$-bites vektornak.)

(c) Ha $f(x)$ bent függvény, akkor az (a)-beli okoskodás igazolja, hogy $s(y) = 2^{n/2}(-1)^{g(y)}$ valamely $g(y)$ Boole-függvényre. Ez a függvény szintén bent függvény, mivel $\sum_y (-1)^{g(y)+w\cdot y} = 2^{-n/2} \sum_{x,y} (-1)^{f(x)+x\cdot y+w\cdot y} = 2^{n/2} \sum_x (-1)^{f(x)}[x = w] = 2^{n/2}(-1)^{f(w)}$ minden w-re. Következéskép a segítség miatt $\sum_x (-1)^{f(x)+f(x\oplus z)} = 0$ minden nemzéró z-re.

Fordítva, tegyük fel, hogy $f(x)$ teljesíti a megadott feltételeket, és hogy $f(x) = 1$ az x-nek pontosan k értékére. Ha y egy tetszőleges Boole-vektor, akkor a $g(x) = (f(x) + x \cdot y) \mod 2$ Boole-függvény szintén teljesíti a feltételt. Ezért csak azt kell bizonyítani, hogy $k = 2^{n-1} \pm 2^{n/2-1}$.

Legyen A egy $2^n \times 2^n$ mátrix, ahol az x sorban és az y oszlopban az $f(x\oplus y)$ található. Legyen J egy csupa 1-esekből álló $2^n \times 2^n$ mátrix. Ekkor kapjuk, hogy $J^2 = 2^n J$ and $JA = AJ = kJ$ és így

$$2^n I \;=\; (J - 2A)^2 \;=\; 2^n J - 4kJ + 4A^2;$$

Amiből következik, hogy ha $y \ne 0\ldots 0$, akkor az olyan x-ek száma $k - 2^{n-2}$, amelyekre $f(x) = 1$ és $f(x \oplus y) = 1$. Más szóval, pontosan $k - 2^{n-2}$ darab olyan rendezett (w, x) vektorpár van, hogy $f(w) = f(x) = 1$ és $w \oplus x = y$. Az összes y feletti összegzéssel kapjuk, hogy $(2^n - 1)(k - 2^{n-2}) = k(k - 1)$. Ennek a kvadratikus egyenletnek a megoldása $k = 2^{n-1} \pm 2^{n/2-1}$.

(d) A 11. gyakorlat alapján az $x_1 \ldots x_r$ tag akkor és csak akkor fordul elő, ha az $f(x_1, \ldots, x_r, 0, \ldots, 0) = 1$ egyenletnek páratlan számú megoldása van. Egy ezzel ekvivalens feltétel:

$$\Big(\sum_{x_1,\ldots,x_r} (-1)^{f(x_1,\ldots,x_r,0,\ldots,0)} \Big) \mod 4 = 2\,.$$

A (c) részben láttuk, hogy ez az összeg

$$2^{-n} \sum_{x_1,\ldots,x_r,y} s(y)(-1)^{x_1y_1+\cdots+x_ry_r} \;=\; 2^{r-n} \sum_{y_{r+1},\ldots,y_n} s(0,\ldots,0,y_{r+1},\ldots,y_n).$$

Ha $r = n$, akkor az utolsó összeg $\pm 2^{n/2}$; másként szólva ez páros számú összeadandót tartalmaz, amelyek mindegyike $\pm 2^{r-n/2}$. Így az eredmény 4-nek többszöröse.

[A bent függvényeket O. S. Rothaus [?] vezette be 1966-ban; ezt a személyesen terjesztett cikket 1976-ban pulikálta a *J. Combinatorial Theory* **A20** (1976), 300–305. J. F. Dillon [?], *Congressus Numerantium* **14** (1975), 237–249, a bent függvények egy új családját fedezte fel, és $n \ge 8$ és n páros esetre sok más példát is talált. Bent függvények nem léteznek, ha n páratlan, de egy $g(x_1, \ldots, x_{n-1}) \oplus x_n \wedge h(x_1, \ldots, x_{n-1})$-hez hasonló függvénynek az összes affin függvénytől való távolsága $2^{n-1} - 2^{(n-3)/2}$, ha g és h bent függvények. Az $n = 15$ esetre N. J. Patterson[?] [?] és D. H. Wiedemann[?][?] jobb konstrukciót találtak *IEEE Transactions* **IT-29** (1983), 354–356, **IT-36** (1990), 443, ahol a kapott távolság $2^{14} - 108$.]

133. Legyen $p_k = 1/(2^{2^{n-k}} + 1)$, úgy hogy $\bar p_k = 2^{2^{n-k}}/(2^{2^{n-k}} + 1)$. Let $p_k = 1/(2^{2^{n-k}} + 1)$, so that $\bar p_k = 2^{2^{n-k}}/(2^{2^{n-k}}+1)$. [Ph.D. thesis (MIT, 1994).]

IRODALOMJEGYZÉK

[1] M. Ajtai, J. Komlós, E. Szemerédi. Sorting in $c \log n$ parallel steps. *Combinatorica*, 3(1):1–19, 1983. MR0716418 (85d:68017). 46

[2] B. I. Aspvall, M. F. Plass, R. E. Tarjan. A linear-time algorithm for testing the truth of certain quantified Boolean formulas. *http://www.sciencedirect.com/science/journal/00200190*, 8(3):121–123, 1979. MR0526451 (80b:68050). 62

[3] M. Ball. Matroids and a reliability analysis problem. *Mathematics of Operation Research*, 4(2):132–143, 1979. MR0543925 (80g:90057). 59

[4] O. Ball. Disjoint products and efficient computation of reliability. *Operation Research*, 36(5):703–715, 1988. MR0967305 (89k:90071). 59

[5] B. A. Bernstein. *University of California Publications in Mathematics*, 1:87–96, 1914. 53

[6] E. Boros, Y. J-M. M. Crama, O. Ekin, P., T. Ibaraki, A. Y. Kogan. Boolean normal forms, shellability, and reliability computations. *SIAM Journal on Discrete Mathematics*, 13(2):212–226, 2000. MR1760339 (2000m:06020). 59

[7] A. K. Chandra. On the number of prime implicants. *Discrete Mathematics*, 24:7–11, 1978. MR0522729 (82m:94055). 57, 74

[8] R. A. Cutler, S. Muroga. Derivation of minimal sums for completely specified functions. *IEEE Transactions on Computers*, 36(3):277–292, 1987. MR0886129 (89b:94035). 56

[9] A. De Morgan. *Transactions of the Cambridge Pholosophical Society*, 10:208–208, 1858. 6

[10] W. F. Dowling, J. H. Gallier. Linear-time algorithms for testing the satisfiability of propositional Horn formulae. *Discrete Mathematics*, 1(3):267–284, 1984. MR0770156 (86g:68144). 15

[11] C. C. Elgot. Decision problems of finite automata design and related arithmetics. *Transactions of the American Mathematical Society*, 98:21–51, 1961. MR0139530 (25 #2962). 69

[12] A. C. Ewing, J. P. Roth, E. Wagner. *AIEE Transactions*, 80(Part 1):450–458, 1961. 57

[13] T. Feder. Stable networks and product graphs. *Memoirs of the American Mathematical Society*, 116(555):1–223, 1995. MR1129115 1271694 (96a:68021). 28

[14] P. Fišer, J. Hlavička. Boom - a heuristic Boolean minimizer. *Computing and Informatics*, 22(1):19–51, 2003. 10

[15] M. Fredman, L. Khachiyan. On the complexity of dualization of monotone disjunctive normal forms. *Journal of Algorithms*, 21:618–628, 1996. MR1417667 (97e:68047). 56

[16] V. Gurvich, L. G. Hacsiján. On the frequency of the most frequently occurring variable in dual monotone DNFs. *Discrete Mathematics*, 169(1–3):245–248, 1997. MR1449725 (98b:06020). 55

[17] J. Hagauer, W. Imrich, S.. Recognizing median graphs in subquadratic time. *Theoretical Computer Science*, 215(1–2):123–136, 1999. MR1678773 (2000b:68173). 24

[18] A. Horn. On sentences which are true of direct unions of algebras. *Journal of Symbolic Logic*, 16:14–21, 1951. MR0040233 (12,662a). 12

[19] G. Istrate. The phase transition in random horn satisfiability and its algorithmic implications. *Random Structures and Algorithms*, 20:483–506, 2002. MR1908739 (2003c:68092). 61

[20] P. K. Jha, G. Slutzki. Convex-expansions algorithms for recognition and isometric embedding of median graphs. *Ars Combinatoria*, 34:75–92, 1992. MR1206551 (93m:05165). 24

[21] M. Karpinski. Functional decomposition and switching circuit design. *Journal of Society for Industrial and Applied Mathematics*, 11:291–335, 1963. MR0155728 (27 #5662). 63

[22] S. Kauffman. *Lectures on Mathematics in the Life Sciences*, 63–116. o., 1972. 32

[23] D. E. Knuth, R. W. Moore. An analysis of alpha-beta pruning. *Artificial Intelligence*, 6(4):273–326, 1975. MR0388881 (52 #9714). 55

[24] M. Krom. The decision problem for a class of first-order formulas in which all disjunctions are binary. *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik*, 13:15–20, 1967. MR0209120 (35 #24). 17

[25] M. Krom. The decision problem for formulas in prenex conjunctive normal form with binary disjunctions. *Journal of Symbolic Logic*, 35:210–216, 1970. MR0274290 (43 #55). 62

[26] J-M. K. Laborde. Sur le cardinal maximum de la base complete d'une fonction booléenne, en fonction du nombre de conjonctions de l'une de ses formes normales (franciául). *Discrete Mathematics*, 32:209–212, 1980. MR0592857 (81m:94035). 57

[27] L. B. Lamport. Time, clocks, and the ordering of events in a distributed system. *Communications of the ACM*, 21(7):558–565, 1978. 43

[28] H. A. Lewis. Renaming a set of clauses as a Horn set. *Journal of ACM*, 25(1):134–135, 1978. MR0468315 (57 #8151). 62

[29] G. Markowsky. Primes, irreducibles and extremal lattices. *Order*, 9(3):265–290, 1992. MR1211380 (94a:06015). 74

[30] W. S. McCullough, W. H. Pitts. A logical calculus of the ideas immanent in nervous activity. *Bulletin of Mathematical Biophysics*, 5:115–133, 1943. MR0010388 (6,12a). 30

[31] H. S. Miiller, R. O. Winder. *IRE Transactions on Electronic Computers*, EC–11:89–90, 1962. 19

[32] F. Mileto, G. Putzolu. Average values of quantities appearing in Boolean function minimization. *IEEE Transactions on Computers*, EC–13:87–92, 1964. MR0173596 (30 #3809). 58

[33] R. Minnick. Linear-input logic. *IRE Transactions on Electronic Computers*, EC–10:6–16, 1961. MR0122655 (22 #13378). 32, 69

[34] E. Morreale. *IEEE Transactions on Computers*, EC-16(?):611–620, 1967. 57

[35] C. S. S. Peirce. On an improvement in Boole's calculus of logic. *Proceedings of the American Arts and Sciences*, 7:250–261, 1867. 3

[36] C. S. S. Peirce. On the algebra of logic. *The American Journal of Mathematics*, 3:15–57, 1880. 3, 8

[37] E. L. Post. *Annals of Mathematics Studies*, 5:74–75, 1941. 18

[38] W. Quine. The problem of simplifying truth functions. *American Mathematical Monthly*, 59:521–531, 1952. MR0051191 (14,440e). 9

[39] W. Quine. Two theorems about truth functions. *Boletín de la Sociedad Matemática Mexicana*, 10:64–70, 1953. MR0057821 (15,277j). 10

[40] J. P. Robinson. A machine-oriented logic based on the resolution principle. *Journal of ACM*, 12(1):23–41, 1965. MR0170494 (30 #732). 57

[41] H. Scheffer. A set of five independent postulates for Boolean algebras, with application to logical constants. *Transaction of the American Mathematical Society*, 14(4):481–488, 1913. 5, 52

[42] C. E. Shannon, Jr. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 623–656, 1948. MR0026286 (10,133e). 2

TÁRGYMUTATÓ

NÉVMUTATÓ

MAGYAR NÉVMUTATÓ