Keresés matroidokban

Szakdolgozat

Szalkai Ákos

Témavezető: Katona O. H. Gyula

1996.

Tartalom

1. Keresés [1]

1.1. Definíciók

1.1.1. Keresési feladatok

Mielőtt pontosan definiálnánk, hogy mit fogunk keresés alatt érteni, tekintsünk néhány mindenki által ismert klasszikus példát. Természetesen olyan definíciót szeretnénk majd, amelybe az alábbiak mindegyike beletartozik.

1. Talán a legközismertebb keresési feladat a Barkochba játék.

2. Egy másik régről ismert problémakör a hamis érme keresése. Ennek több változata is létezik. Az alapváltozatban azt tudjuk, hogy n érme között pontosan 1 hamis van, ráadásul ez könnyebb, mint a többi, melyek egyforma tömegűek. Ezek után egy kétkarú mérleg segítségével kell a lehető legkevesebb méréssel megtalálni a hamis érmét. Ebből az egyszerű problémából egyszerűen kaphatunk jóval nehezebbeket is, ha több hamis érme is van, illetve, ha nem tudjuk előre, hogy a hamis érme könnyebb, vagy nehezebb[8, 9].

   E probléma egy másik, lényegesen különböző változatát kapjuk, ha van néhány egyforma tömegű valódi érménk és néhány, ugyancsak egyforma tömegű hamis érménk, ráadásul ismerjük is ezeket a tömegeket. Most egy egykarú (azaz a tálkájába tett érmék össztömegét jelző) mérleg segítségével kell minél kevesebb méréssel meghatározni a hamis pénzeket.

3. Az előzőekkel ellentétben egy komoly gyakorlati jelentőségű feladat a következő: adott egy lineárisan rendezett sorozat és egy a sorozat tagjaival összehasonlítható elem. A lehető legkevesebb összehasonlítás elvégzésével „tegyük a helyére” az elemet a sorozatban.

4. A következő probléma talán kevésbé közismert, pedig történetileg az első matematikailag vizsgált keresési feladat [2]: a lakosságból néhány

embert megfertőzött egy betegség, amelyet vérvétel után költséges vizsgálattal lehet csak kimutatni. Ezért a következő tesztet alkalmazzuk: egy általunk kiválasztott csoport tagjaitól vett vért összeöntjük, és az így kapott mintára csak egyszer elvégezve a vizsgálatot, megállapíthatjuk, hogy a vizsgált csoportban fertőzött volt-e valaki. A célunk a szokásos: a lehető legkevesebb ilyen teszt felhasználásával elkülöníteni a fertőzötteket.

Látható, hogy a fenti példák mindegyikében egy adott alaphalmazon kell megtalálnunk egy vagy több ismeretlen elemet, bizonyos megengedett tesztek segítségével. Mindezek alapján könnyen adódik az általános definíció:

1. Definíció. Legyenek $S \neq \emptyset$ egy adott halmaz (a keresés *alaphalmaza*), benne egy rögzített $x^* \in S$ elem; továbbá $\mathcal{F}$ egy S-en értelmezett függvénycsalád. $\mathcal{F}$ elemeit *keresőfüggvény*eknek nevezzük. Az első lépés során kérdésként kiválaszthatunk egy $f_1 \in \mathcal{F}$ keresőfüggvényt, amire válaszul $f_1(x^*)$-ot kapjuk. A következő lépésekben már az addig kapott válaszok figyelembevételével választhatunk új keresőfüggvényeket. Az $f_1, f_2, f_3, \dots \in \mathcal{F}$ függvények egy olyan sorozatát, melyre az $f_1(x^*), f_2(x^*), f_3(x^*), \dots$ értékek egyértelműen meghatározzák x^*-ot, *(sikeres) keresőalgoritmus*nak nevezzük. (Hallgatólagosan mindig feltesszük, hogy legalább egy ilyen algoritmus létezik.) Végül, az $(S, \mathcal{F})$ rendezett párt *keresési feladat*nak hívjuk.

Megállapodunk abban, hogy bár a k-adik keresőfüggvény ($f_k \in \mathcal{F}$) kiválasztása függ a az előzőleg kapott $f_1(x^*), f_2(x^*), f_3(x^*), \dots$ értékektől, legtöbbször mégis az ezt nem tükröző $(f_1, f_2, f_3, \dots)$ jelölést fogjuk alkalmazni a keresőalgoritmusokra.

A szokásos módon definiálhatjuk a különböző „keresési bonyolultságokat" is, véges S alaphalmaz és $\mathcal{F}$ keresőfüggvény-család mellett.

2. Definíció. Tegyük fel, hogy adott egy $L(S, \mathcal{F})$ keresési feladat, és ehhez egy $\mathcal{A} = (f_1, f_2, \dots)$ sikeres keresőalgoritmus, azaz amelyre a kapott $f_1(x^*), f_2(x^*), \dots, f_{l(x^*)}(x^*)$ értékek egyértelműen meghatározzák x^*-ot. Ekkor a — természetesen x^*-tól függő — $l(x^*)$ számot az x^* *($\mathcal{A}$ algoritmus melletti keresési) hossz*ának nevezzük, $L(\mathcal{A}) := \max_{x^* \in S} l(x^*)$-gal pedig az $\mathcal{A}$ *algoritmus hosszá*t jelöljük.

Ha emellett még S-en adott egy $\underline{p} = (p(x^*) : x^* \in S)$ valószínűségeloszlás is, akkor az $\overline{L}(\mathcal{A}; \underline{p}) := \sum_{x^* \in S} p(x^*)\, l(x^*)$ számot az $\mathcal{A}$ *algoritmus ($\underline{p}$ eloszlás melletti) átlagos hosszá*nak nevezzük. Ha nincs előre megadott eloszlásunk S-en, akkor átlagos hossz alatt az egyenletes eloszlás melletti átlagos hosszt értjük. (Tehát ekkor $\overline{L}(\mathcal{A}) = \frac{1}{n} \sum_{x^* \in S} l(x^*)$.)

Végül legyen $L(S,\mathcal{F}) := \min_{\mathcal{A}} L(\mathcal{A})$, illetve egy adott $\underline{p}$ eloszlás mellett $\overline{L}(S,\mathcal{F};\underline{p}) := \min_{\mathcal{A}} \overline{L}(\mathcal{A};\underline{p})$. Ezeket rendre az $(S,\mathcal{F})$ keresési feladat *(legrosszabb esetbeli) komplexitás*ának, illetve *átlagos komplexitás*ának nevezzük.

Egy $\mathcal{A}$ algoritmust, melyre $L(\mathcal{A}) = L(S,\mathcal{F})$, illetve $\overline{L}(\mathcal{A};\underline{p}) = \overline{L}(S,\mathcal{F};\underline{p})$, rendre (L)-optimális, illetve $(\overline{L})$-optimális algoritmusnak fogunk hívni.

Mivel a keresésre adott fenti definíció még rendkívül tág, érdemes a keresési feladatok több típusát megkülönböztetnünk.

1. S számossága szerint: ha S véges vagy megszámlálható, akkor *diszkrét*, egyébként *folytonos* feladatról beszélünk.

2. A megengedett $\mathcal{F}$-beli keresőfüggvények szerint is osztályozhatjuk a feladatokat. Ez történhet a keresőfüggvények értékkészletének elemszáma szerint is, de természetesen $\mathcal{F}$ különbözteti meg például a rendezési feladatokat a hamis érmét kereső feladatoktól.

3. Nagyon fontos különbséget tehetünk az algoritmusok típusa alapján. Egy $\mathcal{A}$ algoritmust *adaptív*nak nevezünk, ha az f_k keresőfüggvény kiválasztása függ az addig válaszul kapott $f_1(x^*),\ldots,f_{k-1}(x^*)$ értékektől. Ha viszont az $f_1, f_2, \ldots$ függvényeket előre rögzítjük, akkor $\mathcal{A}$-t *nemadaptív* algoritmusnak hívjuk. Nyilvánvalóan látszik, hogy a nemadaptív algoritmusok az adaptívak speciális esetei, így persze legalább olyan hosszúak lesznek, mint az optimális adaptív algoritmusok. A nemadaptív algoritmusok hosszát $L_{\mathrm{pre}}(S,\mathcal{F})$-fel fogjuk jelölni.

4. Végül optimalizálási szempontból is szétválaszthatjuk a feladatokat. Lehet az a célunk, hogy a minimális hosszú legrosszabb esetbeli algoritmust találjuk meg, de lehet az is, hogy a minimális átlagos hosszú algoritmust. Könnyen látható, hogy ezek ténylegesen különböző feladatok.

Bár a későbbiekben nem foglalkozunk ezzel, érdemes megemlíteni, hogy értelmes problémákat kapunk akkor is, ha a definícióban nem tesszük fel, hogy az algoritmusnak egyértelműen meg kell határozni x^*-ot. Ehelyett a szokásos módon itt is beszélhetünk *valószínűségi algoritmus*okról, ha csak „majdnem” egyértelműen, azaz mondjuk $\geq 1-\varepsilon$ valószínűséggel kell x^*-ot megtalálnunk. Egy másik lehetőség az, hogy az algoritmus akkor fejeződik be, ha tudjuk, hogy x^* az alaphalmaz egy „kis” részhalmazában van. (Tehát például, ha a $[0,1]$ intervallumban keresünk, akkor elegendő lehet meghatározni — előre adott $\delta > 0$ esetén — egy $\leq \delta$ hosszú intervallumot, amely tartalmazza x^*-ot.) Ezt *közelítő algoritmus*nak hívjuk.

Mielőtt továbblépnénk, rögzítjük, hogy a dolgozat hátralévő részében milyen típusú keresési feladatokról lesz szó.

1. Az S alaphalmaz véges, S elemszámát legtöbbször n-nel jelöljük.

2. Az $\mathcal{F}$ függvénycsalád véges. Mivel S végessége miatt minden $f \in \mathcal{F}$ függvény csak véges sok értéket vehet fel, így feltehetjük, hogy $f(S) \subseteq \{0, 1, \ldots, q-1\}$, tetszőleges $f \in \mathcal{F}$ esetén. Egy $(S, \mathcal{F})$ feladatot, ahol $|S| = n \geq 1$ és minden $f \in \mathcal{F}$ esetén $f(S) \subseteq \{0, 1, \ldots, q-1\}$, $q \geq 2$, egyszerűen (n, q)-feladatnak is fogunk nevezni.

A keresési feladatok legfontosabb és legjobban átlátott esete a $q = 2$ eset, azaz amikor egy keresőfüggvény legfeljebb két különböző értéket adhat (mint például a Barkochbában). Az ilyen feladatokat *bináris keresési feladat*oknak nevezzük. Könnyen látható, hogy ekkor egy $f \in \mathcal{F}$ keresőfüggvény és a hozzá tartozó $A = \{x \in S : f(x) = 1\}$ halmaz egyértelműen meghatározzák egymást. Így $\mathcal{F}$-et azonosíthatjuk egy $\mathfrak{A} \subseteq 2^S$ halmazcsaláddal, egy adott algoritmust pedig az $A_1, A_2, \ldots$ halmazsorozattal. A továbbiakban ezeket az $A_1, A_2, \ldots$ halmazokat *keresőhalmaz*oknak fogjuk nevezni.

1.1.2. Döntési fák

Egy $(S, \mathcal{F})$ feladathoz tartozó $\mathcal{A} = (f_1, f_2, \ldots)$ algoritmusnak szemléletes és jól használható leírását adhatjuk (gyökeres) fák segítségével. Első célunk ennek a pontos definiálása lesz, azonban először lássunk egy elnevezést:

3. Definíció. A T gyökeres fát (n, q)-*fá*nak nevezzük, ha pontosan n levele van, és minden belső csúcsnak legfeljebb q fia van (fiúnak a közvetlen leszármazottakat, azaz a gyökértől távolabbi szomszédokat fogjuk nevezni). T *reguláris* (n, q)-*fa*, ha minden belső csúcsnak pontosan q fia van. ($q = 2$ esetén *bináris fá*ról beszélünk.)

Figyeljük meg, hogy az első k teszt elvégzése után a következő információ áll rendelkezésünkre: a keresett x^* elem az

$$S_k(x^*) := \{x \in S : f_1(x) = f_1(x^*), \ldots, f_k(x) = f_k(x^*)\}$$

halmazhoz tartozik. Látható, hogy $l(x^*)$ definíciója alapján

$$S = S_0(x^*) \supseteq S_1(x^*) \supseteq \cdots \supseteq S_{l(x^*)}(x^*) = \{x^*\}.$$

Sőt, érdemes kicsit kiterjeszteni az előző jelölést. Tetszőleges $e_1, \ldots, e_k \in \{0, 1, \ldots, q-1\}$ esetén legyen

$$S(e_1, \ldots, e_k) := \{x \in S : f_1(x) = e_1, \ldots, f_k(x) = e_k\},$$

azaz $S(e_1, \ldots, e_k)$ jelöli azon $x \in S$ elemek halmazát, amelyek még lehetnek az ismeretlen elem, ha az első k teszt eredménye rendre $e_1, \ldots, e_k$ volt. Könnyen látható, hogy ezen halmazok közül az összes nemüreset, valamint még S-et véve, egyértelműen leírtuk az $\mathcal{A}$ algoritmust.

A döntési fa megkonstruálásához minden nemüres $S(e_1, \ldots, e_k)$ halmazhoz, illetve az S-hez rendeljünk egy csúcsot, az $S(e_1, \ldots, e_k)$-hoz tartozó csúcs fiai pedig legyenek az $S(e_1, \ldots, e_k, e)$, $(e \in \{0, 1, \ldots, q-1\})$ csúcsok. (Értelemszerűen az S lesz fa gyökere, és a leszármazottai az $S(e)$ csúcsok lesznek.) Nyilvánvaló, hogy ekkor a levelek éppen az egyelemű halmazoknak (azaz S elemeinek) felelnek meg.

Látható, hogy ha adott az $(S, \mathcal{F})$ (n, q)-feladat és egy hozzá tartozó $\mathcal{A}$ algoritmus, akkor az ehhez konstruált fa is (n, q)-fa lesz; az x^* elemhez rendelt levél mélysége éppen $l(x^*)$, és így persze a fa mélysége (amit ezentúl $L(T)$-vel jelölünk) is egyenlő az algoritmus hosszával. Továbbá, egy v belső csúcshoz rendelt $S(e_1, \ldots, e_k)$ halmaz is egyszerűen meghatározható a fa segítségével, hiszen éppen azon levelekhez tartozó elemekből fog állni, melyek v leszármazottai.

Összefoglalva, azt láttuk tehát, hogy minden (n, q)-feladathoz tartozó $\mathcal{A}$ algoritmushoz egyértelműen hozzárendelhető egy (n, q)-fa, amit az $\mathcal{A}$ algoritmus döntési fájának hívunk.

Érdemes megnézni a megfordítást is, azaz, hogy egy tetszőleges (n, q)-fához létezik egy (n, q)-feladat és egy hozzá tartozó $\mathcal{A}$ algoritmus, amelynek éppen T a döntési fája. Ennek belátásához álljon S a T fa leveleiből, a T belső csúcsaiból kivezető éleket pedig tetszőlegesen címkézzük meg a $0, 1, \ldots, q-1$ számokkal (arra kell csak figyelnünk, hogy egy csúcsból kiinduló [tehát a fiú felé menő] két él ne kapja ugyanazt a címkét). Ekkor az $f_k : S \to \{0, 1, \ldots, q-1\}$, $\quad (k = 1, \ldots, L(T))$ keresőfüggvényeket a következőképpen definiálhatjuk:

$$f_k(x^*) = \begin{cases} j & \text{ha } k \leq l(x^*) \text{ és az } r\text{-ből } x^*\text{-ba vezető úton} \\ & \text{a } k\text{-adik él címkéje } j \\ 0 & \text{ha } k > l(x^*) \end{cases}$$

Azonnal látszik, hogy ezzel egy nemadaptív algoritmust kaptunk: a k-adik lépésben, függetlenül az addigi válaszoktól — hacsak meg nem találtuk már x^*-ot, azaz véget nem ért az algoritmus —, mindig f_k-t kérdezzük meg. Nyilvánvaló, hogy az ehhez tartozó döntési fa éppen T.

A fentiekből az is rögtön adódik, hogy ha minden keresőfüggvény meg van engedve, azaz $\mathcal{F} = \{0, 1, \ldots, q-1\}^S$, akkor minden adaptív algoritmust átalakíthatunk ugyanolyan hosszú nemadaptívvá (persze csak a legrosszabb esetben igaz ez, az átlagosban nem), tehát $L(S, \mathcal{F}) = L_{\text{pre}}(S, \mathcal{F})$.

Még néhány elnevezés fákra illetve algoritmusokra:

4. Definíció. Egy (n,q)-feladathoz tartozó $\mathcal{A}$ algoritmust *reguláris*nak nevezünk, ha $|S(e_1,\ldots,e_k)| \geq 2$ esetén $S(e_1,\ldots,e_k,e) \neq \emptyset$ teljesül minden $e \in \{0,1,\ldots,q-1\}$-re. Az $\mathcal{A}$ algoritmus *irreducibilis*, ha minden nemüres $S(e_1,\ldots,e_k)$ esetén $S(e_1,\ldots,e_k) \supsetneqq S(e_1,\ldots,e_k,e)$ teljesül. Analóg módon egy (n,q)-fát *irreducibilis*nek hívunk, ha minden belső csúcsának legalább két fia van.

1.2. Keresés az $\mathcal{F} = \{0,1,\ldots,q-1\}^S$ esetben

1.2.1. A legrosszabb eset

Az előző rész végén tett megállapításainkat figyelembe véve, most elég (n,q)-típusú keresési feladatok helyett csak (n,q)-fákkal foglalkoznunk. Először egy egyszerű, de a keresésben alapvető fontosságú állítást látunk be. Jelöljük ehhez $\mathcal{T}(n,q)$-val az összes (n,q)-fa halmazát.

5. Állítás. *Legyen $T \in \mathcal{T}(n,q)$, és jelöljük $I = I(T)$-vel T belső csúcsainak halmazát. Ekkor*

i) $|I| \geq \lceil \frac{n-1}{q-1} \rceil$,

ii) *T pontosan akkor reguláris, ha $|I| = \frac{n-1}{q-1}$. Speciálisan, egy reguláris fára $q-1|n-1$.*

Megfordítva, minden (n,q) párhoz ($n \geq 1, q \geq 2$) létezik egy (n,q)-fa, amelyre $|I| = \lceil \frac{n-1}{q-1} \rceil$. (Így persze ez az (n,q)-fa reguláris, és $|I| = \frac{n-1}{q-1}$, ha $q-1|n-1$.)

Bizonyítás. Legyen $T \in \mathcal{T}(n,q)$. Összeszámoljuk kétféleképpen a fa éleit. Egyrészt minden csúcsba pontosan egy él megy be, kivéve természetesen a gyökeret. Másfelől minden belső csúcsból legfeljebb q él vezet ki. Ezek alapján

$$n + |I| - 1 \leq |I|\, q,$$

amiből i) és ii) azonnal következik.

A megfordításhoz teljes indukciót alkalmazunk $k = \lceil \frac{n-1}{q-1} \rceil$-re. $k = 0$, azaz $n = 1$ esetén az állítás triviális. $k = 2$-re a fa a gyökérből és $n \leq q$ levélből áll, melyek mind a gyökérrel szomszédosak. Legyen tehát $k \geq 2$ és $n - 1 = k(q-1) - r$, ahol $0 \leq r < q-1$. Ekkor $n - q = (k-1)(q-1) - r$, tehát az indukciós feltevés szerint létezik egy T' $(n-q+1,q)$-fa, amelyre $|I(T')| = k-1$. Kiválasztva T' egy tetszőleges levelét, és ezt kicserélve a triviális (q,q)-fára (azaz amelyben a gyökéren kívül q vele szomszédos levél van), egy $T \in \mathcal{T}(n,q)$ fát kapunk, amelyre $|I(T)| = k = \lceil \frac{n-1}{q-1} \rceil$ teljesül. $\square$

Az alábbiakban az $|I| = \lceil \frac{n-1}{q-1} \rceil$ egyenlőséget teljesítő (n,q)-fák egy nagyon fontos típusát fogjuk definiálni. Egy rögzített $T \in \mathcal{T}(n,q)$ fára E jelölje a levelei halmazát, S_k a k-adik szinten lévő csúcsait (azaz $S_k := \{v \in V : l(v) = k\}$, ahol $k = 0,1,\ldots,L$), és $L(T)$ helyett írjunk csak L-et.

6. Definíció. Egy $T \in \mathcal{T}(n,q)$ fát *teljes*nek nevezünk, ha

i) Tetszőleges $k \le L-2$ esetén minden $v \in S_k$ csúcsnak pontosan q fia van.

ii) T-nek az i) által megengedett lehető legtöbb levele van S_{L-1}-ben. (Persze i)-ből következik, hogy $E \subseteq S_{L-1} \cup S_L$.)

$L = 0$-ra a feltételek triviálisan teljesülnek, így feltehetjük, hogy $L \ge 1$. i) miatt $k = 0,1,\ldots,L-1$ esetén $|S_k(T)| = q^k$. Tegyük fel, hogy az S_{L-1} halmaz a darab levelet tartalmaz, vagyis így $b = q^{L-1} - a$ belső csúcsot, ahol $b > 0$, hiszen azt feltételeztük, hogy a fa mélysége L. Ekkor az L-edik szinten persze $n-a$ levélnek kell lennie, viszont másrészt semmiképpen sem lehet qb levélnél több it. Ezek alapján a $qb \ge n-a$ egyenlőtlenségből $(q-1)b \ge n-a-b \ge n-q^{L-1}$-et kapjuk, amiből pedig

$$b \ge \left\lceil \frac{n-q^{L-1}}{q-1} \right\rceil$$

következik.

Ezek szerint b-re a lehető legkisebb érték a $b = \lceil \frac{n-q^{L-1}}{q-1} \rceil$, amiből a legfeljebb $\lfloor \frac{q^L-n}{q-1} \rfloor$ lehet. Most már látható, hogy $|I| = \sum_{k=0}^{L-2} q^k + b = \frac{q^{L-1}}{q-1} + \lceil \frac{n-q^{L-1}}{q-1} \rceil = \lceil \frac{n-1}{q-1} \rceil$. Mivel $b > 0$ és $a \ge 0$, ezért $q^{L-1} < n \le q^L$, azaz $L = \lceil \log_q n \rceil$, ami azt jelenti, hogy i) és ii) egyértelműen meghatározzák L-et.

Összefoglalva, egy teljes (n,q)-fának $L = \lceil \log_q n \rceil$ a mélysége, $\lfloor \frac{q^L-n}{q-1} \rfloor$ levele van S_{L-1}-ben, és $\lfloor \frac{nq-q^L}{q-1} \rfloor$ levele van S_L-ben.

Ezek után könnyedén megoldhatjuk a legrosszabb esetbeli problémát az (n,q)-fákra. A rövidség kedvéért alkalmazni fogjuk az $L(n,q) := \min\{L(T) : T \in \mathcal{T}(n,q)\}$ jelölést.

7. Tétel. *Legyen $n \geq 1$, $q \geq 2$. Ekkor*

$$L(n,q) = \lceil \log_q n \rceil$$

Bizonyítás. Legyen $T \in \mathcal{T}(n,q)$, és legyen $L := L(T)$. Mivel minden belső csúcsnak legfeljebb q fia lehet, láthatjuk, hogy a k-adik szintre

$$|S_k(T)| \leq q^k \qquad (k = 0, 1, \ldots, L).$$

Ha v egy olyan levele T-nek, amelyre $l(v) < L$, akkor v-t cseréljük ki egy v'_0 belső csúcsra, melynek leszármazottai $v'_1, v'_2, \ldots, v'_{L-l}$ úgy, hogy $l(v'_i) = l(v)+i$, és v'_{L-l} ismét egy levél lesz. Ezzel az eljárással egy olyan $T' \in \mathcal{T}(n,q)$ fát kapunk, amelyre $E(T') \subseteq S_L(T')$. A fenti egyenlőtlenségből azt kapjuk, hogy $n = |E(T)| = |E(T')| \leq q^L$, és így $L \geq \lceil \log_q n \rceil$, hiszen L egész. Végül azt, hogy ez az alsó korlát el is érhető, a fent definiált teljes fák vizsgálatánál láttuk. □

A fenti tételből azonnal adódik az alábbi állítás tetszőleges (n,q)-feladatokra (tehát most nem tesszük fel, hogy minden keresőfüggvény megengedett).

8. Következmény. *Legyen $(S, \mathcal{F})$ egy (n,q)-feladat. Ekkor*

$$L(S, \mathcal{F}) \geq \lceil \log_q n \rceil$$

Bizonyítás. Láttuk, hogy minden algoritmus reprezentálható egy döntési fával. □

A 8. következménybeli alsó korlátot az $(S, \mathcal{F})$ feladatra vonatkozó *információelméleti alsó korlát*nak nevezzük.

1.2.2. Átlagos eset

Akárcsak a legrosszabb esetben, itt is egy igen fontos lemmával kezdjük:

9. Lemma (Kraft-egyenlőtlenség). *Legyen $T \in \mathcal{T}(n,q)$, és $l_1, \ldots, l_n$ legyenek T leveleinek a mélységei. Ekkor $\sum_{i=1}^{n} q^{-l_i} \leq 1$. Egyenlőség pontosan akkor áll, ha T reguláris.*

Megfordítva, ha az $l_1, \ldots, l_n$ nemnegatív egészek kielégítik a $\sum_{i=1}^{n} q^{-l_i} \leq 1$ egyenlőtlenséget, akkor létezik egy (n,q)-fa, melynek levelei rendre $l_1, \ldots, l_n$ mélységűek.

Bizonyítás. Az első állítás belátásához vegyük észre, hogy egy tetszőleges (n,q)-fából telített (n',q)-fát gyárthatunk úgy, hogy „telítetlen" belső csúcsaira leveleket akasztunk. Ezzel az eljárással $\sum q^{-l_i}$ csak nőhet, így elég azt igazolnunk, hogy egy T reguláris (n,q)-fára $\sum q^{-l_i}=1$. Alkalmazzunk indukciót $k=\frac{n-1}{q-1}$ szerint (k az 5. Állítás miatt egész). $k=0$, vagyis $n=1$ esetén az állítás triviálisan teljesül, így most tegyük fel, hogy $k\geq 1$. Most T-ből töröljünk le q levelet, amelyek egyetlen közös szomszéddal rendelkeznek (tehát mostantól ez a közös szomszéd egy új levél lesz). Így a T' fát kapjuk. Feltehető, hogy éppen az első q levelet töröltük le, és a közös mélységük $l_1=\cdots=l_q=:l$ volt. Ekkor a T'-re az indukciós feltételt alkalmazva kapjuk, hogy

$$\underbrace{\sum_{i=1}^{n} q^{-l_i}}_{T}=\sum_{i=q+1}^{n} q^{-l_i}+q\cdot q^{-l}=\underbrace{\sum_{i=q+1}^{n} q^{-l_i}+q^{-(l-1)}}_{T'}=1.$$

Megfordítva, ha adottak $l_1,\ldots,l_n\in\mathbb{N}_0$, amelyekre $\sum\limits_{i=1}^{n} q^{-l_i}\leq 1$, akkor legyen $w_k:=|\{i: l_i=k\}|$, ahol $k=0,1,\ldots,L=\max\limits_i l_i$, azaz w_k jelöli a k mélységű levelek számát a konstruálandó T fában. A lemma feltétele a w_k-k segítségével átírható:

$$\sum_{k=0}^{L} w_k q^{-k}\leq 1,$$

vagy másképpen,

$$w_0q^L+w_1q^{L-1}+\cdots+w_{L-1}q+w_L\leq q^L. \tag{1.1}$$

Rekurzívan konstruáljuk meg a fát. Ha $w_0=1$, akkor (1.1) alapján $L=0$, azaz T egyetlen pontból áll. Tegyük fel most, hogy már készen vagyunk a konstrukcióval a k-adik szintig. Jelöljük ezt a szintet S_k-val. Ha a felsőbb szinteken minden pontnak q fia lett volna, akkor az S_k-ban most q^k csúcsunk lenne. Az S_i szinten ($i=1,\ldots,k-1$) azonban már w_i csúcsot ki kellett jelölnünk levélnek, ezért persze az ezek „alatti" csúcsokat elvesztettük. Így S_k-ban csak $q^k-\sum\limits_{i=0}^{k} w_iq^{k-i}$ belső csúccsal gazdálkodhatunk. (1.1) szerint

$$w_{k+1}q^{L-k-1}\leq q^L-\sum_{i=0}^{k} w_iq^{L-i},$$

azaz

$$w_{k+1} \leq q^{k+1} - \sum_{i=0}^{k} w_i q^{k+1-i} = q(q^k - \sum_{i=0}^{k} w_i q^{k-i}).$$

Ebből az látszik, hogy a $k+1$-edik szintre előírt w_{k+1} levél mindegyikét el tudjuk érni S_k-beli belső pontból, amivel beláttuk a lemmát. $\square$

Ahhoz, hogy meghatározzuk a komplexitást az átlagos esetben, szükségünk lesz egy technikai jellegű lemmára:

10. Lemma. *Legyenek $s_1, \ldots, s_n$ és $y_1, \ldots, y_n$ pozitív valós számok, amelyekre $\sum_{i=1}^{n} s_i \leq \sum_{i=1}^{n} y_i$. Ekkor*

$$\sum_{i=1}^{n} y_i \log_a \frac{y_i}{s_i} \geq 0 \quad \textit{minden } a > 1 \textit{ esetén}, \tag{1.2}$$

és egyenlőség pontosan akkor áll, ha $s_i = y_i$ minden i-re.

Bizonyítás. Mivel a különböző alapú logaritmusok csak egy konstans szorzóban térnek el egymástól, ezért elég csak a természetes alapú logaritmusra belátnunk a lemmát. Felhasználva azt a közismert tényt, hogy $\ln x \leq x - 1$ minden $x > 0$ esetén, és egyenlőség pontosan akkor áll, ha $x = 1$; rögtön adódik az állítás, hiszen

$$\sum y_i \ln \frac{s_i}{y_i} \leq \sum y_i \Big(\frac{s_i}{y_i} - 1\Big) = \sum s_i - \sum y_i \leq 0.$$

Itt egyenlőség pontosan akkor áll, ha $s_i/y_i = 1$ minden i-re. $\square$

A most következő tétel 1-nél kisebb hibával megoldja az átlagos esetbeli problémát. Legyen $\underline{p} = (p_1, \ldots, p_n)$ egy valószínűségeloszlás az (n,q)-fák levelein, és most is vezessük be a következő jelölést: $\overline{L}(n, q; \underline{p}) := \min\{\overline{L}(T; \underline{p}) : T \in \mathcal{T}(n, q)\}$.

11. Tétel (Shannon [7]). *Legyen $n \geq 1$, $q \geq 2$. Ekkor*

$$-\sum_{i=1}^{n} p_i \log_q p_i \leq \overline{L}(n, q; \underline{p}) < \Big(-\sum_{i=1}^{n} p_i \log_q p_i\Big) + 1$$

Bizonyítás. Feltehetjük, hogy minden i-re $p_i > 0$. A bal oldali egyenlőtlenség bizonyításához azt kell megmutatnunk, hogy minden $T \in \mathcal{T}(n,q)$ fára, melynek levélmélységei $l_1, \ldots, l_n$, teljesül, hogy

$$\sum_{i=1}^{n} p_i l_i \geq -\sum_{i=1}^{n} p_i \log_q p_i.$$

A Kraft-egyenlőtlenség miatt $\sum_{i=1}^{n} q^{-l_i} \leq 1 = \sum_{i=1}^{n} p_i$, így alkalmazhatjuk az 10. Lemmát a $q^{-l_i}, \ldots, q^{-l_n}$, illetve a $p_1, \ldots, p_n$ sorozatokra. Azt kapjuk, hogy $\sum p_i \log_q(p_i q^{l_i}) \geq 0$, azaz $-\sum p_i \log_q p_i \leq \sum p_i l_i$.

A jobb oldali szigorú egyenlőtlenség igazolásához definiáljuk az l_i természetes számokat minden i-re a $-\log_q p_i \leq l_i < -\log_q p_i + 1$ egyenlőtlenséggel. Látható, hogy ez értelmes és egyértelmű. A definíció szerint $1/p_i \leq q^{l_i}$, azaz $q^{-l_i} \leq p_i$ minden i-re, és így

$$\sum_{i=1}^{n} q^{-l_i} \leq \sum_{i=1}^{n} p_i = 1.$$

Ekkor a Kraft-egyenlőtlenség megfordításából következik, hogy létezik egy T (n,q)-fa, amelynek a levélmélységei $l_1, \ldots, l_n$, és így az átlagos mélysége, $\overline{L}(T; \underline{p}) = \sum_{i=1}^{n} p_i l_i$ felülről becsülhető a következőképpen:

$$\sum p_i l_i < \sum p_i(-\log_q p_i + 1) = \left(-\sum p_i \log_q p_i\right) + 1$$

A $p_i > 0$ feltételtől megszabadulhatunk, ha kikötjük, hogy $0 \cdot \log_q 0 = 0$.

$\square$

12. Definíció. A $H(p_1, \ldots, p_n) := -\sum_{i=1}^{n} p_i \log_2 p_i$ kifejezést a $(p_1, \ldots, p_n)$ eloszlás *entrópiá*jának nevezzük.

A definíció alapján a 11. Tételt a következő alakba írhatjuk:

$$\frac{H(p_1, \ldots, p_n)}{\log_2 q} \leq \overline{L}(n, q; \underline{p}) < \frac{H(p_1, \ldots, p_n)}{\log_2 q} + 1$$

Akárcsak a legrosszabb esetben, a 11. Tétel tetszőleges $(S, \mathcal{F})$ keresési feladat átlagos bonyolultságára is alsó korlátot jelent:

13. Következmény. *Legyen $(S, \mathcal{F})$ egy (n,q)-feladat, $\underline{p} = (p_1, \ldots, p_n)$ pedig tetszőleges eloszlás. Ekkor*

$$\overline{L}(S, \mathcal{F}; \underline{p}) \geq -\sum_{i=1}^{n} p_i \log_q p_i = \frac{H(p_1, \ldots, p_n)}{\log_2 q}.$$

Ha már egy 1-nél kisebb hiba erejéig meghatároztuk $\overline{L}(n,q;\underline{p})$-t, foglalkozhatunk pontosabb érték megtalálásával is.

Tekintsük először a $p_1 = \cdots = p_n = 1/n$ egyenletes eloszlást. Ekkor a 11. Tétel szerint

$$\log_q n \leq \overline{L}(n,q;\frac{1}{n},\ldots,\frac{1}{n}) < \log_q n + 1.$$

Legyen $T \in \mathcal{T}(n,q)$, és jelölje T leveleinek halmazát E. Az $e(T) := \sum_{v\in E} l(v)$ összeget a T fa *külső mélységének* nevezzük. Így $e(T) = n\overline{L}(T;\frac{1}{n},\ldots,\frac{1}{n})$, tehát a feladatunk $e(T)$ minimumának a meghatározása. Belátjuk, hogy a minimum pontosan a 6. Definícióban szereplő teljes fákon vétetik fel. A teljes fákra vonatkozó i) feltétel könnyen adódik, hiszen ha létezne $w \in S_k$, $k \leq L-2$ belső csúcs, amelynek kevesebb, mint q fia van, akkor egy, az L-edik szinten lévő levelet felhozhatnánk w fiának, amivel $e(T)$-t csökkentenénk. Ha pedig i) teljesül, ii) triviálisan szükséges az optimalitáshoz.

Jelöljük tehát a minimális külső mélységet $e(n,q)$-val. Ezt könnyen ki is számolhatjuk. Egy teljes fának $a = \lfloor\frac{q^L-n}{q-1}\rfloor$ levele van az $L-1$-edik szinten, és $n-a$ levele az L-ediken. Figyelembe véve, hogy $L = \lceil\log_q n\rceil$, a következő tételt kapjuk:

14. Tétel. *Legyen $n \geq 2$. Ekkor az $e(n,q) := \min\{e(T) : T \in \mathcal{T}(n,q)\}$ jelöléssel:*

$$e(n,q) = n\lceil\log_q n\rceil - \left\lfloor\frac{q^{\lceil\log_q n\rceil}-n}{q-1}\right\rfloor$$
$$\overline{L}(n,q;\frac{1}{n},\ldots,\frac{1}{n}) = \lceil\log_q n\rceil - \frac{1}{n}\left\lfloor\frac{q^{\lceil\log_q n\rceil}-n}{q-1}\right\rfloor.$$

Bizonyítás. A tétel előtti megjegyzések alapján

$$e(n,q) = a(L-1)+(n-a)L = nL-a = n\lceil\log_q n\rceil - \left\lfloor\frac{q^L-n}{q-1}\right\rfloor.$$

□

Érdemes még megnézni, hogy a fent kapott érték mennyiben térhet el a 11. Tételben kapott $\log_q n$ alsó korláttól. Legyen $\lceil\log_q n\rceil = \log_q n + \theta$, ahol $0 \leq \theta < 1$, valamint legyen $\lfloor\frac{q^L-n}{q-1}\rfloor = \frac{q^L-n}{q-1} - r$, ahol $0 \leq r < 1$. Ekkor

$L = \lceil \log_q n \rceil = \log_q n + \theta$ miatt:

$$\begin{aligned}
\overline{L}(n, q; \frac{1}{n}, \ldots, \frac{1}{n}) &= \log_q n + \theta - \frac{1}{n}\frac{q^L}{q-1} + \frac{1}{q-1} + \frac{r}{n} = \\
&= \log_q n + \theta - \frac{q^\theta}{q-1} + \frac{1}{q-1} + \frac{r}{n} = \\
&= \log_q n + \frac{1}{q-1}\big(\theta(q-1) - q^\theta + 1\big) + \frac{r}{n}.
\end{aligned}$$

Az $f(\theta) := \theta(q-1) - q^\theta + 1$ függvényről könnyen belátható, hogy a $[0,1]$ intervallumon nemnegatív, és a maximumát a $\theta_0 = \frac{\ln(q-1) - \ln\ln q}{\ln q}$ pontban veszi fel. Mindezeket összefoglalva:

15. Következmény. *$n \geq 1$, $q \geq 2$ esetén*

$$\log_q n \leq \overline{L}(n, q; \frac{1}{n}, \ldots, \frac{1}{n}) \leq \log_q n + \frac{1}{q-1} - \frac{1 + \ln\ln q - \ln(q-1)}{\ln q} + \frac{r}{n},$$

ahol $\lfloor \frac{q^{\lceil \log_q n \rceil} - n}{q-1} \rfloor = \frac{q^{\lceil \log_q n \rceil} - n}{q-1} - r$, $0 \leq r < 1$.

Speciálisan, bináris fákra $q = 2$ és $r = 0$, így

$$\log_2 n \leq \overline{L}\Big(n, 2; \frac{1}{n}, \ldots, \frac{1}{n}\Big) \leq \log_2 n + \Big(1 - \frac{1 + \ln\ln 2}{\ln 2}\Big) = \log_2 n + 0.086$$

Áttérve az egyenletesről tetszőleges eloszlásra, igen keveset tudunk mondani $\overline{L}(n, q; \underline{p})$ értékéről (ugyanakkor érdemes megemlíteni, hogy adott $\underline{p}$ esetén létezik hatékony algoritmus az optimális döntési fa megkonstruálására [5]). Most csak azt látjuk be, hogy az egyenletes eloszlás extremális tulajdonságú. (Mint az várható is volt, az egyenletes eloszlás hordozza a legtöbb információt, így ebben az esetben a legnagyobb az átlagos bonyolultság).

16. Állítás. *Legyen $\underline{p} = (p_1, \ldots, p_n)$ tetszőleges eloszlás. Ekkor*

$$\overline{L}(n, q; p_1 \ldots, p_n) \leq \overline{L}(n, q; \frac{1}{n}, \ldots, \frac{1}{n}).$$

Bizonyítás. Feltehetjük, hogy $p_1 \geq p_2 \geq \cdots \geq p_n$ Belátjuk, hogy ekkor minden $k = 1, \ldots, n$ esetén $\sum_{i=1}^{k} p_i \geq \frac{k}{n}$ teljesül. Ha ugyanis nem így lenne, azaz létezne $k < n$, amelyre $\sum_{i=1}^{k} p_i < \frac{k}{n}$ volna, akkor $p_k = \min\{p_1, \ldots, p_k\} < \frac{1}{n}$

teljesülne, és így $p_j < \frac{1}{n}$ is igaz lenne minden $j > k$ esetén. Viszont ebből $\sum_{j=k+1}^{n} p_j < \frac{n-k}{n}$ következne, és így $\sum_{i=1}^{n} p_i < 1$, ami ellentmondás.

Már láttuk, hogy egyenletes eloszlás esetén egy optimális fának $a = \lfloor \frac{q^{\lceil \log_q n \rceil} - n}{q-1} \rfloor$ levele van $\lceil \log_q n \rceil - 1$ mélységben, és $n - a$ levele $\lceil \log_q n \rceil$ mélységben. Rendeljük most az a legnagyobb valószínűséget a $\lceil \log_q n \rceil - 1$-edik szinten lévő levelekhez, a többit pedig a többi levélhez. Az így megadott T fa átlagos mélysége ekkor

$$\begin{aligned}
\overline{L}(T;\underline{p}) &= \sum_{i=1}^{a} p_i(\lceil \log_q n \rceil - 1) + \sum_{j=a+1}^{n} p_j \lceil \log_q n \rceil \\
&= \lceil \log_q n \rceil - \sum_{i=1}^{a} p_i \leq \lceil \log_q n \rceil - \frac{a}{n} \\
&= \lceil \log_q n \rceil - \frac{1}{n} \left\lfloor \frac{q^{\lceil \log_q n \rceil} - n}{q-1} \right\rfloor = \overline{L}(n, q; \frac{1}{n}, \dots, \frac{1}{n}).
\end{aligned}$$

Mivel nyilvánvalóan $\overline{L}(n, q; \underline{p}) \leq \overline{L}(T; \underline{p})$, ezért az állítást beláttuk. □

1.3. Nemadaptív algoritmusok

Röviden foglalkozunk a nemadaptív algoritmusokkal is. Ekkor a döntési fával való reprezentálás helyett egyszerűbben is leírhatjuk az algoritmusokat. Tekintsük ugyanis az $(S, \mathcal{F})$ (n, q)-feladatot, és egy ehhez tartozó $\mathcal{A} = (f_1, \dots, f_L)$ algoritmushoz rendeljünk hozzá egy $M_{\mathcal{A}}$ mátrixot. A mátrix oszlopai feleljenek meg az S halmaz elemeinek, a sorok pedig az $f_1, \dots, f_L$ tesztfüggvényeknek. A mátrix (i, j) koordinátájú mezőjébe az $f_i(x_j)$ számot írjuk. Így tehát $M_{\mathcal{A}}$ egy $L \times n$-es mátrix a $\{0, 1, \dots, q-1\}$ halmaz felett. Az is rögtön látszik, hogy ha $\mathcal{A}$ sikeres algoritmus, akkor az $M_{\mathcal{A}}$ mátrix oszlopai különbözőek.

A megfordítás is nyilvánvaló, csak meg kell fogalmazni: ha M egy n oszlopos mátrix, melynek sorai megengedettek ($\mathcal{F}$ szerint), továbbá páronként különbözőek, akkor M-nek megfelel egy sikeres nemadaptív algoritmus az $(S, \mathcal{F})$ feladatra. Egyszerűen csak úgy kell megválasztani az $f_1, \dots, f_L$ függvényeket (ahol tehát L az M mátrix sorainak a számát jelöli), hogy megfeleljenek M sorainak. Ekkor persze akármilyen válaszokat is kapunk, M oszlopainak különbözősége biztosítja azt, hogy x^*-ot egyértelműen meg tudjuk határozni.

17. Definíció. Legyen $S = \{x_1, \dots, x_n\}$, és $(S, \mathcal{F})$ egy (n, q)-típusú keresési feladat. Egy n oszlopos, a $\{0, 1, \dots, q-1\}$ halmaz feletti M mátrixot az

$(S,\mathcal{F})$ feladathoz tartozó *keresőmátrix*nak hívunk, ha M oszlopai páronként különbözőek, továbbá minden sora $(f(x_1),\dots,f(x_n))$ alakú valamilyen $f\in\mathcal{F}$ tesztfüggvényre.

Ezzel a nemadaptív legrosszabb esetbeli problémát minimális számú sorral rendelkező keresőmátrixok keresésére redukáltuk.

1.4. Játékelméleti megközelítés

Egy $(S,\mathcal{F})$ keresési feladat legrosszabb esetbeli megoldását *keresési játék*ként is felfoghatjuk, melyben két játékos vesz részt, A és B. A játék során A $f_1,f_2,\dots\in\mathcal{F}$ tesztfüggvényeket választ ki, és megkérdezi B-től $f_i(x^*)$ értékét. A minél kevesebb kérdés segítségével akarja meghatározni x^*-ot. Egy $f_1,f_2,\dots$ sorozatot, amely meghatározza az ismeretlen $x^*\in S$ elemet, szokás szerint az A játékos egy *algoritmus*ának fogunk nevezni.

A másik oldalon azonban B arra akarja kényszeríteni A-t, hogy minél több kérdést fel kelljen tennie. Ezért B-nek nem kell előre kiválasztania egy x^*-ot, hanem A kérdéseire kedve szerint adhat értelmes válaszokat, azaz olyanokat, amelyek egyrészt benne vannak az éppen megkérdezett f_i keresőfüggvény értékkészletében, másrészt a még x^*-ként szóba jöhető elemek halmazát nem teszik üressé. Egy ilyen válaszsorozatot B *stratégiá*jának nevezünk.

A játék természetesen akkor ér véget, ha A meghatározza x^*-ot, a *játék hosszá*nak pedig a feltett kérdések számát nevezzük. Tegyük fel, hogy A az $\mathcal{A}_0$ algoritmust, míg B az $\mathcal{S}_0$ stratégiát alkalmazza. Az ekkor lezajló játék hosszát $L(\mathcal{A}_0,\mathcal{S}_0)$-lal jelöljük. Bevezetjük a következő szokásos játékelméleti jelöléseket is:

$$L(\mathcal{A}_0):=\max_{\mathcal{S}} L(\mathcal{A}_0,\mathcal{S})$$
$$L(\mathcal{S}_0):=\max_{\mathcal{A}} L(\mathcal{A},\mathcal{S}_0).$$

$L(\mathcal{A}_0)$-t és $L(\mathcal{S}_0)$-t rendre $\mathcal{A}_0$ illetve $\mathcal{S}_0$ *hosszá*nak nevezzük.

18. Állítás. *Legyen $(S,\mathcal{F})$ egy keresési feladat. Ekkor*

$$\min_{\mathcal{A}}\max_{\mathcal{S}} L(\mathcal{A},\mathcal{S})=\max_{\mathcal{S}}\min_{\mathcal{A}} L(\mathcal{A},\mathcal{S}),$$

vagy ami ezzel ekvivalens

$$\min_{\mathcal{A}} L(\mathcal{A})=\max_{\mathcal{S}} L(\mathcal{S}). \tag{1.3}$$

Továbbá, ez a közös hossz éppen $L(S,\mathcal{F})$, azaz az $(S,\mathcal{F})$ feladat legrosszabb esetbeli bonyolultsága.

Bizonyítás. Tetszőleges rögzített $\mathcal{A}_0$ és $\mathcal{S}_0$ esetén nyilvánvalóan

$$L(\mathcal{A}_0) = \max_{\mathcal{S}} L(\mathcal{A}_0, \mathcal{S}) \geq \min_{\mathcal{A}} L(\mathcal{A}, \mathcal{S}_0) = L(\mathcal{S}_0),$$

és így

$$\min_{\mathcal{A}} L(\mathcal{A}) \geq \max_{\mathcal{S}} L(\mathcal{S}),$$

amiből (1.3) belátása után rögtön következik a tétel utolsó állítása.

(1.3) igazolásához indukciót alkalmazunk n-re. $n = 1$ esetén mindkét oldal nullával egyenlő. Tegyük most fel, hogy $(S, \mathcal{F})$ egy (n, q)-feladat. Egy $\mathcal{A}_0$ algoritmust *optimális*nak nevezünk, ha $L(\mathcal{A}_0) = \min_{\mathcal{A}} L(\mathcal{A})$. Hasonlóan, az $\mathcal{S}_0$ stratégia *optimális*, ha $L(\mathcal{S}_0) = \max_{\mathcal{S}} L(\mathcal{S})$. Ha f az $\mathcal{A}_0$ algoritmus által elsőként megkérdezett keresőfüggvény, akkor jelölje $\pi(f) = \{S_0, S_1, \ldots, S_{q-1}\}$ az S-en f által indukált partíciót, azaz $S_i := \{x \in S : f(x) = i\}$, $i = 0, 1, \ldots, q-1$. Feltehetjük, hogy f legalább két különböző értéket felvesz, azaz minden i esetén $S_i \subsetneqq S$. Tegyük fel, hogy $\mathcal{A}(S_i)$ egy optimális algoritmus az $(S_i, \mathcal{F}_i)$ részfeladathoz (ahol persze $\mathcal{F}_i$ az $\mathcal{F}$ megszorítása S_i-re). Az $\mathcal{A}(S_i)$ feladatokat triviális módon összekombinálva, és úgy választva az első tesztfüggvényt, hogy a részfeladatok hossza a lehető legkisebb legyen, nyilvánvalóan egy optimális $\mathcal{A}_0$ algoritmust nyerünk az $(S, \mathcal{F})$ feladathoz, amelyre

$$L(\mathcal{A}_0) = 1 + \min_f \max\{L(\mathcal{A}(S_i)) : S_i \in \pi(f)\}.$$

Analóg módon, legyen $\mathcal{S}(S_i)$ optimális stratégia az $(S_i, \mathcal{F}_i)$ részfeladathoz. Ismét összekombinálhatjuk az $\mathcal{S}(S_i)$ stratégiákat, illetve olyan választ adhatunk az első kérdésre, hogy a részfeladat hossza a lehető legnagyobb legyen. Ekkor egy $\mathcal{S}_0$ optimális stratégiát nyerünk az $(S, \mathcal{F})$ feladatra, amelyre

$$L(\mathcal{S}_0) = 1 + \min_f \max\{L(\mathcal{S}(S_i)) : S_i \in \pi(f)\}.$$

Mivel az $\mathcal{A}(S_i)$ illetve $\mathcal{S}(S_i)$ stratégiák mind optimálisak, alkalmazhatjuk az indukciós feltételt, amiből minden i és f esetén $L(\mathcal{A}(S_i)) = L(\mathcal{S}(S_i))$, és így $L(\mathcal{A}_0) \leq L(\mathcal{S}_0)$. $\square$

$\mathcal{A}_0$-t és $\mathcal{S}_0$-t úgy konstruáltuk meg, hogy

$$L(\mathcal{A}_0) = L(\mathcal{A}_0, \mathcal{S}_0) = L(\mathcal{S}_0),$$

így azt mondhatjuk, hogy a feladat legrosszabb esetbeli bonyolultsága éppen a hozzá tartozó keresési játék hossza, amikor mindkét játékos optimálisan játszik.

Az előbbi tételben lényegében belátott

$$L(\mathcal{S}) \leq L \leq L(\mathcal{A}) \quad \text{tetszőleges } \mathcal{A} \text{ és } \mathcal{S} \text{ esetén}$$

egyenlőtlenséget gyakran fel lehet használni arra is, hogy korlátokat bizonyítsunk $L = L(S, \mathcal{F})$-re. A jobb oldali rész miatt egy tetszőleges algoritmus felső korlátot szolgáltat L-re. Persze ez nem újdonság; az viszont érdekesebb, hogy a bal oldal szerint egy $\mathcal{S}$ stratégia $L(\mathcal{S})$ hossza alsó korlátot ad L-re. Ennek egyszerű alkalmazásaként ismét belátjuk a 8. Következményt.

Ehhez nem is kell mást tennünk, mint az $(S, \mathcal{F})$ (n, q)-feladatot keresési játékként felfognunk. Ekkor kövesse B a következő stratégiát: ha a k-adik lépésben S_k a még szóba jöhető x^*-ok halmaza, f pedig A aktuális kérdése, akkor az $S_{k,i} = \{x \in S_k : f(x) = i\}$, $i = 0, 1, \ldots, q-1$ halmazok közül válassza a legnagyobb elemszámút. Ekkor $|S_{k+1}| \geq \frac{|S_k|}{q}$, amiből $1 = |S_L| \geq \frac{|S|}{q^L}$, azaz $L \geq \lceil \log_q n \rceil$.

Természetesen teljesen hasonlóan definiálhatunk keresési játékokat az átlagos hosszra, sőt, a nem-adaptív esetben is (ekkor A „nyílt kártyákkal" játszik).

1.5. Bináris keresés

A keresési feladatok legfontosabb és legjobban ismert esete a $q = 2$ eset, azaz a bináris keresési feladatok. Ekkor az 5. állításbeli $q - 1 | n - 1$ feltétel triviálisan teljesül, és a regularitás illetve az irreducibilitás is egybeesnek. Már említettük, hogy egy $f : S \to \{0, 1\}$ tesztfüggvényt azonosíthatunk egy $A = \{x \in S : f(x) = 1\}$ halmazzal, és így az $\mathcal{F}$ halmazt egy $\mathfrak{A}$ halmazrendszerrel. Ezért a bináris keresési feladatokat legtöbbször $(S, \mathfrak{A})$-val fogjuk jelölni. Így minden $\mathcal{A}$ algoritmushoz tartozik egy $\mathcal{U} = (A_1, A_2, \ldots)$ halmazsorozat, amelyre $\bigcap\limits_{A \in \mathcal{U}} A = \{x^*\}$. Egy $\mathcal{U} = (A_1, A_2, \ldots, A_L)$ nem-adaptív algoritmust pedig *elválasztó (szeparáló) halmazrendszer*nek fogunk nevezni, mivel minden $x \neq y \in S$ elempár esetén létezik $A_i \in \mathcal{U}$, amelyik „elválasztja" x-et y-tól, azaz amely x és y közül pontosan az egyiket tartalmazza.

Eddigi eredményeinket a következő tételben foglaljuk össze:

19. Tétel. *Legyen $n \geq 1$, $\underline{p} = (p_1, \ldots, p_n)$ adott eloszlás, $(S, \mathfrak{A})$ pedig egy tetszőleges bináris keresési feladat. Ekkor*

i) $L(n, 2) = L_{pre}(n, 2) = \lceil \log_2 n \rceil$

ii) $L(n, 2; \frac{1}{n}, \ldots, \frac{1}{n}) = \overline{L}_{pre}(n, 2; \frac{1}{n}, \ldots, \frac{1}{n}) = \lceil \log_2 n \rceil - \frac{1}{n} 2^{\lceil \log_2 n \rceil} + 1$

$$\begin{array}{llcl} iii) & H(p_1,\dots,p_n) \;\le & \overline{L}(n,2;\underline{p}) & = \overline{L}_{pre}(n,2;\underline{p}) \\ & & \overline{L}(n,2;\underline{p}) & < H(p_1,\dots,p_n)+1 \\ & & \overline{L}(n,2;\underline{p}) & \le \lceil \log_2 n\rceil - \frac{1}{n}2^{\lceil \log_2 n\rceil}+1 \end{array}$$

iv) $\lceil \log_2 n\rceil \le L(S,\mathfrak{A}) \le L_{pre}(S,\mathfrak{A})$.

v) $H(p_1,\dots,p_n) \le \overline{L}(S,\mathfrak{A};\underline{p}) \le \overline{L}_{pre}(S,\mathfrak{A};\underline{p})$.

Most jött el az idő, hogy megvizsgáljunk egy viszonylag egyszerű bináris keresési feladatot, ami azonban a dolgozat további részének fő témája lesz. Egy S halmazon keresünk, azzal a megkötéssel, hogy a keresőhalmazaink elemszáma legfeljebb egy előre rögzített k szám lehet; azaz egy $(S,\mathfrak{A}_{\le k})$ feladatról van szó, ahol $\mathfrak{A}_{\le k} = \{A \subseteq S : |A| \le k\}$.

20. Tétel. *Legyen* $|S| = n$, $k \le n$. *Ekkor*

i) $L(S,\mathfrak{A}_{\le k}) = \lceil \log_2 n\rceil$, *ha* $k \ge \frac{n}{2}$

ii) $L(S,\mathfrak{A}_{\le k}) = t + \lceil \log_2(n-tk)\rceil$, *ahol* $t = \lceil \frac{n}{k}\rceil - 2$, *ha* $k < \frac{n}{2}$.

Bizonyítás. Ha $k \ge \frac{n}{2}$, az persze semmi megkötést nem jelent számunkra, hiszen mindegy, hogy egy halmazt, vagy a komplementerét teszteljük. Így i) triviális.

ii) bizonyításához legyen $f_k(n) = L(S,\mathfrak{A}_{\le k})$, ahol $n = |S|$. Látható, hogy ez a definíció értelmes, hiszen $L(S,\mathfrak{A}_{\le k})$ csak $|S|$-től függ. Belátjuk, hogy rögzített k esetén $f_k(n)$ monoton nő. Legyen ugyanis $T \subsetneq S$, $\mathcal{U}$ pedig legyen egy L hosszú optimális algoritmus a $(S,\mathfrak{A}_{\le k})$ feladatra. Ekkor persze $\mathcal{U}' := \{A\cap T : A \in \mathcal{U}\}$ egy sikeres, és legfeljebb L hosszú algoritmus a $(T,\mathfrak{A}'_{\le k})$ feladatra. Tegyük most fel, hogy A_1 az első keresőhalmaz egy optimális algoritmus során, és legyen $|A_1| = l \le k$. Ekkor A_1-ben illetve $S - A_1$-ben optimálisan kereső algoritmusokat tekintve felírhatjuk a következő rekurziót:

$$f_k(n) \ge 1 + \max\bigl(f_k(l), f_k(n-l)\bigr) \ge 1 + f_k(n-l) \ge 1 + f_k(n-k),$$

ahol közben kihasználtuk az f_k függvény monotonitását. A rekurziót iterálva a következőt kapjuk:

$$f_k(n) \ge 1 + f_k(n-k) \ge \dots \ge t + f_k(n-tk) = t + \lceil \log_2(n-tk)\rceil,$$

ahol i) alapján t a legkisebb olyan szám, amelyre $k \ge \frac{n-tk}{2}$, vagyis $t = \lceil \frac{n}{k}\rceil - 2$. Ezzel tehát beláttuk, hogy $L(S,\mathfrak{A}_{\le k}) \ge t + \lceil \log_2(n-tk)\rceil$.

Pontosan ennyi kérdésből álló algoritmust viszont már könnyen konstruálhatunk. Az első t keresőhalmazunk a következő lesz:

$$A_1 = \{x_1,\dots,x_k\}, A_2 = \{x_{k+1},\dots,x_{2k}\},\dots, A_t = \{x_{(t-1)k+1},\dots,x_{tk}\}.$$

Ha ezek után $x^* \in \bigcup_{i=1}^{t} A_i$, akkor x^*-ot meghatározhatjuk $\lceil \log_2 k \rceil$ további kérdés segítségével, hiszen az A_i halmazokban semmi megszorításunk nincs már a keresőhalmazokra. Ha viszont $x^* \notin \bigcup_{i=1}^{t} A_i$, azaz $x^* \in \{x_{tk+1}, \ldots, x_n\}$, akkor $\lceil \log_2(n - tk) \rceil$ további kérdés segítségével megtalálhatjuk x^*-ot, hiszen $k \geq \frac{n-tk}{2}$. Ha még figyelembe vesszük, hogy t definíciójából következően $k < \frac{n-(t-1)k}{2}$, azaz $n - tk > k$, azt kapjuk hogy az algoritmusunknak legfeljebb $t + \lceil \log_2(n - tk) \rceil$ kérdésre van szüksége. $\square$

Ugyanezen probléma nemadaptív esetben már némiképp bonyolultabb, de kezelhető [6, 10].

2. Matroidok [3]

2.1. Definíciók

A matroidok olyan absztrakt kombinatorikus struktúrák, amelyek a függetlenség, különösképpen a lineáris függetlenség fogalmát általánosítják. (A matroidokat H. Whitney vezette be 1933-ban.) Ezért a következőképpen definiáljuk őket: kiválasztjuk a lineáris függetlenség néhány algebrában bizonyított tulajdonságát, és ezeket tesszük meg axiómáknak.

21. Definíció (Függetlenségi axiómák). Legyen S egy véges halmaz; $\mathfrak{F}$ pedig S részhalmazaiból álló halmazrendszer. Az $\mathcal{M} = (S, \mathfrak{F})$ párt *matroid*nak nevezzük, ha a következők teljesülnek:

I1) $\emptyset \in \mathfrak{F}$.

I2) Ha $Y \in \mathfrak{F}$, és $X \subseteq Y$, akkor $X \in \mathfrak{F}$.

I3) Minden $X \subseteq S$ halmazra az $\mathfrak{F}$ halmaz tartalmazásra nézve maximális X-beli tagjai azonos elemszámúak. (Azaz az X-ben fekvő elemszámra maximális $\mathfrak{F}$-beliek azonosak a tartalmazásra maximálisakkal.)

Az $\mathfrak{F}$ halmaz tagjait *független halmaz*oknak nevezzük, S többi részhalmazát pedig *függő*nek. I3) szerint egy X részhalmazban lévő nem bővíthető függetlenek elemszáma ugyanaz; csak X-től függ. Ezt a számot $r(X)$-szel jelöljük, és X *rang*jának nevezzük. $r(S)$-et a *matroid rangjá*nak hívjuk. S egy maximális független részhalmazát S *bázis*ának nevezzük.

Látható, hogy ezzel tulajdonképpen egy $r : 2^S \to \mathbb{N}$ függvényt definiáltunk, amit *rangfüggvény*nek nevezünk.

Rögtön látszik, hogy I1) helyett az $\mathfrak{F} \neq \emptyset$ feltételt is kiköthettük volna. Ennél sokkal fontosabb, hogy ha I3)-at kicseréljük az alábbi I3') axiómára, akkor ekvivalens axiómarendszert kapunk:

I3') *Legyen $K, N \in \mathfrak{F}$, amelyekre $|K| < |N|$. Ekkor létezik olyan $x \in N - K$, amelyre $K + x \in \mathfrak{F}$.*

22. Állítás. *Az {I1), I2), I3)} axiómarendszer ekvivalens a {I1), I2), I3')} axiómarendszerrel.*

Bizonyítás. $\Longrightarrow$: Legyenek $K, N \in \mathfrak{F}$, $|K| < |N|$, és legyen $S' := K \cup N$. Ekkor I3) miatt S' minden nem bővíthető részhalmaza legalább $|N|$ elemű, amiből I3') következik.

$\Longleftarrow$: Tegyük most fel, hogy $A, B \subseteq X$ függetlenek, és $|A| < |B|$. Ekkor I3') miatt létezik $x \in B - A$, amelyre $A + x$ független, és így A nem lehetett (tartalmazásra) maximális.

$\square$

23. Definíció. A 21. definícióból azonnal következik, hogy ha $\mathcal{M} = (S, \mathfrak{F})$ matroid és $S' \subseteq S$, akkor $\mathcal{M}' = (S', \mathfrak{F}')$ is matroid, ahol $\mathfrak{F}' := \{F \subseteq S' : f \in \mathfrak{F}\}$. Az így definiált $\mathcal{M}'$-t az $\mathcal{M}$ *részmatroid*jának nevezzük. Azt is mondhatjuk, hogy az $\mathcal{M}'$ matroid az $\mathcal{M}$ matroidból a $Z := S - S'$ halmaz *elhagyás*ával keletkezik. Ezt $\mathcal{M}' = \mathcal{M} - Z$-vel jelöljük.

2.1.1. Példák matroidokra

A legegyszerűbb matroidok a triviálisak: egy matroid *teljes* vagy *szabad*, ha minden részhalmaza független, illetve *üres* vagy *triviális*, ha csak az üres halmaz független.

Mátrix-matroid Ez példa azt hivatott mutatni, hogy tényleg jól sikerült absztrahálni a lineáris függetlenség fogalmát, azaz egy vektortér néhány vektora a lineáris függetlenséggel tényleg matroidot alkot.

Legyen tehát adott egy A mátrix (tetszőleges test felett), és jelölje S az A oszlopainak halmazát. Egy $F \subseteq S$ halmaz pontosan akkor tartozzék $\mathfrak{F}$-hez, ha az F-beli oszlopvektorok lineárisan függetlenek. Ekkor $(S, \mathfrak{F})$ matroidot alkot, hiszen I1) és I2) triviálisan teljesül, míg I3) egy elemi tétel lineáris algebrából. Az is látható, hogy egy X halmaz rangja éppen az X-beli oszlopvektorok által alkotott mátrixok rangja.

Uniform matroid Ezek nagyon egyszerű szerkezetű matroidok. Legyen S tetszőleges, $|S| = n$, továbbá $0 \leq k \leq n$ egész szám. Álljon $\mathfrak{F}$ az S összes legfeljebb k elemű részhalmazából. Ekkor nyilvánvaló, hogy mindhárom axióma fennáll. Az így kapott uniform matroidot $\mathcal{U}_{n,k}$-val jelöljük. Látható, hogy egy $X \subseteq S$ halmaz rangja $r(X) = \min(|X|, k)$.

Körmatroid Legyen $G = (V, E)$ irányítatlan gráf. A definiálandó matroid alaphalmaza legyen $S := E$. Az élek egy halmazát függetlennek definiáljuk, ha nem tartalmaz gráfbeli kört, azaz ha erdő. Az első két axióma itt is triviális, és I3) is következik abból a jólismert állításból, hogy egy gráfban egy nem bővíthető erdő élszáma éppen a pontok és a komponensek számának a különbsége.

Matroidok direkt összege Legyen adott k matroid, $\mathcal{M}_i = (S_i, \mathfrak{F}_i)$, úgy, hogy az alaphalmazaik diszjunktak. Legyen $S := \cup S_i$ és $\mathfrak{F} := \{I \subseteq S : I \cap S_i \in \mathfrak{F}_i, i = 1, \ldots, k\}$, vagyis egy I halmaz pontosan akkor legyen független, ha minden S_i-be eső része független az $\mathcal{M}_i$ matroidban. A függetlenségi axiómák ismét könnyen ellenőrizhetőek. Az így definiált matroidot az $\mathcal{M}_i$ matroidok direkt összegének nevezzük. Rangfüggvénye is egyszerűen megadható: $r(X) = \sum r_i(X \cap S_i)$.

A direkt összeghez a szokásos módon kapcsolódik az összefüggőség fogalma:

24. Definíció. Egy matroidot *összefüggő*nek nevezünk, ha nem lehet direkt összegként előállítani.

Partíciós matroid Legyen $\{S_1, \ldots, S_k\}$ az S alaphalmaz egy partíciója, és legyenek $g_1, \ldots, g_k$ nemnegatív egészek. Egy I halmaz pontosan akkor legyen független, ha $|I \cap S_i| \leq g_i$ minden i-re. Itt ellenőriznünk sem kell az axiómákat, ugyanis rögtön látszik, hogy a partíciós matroid tulajdonképpen uniform matroidok direkt összege. A rangfüggvény $r(X) = \sum_i \min(g_i, |X \cap S_i|)$.

Párosítás-matroid Legyen $G = (V, E)$ egyszerű irányítatlan gráf. A körmatroiddal ellentétben most legyen $S := V$. Egy $U \subseteq V$ részhalmaz pontosan akkor legyen független, ha létezik G-ben olyan párosítás, amely U-nak minden pontját fedi.

25. Állítás. *Az így definiált $(V, \mathfrak{F})$ pár matroidot alkot.*

Bizonyítás. I1) és I2) ismét triviális. I3) helyett most I3')-t fogjuk igazolni. Legyenek $K, N \in \mathfrak{F}$, $|K| < |N|$, és tegyük fel, hogy a P_K párosítás fedi K-t, a P_N párosítás pedig fedi N-et. Feltehetjük azt is, hogy P_K minimális abban az értelemben, hogy minden elemének legalább az egyik végpontja K-ban van.

Ha létezik olyan P_K-beli él, melynek másik végpontja egy $N - K$-beli x pontban végződik, akkor készen is vagyunk; $K + x$ is független. Tegyük fel tehát, hogy nincs ilyen él.

Tekintsük most a $P_N \oplus P_K$ szimmetrikus differenciát. Ebben minden pont foka legfeljebb 2, így $P_N \oplus P_K$ alternáló utakból és alternáló körökből áll. Mivel $N - K$ mindegyik pontját fedi P_N, de egyiket sem fedi P_K, ezért $N-K$ minden pontja végpontja egy alternáló útnak. Ha van olyan $x \in N-K$ pont, amelyből induló R alternáló út másik vége is $N-K$-ba esik, akkor ismét készen vagyunk, mert $P_K \oplus R$ egy olyan párosítás, amely fedi $K+x$-et, azaz $K+x$ független.

Így végül az az eset maradt, amikor az $N-K$-ban végződő alternáló utak mind különbözőek. Ekkor ezek között biztosan van olyan R út, aminek a másik vége nem $K-N$-beli, hiszen a feltétel szerint $|K-N| < |N-K|$. R nem végződhet $K \cap N$-ben sem, hiszen ott egyáltalán nem végződhet alternáló út. Így R-nek mindkét szélső éle P_N-beli, de akkor $P_K \oplus R$ megint olyan párosítás, amely fedi $K+x$-et. □

Párhuzamos többszörözés Az $\mathcal{M}$ matroid egy s független elemének párhuzamos többszörözésén azt értjük, hogy s-et helyettesítjük az S-től diszjunkt $S' = \{s_1, \dots s_k\}$ halmazzal, és az így kapott $S - s \cup S'$ alaphalmazon egy $X \subseteq S - s \cup S'$ halmazt akkor definiálunk függetlennek, ha $X \subseteq S - s$ és X független $\mathcal{M}$-ben, vagy ha $|X \cap S'| = 1$ és $X - S' + s$ független $\mathcal{M}$-ben. Könnyen látható, hogy ezzel matroidot kaptunk. (Gráf körmatroidjában ez nyilvánvalóan annak felel meg, hogy egy élt k párhuzamos éllel helyettesítünk.)

2.2. A rangfüggvény

Legelőször vegyük észre, hogy különböző matroidok rangfüggvénye különböző, hiszen egy halmaz pontosan akkor független, ha elemszáma egyenlő a rangjával. Így a független halmazok családja a következő:

$$\mathfrak{F} = \{X \subseteq S : r(X) = |X|\}. \tag{2.1}$$

Most belátjuk a rangfüggvény egy alapvető tulajdonságát:

26. Állítás. *A rangfüggvény (teljesen) szubmoduláris, azaz minden $X, Y \subseteq S$ esetén kielégíti a következő egyenlőtlenséget:*

$$r(X) + r(Y) \geq r(X \cap Y) + r(X \cup Y)$$

Bizonyítás. Legyen $X \cap Y$ egy bázisa F. Ekkor $|F| = r(X \cap Y)$, másrészt F kibővíthető $X \cup Y$-ban egy N bázissá, amelyre persze $|N| = r(X \cup Y)$ teljesül. F maximalitása miatt $N \cap X \cap Y = F$, és így $|N \cap X| + |N \cap Y| = |F| + |N|$.

Viszont $|N \cap X|$ független X-ben, így $r(X) \geq |N \cap X|$, és hasonlóan $r(Y) \geq |N \cap Y|$. Mindezeket összevetve kapjuk, hogy $r(X) + r(Y) \geq |N \cap X| + |N \cap Y| = |F| + |N| = r(X \cap Y) + r(X \cup Y)$. □

Összefoglalva, a rangfüggvény néhány lényeges tulajdonsága:

27. Állítás. *Legyen $\mathcal{M} = (S, \mathfrak{F})$ egy matroid, r a rangfüggvénye. Ekkor r-re teljesülnek a következők:*

R1) $r(\emptyset) = 0$

R2) $X \subseteq Y$ *esetén* $r(X) \leq r(Y)$ *(monotonitás)*

R3) $r(X) \leq |X|$ *(szubkardinalitás)*

R4) minden $X, Y \subseteq S$ *halmazra* $r(X) + r(Y) \geq r(X \cap Y) + r(X \cup Y)$ *(szubmodularitás)*

Bizonyítás. R1), R2) és R3) a rangfüggvény definíciójából következnek, R4)-et pedig éppen az előbb láttuk be. □

Célunk (2.1) megfordítása bizonyos értelemben. Azt kérdezzük, hogy melyek a rangfüggvény azon tulajdonságai, amelyeket megkövetelve a (2.1) által definiált $\mathfrak{F}$ halmazrendszer kielégíti a függetlenségi axiómákat. Először azonban lássunk két elnevezést, és egy hozzájuk kapcsolódó lemmát:

28. Definíció. Az X halmaz *lezárt*ja a következő halmaz:

$$\mathrm{cl}(X) := \{x \in S : r(X + x) = r(X)\},$$

azaz mindazon elemek halmaza, amelyek X-hez vétele nem növeli a rangot. X-et *zárt*nak nevezzük, ha $\mathrm{cl}(X) = X$.

29. Lemma. *Legyen $A \subseteq S$ és $e_1, \ldots, e_k \in S - A$. Ha $r(A + e_1) = \cdots = r(A + e_k) = r(A)$, akkor $r(A \cup \{e_1, \ldots, e_k\}) = r(A)$. (Azaz, ha bizonyos elemek egyikének hozzávétele sem növeli egy halmaz rangját, akkor az összes hozzávétele sem növeli. Speciálisan, $r(\mathrm{cl}(X)) = r(X)$.)*

Bizonyítás. Indukciót alkalmazunk k-ra. $k = 1$ esetén az állítás triviális. Tegyük fel, hogy az állítás $k-1$-re érvényes, azaz az $A' := A \cup \{e_1, \ldots, e_{k-1}\}$ jelöléssel $r(A') = r(A)$. Ekkor R2) és R4) alapján $r(A) + r(A) = r(A + e_k) + r(A') \geq r((A + e_k) \cap A') + r((A + e_k) \cup A') = r(A) + r(A \cup \{e_1, \ldots, e_k\}) \geq r(A) + r(A)$, amiből a lemma azonnal következik. □

Most már kimondhatjuk és bebizonyíthatjuk a tételt arról, hogy mikor lesz egy halmazfügvény egy matroid rangfüggvénye:

30. Tétel. *Az $r : 2^S \to \mathbb{Z}_+$ (nemnegatív, egészértékű) halmazfüggvény pontosan akkor egy matroid rangfüggvénye, ha kielégíti az R1), R2), R3), R4) rangaxiómákat.*

Bizonyítás. Azt, hogy a rangfüggvény kielégíti a rangaxiómákat, már láttuk. Megfordítva, tegyük fel, hogy r kielégíti a rangaxiómákat, és lássuk be, hogy ekkor a (2.1) által definiált $\mathfrak{F}$ halmazrendszer kielégíti a függetlenségi axiómákat. I1) következik R1)-ből. I2) igazolásához vegyük észre, hogy

$$r(A+e) \le r(A)+1, \quad \text{ha } A \subseteq S,\ e \in S-A. \tag{2.2}$$

Valóban, R1)-et és R4)-et használva $r(A)+1 \ge r(A)+r(e) \ge r(A\cap\{e\}) + r(A\cup\{e\}) = r(\emptyset)+r(A+e) = r(A)$ adódik. Legyen most $Y \in \mathfrak{F}$ és $X \subseteq Y$. Ekkor (2.2) ismételt alkalmazásával kapjuk, hogy $r(Y) \le r(X)+|Y-X|$, amiből $r(Y)=|Y|$ miatt $r(X) \ge |X|$. Figyelembe véve R3)-at, $r(X)=|X|$, azaz $X \in \mathfrak{F}$ adódik.

I3') igazolásához legyen $K, N \in \mathfrak{F}$, $|K| < |N|$. Ekkor $r(K) = |K|$ és $r(N)=|N|$. Ha valamely $x \in N-K$ elemre $K+x \notin \mathfrak{F}$, akkor $r(K+x) = r(K)$. Ha ez minden $x \in N-K$ elemre fennállna, akkor a 29. Lemma és R2) szerint $|K| = r(K) = r(K\cup(N-K)) = r(K\cup N) \ge r(N) = |N|$, ami ellentmondás.

Ezzel beláttuk, hogy $\mathcal{M} = (S, \mathfrak{F})$ matroid. Be kell még bizonyítanunk, hogy $\mathcal{M}$-nek tényleg r a rangfüggvénye. Jelölje tehát $r_{\mathcal{M}}$ az $\mathcal{M}$ rangfüggvényét. Tekintsünk egy $X \subseteq S$ halmazt, és legyen ebben K egy maximális független. Ekkor R2) miatt $r_{\mathcal{M}}(X) = |K| = r(K) \le r(X)$. Viszont itt nem lehet, hogy $r_{\mathcal{M}}(X) < r(X)$, mert akkor a 29. Lemma miatt létezne $e \in X-K$ elem, amelyre $r(K+e) = r(K)+1$, amiből $|K|+1 = |K+e| \ge r(K+e) = r(K)+1 = |K|+1$. Ez pedig azt jelentené, hogy $|K+e| = r(K+e)$, vagyis $K+e$ is függetlne volna X-ben, ami ellentmond K maximalitásának. $\square$

2.3. Polimatroid függvények

31. Definíció. Legyen $b : 2^S \to \mathbb{N}_+$ (nemnegatív, egész értékű) függvény. Azt mondjuk, hogy b *polimatroid függvény*, ha kielégíti az R1), R2), R4) axiómákat (de az R3) szubkardinalitás nincs megkövetelve).

A következő célunk annak igazolása, hogy nemcsak a rangfüggvények, de a polimatroid függvények is alkalmasak matroidok definiálására. (Természetesen a matroidból már nem lesz kiolvasható az őt definiáló polimatroid függvény.)

32. Tétel. *Legyen*

$$\mathfrak{F}_b := \{I \subseteq S : b(Y) \geq |Y \cap I| \text{ minden } Y \subseteq S\text{-re}\}. \tag{2.3}$$

Ekkor $\mathcal{M} = (S, \mathfrak{F}_b)$ *matroid, amelynek rangfüggvénye*

$$r_b(Z) = \min\{b(X) + |Z - X| : X \subseteq Z\}. \tag{2.4}$$

Bizonyítás. Mindenekelőtt jegyezzük meg, hogy b monotonitása miatt (2.3) a következő, ekvivalens alakba írható:

$$\mathfrak{F}_b := \{I \subseteq S : b(Y) \geq |Y| \text{ minden } Y \subseteq I\text{-re}\}. \tag{2.5}$$

I1) és I2) ismét triviálisan teljesül. A bizonyítás során I3)-at és a (2.4) egyenlőséget egyszerre fogjuk belátni. Vegyük észre, hogy minden $I \subseteq Z$, $I \in \mathfrak{F}_b$ esetén $|I| \leq b(X) + |Z - X|$, ahol $X \subseteq Z$, hiszen (2.3) szerint $|I \cap X| \leq b(X)$, amiből

$$|I| = |I \cap X| + |I - X| \leq b(X) + |Z - X| \tag{2.6}$$

következik. Látható, hogy (2.6)-ban pontosan akkor áll egyenlőség, ha

$$|I \cap X| = b(X) \text{ és } Z - X \subseteq I \tag{2.7}$$

Így ha I kielégíti (2.7)-et valamely X halmazra, akkor $|I|$ éppen a (2.4) jobb oldalán álló minimummal egyenlő.

Tetszőleges $X \subseteq Z$ részhalmazra vezessük most be az $m(X) := |I \cap X|$ jelölést. Nyilvánvaló, hogy $m(X) + m(Y) = m(X \cap Y) + m(X \cup Y)$. Az $I \in \mathfrak{F}_b$ feltétel azzal ekvivalens, hogy minden $X \subseteq Z$-re $m(X) \leq b(X)$. Nevezzük X-et (I-re nézve) pontosnak, ha $m(X) = b(X)$. Nyilvánvaló, hogy az üres halmaz pontos. Belátjuk, hogy két pontos halmaz metszete és uniója is pontos. Valóban, legyenek X és Y pontos halmazok. Ekkor $m(X) + m(Y) = b(X) + b(Y) \geq b(X \cap Y) + b(X \cup Y) \geq m(X \cap Y) + m(X \cup Y) = m(X) + m(Y)$, amiből következik az állítás.

Legyen most $I \subseteq Z$, olyan $\mathfrak{F}_b$-beli halmaz, amely ($\mathfrak{F}_b$-ben maradva) már nem bővíthető Z-beli elemmel. Ez azt jelenti, hogy $Z - I$ minden eleméhez létezik egy $X_z \subseteq I + z$ halmaz, amelyre $b(X_z) \leq m(X_z)$. Persze X_z-nek tartalmaznia kell z-t, így $m(X_z) = |X_z| - 1$, továbbá $b(X_z) \geq b(X_z - z) \geq |X_z - z| = |X_z| - 1 \geq b(X_z)$. Ezzel beláttuk, hogy X_z pontos.

Ekkor viszont az összes X_z halmaz uniója is pontos lesz, tehát egy olyan pontos X halmazt találtunk, amely tartalmazza $Z - I$ összes elemét, vagyis kielégíti (2.7)-et, azaz (2.6) egyenlőséggel teljesül. Ebből következik, hogy egy nem bővíthető I halmaz elemszáma mindig ugyanaz a Z-től függő szám, azaz I3) is fennáll, és egyúttal (2.4)-et is beláttuk. □

2.4. Rado tétele és következményei

Polimatroid függvények előállítására egy lehetséges mód a következő. Legyen $\mathcal{M} = (S, \mathfrak{F})$ matroid r rangfüggvénnyel, T tetszőleges halmaz, $\varphi : S \to T$ pedig egy szürjekció. Definiáljuk a $b_r : 2^S \to \mathbb{N}_+$ a következőképpen: $b_r(X) := r(\varphi^{-1}(X))$.

33. Állítás. *Az így definiált b_r polimatroid függvény.*

Bizonyítás. Először is $b_r(\emptyset) = r(\varphi^{-1}(\emptyset)) = r(\emptyset) = 0$. Másodszor, b_r monoton, hiszen r monoton, és $X \subseteq Y$ esetén $\varphi^{-1}(X) \subseteq \varphi^{-1}(Y)$. Végül b_r szubmoduláris, hiszen $b_r(X) + b_r(Y) = r(\varphi^{-1}(X)) + r(\varphi^{-1}(Y)) \geq r(\varphi^{-1}(X) \cap \varphi^{-1}(Y)) + r(\varphi^{-1}(X) \cup \varphi^{-1}(Y)) = r(\varphi^{-1}(X \cap Y)) + r(\varphi^{-1}(X \cup Y)) = b_r(X \cap Y) + b_r(X \cup Y)$. □

34. Definíció. A fent definiált b_r függvényhez tartozó matroidot $\varphi(\mathcal{M})$-mel jelöljük, és az $\mathcal{M}$ *homomorf kép*ének nevezzük.

(2.5) alapján $\varphi(\mathcal{M})$-ben egy I halmaz pontosan akkor független, ha minden $X \subseteq I$ esetén $r(\varphi^{-1}(X)) \geq |X|$. Ebből persze rögtön következik, hogy egy olyan $X \subseteq I$ halmaz, amelyre $r(\varphi^{-1}(X)) < |X|$, tanú I függőségére. A következő tétel tanút szolgáltat a függetlenségre is:

35. Tétel (R. Rado). *$I \subseteq T$ pontosan akkor független $\varphi(\mathcal{M})$-ben, ha létezik $\mathcal{M}$-ben egy független F halmaz, amelyre $I = \varphi(F)$, $|I| = |F|$. (Vagyis az $\mathcal{M}$-beli független halmazok képeként előálló halmazok a függetlenek $\varphi(\mathcal{M})$-ben.)*

Bizonyítás. $\varphi(\mathcal{M})$ definíciójából nyilvánvaló, hogy egy $\mathcal{M}$-ben független F halmaz $\varphi(F)$ képe független $\varphi(\mathcal{M})$-ben. A másik irány igazolásához legyen $I \subseteq T$ független. Indukciót alkalmazunk $|\varphi^{-1}(I)|$-re. Ha minden $t \in I$-re $\varphi^{-1}(t)$ egyelemű, akkor legyen $F := \varphi^{-1}(I)$. Ekkor $|I| = |F|$, és $r(F) = r(\varphi^{-1}(I)) \geq |I| = |F|$, azaz I tényleg előáll $\mathcal{M}$-beli független halmaz, nevezetesen F képeként.

Feltehető tehát, hogy léteznek $t \in I$ és $a, b \in S$ elemek úgy, hogy $\varphi(a) = \varphi(b) = t$. Ha az $\mathcal{M}$ matroidból a-t elhagyva I független marad, azaz

$$r(\varphi^{-1}(X)) \geq |X| \text{ minden } X \subseteq I \text{ esetén,} \tag{2.8}$$

akkor indukcióval készen vagyunk. Ugyanígy készen vagyunk, ha b-t elhagyva marad fenn (2.8). Azt kell tehát belátnunk, hogy nem lehet, hogy mind a, mind b törlése megsértse (2.8)-at.

Ha a törlése után létezik $X \subseteq I$, amelyre (2.8) már nem áll fenn, akkor $|X| \leq r(\varphi^{-1}(X)) \leq r(\varphi^{-1}(X) - a) + 1 \leq |X|$, azaz itt végig egyenlőség áll.

Így egyrészt $|X| = r(\varphi^{-1}(X))$, azaz X pontos, másrészt $r(\varphi^{-1}(X)) - 1 = r(\varphi^{-1}(X) - a)$, vagyis a a $\varphi^{-1}(X)$ minden maximális függetlenjében benne van; másszóval az a elem a $\varphi^{-1}(X)$ *híd*ja.

Láttuk a 32. Tétel bizonyításában, hogy pontos halmazok metszete is pontos, így létezik egy legszűkebb P pontos halmaz, amely tartalmazza t-t. Mivel a hídja egy t-t tartalmazó halmaz ősképének, ezért hídja az ennél nem bővebb $\varphi^{-1}(P)$-nek is Ugyanezek a meggondolások érvényesek b-re is, így azt kaptuk, hogy a és b is hídja $\varphi^{-1}(P)$-nek. Ekkor azonban $P' := P - t$-re $r(\varphi^{-1}(P')) \leq r(\varphi^{-1}(P) - \{a, b\}) = r(\varphi^{-1}(P)) - 2 = |P| - 2 = |P'| - 1$, ami ellentmond annak, hogy I független $\varphi(\mathcal{M})$-ben. $\square$

Rado eredetileg kicsit általánosabb formában mondta ki tételét:

36. Tétel. *Legyen $G = (A, B; E)$ páros gráf, M egy A alaphalmazú matroid r rangfüggvénnyel. Pontosan akkor létezik olyan B-t fedő párosítás G-ben, amelynek A-beli végponthalmaza független M-ben, ha minden $X \subseteq B$ esetén $r(\Gamma(X)) \geq |X|$, ahol $\Gamma(X) \subseteq A$ az X szomszédainak halmazát jelöli.*

Bizonyítás. Definiáljuk E-n a következő $\mathcal{M}_E$ matroidot. Legyen $F \subseteq E$ független $\mathcal{M}_E$-ben, ha az F-fel érintkező A-beli pontok halmaza független M-ben. Könnyen látható, hogy így tényleg matroidot kaptunk, hiszen semmi mást nem csináltunk, mint minden $a \in A$ elemet $d(a)$-szor párhuzamosan megtöbbszöröztünk az $\mathcal{M}$ matroidban. Jelölje r_E az $\mathcal{M}_E$ rangfüggvényét, és definiáljuk a $\varphi : E \to B$ leképezést úgy, hogy $\varphi(e)$ legyen az e él B-beli végpontja.

B pontosan akkor független $\varphi(\mathcal{M}_E)$-ben, ha létezik olyan B-t fedő G-beli párosítás, amelynek A-ba eső végponthalmaza független $\mathcal{M}$-ben. Vegyük még észre, hogy minden $X \subseteq B$ halmazra teljesül, hogy $r_E(\varphi^{-1}(X)) = r(\Gamma(X))$. Ekkor az állítás következik a 35. Tételből. $\square$

37. Következmény. *Legyen adott a $G = (S, T; E)$ páros gráf S pontosztályán egy $\mathcal{M}$ matroid. Egy $T \subseteq I$ halmazt definiáljunk függetlennek, ha létezik olyan I-t fedő G-beli párosítás, amelynek S-beli végponthalmaza független M-ben. Így egy $\mathcal{M}_T$ matroidot kapunk, amelynek rangfüggvénye*

$$r_T(Z) = \min\{r(\Gamma(X)) + |Z - X| : X \subseteq Z\}. \quad \square$$

38. Definíció. Legyen adott az S alaphalmazon k matroid, $r_1, \ldots r_k$ rangfüggvényekkel, és legyen $b := \sum_{i=1}^{k} r_i$. Könnyen ellenőrizhető, hogy b polimatroid függvény. A hozzá tartozó $\mathcal{M}_ö$ matroidot a k kiindulási matroid *összeg*ének nevezzük. Ennek rangfüggvénye a 32. tétel alapján

$$r_{ö}(Z) = \min\{\sum_{i=1}^{k} r_i(X) + |Z - X| : X \subseteq Z\}. \tag{2.9}$$

39. Állítás. *Az $\mathcal{M}_1, \ldots, \mathcal{M}_k$ matroidok összegében egy F halmaz pontosan akkor független, ha előáll $F = \bigcup_{i=1}^{k} F_i$ alakban, ahol F_i független az $\mathcal{M}_i$ matroidban.*

Bizonyítás. Készítsük el az S alaphalmaz k egymástól és S-től is diszjunkt kópiáját (legyenek ezek $S_1, \ldots S_k$), és tekintsük az S_i alaphalmazon az $\mathcal{M}_i$ matroidot. Definiáljuk az $S^* := \cup S_i$ alaphalmazon az $\mathcal{M}_i$ matroidok $\mathcal{M}^*$ direkt összegét, és vegyük azt a $\varphi : S^* \to S$ leképezést, amely minden S_i-beli elemhez a neki megfelelő S-beli elemet rendeli. Ekkor látható, hogy $\varphi(\mathcal{M}^*)$ éppen $\mathcal{M}_{ö}$ lesz, így Rado tételéből adódik az állítás. $\square$

40. Következmény (Partíciós tétel). *Adott az S alaphalmazon k matroid. S pontosan akkor bomlik fel k halmaz egyesítésére úgy, hogy az i-edik halmaz független az i-edik matroidban, ha $\sum_{i=1}^{k} r_i(X) \geq |X|$ teljesül minden $X \subseteq S$ részhalmazra.* $\square$

41. Következmény. *Adott az S alaphalmazon egy matroid. S pontosan akkor bomlik fel k független halmaz egyesítésére, ha*

$$kr(X) \geq |X| \tag{2.10}$$

teljesül minden zárt, összefüggő $X \subseteq S$ halmazra.

Bizonyítás. Csupán azt kell belátnunk, hogy (2.10)-et elég zárt és összefüggő halmazokra megkövetelni. Tegyük tehát fel, hogy létezik $X' \subseteq S$ halmaz, amelyik megsérti (2.10)-et. Ekkor persze $X := \mathrm{cl}(X)$ is megsérti. Láttuk, hogy X egyértelműen felbomlik $X_1, \ldots X_t$ diszjunkt, nemüres, összefüggő részekre. X zártságából következik, hogy az X_i halmazok is zártak. Ezek egyike meg kell, hogy sértse (2.10)-et, különben $r(X) = \sum_{i=1}^{t} r(X_i) \geq \sum_{i=1}^{t} k|X_i| = k|X|$ miatt X sem sértené meg. $\square$

2.5. Matroidok partíciós algoritmusa

Legyenek $\mathcal{M}_i = (S, \mathfrak{F}_i)$, $k = 1, \ldots, k$ matroidok. Az $\mathcal{M}_i$ matroid rangfüggvénye legyen r_i, és jelölje $\mathcal{M}_ö$ a matroidok összegét. A partíciós algoritmus célja az összegmatroid maximális $F_1 \cup \cdots \cup F_k$ alakú függetlenjének előállítása, ahol az F_i halmazok páronként diszjunktak, és F_i független $\mathcal{M}_i$-ben.

(2.9)-et az $X = S$ esetben alkalmazva:

$$r_ö(S) = \min_{Y \subseteq S} \Big(\sum_{i=1}^{k} r_i(Y) + |S - Y| \Big). \tag{2.11}$$

Az, hogy (2.11) bal oldala legfeljebb akkora, mint a jobb oldal, következik abból, hogy $\mathcal{M}_ö$ egy maximális $F_1 \cup \cdots \cup F_k$ alakú függetlenje legjobb esetben kitölti $S - Y$-t, és teljesíti az $|F_i \cap Y| = r_i(Y)$ egyenlőtlenséget. (Ez a „legjobb eset" szerepel éppen a jobb oldalon.) Így az algoritmus során éppen egy ilyen Y fogja tanúsítani számunkra, hogy megtaláltuk a maximális független halmazt.

Az algoritmus leírása

Válasszunk ki először tetszőleges diszjunkt F_i halmazokat, amelyek rendre függetlenek az $\mathcal{M}_i$ matroidokban. Ha esetleg $F_1 \cup \cdots \cup F_k = S$, akkor az $Y = \emptyset$ választással készen is vagyunk. Tegyük tehát fel, hogy ez nem teljesül. Definiálunk egy irányított gráfot az $S \cup t_1 \cup \cdots \cup t_k$ ponthalmazon, ahol $t_1, \ldots t_k$ új (azaz eddig nem szereplő) pontok.

i) Legyen $\overrightarrow{xt_i}$ él, ha $x \in F_i$, és $F_i + x$ független $\mathcal{M}_i$-ben.

ii) Legyen $\overrightarrow{xy}$ él, ha $y \in F_i$ valamilyen i-re, $x \notin F_i$, és $F_i + x - y$ független $\mathcal{M}_i$-ben, de $F_i + x$ nem az.

E gráf segítségével fogjuk bővíteni az eddig megkonstruált független halmazunkat, illetve, ha ez nem megy, akkor megadni Y-t. Legyen $R := S - (F_1 \cup \cdots \cup F_k)$. Irányított utat szeretnénk találni R egy pontjából valamelyik t_i-be, és egy ilyen út mentén fogjuk bővíteni a matroidot úgy, hogy az útban lévő $\overrightarrow{xt_i}$ élekre x-et hozzávesszük F_i-hez, míg az $\overrightarrow{xy}$ élekre (ahol $y \in F_i$), x-et hozzávesszük F_i-hez, y-t pedig elhagyjuk belőle. Az így kapott $F_1' \cup \cdots \cup F_k'$ halmaz persze nagyobb elemszámú lesz az előzőnél, így csak arra kell ügyelnünk, hogy az utat úgy válasszuk meg, hogy a kapott halmaz független maradjon $\mathcal{M}_ö$-ben.

I. eset Létezik irányított út R-ből a $T = \{t_1, \ldots t_k\}$ halmazba. Ekkor belátjuk a következő állítást:

42. Állítás. *Ha egy legrövidebb irányított L utat veszünk R-ből T-be, akkor a fenti cserélgetéssel kapott $F_1' \cup \dots \cup F_k'$ halmaz független lesz az összegmatroidban.*

Bizonyítás. Azt igazoljuk, hogy tetszőleges i-re F_i' független lesz $\mathcal{M}_i$-ben. Ehhez az irányított úton visszafelé haladva fogjuk cserélgetni az elemeket. Ha van $\overrightarrow{xt_i}$ él L-en, akkor x-et nyugodtan hozzávehetjük F_i-hez. Legyenek $\overrightarrow{x_1y_1}, \dots, \overrightarrow{x_ly_l}$, az F_i-be belépő L-beli élek, úgy sorszámozva, ahogy R-ből t_i felé haladva elhelyezkednek az úton. Látható, hogy x_l-et betéve F_i-be, és y_l-et kivéve onnan, a többi x_j elem F_i-re vonatkozó alapköre nem változik, hiszen nincs $\overrightarrow{x_iy_l}$, $i < l$ él, mivel L-nek az egyik legrövidebb utat választottuk. Ezt a cserélgetést folytatva, a végül kapott F_i' halmaz is független lesz. $\square$

Ezt az eljárást ismételjük addig, amíg elő nem áll a

II. eset Nem létezik irányított út R-ből T-be. Belátjuk, hogy ekkor az R-ből irányított úton elérhető pontok halmaza (ebbe R-et is beleértjük) megfelel Y-nak.

Jelöljük tehát a fenti halmazt Y-nal. Az nyilvánvaló, hogy $F_1 \cup \dots \cup F_k$ kitölti $S - Y$-t, így csak azt kell belátnunk, hogy minden i-re $|F_i \cap Y| = r_i(Y)$. Mivel Y-ból a feltétel szerint nem lép ki él, ezért tetszőleges $x \in Y - F_i$ elemnek az F_i-re vonatkozó alapköre $F_i \cap Y$-ban van. Így $r_i\big((F_i \cap Y) + x\big) = r_i(F_i \cap Y) = |F_i \cap Y|$. Ebből rögtön következik (29. Lemma), hogy $r_i(Y) = r_i(F_i \cap Y) = |F_i \cap Y|$.

Látható, hogy az algoritmus polinomiális (ha a matroidoknál szokásos módon van egy függetlenségi orákulumunk, ami tetszőleges halmazról egy lépésben eldönti, hogy független-e vagy sem), hiszen ha $|S| = n$, akkor a segédgráf felépítéséhez legfeljebb $n(n-1)+nk \le 2n^2$ lépésre van szükségünk. Egy lépés során szintén $\mathrm{O}(n^2)$ időben kereshetünk irányított utat R-ből T-be, és minden lépés során eggyel csökken $|R|$, tehát legfeljebb n lépésre lehet szükségünk. Így az algoritmus lépésszáma $\mathrm{O}(n^3)$.

3. Keresés matroidokban

3.1. A feladat

Ha valaki találkozik a kereséssel foglalkozó fejezet végén található feladattal (lásd 20. Tétel), ráadásul tudja, hogy mi az a matroid, akkor könnyen feltűnhet neki, hogy a feladatban tulajdonképpen egy matroidról van szó. Hiszen adott az S alaphalmaz, valamint ezen adott az $\mathcal{U}_{n,k}$ uniform matroid, és ekkor a következő keresési feladattal állunk szemben: az S alaphalmazon binárisan keresünk egy elemet úgy, hogy a keresőhalmazok éppen a matroid független részhalmazai.

43. Definíció. Az $(S, \mathfrak{F})$ matroid egy egyelemű részhalmazát *hurok*nak nevezzük, ha a rangja 0. $(S, \mathfrak{F})$ *hurokmentes*, ha nem tartalmaz hurkot.

44. Definíció. Egy $(S, \mathfrak{F})$ bináris keresési feladatot (azaz most $\mathfrak{F} \subseteq 2^S$) *matroidban való keresés*nek nevezünk, ha az $(S, \mathfrak{F})$ pár hurokmentes matroidot alkot.

Könnyen látható, hogy a hurokmentességre lényegében szükségünk van. Ha az $\mathcal{M}$ matroidban van legalább két hurok, akkor ezeket keresési szempontból nem tudjuk megkülönböztetni, mivel egyikük sem lehet benne egyik keresőhalmazban sem. Így csak az az eset ad értelmes feladatot, amikor pontosan egy hurkot tartalmaz $\mathcal{M}$, de ezzel nem fogunk foglalkozni. (Ekkor egy olyan keresési feladatot kapunk, amikor nem tudjuk, hogy pontosan egy x^* elemet kell megkeresnünk, csak azt, hogy legfeljebb egyet.) A továbbiakban matroidon mindig hurokmentes matroidot fogunk érteni.

A feladatot a dolgozat hátralévő részében a legrosszabb esetben vizsgáljuk. Első példának megemlítjük azt a nyilvánvaló tényt, hogy ha maga az S alaphalmaz független, akkor természetesen semmi megkötésünk nincs a keresőhalmazokra, tehát a keresés $\lceil \log_2 n \rceil$ lépésben elvégezhető (megállapodunk abban, hogy a továbbiakban is mindig $|S| = n$).

Mindenekelőtt azt vizsgáljuk meg, hogyan kell kinéznie egy optimális algoritmusnak. Az első lépésben nyilván nem tehetünk mást, mint hogy rákérdezünk egy $F \subseteq S$ független halmazra. Ha azt a választ kapjuk, hogy a keresett elem benne van F-ben, akkor szinte készen is vagyunk; F-ben a felezéses eljárás segítségével $\lceil \log_2 |F| \rceil$ lépésben megtalálhatjuk x^*-ot. Ha viszont a válasz az, hogy $x^* \notin F$, akkor nyilvánvaló, hogy F-ről akár el is felejtkezhetünk: a feladatot egy kérdés elhasználásával az $S - F$ részmatroidban való keresési feladatra vezettük vissza.

Ebből rögtön látható, hogy csak azok a sikeres algoritmusok érdekesek a számunkra, amelyek leírhatók egy $(F_1, F_2, \ldots, F_k)$ rendezett k-assal, ahol $F_1 \cup \cdots \cup F_k$ az S alaphalmaz partíciója független halmazokra. Itt a keresés során először az F_1 halmazra kérdezünk rá, ha ebben nincs a keresett elem, akkor az F_2-re, és így tovább. Végül, ha F_{k-1} sem tartalmazza x^*-ot, akkor persze már tudjuk, hogy F_k-ban van, így erre nem kell külön kérdést elpazarolni.

Megfordítva, az is nyilvánvaló, hogy $\mathcal{M}$ egy tetszőleges, csupa nemüres független halmazra való partíciójához (ezeket a továbbiakban röviden csak partícióknak fogjuk nevezni) a fent leírt módon egyértelműen tartozik egy sikeres keresőalgoritmus is. Az egyszerűség kedvéért mostantól azonosítani fogjuk a számunkra érdekes algoritmusokat a hozzájuk tartozó partíciókkal.

Most az $\mathcal{M}$ matroid egy $(F_1, \ldots, F_k)$ partíciójához rendeljük hozzá az $\big(L(F_1), \ldots, L(F_k)\big)$ szám-k-ast, ahol

$$L(F_i) = \begin{cases} i + \lceil \log_2 |F_i| \rceil & \text{ha } i < k \\ k - 1 + \lceil \log_2 |F_k| \rceil & \text{ha } i = k. \end{cases}$$

Itt $L(F_i)$-t az F_i halmaz (az adott algoritmushoz tartozó) *hossz*ának nevezzük. Látható, hogy ekkor az $(F_1, \ldots, F_k)$ algoritmus hossza éppen $\max\limits_{1 \le i \le k} L(F_i)$ lesz. Vegyük észre azt is, hogy egy rögzített $(F_1, \ldots, F_k)$ partíció tagjait permutálva különböző algoritmusokat kapunk, amelyeknek a hosszuk is különböző lehet. Nyilvánvaló, hogy ez a hossz akkor lesz a legkisebb, ha $|F_1| \ge |F_2| \ge \cdots \ge |F_k|$ teljesül. Így tehát csak a következő halmazban lévő algoritmusokkal kell foglalkoznunk:

$$\mathfrak{P} := \bigcup_{k=1}^{n} \{(F_1, \ldots, F_k) \in \mathfrak{F}^k : F_1, \ldots, F_k \text{ partíció } \mathcal{M}\text{-ben}, |F_1| \ge \cdots \ge |F_k|\}.$$

A továbbiakban algoritmuson csak $\mathfrak{P}$-beli algoritmusokat értünk.

Ezzel beláttuk a következő állítást:

45. Állítás. *Az $\mathcal{M} = (S, \mathfrak{F})$ matroidhoz tartozó keresési feladat bonyolultsága a következő:*

$$L(S, \mathfrak{F}) = \min_{1 \le k \le n} \min_{(F_1, \ldots, F_k) \in \mathfrak{P}} \max_{1 \le i \le k} L(F_i) \tag{3.1}$$

Az eddigiekben láthatóan csak triviálisan átfogalmaztuk a definíciókat, és így persze pontos, de használhatatlan értéket kaptunk a keresési bonyolultságra. A továbbiakban a célunk egy picivel jobban használható, de már nem feltétlenül egybeeső alsó és felső korlátokat találni.

3.2. Alsó korlát

Az alsó korláthoz először megszabadulunk a (3.1)-beli első minimumtól. Mindenekelőtt jegyezzük meg, hogy

$$L(S,\mathfrak{F}) \leq \min_{1\leq k\leq n} \min_{(F_1,\ldots,F_k)\in\mathfrak{P}} L(F_{k-1}).$$

Így elég azt vizsgálnunk, hogy $\mathcal{M}$ egy partíciójában mekkora a második legkisebb független halmaz (azaz F_{k-1}) hossza.

46. Definíció. Az $\mathcal{M} = (S,\mathfrak{F})$ matroid *partíciós szám*ának azt a legkisebb $K = K(\mathcal{M})$ számot nevezzük, amelyre $\mathcal{M}$ felbontható K független részhalmazának diszjunkt uniójára. Egy pontosan K halmazból álló partíciót *minimális partíció*nak fogunk hívni.

Jegyezzük meg, hogy a definíció értelmes, hiszen csak hurokmentes matroidokkal foglalkozunk, és így $1 \leq K \leq n$. A 41. Következmény szerint

$$K = \max_{X\subseteq S} \left\lceil \frac{|X|}{r(X)} \right\rceil.$$

A továbbiakban, ha egyértelmű, hogy melyik matroidról van szó, $K(\mathcal{M})$ helyett csak K-t fogunk írni.

47. Definíció. Az $X \subseteq S$ halmazt *pontos*nak nevezzük, ha $\lceil \frac{|X|}{r(X)} \rceil = K$ teljesül rá. Általánosabban, $X \subseteq S$ *majdnem pontos*, ha $K-1 \leq \lceil \frac{|X|}{r(X)} \rceil \leq K$. Jelölje rendre $\mathfrak{H}$, illetve $\mathfrak{H}'$ a pontos, illetve a majdnem pontos halmazokból álló halmazrendszereket. (A $\mathfrak{H}_{\mathcal{M}}$ illetve $\mathfrak{H}'_{\mathcal{M}}$ jelöléseket használjuk, ha fel akarjuk tüntetni, hogy melyik matroidról van szó.)

48. Tétel. *Legyen $\mathcal{M} = (S,\mathfrak{F})$ matroid, $F \in \mathfrak{F}$ tetszőleges független halmaz. Pontosan akkor létezik $\mathcal{M}$-nek olyan minimális partíciója, amelynek egyik eleme F, ha F lefogja $\mathfrak{H}$-t.*

Bizonyítás. Nyilvánvaló, hogy pontosan akkor létezik $\mathcal{M}$-nek olyan minimális (tehát K halmazból álló) partíciója, amelynek egyik eleme F, ha az $\mathcal{M}' =$

$\mathcal{M} - F$ részmatroidnak létezik $K-1$ halmazból álló (persze szükségképpen minimális) partíciója, azaz ha minden $X \subseteq S - F$-re

$$\left\lceil \frac{|X|}{r'(X)} \right\rceil \leq K - 1 \tag{3.2}$$

teljesül. Mivel $X \subseteq S - F$ esetén $r'(X) = r(X)$, ezért (3.2) pontosan akkor lesz igaz, ha minden $P \in \mathfrak{H}_{\mathcal{M}}$ pontos halmazra $P \not\subseteq S - F$, vagyis F minden pontos halmazt metsz. □

49. Következmény. *Legyen $F_1 \cup \cdots \cup F_{K+r}$ egy partíciója az $\mathcal{M}$ matroidnak, ahol $r \geq 0$. Ekkor tetszőleges $r+1$ (illetve $r+2$) halmazt kiválasztva az uniójuk lefogja $\mathfrak{H}$-t (illetve $\mathfrak{H}'$-t).*

Bizonyítás. A bizonyítás teljesen hasonló az előző tételéhez. □

Az alsó korlátról szóló tételhez szükségünk lesz a következő igen egyszerű lemmára, ami a keresési feladat megoldása egy igen speciális esetben.

50. Lemma. *Ha az $\mathcal{M} = (S, \mathfrak{F})$ matroid előáll két független halmazának uniójaként, akkor keresési bonyolultsága*

$$L(S, \mathfrak{F}) = \lceil \log_2 n \rceil. \tag{3.3}$$

Bizonyítás. Az információelméleti alsó korlát miatt $L(S, \mathfrak{F}) \geq \lceil \log_2 n \rceil$. Így elég belátnunk, hogy tudjuk a felezéses eljárást alkalmazni. Ehhez azt igazoljuk, hogy $\mathcal{M}$ felbontható egy $\lceil \frac{n}{2} \rceil$ és egy $\lfloor \frac{n}{2} \rfloor$ méretű független halmaz uniójára. (Persze ebből következik, hogy a halmazok diszjunktak lesznek.) Ez viszont azonnal adódik a matroidokra vonatkozó I3') axiómából, hiszen ha az egyik független mérete nagyobb, mint $\lceil \frac{n}{2} \rceil$, akkor ebből áttehetünk egy elemet a másikba úgy, hogy továbbra is mindketten függetlenek maradjanak. □

51. Tétel. *Legyen $\mathcal{M} = (S, \mathfrak{F})$ hurokmentes matroid. Ekkor a hozzá tartozó keresési feladatra*

$$L(S, \mathfrak{F}) \geq K(\mathcal{M}) - 2 + \lceil \log_2 \tau(\mathfrak{H}') \rceil, \tag{3.4}$$

ahol $\tau(\mathfrak{H}')$ a $\mathfrak{H}'$ halmazt lefogó pontok minimális számát jelöli.

Bizonyítás. A 1.4. fejezetben látottak alapján elég egy stratégiát megadnunk a válaszoló számára, amely legalább $K(\mathcal{M}) - 2 + \lceil \log_2 \tau(\mathfrak{H}') \rceil$ kérdésre kényszeríti a kereső játékost. Ez a következő lesz: az első $K-2$ kérdésre nemmel válaszolunk. Ekkor a 49. Következmény miatt, akármilyen ügyes volt is a kérdező, legalább $\tau(\mathfrak{H}')$ elem maradt, amelyekről semmi egyebet nem tud, mint hogy köztük van x^*. Az információelméleti alsó korlát szerint így még legalább $\lceil \log_2 \tau(\mathfrak{H}') \rceil$ kérdésre lesz szüksége (és innentől kezdve úgy válaszolunk, hogy a két halmaz közül mindig a nagyobban kelljen folytatnia a keresést). $\square$

Bár általában nem lényeges, hogy egy alsó korlát algoritmikusan meghatározható legyen, és ráadásul az is közismert [4], hogy tetszőleges halmazrendszer esetén τ kiszámítása NP-nehéz, mégis a fenti tételbeli alsó korlát értéke polinom időben meghatározható a partíciós algoritmus segítségével. $\tau(\mathfrak{H}')$ kiszámításához határozzuk meg először a matroid K partíciós számát (lásd a következő fejezetet), majd az Edmonds-algoritmus segítségével egy maximális $K-2$ elemű részpartíciót. Ekkor nyilván a kimaradó $R = S - \bigcup_{i=1}^{K-2} F_i$ halmaz elemszáma lesz $\tau(\mathfrak{H}')$. Látni fogjuk, hogy néhány speciális esetben az alsó korlát pontos, és általában is közel van a keresőalgoritmus által adott felső korláthoz — a két korlát közötti különbség ugyanis a matroid szabálytalanságából adódik, és például az uniform matroid esetében teljesen el is tűnik.

3.3. Algoritmus

Az előző két fejezetből tulajdonképpen adódik is a keresőalgoritmus, csak néhány technikai nehézséggel kell megbirkóznunk. Az algoritmus lényegében úgy fog kinézni, hogy a matroidot pontosan K darab függetlenre particionáljuk, ezeket nagyság szerint csökkenő sorrendbe rakjuk, és ebben a sorrendben kérdezünk rájuk. Ha egyszer azt a választ kapjuk, hogy valamelyikükben benne van a keresett elem, akkor abban a halmazban a felezéses eljárással folytatjuk a keresést.

Természetesen a partícióban szereplő független halmazok megválasztásában szabadok vagyunk. Azt, hogy ez mennyire fontos lépése az algoritmus megtervezésének, a következő egyszerű példa illusztrálja.

52. Példa. Tekintsük az $\mathbb{R}^{1996}$ vektortér következő elemeit: $e_1 = (1, 0, \ldots, 0)$, $\ldots$, $e_{1996} = (0, \ldots, 0, 1)$; $f_1 = (0, \ldots, 0, 2)$, $\ldots$, $f_4 = (0, \ldots, 0, 5)$. Láttuk már, hogy ezek a lineáris függetlenséggel matroidot alkotnak, ami persze hurokmentes is. Könnyen ellenőrizhető, hogy a matroid egy minimális partíciója 5 függetlenből áll. Ha úgy bontjuk fel, hogy az első független halmaz az $e_1, \ldots, e_{1996}$ elemekből áll, míg többi elem egyelemű függetleneket alkot, akkor látható, hogy a keresés hossza (a legrosszabb esetben) $1 + \lceil \log_2 1996 \rceil = 12$. Vegyük azonban észre, hogy ha az $e_{1996}, f_1, f_2, f_3, f_4$

elemeket külön halmazokba tesszük, akkor a többi elemet tetszésünk szerint oszthatjuk el ezekbe a halmazokba, így elég csak az elemszámokat tekinteni. Így például ha az mindegyik halmazba 400 elemet teszünk, akkor az így kapott algoritmus hossza már $4+\lceil\log_2 400\rceil=13$ lesz. Viszont ha az elemszámokat a következőképpen választjuk meg: $1000, 500, 250, 125, 125$, akkor a hossz csak $4+\lceil\log_2 125\rceil=11$.

Bár az általános esetben nem lesz ekkora szabadságunk az elemek megválasztásával (hiszen a példabeli matroid „majdnem" szabad matroid volt), számunkra mégis a halmazok elemszámai lesznek a kezelhetőek. Azt fogjuk igazolni, hogy nagyon különböző elemszámú független halmazokra való felbontásból (mint az első eset az előző példában) legyárthatunk egy keresési szempontból egyenletes partíciót (mint a harmadik eset a példában).

Először azonban foglalkozzunk K meghatározásával. Az Edmonds-féle partíciós algoritmus ismeretében ez igen egyszerű, hiszen csak egy olyan számot kell keresnünk, hogy annyi függetlenre még éppen felbontható a matroid, de kevesebbre már nem. Tudjuk, hogy $1 \le K \le n$, és így K-ra a felezéses eljárást alkalmazhatjuk, minden lépésben lefuttatva a partíciós algoritmust. Mivel a partíciós algoritmus lépésszáma $O(n^3)$, ezért K-t meghatározhatjuk $O(n^3\lceil\log_2 n\rceil)$ lépésben. Eközben persze kapunk is egy K elemű partíciót.

A példából látható, hogy gondot az okozhat, ha a partícióbeli független halmazok méretei között túl nagy ugrások vannak. Ennek kiküszöböléséhez megadunk egy eljárást, ami az algoritmus szempontjából egyenletessé teszi a méreteket.

53. Lemma. *Ha egy $(F_1, \dots, F_K)$ sikeres algoritmusban valamilyen $1 \le i \le K-2$ indexre $|F_i| > 2|F_{i+1}|$, akkor gyárthatunk egy legfeljebb ilyen hosszú $(F_1, \dots, F_i', F_{i+1}', \dots, F_K)$ sikeres algoritmust, amelyre $|F_i| \le 2|F_{i+1}|$.*

Bizonyítás. Legyen $|F_i| = 2a + b$, $|F_{i+1}| = a$, ahol a, b egészek, és $b > 0$. Az I3') függetlenségi axióma ismételt alkalmazásával kapjuk, hogy ekkor F_i-ből áttehetünk $\lceil\frac{b}{3}\rceil$ elemet F_{i+1}-be, úgy, hogy az így kapott F_i' illetve F_{i+1}' halmazok is függetlenek lesznek. Könnyen belátható, hogy tetszőleges egész b-re $\lfloor\frac{2b}{3}\rfloor + \lceil\frac{b}{3}\rceil = b$, így $|F_i'| \le 2|F_{i+1}|$ tényleg teljesül. Az új algoritmus nyilván sikeres lesz, ha az eredeti is az volt, így azt kell még belátnunk, hogy tényleg nem lett hosszabb, azaz

$$i + \lceil\log_2(2a+b)\rceil \ge i + 1 + \left\lceil\log_2\left(a + \left\lceil\frac{b}{3}\right\rceil\right)\right\rceil.$$

Ez triviálisan teljesül, ha a és b olyanok, hogy $(2a+b) \ge 2(a + \lceil\frac{b}{3}\rceil)$. Ez pontosan akkor nem áll fenn, ha $b = 1$, tehát azt kell igazolnunk, hogy

$$\lceil\log_2(2a+1)\rceil \ge 1 + \lceil\log_2(a+1)\rceil, \qquad (3.5)$$

tetszőleges $a \geq 0$ egész esetén. Ez viszont igaz, hiszen ha az $l \geq 0$ egész szám olyan, hogy $2^l < 2a+1 \leq 2^{l+1}$, akkor $2a+1$ páratlansága miatt $2a+1 \leq 2^{l+1}-1$, de így $a+1 \leq 2^l$, azaz (3.5) bal oldalán pontosan $l+1$, míg a jobb oldalán legfeljebb $l+1$ áll. □

54. Definíció. Egy $(F_1, \ldots, F_K)$ algoritmust *egyenletes*nek nevezünk, ha $|F_{K-1}| - |F_K| \leq 1$, továbbá minden $1 \leq i \leq K-2$ esetén $|F_i| \leq 2|F_{i+1}|$.

55. Tétel. *Egy nem egyenletes algoritmus* $\mathrm{O}(Kn)$ *lépésben egyenletessé tehető.*

Bizonyítás. A következő algoritmus adódik az eddigiek alapján:

0. lépés Legyen $i = 1$.

1. lépés Ha $|F_i| > 2|F_{i+1}|$, akkor az 53. Lemmában leírt módszerrel ezt javítsuk ki, és növeljük meg i-t 1-gyel. Ha $i \leq K-2$, akkor vissza az 1. lépés elejére, különben tovább a 2. lépésre.

2. lépés Ha $|F_{K-1}| - |F_K| > 1$, akkor az I3') függetlenségi axióma alapján átrakhatunk F_{K-1}-ből F_K-ba annyi elemet, hogy $|F_{K-1}| - |F_K| \leq 1$ legyen, és persze függetlenek maradjanak a halmazok.

3. lépés Ha az algoritmus még nem egyenletes, akkor vissza a 0. lépésre, különben pedig készen vagyunk.

Az algoritmus végessége és a lépésszámra vonatkozó állításunk is következik abból az egyszerű megfigyelésből, hogy a matroid minden eleme az algoritmus minden lépése során csak nagyobb indexű halmazba kerülhet. Mivel az I3') axióma minden alkalmazása során legalább 1 elem nagyobb indexű halmazba kerül, így az axiómát legfeljebb Kn-szer alkalmazzuk. □

Ezek alapján a keresőalgoritmusunk a következőképpen néz ki.

I. lépés Veszünk egy tetszőleges K elemű partíciót, majd előkészítjük a matroidot a 55. Tétel alkalmazásához. Ehhez először F_1-et $\mathcal{M}$ bázisává bővítjük $F_2 \cup \cdots \cup F_K$-beli elemekkel, majd F_1-et már nem változtatva F_2-t $\mathcal{M} - F_1$ bázisává, és így tovább. Könnyen látható, hogy ezt egy függetlenségi orákulum segítségével mindenféle trükkök nélkül is $\mathrm{O}(Kn)$ időben megtehetjük. (Megjegyezzük, hogy az algoritmus itt erősen javítható lenne — ugyanis a következő lépés szempontjából nem mindegy, hogy milyen partícióból indulunk ki. Nyilvánvalóan látható lesz, hogy igazából egy olyan partíciós algoritmusra lenne szükségünk [amennyiben egyáltalán létezik ilyen], amely a kiindulási matroid egy olyan $(F_1, \ldots, F_K)$ partícióját adja meg, hogy minden i-re F_i

rangja a lehető legnagyobb (azaz bázis), de ko-rangja a lehető legkisebb $\mathcal{M} - (F_1 \cup \cdots \cup F_{i-1})$-ben.)

II. lépés Az így kapott partíciót a 55. Tétel alapján egyenletessé tesszük, és máris rendelkezésünkre áll egy érezhetően elég jó algoritmus a matroidban való keresésre. (Főleg ha sikerülne egy olyan algoritmust találni, amely megfelel az előbbi zárójeles megjegyzésben szereplő kívánalmaknak.)

Ezzel megadtunk egy algoritmust matroidokban való keresésre. Szokás azt is megkérdezni, hogy mit tudunk előre, azaz algoritmus nélkül mondani a keresési bonyolultságról. Erre egyelőre csak egy triviális felső becslést tudok mondani: nyilvánvalóan mindig ki tudjuk úgy egyenlíteni az algoritmust, hogy a független halmazok elemszámai $\lceil \frac{n}{K} \rceil$, illetve $\lfloor \frac{n}{K} \rfloor$ legyenek, tehát az keresési bonyolultság (és persze a fenti algoritmus hossza is) legfeljebb $K-1+\lceil \log_2 \lceil \frac{n}{K} \rceil \rceil$. Ez természetesen abból a szempontból pontos is, hogy rengeteg olyan matroid létezik, amelyre a legjobb algoritmus pontosan ilyen hosszú.

3.4. Alkalmazások

Először a 20. Tételben szereplő keresési feladatot oldjuk meg. Erre persze elvárjuk, hogy pontos értéket kapjunk.

3.4.1. Keresés legfeljebb k elemű keresőhalmazokkal

Mint már láttuk, ez tulajdonképpen az $\mathcal{U}_{n,k}$ uniform matroidban való keresés problémája. (Az egyszerűség kedvéért feltesszük, hogy $n > 2k$.) Az alsó korláthoz most könnyen meg tudjuk határozni a $\mathfrak{H}'$ halmazrendszert. Először is, $K = \lceil \frac{n}{k} \rceil$ lesz, és mivel egy $X \subseteq S$ halmaz rangja $\min(|X|, k)$, ezért

$$\mathfrak{H}' = \{X \subseteq S : |X| > k(K-2)\},$$

azaz az összes legalább $k(K-2)+1$ elemű halmazt kell lefognunk. Könnyen látható, hogy ekkor $\tau(\mathfrak{H}') = n - k(K-2)$, tehát a 51. Tétel alapján azt kaptuk, hogy

$$L \geq K - 2 + \lceil \log_2 n - k(K-2) \rceil, \quad \text{ahol } K = \lceil \frac{n}{k} \rceil.$$

Már most láthatjuk, hogy az alsó korlát megegyezik a 20. Tételben kapott (pontos) alsó korláttal. (Csak ott $K-2$-t t-vel jelöltük.)

Az előző részben megadott keresőalgoritmust tekintve is könnyű a dolgunk ennél a feladatnál, hiszen tetszőleges K halmazból álló partíciót véve az I. lépésben, az előkészítés után lényegében (azaz az elemszámokat tekintve) mindig ugyanazt a partíciót kapjuk: $|F_1| = \cdots = |F_{K-1}| = k$, és $|F_K| = n \bmod k$ lesz. Mivel a II. lépés során csak az F_{K-1} és F_K közötti ugrást kell kiegyenlíteni, és $|F_K| \geq 1$ miatt ez nem rontja el sehol máshol az egyenletességet, ezért éppen a 20. Tételben leírt algoritmust kapjuk vissza.

3.4.2. Egy egyszerű speciális eset

Az általános eredményeink igen jól viselkednek abban az esetben, amikor a matroid eleget tesz az alábbi egyenletességi követelménynek:

$$\lceil \frac{|S|}{r(S)} \rceil = K. \tag{3.6}$$

Ekkor nyilvánvaló, hogy a $t := n \bmod r(S)$ jelöléssel az alsó korlát legalább $K-2+\lceil \log_2(r(S)+t) \rceil$ lesz. (Hiszen ha az első $K-2$ halmaz mindegyike $r(S)$ elemű, az utolsó két halmazba még akkor is be kell férnie $r(S)+t$ elemnek.) Másrészt könnyen látható, hogy akármilyen K elemű partíciót kapunk is az algoritmus I. lépésében, csak az utolsó két halmaz méretét kell kiegyenlíteni (ezt pedig még az alsó korlát is tartalmazza).

A (3.6) feltételt kielégítő matroidra példa egy teljes gráf körmatroidja. Erre kiszámolva az alsó korlátot, és megnézve az algoritmus működését, tényleg látható, hogy ebben az esetben meglehetősen közel vannak egymáshoz a korlátok.

Felhasznált irodalom

[1] M. Aigner. *Combinatorial Search.* Wiley–Teubner Series in Computer Science. Wiley–Teubner, 1988.

[2] R. Dorfman. The detection of defective members of large populations. *Ann. Math. Statist.*, 14:436–440, 1943.

[3] A. Frank. Matroidok. Sokszorosított jegyzet, 1995.

[4] M. R. Garey and D. S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness.* Freeman, 1979.

[5] D. A. Huffman. A method for the construction of minimum redundancy codes. *Proc. I. R. E.*, 40:1098–1101, 1952.

[6] G. O. H. Katona. On separating systems of a finite set. *J. Combinatorial Theory*, 1:174–194, 1966.

[7] C. E. Shannon. A mathematical theory of communication. *Bell System Techn. J.*, 27:379–424, 623–657, 1948.

[8] R. Tošić. Two counterfeit coins. *Discrete Math.*, 46:295–298, 1983.

[9] R. Tošić. Four counterfeit coins. *Review of Research Fac. Sci. Univ. Novi Sad*, 14:99–108, 1984.

[10] I. Wegener. On separating systems whose elements are sets of at most k elements. *Discrete Math.*, 28:219–222, 1979.