Eötvös Loránd Tudományegyetem
Természettudományi Kar

Lenger Dániel Antal
Matematikus MSc

Kombinatorikus keresési problémák

Szakdolgozat

Témavezető: Katona Gyula egyetemi tanár
Számítógéptudományi Tanszék

Budapest, 2016

Köszönetnyilvánítás

Szeretném megköszönni témavezetőmnek, Katona Gyulának, hogy segített megismerni ezen izgalmas témakör problémáit, és jó néhány alapprobléma megoldását. Szeretném továbbá megköszönni a keresési szemináriumon többi résztvevőjének, hogy hétről hétre ilyen érdekes problémákról beszélgetünk. Közülük is külön szeretném megköszönni Gerbner Dánielnek, aki az utolsó két fejezetben ismertetett problémákat alaposan körüljárta és megoldását elmondta nekünk. Végezetül, nagy köszönettel tartozom még családomnak, ismerőseimnek is, akik – bár sokat nem értettek belőle – hősiesen átnézték a dolgozatomat helyesírási, és egyéb hibákat keresve.

Tartalomjegyzék

1. Bevezető

A szakdolgozatom célja bemutatni néhány kombinatorikus keresési problémát. Ezeket a problémákat általában a gyakorlat veti fel, emiatt a legtöbbhöz lehet mondani egy-egy alkalmazást, vagy legalább "mesét", mellyel jobban megérthető a probléma. Nagy általánosságban van egy X alaphalmazunk, abban egy bizonyos (defektív, rossz vagy ismeretlen) elem, és X bizonyos részhalmazaira kérdezhetünk rá (vagy tesztelhetünk), hogy benne van-e a defektív elem. Célunk hogy, minél kevesebb kérdéssel megtaláljuk az elemet.

A következő fejezetben bemutatok néhány példát, és ezeken keresztül megmutatom, hogy mi alapján lehet osztályozni a problémákat. A rákövetkező fejezetekben mélyebben elmerülök ezekben a problémákban. A harmadiktól a hetedik fejezetig korábban ismert, mondhatni klasszikus problémák megoldását írom le, a nyolcadik és kilencedik fejezetben viszont egy teljesen újfajta megközelítést vizsgálok, amikor az elemek (akikre mondjuk számítógépekként vagy emberekként is tekinthetünk) ismerik a választ azokra a kérdésekre, melyekben ők szerepeltek.

2. A problémák felvetése

Természetesen nincsen pontos definíció, hogy mit is nevezünk kombinatorikus keresési problémának, de általában igaz, hogy van egy X véges alaphalmazunk, abban egy (esetleg több) bizonyos elem (melyet defektívnek, rossznak esetleg ismeretlennek nevezzük), és X bizonyos részhalmazaira kérdezhetünk rá (vagy tesztelhetünk), hogy benne van-e a defektív elem. Célunk hogy, minél kevesebb kérdéssel megtaláljuk az elemet.

2.0.1. Példa. *A barkochba nevű játék: Az egyik játékos gondol valamire, míg a másik játékos eldöntendő kérdéseket tesz fel, amelyek segítségével előbb-utóbb kitalálja, hogy az első játékos mire gondolt.*

Ezzel viszonylag sok probléma felmerül. Kezdve azzal, hogy az X alaphalmazba elvileg minden beletartozik, vagyis matematikai értelemben még csak nem is alkot halmazt. Ezt persze a gyakorlatban feloldhatjuk azzal, hogy az első játékos nyilván csak véges karaktersorozatra gondolhat (így X már halmaz lesz), sőt valószínűsíthető, hogy amire gondol, az leírható mondjuk legfeljebb 1000 karakterrel, így már X véges halmaz lesz.

A másik probléma, hogy a második játékos által megkérdezhető részhalmazokat nem tudjuk leírni. Elvben minden részhalmazt megkérdezhet, de a gyakorlatban "értelmes" kérdést kell feltenni, ami nem egy matematikai fogalom, így ez a feladat kezelhetetlen a mi szempontunkból.

Ezért próbáljuk precízebben megfogalmazni a játékot. A későbbiekben már erre fogok barkochba néven hivatkozni.

2.0.2. Példa. *Az első játékos gondol egy egész számra az $\{1, 2, 3, \ldots, n\}$ halmazból, míg a második játékos $\{1, 2, 3, \ldots, n\}$ tetszőleges részhalmazára rákérdezhet. A cél, hogy bármire is gondolt az első játékos, legfeljebb t kérdésből kitalálja azt a második. A kérdés pedig, hogy mi a legkisebb t, melyre ez még megtehető.*

Jelölés. *Igazából mindegy, hogy milyen n elemű halmazt választunk, mindössze a meghatározottság és a könnyebb hivatkozás érdekében választjuk az első n pozitív egész számot. A továbbiakban jelölje $[n] := \{1, 2, 3, \ldots n\}$. Ennek a hatványhalmazát, vagyis az $[n]$ részhalmazait tartalmazó halmazt $2^{[n]}$-nel jelölöm, míg a pontosan k méretű részhalmazainak halmazát $\binom{[n]}{k}$-val jelölöm.*

Ezt a játékot kétféleképpen is lehet játszani. Az egyik az úgynevezett **adaptív**, vagyis a második játékos minden kérdésére egyből válaszol az első játékos (ahogy ezt a sima barkochbában megszoktuk), így a második játékos ezen válaszok ismeretében teheti fel az újabb kérdéseket. A másik pedig az úgynevezett **nem adaptív**, vagyis hogy az első játékosnak előre meg kell adnia az összes kérdést, melyekre a második játékos egyszerre válaszol, és ebből a válaszsorozatból kell kitalálni a gondolt elemet.

A következő fejezetben részletesebben megvizsgálom mindkét játékmódot, és kiderül, hogy mindkét esetben $\lceil \log n \rceil$ lesz a válasz. Általában viszont eltér az adaptív és nem adaptív válasz.

Szintén érdekes kérdés, hogy mi van akkor, ha nem a *legrosszabb* esetben vagyunk kíváncsiak a kérdések számára, hanem az érdekel minket, hogy *várhatóan* hány kérdés kell. Ehhez persze fel kell tételezni valami eloszlást $[n]$-en, és a valószínűségszámítás eszközeit kell segítségül hívnunk, így ilyen irányú problémákkal a szakdolgozatomban nem foglalkozom.

Jelölés. *A vizsgált problémák természetéből adódóan a* log *mindig a 2-es alapú logaritmust jelenti. Amennyiben más alapra is szükségem lesz, azt majd külön jelzem.*

$\lceil x \rceil$ *jelöli* x *felső egészrészet, vagyis a legkisebb egész számot, mely nem kisebb* x*-nél.*

$\lfloor x \rfloor$ *jelöli* x *alsó egészrészet, vagyis a legnagyobb egész számot, mely nem nagyobb* x*-nél.*

2.0.3. Példa. *Vérvizsgálat egy egész hadseregen. Tegyük fel, hogy egy nagy létszámú csoport (például egy hadsereg) néhány tagja megfertőzödött egy bizonyos betegséggel, melynek jelenléte kimutatható a vérből. Ráadásul a tesztünk olyan, hogy ha több mintát összeöntünk, és azt teszteljük le, a teszt pozitív eredményt ad, ha akárcsak egy fertőzött minta is volt köztük.*

Ez általánosítása az előző példának, hiszen itt nem csak egy defektív elemünk lehet. Ha nem tudunk a defektív elemek számáról semmit, akkor ez egy nehezen kezelhető probléma. Viszont ha feltesszük például azt, hogy pontosan (vagy legfeljebb) d defektív elem van, vagy azt, hogy egy elem p valószínűséggel lesz defektív, akkor vannak részeredmények. Előbbiről a hetedik fejezetben fogok néhány ismert eredményt bemutatni, utóbbi viszont szintén egy valószínűségszámítás témakörébe tartozó probléma, így nem foglalkozom vele a szakdolgozatomban.

A vérvizsgálattal kapcsolatban egy újabb érdekes kérdés vetődhet fel.

2.0.4. Példa. *Tudatlan páciensek. Van n személy, akik közül egynek van valamilyen betegsége, amely vérteszttel kimutatható. A vérteszt elvégezhető úgy is, hogy több ember mintáját összeöntjük, ekkor a teszt alapján azt tudjuk, hogy köztük van-e a beteg. A tesztek eredményét az összes benne résztvevő személynek elküldjük a benne résztvevők listájával egyetemben. Az orvosoknak (akik látják az összes teszt eredményét) céljuk, hogy megtalálják a beteget. Lehet-e úgy feltenni a kérdéseket, hogy biztosan ne derüljön ki egyik résztvevő számára se, hogy ki a beteg?*

Ezt a problémát a kilencedik fejezetben vizsgálom, és megmutatom, hogy nem lehet így feltenni a kérdéseket. Ugyanakkor a másik irányú probléma is érdekes: úgy feltenni a kérdéseket, hogy az elemek mind ki tudják találni, hogy ki a defektív. Ez a probléma a számítás-technika a világából érkezett.

2.0.5. Példa. *Van n számítógép, de közülük egy hibásan működik. Ha kiválasztunk néhány gépet, lefuttathatunk egy tesztprogramot, amely minden résztvevő számítógép számára jelzi, hogy köztük van-e a hibás. A feladat minél kevesebb kérdéssel megoldani, hogy az összes számítógép ki tudja találni, hogy melyik a hibás közülük.*

Ezt a problémát a nyolcadik fejezetben vizsgálom. Megmutatom, hogy a szükséges kérdések száma asszimptotikusan $c \log n$, ahol $c = \frac{1}{\log(3/2)}$.

Ez utóbbi két példa újfajta megközelítésnek számít, de van még néhány klasszikus példa, amit szeretnék bemutatni.

2.0.6. Példa. *Van egy kétkarú mérlegünk, és néhány pénzérménk, melyek közül az egyik hamis, így kicsit nehezebb, mint a többi. Mérést úgy végezhetünk, hogy a mérleg mindkét oldalára felteszünk néhány érmét, miután a mérleg vagy egyensúlyban marad, vagy eldől valamelyik irányba. Előbbi esetben a defektív elem a fel nem rakottak között található, utóbbi esetben pedig azok között, melyek a nehezebbek voltak.*

Míg a barkochbánál két részre oszhattuk fel az alaphalmazt, és tudhattuk meg, hogy melyikben van a defektív elem, itt három részre oszthatjuk, azzal a megkötéssel, hogy ebből kettő mérete (melyeket felrakjuk a két oldara) meg kell, hogy egyezzen. Emiatt itt a szükséges mérések száma $\lceil \log_3 n \rceil$ lesz, ahol $\log_3$ a 3-as alapú logaritmust jelöli. Sőt, itt is igaz, hogy mind az adaptív, mind a nem adaptív esetben ennyi lesz a válasz.

Eddig olyan példákat láthattunk, ahol a megkérdezett részhalmazokra nem volt szinte semmi megkötés, most lássunk néhány motivációt arra, milyen megkötések kerülhetnek elő.

2.0.7. Példa. *Ugyanúgy mint az előbb, van egy kétkarú mérlegünk, sok érménk, melyek tömege az* $[1, 1+\delta]$ *intervallumba esik, és egy hamis érménk, mely nehezebb, hiszen tömege pontosan* $1+\varepsilon$*, ahol* $\varepsilon > \delta$*.*

Ekkor, ha $\left\lfloor \frac{\varepsilon}{\delta} \right\rfloor$-nál több érmét pakolunk fel mindkét oldalra, előfordulhat, hogy a defektívvel együtt csupa 1 tömegűt tettünk fel, míg a másik oldalra csupa $1+\delta$ tömegűt, és így a mérleg utóbbi felé dől, hiszen $1+\varepsilon+k-1 < k(1+\delta)$ teljesül, amennyiben $k > \left\lfloor \frac{\varepsilon}{\delta} \right\rfloor$. Ezalapján felmerülhet az alábbi probléma:

2.0.8. Példa. *Barkochba korlátos méretű kérdéssel. Azaz az alaphalmazunkban egy defektív elem van, viszont a kérdezett részhalmazok mérete legfeljebb egy* k *szám lehet.*

Ez a megkötés a részhalmazokra eléggé természetes. Ha a vérvizsgálatra gondolunk, a valóságban elég gyakori az, hogy bizonyos koncentráció alatt nem lehet kimutatni a betegséget, így legfeljebb k mintát érdemes összeönteni a biztos eredményhez. Ezt a példát a hatodik fejezetben vizsgálom részletesebben. Most viszont még lássunk egy újabb példát, hogyan lehet korlátozni a megkérdezett részhalmazt.

2.0.9. Példa. *Van egy nagyon fontos gépezetünk, melyen észrevettük, hogy hiányzik egy anyacsavar, amely korábban egy mára eléggé elrozsdásodott csavart rögzített. Így aztán fogjuk a rozsdás csavart, és elmegyünk a barkácsáruházba beszerezni egy megfelelő méretű anyacsavart hozzá. A barkácsáruházban szerencsére az anyacsavarok átmérő szerint növekvő sorrendben vannak rendezve, mi pedig kipróbálhatjuk mindegyiket, hogy belemegy-e a csavar. Mivel a csavar elég rozsdás, ezért csak annyit tudunk megállapítani, hogy rámegy-e a csavar, vagy sem. De szerencsére tudjuk, hogy nekünk a legkisebb méretű kell, mely még rámegy. Továbbá feltehetjük, hogy a boltban biztosan kapható olyan csavar, ami nekünk kell.*

Vagyis van egy elemünk az $[n]$ halmazból, és ha megkérdezünk egy $k \in [n]$ számot, megtudhatjuk, hogy a defektív elemünk az $\{1, 2, \ldots, k\}$ (vagyis ráment a csavar), vagy a $\{k+1, k+2, \ldots, n\}$ (vagyis nem ment rá a csavar) halmazban van. Itt az adaptív esetben $\log n$ a válasz, míg a nem adaptívnál $n-1$, azaz kénytelenek vagyunk mindent kipróbálni. Ezt az ötödik fejezetben fejtem ki.

3. Barkochba

Mint a legáltalánosabb példa, ez tökéletesen alkalmas lesz a témakörben használt módszerek bemutatására.

3.1. Adaptív eset

3.1.1. Állítás. *Ha adaptív módon kérdezünk, akkor pontosan* $\lceil \log n \rceil$ *kérdésre van szükségünk, hogy megkapjuk a választ.*

Bizonyítás. Először megadunk egy kérdéssorozatot, mellyel ennyi kérdésből megtalálható a defektív elem. Az i. kérdés legyen az, hogy a szám hátulról i. jegye kettes számrendszerben 0-e, azaz $A_i = \{k \in [n] \mid j_i(k) = 0\}$, ahol $j_i(k)$ jelenti a k szám kettes számrendszerbeli alakjának hátulról i. jegyét. Mivel n egymást követő számunk van, ezért az utolsó $\lceil \log n \rceil$ jegye bármely kettőnek eltér legalább egy jegyben, hiszen $n \leq 2^{\lceil \log n \rceil}$. Így tehát ezen kérdésekre kapott válaszokból egyértelműen kitalálható, melyik a defektív elem.

Most pedig lássuk, hogy ennyi kérdésre szükség is van. Ezt kétféleképpen is megmutatom, mindkettő egy-egy elég gyakori módszer az ilyen problémák megoldására. Először bevezetjük a *döntési fa* fogalmát. Erre gondolhatunk úgy, hogy a gyökérből (0. szint) indul ki két él, melyek azt jelölik, hogy az első kérdésre mi volt a válasz. Aztán mindkét szomszédjából (1. szint) indul ki még (legfeljebb) 2-2 újabb él, melyek azt jelölik, hogy a második kérdésre mi volt a válasz, és így tovább. Ha egy pontban már nem kell több kérdést feltenni (mert például már megtaláltuk a defektív elemet), akkor az egyszerűség kedvéért feltesszük, hogy egy él megy a következő szintre, csak hogy minden út leérjen az alsó szintre.

Az utolsó, vagyis t. szinten (ha bármely esetben legfeljebb t kérdést tettünk fel) pedig szerepelnek, hogy az ilyen kapott válaszok esetén mik jöhetnek szóba, mint defektív elem. Ha jók a kérdéseink, azaz minden esetben meg tudjuk találni a defektív elemet, akkor egy alsó szinten lévő csúcsra nem kerülhet egynél több lehetséges elem. Az persze előfordulhat, hogy egy alsó szinten lévő csúcsra nem kerül semmi sem. Ha tehát minden csúcsra legfeljebb egy elem kerülhet, akkor legalább n csúcsnak kell lennie az alsó szinten. Ugyanakkor tudjuk, hogy ott 2^t csúcs van, vagyis $2^t \geq n$, ami pont azt jelenti, hogy $t \geq \lceil \log n \rceil$, és épp ezt akartuk belátni.

Ezzel beláttuk az állítást, de mint ígértem, mutatok egy másik módszert is, ez pedig a *gonosz manó* módszere. Ez azt jelenti, hogy tetszőleges kérdésre

előre meghatározzuk, hogy a gonosz manó hogyan fog válaszolni, és ez valamilyen értelemben mindig a "rosszabb" lehetőség, vagyis amelyik "kevesebb" információt tartalmaz.

Most ha a második játékos feltesz egy kérdést, azzal az alaphalmazt két részre osztja az alapján, hogy mi lesz a válasz. A további kérdéseknél tekinthetjük úgy, hogy az alaphalmaz lecsökkent azokra a számokra, amelyek minden eddigi kérdésre megfelelnek, és ezt az új alaphalmazt osztja két részre az újabb kérdés. A gonosz manónak pedig legyen az a stratégiája, hogy mindig a nagyobbat választja ezen két halmaz közül. Ha a két halmaz mérete egyforma, akkor mindegy melyiket. Így az első kérdés feltevése előtt még n lehetséges (vagyis az összes) defektív elem van. Egy kérdés feltevése után még mindig van $\lceil \frac{n}{2} \rceil \geq \frac{n}{2}$ lehetséges elem, újabb kérdés feltevése után legalább $\left\lceil \frac{\lceil \frac{n}{2} \rceil}{2} \right\rceil \geq \frac{n}{4}$, és így tovább: t kérdés feltevése után legalább $\frac{n}{2^t}$ lehetséges defektív elem még mindig van. Ha $t < \lceil \log n \rceil$ kérdést tettünk fel, akkor még mindig van legalább $\frac{n}{2^t} \geq \frac{n}{2^{\lceil \log n \rceil - 1}} > 1$ lehetséges defektív elem, vagyis a gonosz manó el tudja érni, hogy ennyi kérdésből még ne tudjuk megtalálni a defektív elemet. Vagyis szükség van legalább $\lceil \log n \rceil$ darab kérdésre.

□

3.2. Nem adaptív eset

3.2.1. Állítás. *Ha nem adaptív módon kérdezünk, akkor is pontosan* $\lceil \log n \rceil$ *kérdésre van szükségünk, hogy megkapjuk a választ.*

Bizonyítás. Általában is igaz, hogy a nem adaptív esetben legalább annyi kérdésre van szükség, mint az adaptív esetben, hiszen a nem adaptív kérdéseit fel lehet tenni adaptív módon, ám ez általában nem optimális. Fordítva viszont általában nem igaz, hogy fel lehet tenni a kérdéseket, de az adaptív esetben pont olyan kérdéseket adtam meg, melyek nem adaptívan is feltehetők, és így $\lceil \log n \rceil$ kérdésből meg lehet találni a defektív elemet.

□

Bár beláttam az állítást az adaptív esetre hivatkozva, ám érdemes egy másik bizonyítást is megnézni. Ez a nem adaptív esetben egy elég gyakori módszer.

3.2.2. Definíció. *Azt mondjuk, hogy az* $\mathscr{A} = \{A_1, A_2, \ldots, A_m\} \subseteq 2^{[n]}$ *egy szeparáló halmazrendszer, ha bármely* $i, j \in [n]$ *két különböző elemhez létezik egy* $A_k \in \mathscr{A}$*, hogy vagy* $i \in A_k$*, de* $j \notin A_k$*, vagy* $i \notin A_k$*, de* $j \in A_k$*.*

Vegyük fel azt az $M \in \{0,1\}^{m \times n}$ mátrixot, melynek i-edik oszlopának k-adik eleme pontosan akkor 1, ha $i \in A_k$, különben 0.

3.2.3. Lemma. *Az $\mathscr{A} = \{A_1, A_2, \ldots, A_m\} \subseteq 2^{[n]}$ halmazrendszer pontosan akkor szeparáló, ha M bármely két oszlopa különböző.*

Bizonyítás. Legyen $i, j \in [n]$ két különböző elem. A szeparálóság miatt létezik egy $k \in [m]$, hogy $i \in A_k$, de $j \notin A_k$, vagy $i \notin A_k$, de $j \in A_k$, ami pont azt jelenti, hogy a k-adik koordinátája eltér a két oszlopnak, így tehát különbözik a két oszlop.

Hasonlóan visszafelé, bármely két oszlop eltér legalább egy koordinátában, ami azt jelenti, hogy az adott kérdésben az egyiket megkérdeztük, a másikat nem.

□

3.2.4. Állítás. *Ha az $\mathscr{A} = \{A_1, A_2, \ldots, A_m\} \subseteq 2^{[n]}$ halmazrendszer szeparáló, akkor $m \geq \lceil \log n \rceil$.*

Bizonyítás. Mint láttuk, M bármely két oszlopának el kell térnie. m hosszú 0-1 sorozatból pontosan 2^m van, így legfeljebb ennyi oszlopa lehet M-nek, de tudjuk, hogy pontosan n van neki, vagyis $2^m \geq n$, tehát $m \geq \lceil \log n \rceil$.

□

4. Mérleg

4.1. Adaptív

4.1.1. Állítás. *Ha adaptív módon kérdezünk, akkor pontosan $\lceil \log_3 n \rceil$ mérésre van szükségünk, hogy megtaláljuk a nehezebb érmét.*

Bizonyítás. Hogy legalább ennyi mérésre szükség van, az könnyen belátható például a gonosz manó módszerével vagy döntési fával. Az eddig látottakhoz képest a döntési fánál annyi módosítást kell végrehajtani, hogy egy szinten nem feltétlenül ugyanazt a kérdést tesszük fel, de így is csak 3 él mehet belőle lefelé, vagyis a t. szinten legfeljebb 3^t csúcs lehet. Vagyis legalább $\lceil \log_3 n \rceil$ szintre van szükség az n érméhez.

Most megmutatom, hogy ennyi kérdésből meg lehet találni. Jelölje $q(k)$ a szükséges kérdések számát k érme esetén. k szerinti indukcióval belátjuk, hogy $q(k) \leq \lceil \log_3 n \rceil$.

$k = 1$-re nem kell egy mérés se, $k = 2$-re és $k = 3$-ra pedig elég 1 mérés. Most tegyük fel, hogy minden $k < n$-re tudjuk, hogy $q(k) \leq \lceil \log_3 n \rceil$.

Az n érmét az első kérdéssel három részre osztjuk fel, ezek mérete legyen: k, k és $n - 2k$. Ekkor $q(n) \leq \max\{q(k), q(n-2k)\} + 1$, hiszen bármelyik részhalmazban is lesz, azt utána legfeljebb ennyi kérdésből meg tudjuk oldani. (Sőt a gonosz manó módszerét alkalmazva az is látható, hogy $q(n) = \min_{1 \leq k \leq n/2} \max\{q(k), q(n-2k)\} + 1$, de nekünk ehhez az irányhoz elég a felsőbecslést megmutatni.)

A feladatunk már csak egy jó k választása. Tegyük fel, hogy $n = 3s + m$, ahol $s \in \mathbb{N}$ és $m \in \{0, 1, 2\}$, illetve $3^l + 1 \leq n \leq 3^{l+1}$.

Ha $m = 0$, akkor $k = s$ esetén $\frac{3^l+1}{3} \leq k \leq 3^l$, és mivel k egész, így $3^{l-1} + 1 \leq k \leq 3^l$, vagyis az indukció miatt $q(k) = q(2n - k) \leq \lceil \log_3 k \rceil$, és így $q(n) \leq \lceil \log_3 n \rceil$.

Ha $m = 1$, akkor $k = s$, így $n - 2k = s + 1$, továbbá $3^l + 1 \leq n = 3s + 1 \leq 3^{l+1} - 2$ a hármas maradék miatt, és így $3^{l-1} \leq s \leq 3^l - 1$, illetve $3^{l-1}+1 \leq s+1 \leq 3^l$, emiatt pedig $q(k) = q(s) \leq l$ és $q(n-2k) = q(s+1) \leq l$, ahol $l = \lceil \log_3 n \rceil - 1$, vagyis $q(n) \leq \lceil \log_3 n \rceil$.

Végül pedig ha $m = 2$, akkor $k = s + 1$, így $n - 2k = s$, továbbá $3^l + 2 \leq n = 3s+2 \leq 3^{l+1}-1$ a hármas maradék miatt, és így $3^{l-1} \leq s \leq 3^l-1$, illetve $3^{l-1}+1 \leq s+1 \leq 3^l$, emiatt pedig $q(k) = q(s+1) \leq l$ és $q(n-2k) = q(s) \leq l$, ahol $l = \lceil \log_3 n \rceil - 1$, vagyis $q(n) \leq \lceil \log_3 n \rceil$.

Ezzel beláttuk az indukciós állítást, vagyis megmutattuk, hogy ennyi mérésből tényleg meg lehet oldani a feladatot.

□

4.2. Nem adaptív

Az egyszerűség kedvéért most csak $n = 3^k$ darab érmével vizsgáljuk a problémát.

4.2.1. Állítás. *Ha nem adaptív módon kérdezünk, akkor pontosan k mérésre van szükségünk, hogy megtaláljuk a nehezebb érmét.*

Bizonyítás. Ekkor a bizonyítás hasonlóan megy, mint a barkochbánál. Először megadunk k darab felhelyezést, melyekkel meg lehet találni a keresett érmét. Minden érme sorszámát írjuk fel 3-as számrendszerben. És "kérdezzünk rá" egyesével az utolsó k darab jegyre, azaz rakjuk fel az i. körben egyik tálcára azokat az érméket, melynek hátulról i. jegye 1, a másikra azokat, melyeknek 2, és ne rakjuk fel azokat, amelyeknek 0. Így mindkét oldalra 3^{k-1} érmét raktunk fel, tehát érvényes a mérésünk. És ha az egyik vagy a másik irányba dől, akkor tudjuk, hogy abban van a nehezebb érme. Ha pedig nem dől semerre, akkor a lent maradtak között. És így megtudhatjuk a defektív érme utolsó k jegyét, amiből egyértelműen ki tudjuk találni, hogy melyikről is van szó.

Hogy ennyi kérdésre szükség van, pedig következik abból, hogy az adaptív esetben is szükség volt ennyi kérdésre.

□

5. Csavarbolt

Eddig olyan példákat láthattunk, ahol az adaptív és a nem adaptív esetben ugyanaz volt a válasz. Most viszont lényegesen el fog térni ez a két szám.

5.1. Adaptív

5.1.1. Állítás. *Ha adaptív módon kérdezünk, akkor pontosan $\lceil \log n \rceil$ kérdésre van szükségünk, hogy megtaláljuk a megfelelő anyacsavart.*

Bizonyítás. Hogy ennyi kérdésre szükség van, az például egy döntési fával könnyen látható. Minden csúcsból két él megy lefelé, vagyis a t. szinten legfeljebb 2^t válaszlehetőség van, vagyis $t \geq \lceil \log n \rceil$ szükséges ahhoz, hogy $2^t \geq n$ legyen.

És most megmutatjuk, hogy ennyi kérdés elég is. Jelölje megint $q(n)$ a szükséges kérdések számát n csavar esetén. n szerinti teljes indukcióval belátjuk, hogy $q(n) \leq \lceil \log n \rceil$

Ha az első mérésünket a k-adik csavarral végezzük, akkor utána biztosak lehetünk benne, hogy a keresett elem vagy az első k vagy az utolsó $n-k$ között van, ezeket pedig meg tudjuk oldani $q(k)$ illetve $q(n-k)$ kérdésből. Vagyis $q(n) \leq \max\{q(k), q(n-k)\} + 1$. Már csak találni kell egy alkalmas k-t. Ez pedig legyen $k = \lfloor \frac{n}{2} \rfloor$.

Ha n páros, akkor $k = n - k = \frac{n}{2}$, így alkalmazható az indukció, tehát $q(k) = q(n-k) \leq \lceil \log \frac{n}{2} \rceil = \lceil \log n \rceil - 1$, tehát $q(n) \leq \lceil \log n \rceil$

Ha n páratlan, akkor $k = \frac{n-1}{2}$ és $n - k = \frac{n+1}{2}$. Tegyük fel, hogy $2^l + 1 \leq n \leq 2^{l+1}$. Mivel páratlan, ezért $2^l + 1 \leq n \leq 2^{l+1} - 1$, és így $2^{l-1} \leq k \leq 2^l - 1$ és $2^{l-1} + 1 \leq n - k \leq 2^l$. Így pedig az indukció miatt $q(k) \leq l = \lceil \log n \rceil - 1$ és $q(n-k) = l = \lceil \log n \rceil - 1$, így pedig $q(n) \leq \lceil \log n \rceil$, tehát beláttuk az indukciós állítást, ezzel pedig a tételt is.

□

5.2. Nem adaptív

5.2.1. Állítás. *Ha nem adaptív módon kérdezünk, akkor pontosan $n-1$ kérdésre van szükségünk, hogy megtaláljuk a megfelelő anyacsavart, vagyis végig kell próbálni az összes lehetőséget.*

Bizonyítás. Az utolsó anyacsavart fölösleges kipróbálni, mivel az biztosan rá fog menni, hiszen feltettük, hogy van olyan csavar, amelyik biztosan jó rá.

Viszont minden más csavart ki kell próbálnunk, különben ha a k-adikat nem próbáljuk ki, akkor egyik kérdés sem választotta el egymástól a k-adik és a $k+1$-edik csavart, így a gonosz manó a válaszaival elérheti, hogy ne tudjuk, hogy e kettő közül melyik a megfelelő csavar.

□

6. Barkochba legfeljebb k méretű kérdésekkel

Először is vegyük észre, hogy egy $A \subseteq [n]$ és egy $[n] \setminus A \subseteq [n]$ megkérdezése ugyanazt az információt biztosítja. Így hogy ha $k \geq \frac{n}{2}$, akkor egy "nagy" A halmaz ($|A| > k$) helyett megkérdezhetjük $[n] \setminus A$ halmazt, hiszen $|[n] \setminus A| = n - |A| < n - k \leq n - \frac{n}{2} = \frac{n}{2} \leq k$.

Így ezt az esetet visszavezettük a korábban már vizsgált problémákra, tehát kimondhatjuk a következő állítást:

6.0.1. Állítás. *Akár adaptív, akár nem adaptív módon kérdezünk úgy, hogy a kérdések mérete legfeljebb k lehet és $k \geq \frac{n}{2}$, akkor pontosan $\lceil \log n \rceil$ kérdésre van szükségünk, hogy megtaláljuk a defektív elemet.*

Így a továbbiakban a $k < \frac{n}{2}$ esetet vizsgáljuk.

6.1. Adaptív

6.1.1. Állítás. *[2]*

Ha adaptív módon kérdezünk úgy, hogy a kérdések mérete legfeljebb k lehet és $k < \frac{n}{2}$, akkor pontosan $v + \lceil \log(n - kv) \rceil$ kérdésre van szükségünk, hogy megtaláljuk a defektív elemet, ahol a $v = \left\lceil \frac{n}{k} \right\rceil - 2$ rövidítést alkalmazzuk.

Bizonyítás. Jelölje $q_k(n)$ a szükséges kérdések számát. Először is vegyük észre, hogy ez n-nek egy monoton növő függvénye. Ugyanis ha $n+1$ elemre meg tudjuk oldani mindig $m = q_k(n+1)$ kérdésekkel, akkor a kérdésekből kihagyva például $n+1 \in [n+1]$ elemet, ez a kérdéssorozat megoldja a problémát az $[n]$ alaphalmazon, hiszen a kérdések megengedettek maradnak, ugyanis méretük nem nő k fölé. Így tehát beláttuk, hogy $q_k(n+1) \geq q_k(n)$.

Most vegyünk egy optimális kérdéssorozatot n elemre. Az első kérdés legyen A_1, és legyen $|A_1| = l \leq k$. A további kérdéseket elmetszve A_1-gyel illetve $[n] \setminus A_1$-gyel kapunk egy-egy (nem feltétlenül optimális) jó kérdéssorozatot A_1-re illetve $[n] \setminus A_1$-re, hiszen a választ megtaláljuk velük, míg a kérdések megengedettek maradnak, hiszen az elmetszéssel nem nőtt a méretük k fölé. Így tehát $q_k(n) \geq 1 + \max\{q_k(l), q_k(n-l)\}$.

Mivel $l \leq k < \frac{n}{2}$, így $l < \frac{n}{2} = n - \frac{n}{2} < n - l$. Tehát a monotonitás miatt $\max\{q_k(l), q_k(n-l)\} = q_k(n-l)$, továbbá $q_k(n-l) \geq q_k(n-k)$ is teljesül, így tehát kapjuk, hogy $q_k(n) \geq 1 + \max\{q_k(l), q_k(n-l)\} = 1 + q_k(n-l) \geq 1 + q_k(n-k)$.

Ezt ismétlejük u-szor, így kapjuk, hogy $q_k(n) \geq u + q_k(n - ku)$. Ha $n - ku \leq 2k$, akkor már tudjuk alkalmazni az általános esetet, vagyis $q_k(n - ku) = \lceil \log(n - ku) \rceil$ lesz. A legkisebb ilyen u, melyre $n - ku \leq 2k$ teljesül, épp $v = \left\lceil \frac{n}{k} \right\rceil - 2$ lesz. Így tehát kaptuk, hogy $q_k(n) \geq v + \lceil \log(n - kv) \rceil$.

Most megmutatjuk, hogy ennyi kérdés elég is. Legyen az első v kérdés (a kapott válaszoktól függetlenül): $A_1 = \{1, 2, \ldots, k\} = [k]$, $A_2 = \{k + 1, k + 2, \ldots, 2k\} = [2k] \setminus [k]$, $\ldots$, $A_v = \{(v - 1)k + 1, (v - 1)k + 2, \ldots, vk\} = [vk] \setminus [(v - 1)k]$. Legyen $B = \{vk + 1, vk + 2, \ldots, n\} = [n] \setminus [vk]$

Ezek után tudjuk, hogy a defektív elem az $A_1, A_2, \ldots A_v, B$ halmazok közül melyikben van. Ha valamelyik A_i-ben, akkor $\lceil \log |A_i| \rceil = \lceil \log k \rceil$ kérdésből meg lehet találni. Ha pedig B-ben van, akkor $\lceil \log |B| \rceil = \lceil \log(n - kv) \rceil$ kérdésből. v definíciója miatt $n - kv > k$, így legrosszabb esetben is $v + \lceil \log(n - kv) \rceil$ kérdésre van szükségünk, és épp ezt akartuk megmutatni.

□

6.2. Nem adaptív

Az eddig tárgyalt problémák közül ez az első, ahol nem tudjuk pontosan a szükséges kérdések számát. Csak egy felső és egy alsó becslést tudunk mondani, melyek viszont elég közel vannak egymáshoz.

6.2.1. Állítás. *Ha nem adaptív módon kérdezünk úgy, hogy a kérdések mérete legfeljebb k lehet és $k < \frac{n}{2}$, akkor legalább $\frac{\log n}{\log(en/k)} \frac{n}{k}$ kérdésre van szükségünk, hogy megtaláljuk a defektív elemet. Ugyanakkor $\left\lceil \frac{\log 2n}{\log(n/k)} \right\rceil \frac{n}{k}$ kérdésből meg lehet találni.*

Ehhez Katona Gyula cikkéből [1] fogom ismertetni a bizonyítást.

6.2.2. Definíció. *Jelölje S a szeparáló halmazrendszerek halmazát.*

$S_k \subseteq S$ legyen azon szeparáló rendszerek halmaza, melyekben minden halmaz mérete pontosan k.

$S'_k \subseteq S$ legyen azon szeparáló rendszerek halmaza, melyekben minden halmaz mérete legfeljebb k.

Mint azt a 3.2. fejezetben már bevezettem, egy $\mathscr{A} = \{A_1, A_2, \ldots, A_M\} \in S$ szeparáló halmazrendszerhez legyen $M \in \{0, 1\}^{m \times n}$ az a mátrix, melynek i-edik oszlopának j-edik eleme pontosan akkor 1, ha $i \in A_j$, különben 0. A 3.2.3. lemmánál láttuk, hogy M bármely két oszlopa különböző.

Most S_k-beli szeparáló rendszerekkel foglalkozunk, később belátjuk, hogy így is ugyanannyi kérdésre van szükségünk, mintha S'_k-beli rendszereket használhatnánk. Így tehát az $|A_i| = k$ feltétel teljesül minden $A_i \in \mathscr{A} \in S_k$ esetén, ami a mátrixok nyelvén azt jelenti, hogy M minden sorában pontosan k darab egyes szerepel.

Így tehát nekünk meg kell határozni azt a legkisebb m egész számot, hogy létezik egy olyan $M \in \{0,1\}^{m\times n}$ mátrix, amelynek nincs két egyforma oszlopa, és minden sora pontosan k darab egyest tartalmaz. Jelölje ezt a legkisebb számot $U = U(n,k)$. Hasonlóan $U'(n,k)$ jelölje, amikor legfeljebb k darab egyest is megengedünk.

6.2.3. Tétel. *Legyen m, n, $1 \le k \le \frac{n}{2}$, s_0, s_1, ..., s_m adott természetes számok. Pontosan akkor létezik egy $M \in \{0,1\}^{m\times n}$ mátrix, amelynek nincs két egyforma oszlopa, minden sora pontosan k darab egyest tartlmaz, és a pontosan i darab egyest tartalmazó oszlopainak száma s_i ha a következő három tulajdonság mindegyike teljesül:*

1. $mk = \sum_{i=0}^{m} i s_i$
2. $n = \sum_{i=0}^{m} s_i$
3. $\forall i \; s_i \le \binom{m}{i}$

Bizonyítás. Ha létezik ilyen M, akkor nyilván teljesülnek a tulajdonságok. Az 1. azért, mert mindkét oldal az M-beli egyesek számát jelöli. A 2.-ban mindkét oldal az M oszlopainak száma. A 3. pedig azért igaz, mert bármely két oszlopnak különbözőnek kell lennie, és i darab egyest tartalmazó oszlopból pontosan $\binom{m}{i}$ van. A másik irányt nehezebb belátni. Ehhez felépítünk egy ilyen mátrixot négy lépésen keresztül. De előtte bevezetünk pár fogalmat.

Jelölés. *Ha $Q_1 \in \{0,1\}^{a\times b_1}$, $Q_2 \in \{0,1\}^{a\times b_2}$,... $Q_q \in \{0,1\}^{a\times b_q}$ olyan mátrixok, melyeknek ugyanannyi soruk van, akkor $[Q_1, Q_2, \ldots, Q_q]$ jelölje azt az $a \times \sum_{j=1}^{q} b_j$ méretű mátrixot, melyet egyszerűen Q_1, Q_2, ... Q_q ilyen sorrendű egymás után írásával kapunk.*

Egy $Q \in \{0,1\}^{a\times b}$ mátrixra és $i \le b$ egész számra jelölje $Q[i]$ azt a mátirxot, mely Q első i sorából áll.

6.2.4. Definíció. *Egy $Q \in \{0,1\}^{a\times b}$ mátrixot megengedettnek nevezünk, ha minden sor ugyanannyi egyest tartalmaz.*

Egy $Q \in \{0,1\}^{a\times b}$ mátrixot majdnem megengedettnek nevezünk, ha az egyesek száma bármely két sor között legfeljebb eggyel tér el.

Egy $Q \in \{0,1\}^{a\times b}$ mátrixot tökéletesnek nevezünk, ha megengedett és minden $i \leq b$ egész számra $Q[i]$ majdnem megengedett.

6.2.5. Megjegyzés. *Néhány triviális megfigyelés, melyeket a későbbiekben használni fogunk:*

Ha két (vagy több) megengedett mátrixot írunk egymás után, az így kapott mátrix is megengedett lesz.

Ha egy $Q_1 \in \{0,1\}^{a\times b_1}$ megengedett és egy $Q_2 \in \{0,1\}^{a\times b_2}$ tökéletes mátrixot rakunk egymás mellé, akkor tetszőleges $b_1 \leq i \leq b_1+b_2$-re $[Q_1,Q_2][i]$ majdnem megengedett.

Ha két tökéletes mátrixot írunk egymás után, akkor az így kapott mátrix is tökéletes lesz.

Ha átrendezzük a sorait egy megengedett/majdnem megengedett/tökéletes mátrixnak, akkor az továbbra is megengedett/majdnem megengedett/tökéletes lesz. Viszont ha az oszlopiat rendezzük át, csak a megengedettség és a majdnem megendettség marad meg, a tökéletesség elromolhat.

6.2.6. Állítás. *Legyen $C \in \{0,1\}^m$ egy oszlopvektor, M_C pedig az a mátrix, melyet úgy kapunk, hogy C összes különböző ciklikus eltoltját leírjuk egymás mellé. Ekkor M_C megengedett.*

Bizonyítás. M_C utolsó sorát rakjuk az első elé, és az így kapott mátrixot nevezzük M'_C-nek. A két mátrix csak az oszlopok sorrendjében tér el, hiszen M'_C-ben is C ciklikus eltoltjai vannak, nyilván mind különböző, és darabra annyian vannak, mint kellenek.

Így tehát az i-edik sorban lévő egyesek száma M_C-ben és M'_C-ben ugyanannyi, tehát M_C i-edik és $(i-1)$-edik sorában ugyannyi egyes van. Ez igaz $i = 2,3,\ldots,m$-ra tehát az összes sorban ugyanannyi egyes van, vagyis M_C megengedett.

□

6.2.7. Állítás. *Ha $D \in \{0,1\}^m$ az az oszlopvektor, melynek első t eleme 1, a többi 0, akkor létezik egy olyan M^* tökéletes mátrix, melynek oszlopait épp D összes ciklikus eltoltja adja.*

Bizonyítás.

Jelölés. *$[m,t]$ jelöli m és t legkisebb közös többszörösét, (m,t) pedig m és t legnagyobb közös osztóját.*

Jelölje $D(j)$ a D j-vel való ciklikus eltolását lefelé. Speciálisan $D(0) = D$. Legyen $M^0 = \left[D(0), D(t), D(2t), \ldots, D\left(\left(\frac{[m,t]}{t} - 1\right) t\right)\right]$.

Ha $t = m$ vagy $t = 0$, az állítás triviális, így feltehető, hogy $0 < t < m$. Ekkor $D(j)$-ben mindig van 0 is és 1 is. Jelölje $r(D(j))$ annak a 0-nak a helyét, amelyik után 1 jön, ha $j \neq 0$, és legyen $r(D(0)) = 0$. Másképpen fogalmazva $r(D(j))$ lesz j-nek az m-es maradéka.

Jelölje $0 \leq r_i < m$ azt a maradékot, amelyre $r_i \equiv r(D(it)) + t \pmod{m}$. Ekkor i-re való indukcióval könnyen látható, hogy $M^0[i]$ első r_i sorában éppen eggyel több egyes van, mint a többiben, vagyis $M^0[i]$ majdnem megengedett.

Most nézzük az $i = \frac{[m,t]}{t} - 1$ esetet. Ekkor $it = \left(\frac{[m,t]}{t} - 1\right) t = \left(\frac{[m,t]}{m} - 1\right) m + (m - t)$, vagyis $r(D(it)) = m - t$, és így $r_i = 0$. Tehát $M^0 = M^0[i]$ megengedett, vagyis M^0 tökéletes.

Ha $(m, t) = 1$, akkor készen vagyunk, hiszen $\frac{[m,t]}{t} = m$ és minden oszlop különbözik, vagyis minden ciklikus eltolt pontosan egyszer szerepel.

Ha $(m, t) = d > 1$, akkor M^0-hoz hasonlóan legyen $i = 1, 2, \ldots d - 1$ esetén $M^i = \left[D(i), D(t + i), D(2t + i), \ldots, D\left(\left(\frac{[m,t]}{t} - 1\right) t + i\right)\right]$.

Mivel M^i megkapható M^0-ból úgy, hogy minden sort i-vel ciklikusan eltolunk, így a 6.2.5-ös megjegyzés alapján M^i is tökéletes, és szintén ezen megjegyzés alapján $M^* = [M^0, M^1, \ldots, M^{d-1}]$ is tökéletes.

M^* minden sora különböző, hiszen az $at + b$ minden mod m maradékosztályt pontosan egyszer vesz fel, ahogy a végigfut a $0, 1 \ldots \frac{[m,t]}{t} - 1$ számokon, b pedig a $0, 1 \ldots (m, t) - 1$ számokon. Így tehát D minden ciklikus eltoltja pontosan egyszer szerepel az oszlopok között.

□

6.2.8. Állítás. *Legyen s_t olyan egész szám, melyre $s_t \leq \binom{m}{t}$. Ekkor létezik egy $N_t \in \{0, 1\}^{m \times s_t}$ majdnem megengedett mátrix, melynek minden oszlopában pontosan t darab egyes van.*

Bizonyítás. Vegyük az összes cikliusan nem egymásba vihető $C \in \{0, 1\}^m$ oszlopvektort, melyekben pontosan t darab egyes szerepel. Ezekhez csináljuk meg a 6.2.6.-os állításban kapott M_C mátrixot, kivéve ahhoz a C-hez, melyben a t darab egyes egymás után helyezkedik el, mert ahhoz a 6.2.7.-es állításban kapott M^* mátrixot vegyük. Legyen ezek mátrixot halamza $\mathfrak{M}$. Mint láttuk, minden $M \in \mathfrak{M}$ megengedett, sőt $M^* \in \mathfrak{M}$ még tökéletes is.

Jelölje $l(M)$ az M oszlopainak számát. Mivel minden t darab egyest tartalmazó oszlop szerepel pontosan az egyik mátrixban, ezért $\sum_{M \in \mathfrak{M}} l(M) =$

$\binom{m}{t}$, továbbá minden $M \in \mathfrak{M}$-re $l(M) \leq m$ és $l(M^*) = m$.

Rendezzük sorba $\mathfrak{M}$ elemeit egyedül arra figyelve, hogy M^* legyen az utolsó: $M_1, M_2, \dots M_q = M^*$, ahol $q = \mathfrak{M}$.

Ha $s_t < \binom{m}{t}$, akkor $\sum_{M \in \mathfrak{M}} l(M) = \binom{m}{t}$ miatt létezik egy i index, hogy $\sum_{j=1}^{i} l(M_j) \leq s_t < \sum_{j=1}^{i+1} l(M_j)$.

Ekkor $s_t - \sum_{j=1}^{i} l(M_j) < l(M_{j+1}) \leq m = l(M^*)$, így az alábbi mátrix értelmes: $N_t = \left[M_1, M_2, \dots, M_i, M^* \left[s_t - \sum_{j=1}^{i} l(M_j)\right]\right]$. Ráadásul épp s_t oszlopa van, sőt a 6.2.5.-ös megjegyzés miatt majdnem megengedett is.

Ha pedig $s_t = \binom{m}{t}$, akkor egyszerűen legyen $N_t = [M_1, M_2, \dots, M_q]$, mely ugyanígy teljesíti a szükséges feltételeket.

□

Ezen állítás által adott mátrixok segítségével most belátjuk a tételt.

Könnyen látható, hogy ha $Q_1 \in \{0,1\}^{a \times b_1}$ és $Q_2 \in \{0,1\}^{a \times b_2}$ két majdnem megengedett mátrix, akkor Q_2 sorait át lehet rendezni úgy egy Q_2' mátrixba, hogy $[Q_1, Q_2']$ is majdnem megengedett.

Legyen N_1' mátrix N_1 sorainak olyan átrendezése, hogy $[N_0, N_1']$ majdnem megengedett. Ezután rekurzívan ha $[N_0, N_1', \dots N_t']$ majdnem megengedett, akkor N_{t+1}' legyen N_{t+1} sorainak olyan átrendezése, hogy $[N_0, N_1', \dots N_t', N_{t+1}']$ is majdnem megengedett. A végén így kapjuk $M = [N_0, N_1', \dots N_m']$ mátrixot, mely teljesíti a tétel feltételeit, ugyanis a konstrukcióból következően minden oszlopa különböző, és a pontosan t darab egyest tartalmazók száma s_t. Már csak azt kell megmutatni, hogy minden sorában k darab egyes van. Tudjuk, hogy az M-beli egyesek száma $\sum_{i=0}^{m} i s_i$, ez az 1. feltétel miatt osztható m-mel. Ez pedig egy majdnem megengedett mátrix esetén azt jelenti, hogy megengedett is, így tehát megint csak az 1. feltétel miatt, minden sorban pontosan k darab egyes szerepel, ezzel beláttuk a tételt.

□

Most nézzük meg, hogy miért elég S_k-t vizsgálni S_k' helyett.

6.2.9. Tétel. *Ha $k < \frac{n}{2}$ és $\mathscr{A}' = \{A_1', A_2', \dots A_m'\} \in S_k'$, akkor létezik egy $\mathscr{A} = \{A_1, A_2, \dots A_m\} \in S_k'$*

Bizonyítás. Legyen $M' \in \{0,1\}^{m \times n}$ az $\mathscr{A}'$ mátrixa, azaz M' i-edik sorának j-edik tagja pontosan akkor 1, ha $j \in A_i'$, különben 0. Jelölje s_t' azon oszlopok számát, melyek pontosan t darab egyest tartalmaznak. Ekkor az előző tételhez hasonlóan könnyen belátható, hogy (a) $mk \geq \sum_{i=0}^{m} i s_i'$, (b) $n = \sum_{i=0}^{m} s_i$, illetve (c) minden $i = 0, 1, \dots m$-re $s_i' \leq \binom{m}{i}$.

Tegyük fel, hogy $m, s_0, s_1, \dots s_m$ olyan természetes számok, melyek kielégítik (a), (b) és (c) feltételeket, ráadásul úgy, hogy $\sum_{i=0}^{m} is_i$ értéke maximális (amennyiben m értéke rögzített).

Ha $mk > \sum_{i=0}^{m} is_i$ és valamely $l \geq$ 1-re $s_l < \binom{m}{l}$ és $s_{l-1} > 0$, akkor $m, s_0, s_1, \dots, s_{l-1} - 1, s_l + 1, \dots, s_m$ is teljesíti (a), (b) és (c) feltételeket, ráadásul $\sum_{i=0}^{l-2} is_i + (l-1)(s_{l-1} - 1) + l(s_l + 1) + \sum_{i=l+1}^{m} is_i > \sum_{i=0}^{m} is_i$, ami ellentmond a maximalitásnak.

Tehát vagy $mk = \sum_{i=0}^{m} is_i$, vagy valamely $j \geq$ 1-re $s_0 = s_1 = \dots = s_{j-1} = 0$ és $s_i = \binom{m}{i}$, ha $i \geq j+1$ és $s_j = \lambda\binom{m}{j}$ alkalmas $0 \leq \lambda \leq$ 1-re. Utóbbi esetben $n = \lambda\binom{m}{j} + \sum_{i=j+1}^{m} \binom{m}{i}$ és $mk \geq j\lambda\binom{m}{j} + \sum_{i=j+1}^{m} i\binom{m}{i}$, amik alapján $k \geq \lambda\frac{j}{m}\binom{m}{j} + \sum_{i=j+1}^{m} \frac{i}{m}\binom{m}{i} = \lambda\binom{m-1}{j-1} + \sum_{i=j}^{m-1} \binom{m-1}{i} \geq \frac{\lambda\binom{m}{j} + \sum_{i=j+1}^{m}\binom{m}{i}}{2} = \frac{n}{2}$, ami ellentmond annak, hogy $k < \frac{n}{2}$.

Tehát $mk = \sum_{i=0}^{m} is_i$ teljesül, és így az $m, s_0, s_1, \dots s_m$ számok kielégítik a 6.2.3. tétel feltételeit, vagyis létezik egy megfelelő $M \in \{0,1\}^{m \times n}$ mátrix, mely meghatároz egy $\{A_1, A_2, \dots A_m\}$ S_k halmazrendszert, és ezzel beláttuk a tételt.

□

6.2.10. Következmény. $U(n,k) = U'(n,k)$.

Bizonyítás. $U(n,k) \leq U'(n,k)$ az előző tétel miatt. $U(n,k) \geq U'(n,k)$ pedig azért, mert $S_k \subseteq S'_k$

□

Hogy a problémát analitikusan tudjuk kezelni, megpróbáljuk elhagyni azt a feltételt, hogy a változók egészek legyenek.

6.2.11. Definíció. *Ha $x \in \mathbb{R}$, és $i \in \mathbb{N}$, akkor* $\binom{x}{i} = \frac{x(x-1)(x-2)\dots(x-i+1)}{i!}$.

6.2.12. Lemma. *Létezik minimuma azon m valós számok halmazának, melyre léteznek $s_0, s_1, \dots, s_{\lceil m \rceil}$ nemnegatív számok, hogy az alábbi három feltétel teljesül*

1. $mk \geq \sum_{i=0}^{\lceil m \rceil} is_i$,
2. $n = \sum_{i=0}^{\lceil m \rceil} s_i$,
3. $\forall i \; s_i \leq \binom{m}{i}$.

Bizonyítás. Ezen m-eknek nyilván létezik infimuma, hiszen például a 0 alsó korlátja a jó m-ek halmazának. Jelölje ezt az infimumot U'. Legyen m^j $(j = 1, 2, \dots)$ egy U'-höz konvegáló sorozat, melynek minden elemére $U' < m^j < \lfloor U' \rfloor + 1$. Legyen az m^j-hez tartozó számok, melyekkel teljesíti az 1., 2., és 3. feltételeket: $s_0^j, s_1^j, \dots, s_{\lfloor U' \rfloor + 1}^j$.

Rögzítetett i-re az s_i^j sorozat korlátos, hiszen $0 \leq s_i^j \leq \binom{m_j}{i} \leq \binom{\lfloor U' \rfloor + 1}{i}$. Így pedig van egy konvergens részsorozata, melynek hatáértéke legyen s_i. Ezt szépen sorban eljátszva minden i-re, kapunk egy részsorozatot, hogy az $(m^j, s_0^j, \dots s_{\lfloor U' \rfloor + 1}^j)$ sorozat konvergál az $(U', s_0, \dots s_{\lfloor U' \rfloor + 1})$ vektorhoz.

Minden j-re teljesülnek az 1., 2. és 3. feltételek, így $(U', s_0, \dots s_{\lfloor U' \rfloor + 1})$ is teljesíti őket. Ha U' nem egész, akkor készen is vagyunk. Ha pedig egész, akkor még meg kell mutatnunk, hogy $s_{\lfloor U' \rfloor + 1} = 0$. Ám ez nyilvávaló abból, hogy $0 \leq s_{\lfloor U' \rfloor + 1}^j \leq \binom{m_j}{\lfloor U' \rfloor + 1}$, hiszen $m_j \to U'$ esetén $\binom{m_j}{\lfloor U' \rfloor + 1} \to 0$.

□

6.2.13. Lemma. $\lceil U' \rceil = U$

Bizonyítás. Legyen $U', s_0, s_1, \dots, s_{\lceil U' \rceil}$ olyan nemnegatív számok, melyek kielégítik az előző lemma feltételeit. Ekkor megmutatjuk, hogy léteznek olyan $\lceil U' \rceil, s_0', s_1', \dots, s_{\lceil U' \rceil}'$ számok, melyek kiellégítik a 6.2.9.-es tétel bizonyításában az (a), (b) és (c) feltételeket.

$\left(\sum_{i=0}^{j+1} \lceil s_i \rceil + \sum_{i=j+2}^{\lceil U' \rceil} \lfloor s_i \rfloor\right) - \left(\sum_{i=0}^{j} \lceil s_i \rceil + \sum_{i=j+1}^{\lceil U' \rceil} \lfloor s_i \rfloor\right) \in \{0, 1\}$ és $\sum_{i=0}^{\lceil U' \rceil} \lfloor s_i \rfloor \leq n \leq \sum_{i=0}^{\lceil U' \rceil} \lceil s_i \rceil$, így létezik egy olyan r, melyre $\sum_{i=0}^{r} \lceil s_i \rceil + \sum_{i=r+1}^{\lceil U' \rceil} \lfloor s_i \rfloor = n$. Ekkor legyen $s_i' = \lceil s_i \rceil$, ha $0 \leq i \leq r$ és $s_i' = \lfloor s_i \rfloor$, ha $r + 1 \leq i \leq \lceil U' \rceil$. Ennek köszönhetően a (b) feltétel automatikusan teljesül.

Felhasználva, hogy $\sum_{i=0}^{r} \lceil s_i \rceil + \sum_{i=r+1}^{\lceil U' \rceil} \lfloor s_i \rfloor = n = \sum_{i=0}^{\lceil U' \rceil} s_i$, kapjuk, hogy $\sum_{i=0}^{\lceil U' \rceil} i s_i = \sum_{i=0}^{r} i \lceil s_i \rceil + \sum_{i=r+1}^{\lceil U' \rceil} i \lfloor s_i \rfloor + \sum_{i=0}^{r} i(s_i - \lceil s_i \rceil) + \sum_{i=r+1}^{\lceil U' \rceil} i(s_i - \lfloor s_i \rfloor) \geq \sum_{i=0}^{r} i \lceil s_i \rceil + \sum_{i=r+1}^{\lceil U' \rceil} i \lfloor s_i \rfloor + r \sum_{i=0}^{r} (s_i - \lceil s_i \rceil) + r \sum_{i=r+1}^{\lceil U' \rceil} (s_i - \lfloor s_i \rfloor) = \sum_{i=0}^{r} i \lceil s_i \rceil + \sum_{i=r+1}^{\lceil U' \rceil} i \lfloor s_i \rfloor + r \left(\sum_{i=0}^{\lceil U' \rceil} s_i - \sum_{i=0}^{r} \lceil s_i \rceil - \sum_{i=r+1}^{\lceil U' \rceil} \lfloor s_i \rfloor \right) = \sum_{i=0}^{r} i \lceil s_i \rceil + \sum_{i=r+1}^{\lceil U' \rceil} i \lfloor s_i \rfloor = \sum_{i=0}^{\lceil U' \rceil} i s_i'$

Ennek és az 1. feltétel segítségével $\lceil U' \rceil k \geq U' k \geq \sum_{i=0}^{\lceil U' \rceil} i s_i \geq \sum_{i=0}^{\lceil U' \rceil} i s_i'$, vagyis teljesül az (a) feltétel is.

Végül (c) a 3. feltételből kapható: $s_i' \leq \lceil s_i' \rceil \leq \left\lceil \binom{U'}{i} \right\rceil \leq \binom{\lceil U' \rceil}{i}$.

Ezzel beláttuk, hogy $\lceil U' \rceil \geq U$. A másik irány pedig triviális, hiszen az (a), (b), (c) feltételek az 1., 2., 3.-nak speciális esetei, vagyis $U' \leq U$ is teljesül, így pedig $\lceil U' \rceil = U$.

□

6.2.14. Lemma. *Ha $U', s_0, s_1, \ldots, s_{\lceil U' \rceil}$ olyan nemnegatív valós számok, melyek a* 6.2.12. *lemma feltételeit kielégítik, és U' minimális, akkor az 1. feltétel egyenlőséggel teljesül.*

Bizonyítás. Megmutatjuk, hogy ha az $m, s_0, s_1, \ldots, s_{\lceil m \rceil}$ számok olyanok, hogy az 1., 2. és 3. feltételt teljesítik, de az 1.-ben nem áll fenn egyenlőség, akkor m értéke csökkenthető, vagyis $m \neq U'$.

Legyen $\varepsilon_1 = mk - \sum_{i=0}^{\lceil m \rceil} i s_i > 0$.

Ha minden r-re $s_r \geq \binom{m}{r}$ lenne, akkor $k > \sum_{i=0}^{\lceil m \rceil} \frac{i}{m}\binom{m}{i} = \sum_{i=0}^{\lceil m \rceil - 1} \binom{m-1}{i} \geq \frac{\sum_{i=0}^{\lceil m \rceil}\binom{m}{i}}{2} \geq \frac{n}{2}$, ami ellentmond annak, hogy $k \leq \frac{n}{2}$. Tehát létezik egy r, melyre $s_r < \binom{m}{r}$. Legyen $\varepsilon_2 = \binom{m}{r} - s_r$.

Legyen $\delta_r = \min\{\frac{\varepsilon_2}{2}, \frac{\varepsilon_1}{2r}, \sum_{i=0}^{r-1} s_i + \sum_{i=r+1}^{\lceil m \rceil} s_i\}$.

$i \neq r$ esetén pedig legyen $0 < \delta_i \leq s_i$, ha $s_i \neq 0$, különben $\delta_i = 0$, továbbá $\delta_r = \sum_{i=0}^{r-1} \delta_i + \sum_{i=r+1}^{\lceil m \rceil} \delta_i$ is teljesüljön. (Ez megtehető δ_r definícója miatt.)

Az új számaink $m - \delta^*, s_0 - \delta_0, s_1 - \delta_1, \ldots, s_{r-1} - \delta_{r-1}, s_r + \delta_r, s_{r+1} + \delta_{r+1}, \ldots s_{\lceil m \rceil} - \delta_{\lceil m \rceil}$ lesznek. Ezekre látható, hogy a 2. feltétel máris teljesül. Most nézzük, hogyan kaphatjuk δ^*-ot.

$i \neq r$, $s_i \neq 0$ esetén legyen $\varrho_i > 0$ olyan, hogy $s_i - \delta_i \leq \binom{m-\varrho_i}{i}$. Folytonosság miatt van ilyen pozitív ϱ_i, hiszen $s_i - \delta_i < \binom{m}{i}$. Ha $s_i = 0$, akkor $\varrho_i = 0$. Végül, ha $i = r$, akkor legyen $\varrho_r > 0$ olyan, hogy $s_r + \delta_r \leq \binom{m-\varrho_r}{r}$. Ilyen is a folytonosság miatt létezik, hiszen $\delta_r \leq \frac{\binom{m}{r} - s_r}{2}$ teljesül δ_r definíciója miatt.

Legyen $\delta^* = \min\{\frac{\varepsilon_1}{2k}, \min\{\varrho_i \mid \varrho_i > 0\}\}$. Ezzel a választással látható, hogy a 3. feltétel is teljesül.

Végezetül, az 1. feltétel azért teljesül, mert $(m - \delta^*)k \geq (m - \frac{\varepsilon_1}{2k})k = mk - \frac{\varepsilon_1}{2} = \sum_{i=0}^{\lceil m \rceil} i s_i + \frac{\varepsilon_1}{2} \geq \sum_{i=0}^{r-1} i s_i + \sum_{i=r+1}^{\lceil m \rceil} i s_i + r(s_r + \delta_r) - r\frac{\varepsilon_1}{2r} + \frac{\varepsilon_1}{2} \geq \sum_{i=0}^{r-1} i(s_i - \delta_i) + r(s_r + \delta_r) + \sum_{i=r+1}^{\lceil m \rceil} i(s_i - \delta_i)$.

□

6.2.15. Lemma. *Ha $U', s_0, s_1, \ldots, s_{\lceil U' \rceil}$ olyan nemnegatív valós számok, melyek a* 6.2.12. *lemma feltételeit kielégítik, és U' minimális, akkor valamely r-re $0 \leq i \leq r-1$ esetén $s_i = \binom{U'}{i}$, és $r+1 \leq i \leq \lceil U' \rceil$ esetén $s_i = 0$.*

Bizonyítás. Megmutatjuk, hogy ha az $m, s_0, s_1, \ldots, s_{\lceil m \rceil}$ számok olyanok, hogy az 1., 2. és 3. feltételt teljesítik, de s_i-k mégsem a lemmában szereplő

értékek, akkor léteznek olyan $m, s'_0, s'_1, \ldots, s'_{\lceil m \rceil}$ számok, melyek szintén teljesítik az 1., 2. és 3. feltételt, de az 1.-ben nem áll fenn egyenlőség, és így az előző lemma miatt m nem minimális.

Feltevésünk miatt létezik egy j, hogy $s_j < \binom{m}{j}$ és $s_{j+1} > 0$. Legyen $\varepsilon = \min\left\{\binom{m}{j} - s_j, s_{j+1}\right\}$, továbbá $s'_j = s_j + \varepsilon$, $s'_{j+1} = s_{j+1} - \varepsilon$, és $i \neq j, j+1$ esetén $s'_i = s_i$.

Ekkor a 2. és a 3. feltétel nyilván teljesül, az 1. pedig így néz ki: $mk \geq \sum_{i=0}^{\lceil m \rceil} i s_i = \sum_{i=0}^{j-1} i s_i + j(s_j + \varepsilon) + (j+1)(s_{j+1} - \varepsilon) + \sum_{i=j+2}^{\lceil m \rceil} i s_i + \varepsilon > \sum_{i=0}^{\lceil m \rceil} i s'_i$, azaz szigorú egyenlőtlenséggel teljesül, és épp ezt akartuk megmutatni.

□

A 6.2.12., 6.2.14. és 6.2.15. lemmák alapján valamilyen $r > 0$-ra teljesül, hogy $U'k = \sum_{i=0}^{r-1} i\binom{U'}{i} + r s_r$, $n = \sum_{i=0}^{r-1} \binom{U'}{i} + s_r$ és $0 \leq s_r < \binom{U'}{r}$. Ebből s_r-et is el tudjuk tüntetni, így az alábbi két feltételt kaptuk:

1. $U'k = \sum_{i=0}^{r-1} i\binom{U'}{i} + r\left(n - \sum_{i=0}^{r-1} \binom{U'}{i}\right)$

2. $\sum_{i=0}^{r-1} \binom{U'}{i} \leq n < \sum_{i=0}^{r} \binom{U'}{i}$

1.-re tekinthetünk úgy, mint U'-re egy egyenlet. 2. pedig kizár néhány gyököt.

Legyen $f_r(x) = \sum_{i=0}^{r-1} i\binom{x}{i} + r\left(n - \sum_{i=0}^{r-1} \binom{x}{i}\right)$.

6.2.16. Lemma. *Rögzített r esetén az 1.-beli egyenletnek (U'-re) pontosan egy nemnegatív gyöke van. Továbbá pontosan egy darab r van, melyre az előbbi gyök 2.-t is teljesíti.*

Bizonyítás. Pozitív x-ekre xk monoton nő, $f_r(x)$ monoton csökken, és $x = 0$ esetén $0k \leq f_r(0)$, vagyis pontosan egy nemnegatív gyök lehet.

A 6.2.12. lemma miatt tudjuk, hogy van egy minimális U', ez teljesíti 1.-et és 2.-t is, így van legalább egy jó r. Tegyük fel, hogy a q-ra kapott x_0 nemnegatív gyök is teljesíti 2.-t. Megmutatjuk, hogy $q < r$ esetén ez nem lehet.

$xk = \sum_{i=0}^{q-1} i\binom{x}{i} + q\left(n - \sum_{i=0}^{q-1} \binom{x}{i}\right) = \sum_{i=0}^{r-1} i\binom{x}{i} + r\left(n - \sum_{i=0}^{r-1} \binom{x}{i}\right) - \left((r-q)n - (r-q)\sum_{i=0}^{q-1} \binom{x}{i} - \sum_{i=q}^{r-1}(r-i)\binom{x}{i}\right)$

U'-re 1.-ben egyenlőség áll. A bal oldala a fenti egyenletnek ugyanaz, a jobbról pedig megmutatjuk, hogy nem nagyobb nála, emiatt a fenti egyenlet x_0 megoldására $x_0 \leq U'$.

$(r-q)n-(r-q)\sum_{i=0}^{q-1}\binom{U'}{i}-\sum_{i=q}^{r-1}(r-i)\binom{U'}{i} \geq (r-q)\left(n-\sum_{i=0}^{r-1}\binom{U'}{i}\right) \geq 0$ teljesül 2. miatt. Így tehát $x_0 \leq U'$.

Ugyanakkor $I_t = \{x \in \mathbb{R}^+ \mid \sum_{i=0}^{t-1}\binom{x}{i} \leq n < \sum_{i=0}^{t}\binom{x}{i}\}$ intervallumokra igaz, hogy $t_1 > t_2$ esetén minden $x_1 \in I_{t_1}$-re és $x_2 \in I_{t_2}$-re $x_1 < x_2$. Ez pedig $t_1 = r$, $t_2 = q$, $x_1 = U'$, $x_2 = x_0$-ra alkalmazva épp azt adja, hogy $x_0 > U'$, vagyis ellentmondást kaptunk.

□

Ezek után már nyilvánvaló a következő tétel.

6.2.17. Tétel. *Ha U a legkisebb egész szám, melyre létezik $\{A_1, A_2, \ldots, A_U\} \in S_k$, és U' gyöke az $xk = \sum_{i=0}^{r-1} i\binom{x}{i} + r\left(n - \sum_{i=0}^{r-1}\binom{x}{i}\right)$ egyenletnek valamilyen r-re, továbbá $\sum_{i=0}^{r-1}\binom{U'}{i} \leq n < \sum_{i=0}^{r}\binom{U'}{i}$, akkor $U = \lceil U' \rceil$.*

6.2.18. Következmény. *Ha $k \geq 1$ és $n > \frac{k(k+1)}{2} + 1$, akkor $U = \left\lceil 2\frac{n-1}{k+1} \right\rceil$.*

Bizonyítás. Ez az előző tétel abban az esetben, ha $r = 2$. Ugyanis ekkor az egyenlet $xk = x + 2(n-1-x)$ lesz, és így $U' = 2\frac{n-1}{k+1}$.

$1 + U' \leq n < 1 + U' + \frac{U'(U'-1)}{2}$-et kell már csak ellenőriznünk. $k \geq 1$ miatt $1 + 2\frac{n-1}{k+1} \leq 1 + 2\frac{n-1}{2} = n$, vagyis a bal oldali teljesül. A jobb oldalihoz pedig az kell, hogy $n < 1 + 2\frac{n-1}{k+1} + \frac{2\frac{n-1}{k+1}(2\frac{n-1}{k+1}-1)}{2} \Leftrightarrow n - 1 < 2\frac{n-1}{k+1} + \frac{(n-1)(2(n-1)-(k+1))}{(k+1)^2} \Leftrightarrow 1 < \frac{2}{k+1} + \frac{2(n-1)-(k+1)}{(k+1)^2} \Leftrightarrow (k+1)^2 < 2(k+1) + 2(n-1) - (k+1) \Leftrightarrow (k+1)k < 2(n-1) \Leftrightarrow \frac{(k+1)k}{2} + 1 < n$. Ezt pedig feltettük, hogy igaz, így készen vagyunk.

□

6.2.19. Tétel. *Ha $\{A_1, A_2, \ldots, A_m\} \in S_k$, akkor $\frac{\log n}{\frac{k}{n}\log\frac{n}{k} + \frac{n-k}{n}\log\frac{n}{n-k}} \leq m$.*

Bizonyítás. Vegyük $[n]$-en az egyenletes eloszlást. Jelölje α_i az A_i indikátor függvényét. Önmagában ez egy olyan valószínűségi változó, mely $\frac{k}{n}$ valószínűséggel veszi fel az 1-et, és $\frac{n-k}{n}$ valószínűséggel a 0-t. Így tehát az entrópiája $H(\alpha_i) = \frac{k}{n}\log\frac{n}{k} + \frac{n-k}{n}\log\frac{n}{n-k}$.

Most nézzük az $(\alpha_1, \alpha_2, \ldots, \alpha_m)$ együttes eloszlását. Összesen 2^m értéket vehetne ez fel, ugyanakkor ezek között legfeljebb n-nek van pozitív valószínűsége, hiszen ennyi elemi esemény van (hiszen $[n]$-en vettük az egyenletes eloszlást).

Ha $i, j \in [n]$ esetén ugyanaz lenne ennek a két vektornak az értéke, akkor minden A_k halmazra $i \in A_k \Leftrightarrow j \in A_k$. Ám a halmazrendszer szeparáló, így szükségképpen $i = j$.

Tehát az $(\alpha_1, \alpha_2, \ldots, \alpha_m)$ vektor minden felvett értékét pontosan egy elemi esemény esetén veszi fel, vagyis pontosan n különböző értéket vesz fel, mindet $\frac{1}{n}$ valószínűséggel, így $H((\alpha_1, \alpha_2, \ldots, \alpha_m)) = \log n$.

Ismert, hogy $H(\alpha_1) + H(\alpha_2) + \cdots + H(\alpha_m) \geq H((\alpha_1, \alpha_2, \ldots, \alpha_m))$.[3] Ebbe behelyettesítve a kiszámolt értékeket, kapjuk a tétel állítását.

□

6.2.20. Következmény. $\frac{n \log n}{k \log \frac{en}{k}} \leq m$

Bizonyítás. Ismert, hogy $\ln(1+x) \leq x$, ahol ln az e alapú logaritmust jelöli. Ezt átírva 2-es alapúra: $\log(1+x) \leq x \log e$. Ezt alkalmazzuk $x = \frac{k}{n-k}$-ra: $\log(1 + \frac{k}{n-k}) \leq \frac{k}{n-k} \log e \Leftrightarrow \log \frac{n}{n-k} \leq \frac{k}{n-k} \log e \Leftrightarrow \frac{n-k}{n} \log \frac{n}{n-k} \leq \frac{k}{n} \log e \Leftrightarrow \frac{k}{n} \log \frac{n}{k} + \frac{n-k}{n} \log \frac{n}{n-k} \leq \frac{k}{n} \log \frac{n}{k} + \frac{k}{n} \log e \Leftrightarrow \frac{k}{n} \log \frac{n}{k} + \frac{n-k}{n} \log \frac{n}{n-k} \leq \frac{k}{n} \log \frac{en}{k}$. Ezt felhasználva: $\frac{n \log n}{k \log \frac{en}{k}} \leq \frac{\log n}{\frac{k}{n} \log \frac{n}{k} + \frac{n-k}{n} \log \frac{n}{n-k}} \leq m$.

□

És ezzel be is láttuk a fejezet elején ígért alsó becslést. Most jöjjön a felső becslés.

6.2.21. Lemma. *Legyen i pozitív egész és $x \geq 2i$. Ekkor $\frac{1}{2} \left(\frac{x}{i}\right)^i \leq \binom{x-1}{i}$.*

Bizonyítás. Ha $i \geq j \geq 2$, akkor nyilván $j \leq 2(j-1)$. Így tehát $ij \leq 2i(j-1) \leq x(j-1)$. Emiatt $ix - ij \geq ix - x(j-1)$, és így $\frac{x-j}{i-j+1} \geq \frac{x}{i}$.

Ha $j = 1$, akkor $\frac{x-1}{i} \geq \frac{x}{2i}$ triviálisan teljesül $x \geq 2i \geq 2$ miatt.

Így tehát $\frac{1}{2} \left(\frac{x}{i}\right)^i \leq \frac{x-1}{i} \frac{x-2}{i-1} \ldots \frac{x-i}{1} = \binom{x-1}{i}$.

□

6.2.22. Tétel. *Tetszőleges $n \geq 1$ és $1 \leq k \leq \frac{n}{2}$ esetén létezik egy olyan $\{A_1, A_2, \ldots A_m\} \in S_k$ szerparáló rendszer, melyre $m = \left\lfloor \left\lceil \frac{\log 2n}{\log(n/k)} \right\rceil \frac{n}{k} \right\rfloor$.*

Bizonyítás. A 6.2.3.-as tételt fogjuk alkalmazni. Mutatunk alkalmas $m, s_0, s_1, \ldots, s_m$ számokat, melyek kielégítik az 1., a 2. és a 3. feltételt.

Legyen i egyelőre nem rögzített pozitív egész, és $0 \leq r < k$ olyan, hogy $in \equiv r \pmod{k}$. Legyen $s_{i-1} = r$, $s_i = n - r$ és $j \neq i, i+1$ esetén $s_j = 0$, illetve $m = \frac{in-r}{k}$.

Ekkor az 1. és 2. feltétel nyilván teljesül, hiszen $\sum_{j=0}^{m} j s_j = (i-1)r + i(n-r) = in - r = mk$ és $\sum_{j=0}^{m} s_j = r + (n-r) = n$.

Legyen $i = \left\lceil \frac{\log 2n}{\log(n/k)} \right\rceil$. $i \geq \frac{\log 2n}{\log(n/k)}$ miatt $n \leq \frac{1}{2}\frac{1}{i^i}\left(\frac{in}{k}\right)^i$ és $k = \frac{k}{n}n \leq \frac{1}{2}\frac{1}{(i-1)^{i-1}}\left(\frac{(i-1)n}{k}\right)^{i-1} \leq \frac{1}{2}\frac{1}{(i-1)^{i-1}}\left(\frac{in}{k}\right)^{i-1}$.

A 6.2.21. lemma segítségével: $n \leq \frac{1}{2}\frac{1}{i^i}\left(\frac{in}{k}\right)^i \leq \binom{\frac{in}{k}-1}{i}$ és $r < k \leq \frac{1}{2}\frac{1}{(i-1)^{i-1}}\left(\frac{in}{k}\right)^{i-1} \leq \binom{\frac{in}{k}-1}{i-1}$.

Végezetül: $n - r \leq n \leq \binom{\frac{in}{k}-1}{i} \leq \binom{\frac{in-r}{k}}{i}$ és $r \leq \binom{\frac{in}{k}-1}{i-1} \leq \binom{\frac{in-r}{k}}{i-1}$, tehát a 3. feltétel is teljesül, így készen vagyunk.

Így tehát $m = \left\lfloor \left\lceil \frac{\log 2n}{\log(n/k)} \right\rceil \frac{n}{k} \right\rfloor$, és épp ezt akartuk belátni.

□

Ezzel beláttuk az ígért felső becslést is.

Végezetül megmutatom, hogy a két becslés megadja a keresett válasz nagyságrendjét, ugyanis arányuk korlátos:

$\frac{\left\lceil \frac{\log 2n}{\log(n/k)} \right\rceil \frac{n}{k}}{\frac{n \log n}{k \log(en/k)}} \leq \frac{\frac{1+\log n}{\log(n/k)}+1}{\frac{\log n}{\log e + \log(n/k)}} \leq \frac{2\frac{2\log n}{\log(n/k)}}{\frac{\log n}{(\log e+1)\log(n/k)}} = 4(1+\log e)$.

Közben felhasználtuk, hogy $\log(n/k) \geq 1$, de ez teljesül, hiszen $k \leq \frac{n}{2}$.

7. Vérvizsgálat hadseregen, avagy barkochba d defektívvel

Ezt a problémát nagyon sokan nagyon sokféleképpen megközelítették már.[4] Ennek ellenére nem ismert pontos válasz már $d = 2$ esetén sem. Rengeteg részeredmény van, én csak néhányat mutatok be.

7.1. Alsó becslés

7.1.1. Állítás. *Ha adaptívan kérdezünk, legalább* $\left\lceil \log \binom{n}{d} \right\rceil$ *kérdésre szükség van, hogy biztosan megtaláljuk a defektív elemet.*

Bizonyítás. Egy döntési fa t. szintjén legfeljebb 2^t csúcs van. Nekünk pedig van $\binom{n}{d}$-féle válaszunk, így tehát $\left\lceil \log \binom{n}{d} \right\rceil \geq t$ szükséges, hogy $2^t \geq \binom{n}{d}$ teljesüljön.

□

7.2. Felső becslés

7.2.1. Állítás. *Ha adaptívan kérdezünk,* $d \lceil \log n \rceil$ *kérdésből meg tudjuk találni az összes defektív elemet.*

Bizonyítás. A szokásos felezgetős módon keresünk először egy elemet. Először "elfelezzük" az alaphalmazt (úgy hogy egyik részhalmaz mérete se legyen nagyobb, mint $2^{\lceil \log n \rceil - 1}$), és megkérdezzük az egyiket. Ha igen a válasz, akkor abban a részhalmazban biztosan van defektív, így azt tekintjük a következő körben alaphalmaznak. Ha nem a válasz, akkor a másik részhalmazban van biztosan, így az lesz az alaphalmaz. Ezt folytatva $\lceil \log n \rceil$ lépésen belül találunk egy defektívet. A maradék $n - 1$ elemben még mindig van $d - 1$ defektív. Hasonló módon $\lceil \log(n-1) \rceil$ lépésben találunk egy második defektívet, $\lceil \log(n-2) \rceil$ lépésben egy harmadikat, és így tovább, a d defektívet megtaláljuk $\sum_{i=0}^{d-1} \lceil \log(n-i) \rceil \leq d \lceil \log n \rceil$ lépésben.

□

Ez a módszer az alsó becslésnél nagyságrendileg $\log(d!)$-sal több kérdést használ.

Most pedig bemutatom Hwang algoritmusát[5], amely az elméleti minimumnál legfeljebb $d - 1$-gyel több kérdésből áll.

Az ötlet az algoritmus mögött az, hogy várhatóan n/d elem között van egy defektív. Tehát nem egy feleakkora halmazt kérdezünk meg elsőre, hanem egy kisebb méretűt.

1. lépés:

Ha $n \leq 2d-2$, akkor teszteljük le mind az n elemet egyesével, és így vége is az algoritmusunknak.

Ha $n \geq 2d-1$, akkor legyen $l := n-d+1$ és $\alpha := \lfloor \log(l/d) \rfloor$.

2. lépés:

Kérdezzünk meg egy 2^α méretű halmazt.

Ha nincs benne defektív elem, akkor ezek mind jók, így a továbbiakban nem kell őket vizsgálni, tehát legyen $n := n-2^\alpha$, és ugorjunk az 1. lépéshez.

Ha van benne defektív elem, akkor a szokásos felezgetős kereséssel találjunk egy defektívet. Közben lehet, hogy néhány elemeről kiderül, hogy biztosan nem defektív, ezek száma legyen x. Őket tehát nem kell tovább vizsgálni, így tehát $n := n-1-x$, $d := d-1$, és ugorjunk az 1. lépéshez.

7.2.2. Definíció. *Jelölje $M(d,n)$ ezen algoritmus kérdéseinek számát a legrosszabb esetben.*

7.2.3. Tétel. *Legyen $l = n-d+1$, $\alpha = \lfloor \log(l/d) \rfloor$, $p = \left\lfloor \frac{l}{2^\alpha} \right\rfloor - d$ és $\theta = l - 2^\alpha d - 2^\alpha p$. Ekkor*

$$M(d,n) = \begin{cases} n & \text{ha } n \leq 2d-2 \\ (\alpha+2)d+p-1 & \text{ha } n \geq 2d-1 \end{cases}$$

Bizonyítás. Az állítást $n+d$ szerinti indukcióval bizonyítjuk.

Ha $n \leq 2d-2$, akkor az algoritmus 1. lépése miatt készen is vagyunk.

Ha $2d-1 \leq n \leq 3d-2$, akkor $\alpha = 0$, tehát az algoritmus megint egyesével vizsgálja végig az elemeket, vagyis $M(d,n) = n$. Továbbá $\theta = 0$, $p = l-d = n-2d+1$, így $(\alpha+2)d+p-1 = 2d+n-2d+1-1 = n = M(d,n)$.

Ha $d = 1$, akkor $l = n-d+1 = n$. Látható, hogy ha $n \neq 2^\alpha$ alakú, akkor az algoritmus a szokásos felezgetős kérdéseket teszi fel, tehát $M(1,n) = \lceil \log n \rceil$. És így $(\alpha+2)d+p-1 = \alpha+1 = \lfloor \log n \rfloor + 1 = \lceil \log n \rceil = M(1,n)$.

Ha viszont $n = 2^\alpha$, az algoritmus eggyel több kérdést tesz fel, ugyanis először megkérdezi a teljes alaphalmazt, vagyis $M(1,n) = \log n + 1$. És így $(\alpha+2)d+p-1 = \alpha+1 = \log n + 1 = M(1,n)$.

Most nézzük az általános esetet, amikor $d \geq 2$, $n \geq 3d-1$. Ekkor az algoritmus 2. lépése miatt két lehetőség van, így $M(d,n) = 1+\max\{M(d,n-$

$2^\alpha), \alpha + M(d-1, n-1)\}$, ugyanis a monotonitás miatt $M(d-1, n-1-x) \leq M(d-1, n-1)$. (Sőt, a gonosz manó miatt feltehető, hogy $x = 0$.)

Az első esetben $n' = n - 2^\alpha$, $d' = d$, $l' = n' - d' + 1 = n - 2^\alpha - d + 1 = l - 2^\alpha = \begin{cases} 2^\alpha d + 2^\alpha(p-1) + \theta & \text{ha } p \geq 1 \\ 2^{\alpha-1}d + 2^{\alpha-1}(d-2) + \theta & \text{ha } p = 0,\ \theta < 2^{\alpha-1} \\ 2^{\alpha-1}d + 2^{\alpha-1}(d-1) + (\theta - 2^{\alpha-1}) & \text{ha } p = 0,\ \theta \geq 2^{\alpha-1} \end{cases}$

Így tehát az indukció miatt:

$$M(d, n-2^\alpha) = \begin{cases} (\alpha+2)d + (p-1) - 1 & \text{ha } p \geq 1 \\ (\alpha+1)d + (d-2) - 1 & \text{ha } p = 0,\ \theta < 2^{\alpha-1} \\ (\alpha+1)d + (d-1) - 1 & \text{ha } p = 0,\ \theta \geq 2^{\alpha-1} \end{cases}$$

Így tehát $M(d, n-2^\alpha) = \begin{cases} (\alpha+2)d + p - 3 & \text{ha } p = 0,\ \theta < 2^{\alpha-1} \\ (\alpha+2)d + p - 2 & \text{egyébként} \end{cases}$

A másik esetben $d' = d-1$, $n' = n-1$, $l' = n' - d' + 1 = l = \begin{cases} 2^\alpha(d-1) + 2^\alpha(p+1) + \theta & \text{ha } p \leq d-3 \\ 2^{\alpha+1}(d-1) + \theta & \text{ha } p = d-2 \\ 2^{\alpha+1}(d-1) + 2^\alpha + \theta & \text{ha } p = d-1 \end{cases}$

Alkalmazva az indukciót:

$$M(d-1, n-1) = \begin{cases} (\alpha+2)(d-1) + (p+1) - 1 & \text{ha } p \leq d-3 \\ (\alpha+3)(d-1) - 1 & \text{ha } d-2 \leq p \leq d-1 \end{cases}$$

És így $\alpha + M(d-1, n-1) = \begin{cases} (\alpha+2)d + p - 3 & \text{ha } p = d-1 \\ (\alpha+2)d + p - 2 & \text{egyébként} \end{cases}$

A két kisebb értéket csak akkor venné fel egyszerre a két eset, ha $p = 0$ és $p = d-1$ egyszerre teljesülne, de ez $d \geq 2$ esetén nem lehet, így szükségképpen $M(d, n) = 1 + \max\{M(d, n-2^\alpha), \alpha + M(d-1, n-1)\} = 1 + (\alpha+2)d + p - 2 = (\alpha+2)d + p - 1$, ezzel beláttuk az állítást.

□

7.2.4. Következmény. *$M(d, n) - \left\lceil \log \binom{n}{d} \right\rceil \leq d-1$, ha $d \geq 2$ és $n \geq 2d-1$.*

Bizonyítás. $\binom{n}{d} = \binom{l+d-1}{d} > \frac{l^d}{d!} = \frac{(2^\alpha d + 2^\alpha p + \theta)^d}{d!} \geq \frac{(2^\alpha d(1+p/d))^d}{d!} = 2^{d\alpha}\frac{d^d}{d!}(1+p/d)^d \geq 2^{d\alpha}2^d 2^p = 2^{(\alpha+1)d+p}$, ahol felhasználtuk, hogy $\frac{d^d}{d!} \geq 2^d$ és $(1+p/d)^d \geq 2^p$.

Így tehát $M(d, n) - \left\lceil \log \binom{n}{d} \right\rceil \leq (\alpha+2)d + p - 1 - ((\alpha+1)d + p) = d-1$.

□

8. Számítógépek

A probléma megfogalmazásából adódóan ezt csak nem adaptív módon fogjuk vizsgálni. Az adaptív esetben ugyanis felmerülne, hogy ki teszi fel a kérdéseket? Ha egy külső szemlélő (aki látja az összes választ), akkor ő például $\lceil \log n \rceil + 2$ kérdésből tudatni tudja az összes géppel, hogy melyik a hibásan működő: először elvégeztet $\lceil \log n \rceil$ tesztet (egy szeparáló rendszert), így ő már tudja ki a defektív, majd elvégeztet az összes jó géppel egy tesztet, végül az egyetlen rossz géppel. Hasonlóan, ha az egyik (előre meghatározott) gép jelölné ki a kérdéseket, ő is el tudna végeztetni egy szeparáló rendszert úgy, hogy ő az összes kérdésben szerepel (például 2-es számrendszerben kérdezgeti a jegyeket úgy, hogy az i-edik kérdésben azokat a gépeket teszteli, akiknek megegyezik a hátulról i-edik jegye az övével), így tudná, hogy ki a defektív, majd két kérdéssel tudatná a többiekkel is. Ez tehát nem túl érdekes probléma, így foglalkozzunk a nem adaptív változattal.

Ezt a problémát Hosszú Éva hozta a keresési problémákkal foglalkozó szemináriumra, és Gerbner Dániel ötlete és megoldása volt, hogy a duális halmazrendszert érdemes vizsgálni, mint mindjárt látni fogjuk. Szintén az ő ötlete volt a másik irányú probléma és annak megoldása, melyet majd a következő fejezetben fogok ismertetni.

8.1. Egyszerű becslések

Jelölje a szükséges kérdések minimális számát $q(n)$. A feltett kérdéseknek mindenképpen szeparáló rendszert kell alkotniuk, vagyis biztosan szükségünk lesz legalább $\lceil \log n \rceil$-re. Ugyanakkor könnyű példát mutatni, hogy kétszer ennyi elég is. Legyenek a halmazok $A_i^a = \{k \in [n] \mid j_i(k) = a\}$ ($i = 1, 2, \ldots, \lceil \log n \rceil$, $a \in \{0, 1\}$), ahol $j_i(k)$ jelöli a k szám kettes számrendszerbeli alakjának hátulról i. jegyét.

Ezek a kérdések jók lesznek, hiszen ha a k. számítógép hátulról i. jegye a, akkor az A_i^a tesztben benne van, és annak eredménye alapján egyértelműen meg tudja határozni a defektív számítógép hátulról i. jegyét. Tehát meg tudja határozni az 1., a 2., és így tovább a $\lceil \log n \rceil$. jegyét is, és ez alapján egyértelműen tudja, hogy melyik a rossz gép.

Vagyis azt kaptuk, hogy $\lceil \log n \rceil \leq q(n) \leq 2\lceil \log n \rceil$ közt található. Kérdés, hogy a $\frac{q(n)}{\log n}$ sorozatról tudunk-e valamit mondani. Meg fogom mutatni, hogy konvergál, és a határértékét is meg fogom határozni.

8.1.1. Megjegyzés. *A számjegyes módszerrel egy kicsit jobb felső becslést is tudunk adni. Ne kettes, hanem hármas számrendszerben írjuk fel a számokat, a kérdések pedig legyenek* $A_i^a = \{k \in [n] \mid j_i'(k) \neq a\}$ *(*$i = 1, 2, \ldots, \lceil \log_3 n \rceil$*,* $a \in \{0, 1, 2\}$*), ahol* $j_i'(k)$ *most a* k *szám hármas számrendszerbeli alakjának hátulról* i*. jegyét jelöli.*

Legyen egy számítógép utolsó jegye 0*. Ekkor az* A_1^1 *és* A_1^2 *kérdésekre tudja a választ. Ha a defektív utolsó jegye* 0*, akkor mindkét kérédsben benne volt, ha* 1*, akkor csak az* A_1^2*-ben, ha* 2*, akkor csak az* A_1^1*-ben. Ezalapján a kiszemelt gépünk meg tudja állapítani a defektív számítógép utolsó jegyét. Hasonlóan az összes számítógép meg tudja állapítani az összes jegyét a defektívnek, így pontosan meg tudja határozni mindegyik, hogy melyik a defektív. Összesen* $3\lceil \log_3 n \rceil$ *kérdést tettünk fel, ami aszimptotikusan jobb, hiszen* $2 \log n > 3 \log_3 n = 3 \log_3(2) \log n \approx 1,89 \log n$*.*

8.2. A duális halmazrendszer

Legyen $\{F_1, F_2, \ldots, F_m\} = \mathscr{F} \subseteq 2^{[n]}$ a feltett kérdések halmaza, és jelölje M azt az $m \times n$-es 0-1 mátrixot, melynek oszlopai az egyes számítógépeknek, sorai pedig a teszteknek felelnek meg, és az i. sor j. eleme 1, ha részt vesz a j. gép a i. tesztben, azaz $j \in F_i$, különben 0.

Mit is kell tudnia $\mathscr{F}$-nek?

1. Bármely $a, b \in [n]$ két különböző elemre kell lennie egy $F \in \mathscr{F}$-nek, hogy $a \in F$, de $b \notin F$. Ellenkező esetben minden $F \in \mathscr{F}$-re melyben a benne van, b is benne lenne. Tehát így a nem tudná megkülönböztetni azt ha ő a defektív attól, hogy ha b. Jelöljünk egy ilyen F-et $a|b$-vel, jelezve, hogy mit követelünk meg, hogy benne van, illetve nincs.

2. Bármely $a, b, c \in [n]$ három különböző elemre kell lennie egy $F \in \mathscr{F}$-nek, hogy $a, b \in F$, $c \notin F$ vagy $a, c \in F$, $b \notin F$. Ez ahhoz kell, hogy az a-t tartalmazó $\mathscr{F}$-beliek szerparáló rendszert alkossanak, vagyis a meg tudja különböztetni b-t c-től. Hasonlóan az előbbihez, jelöljünk egy ilyen F-et $ab|c$-vel vagy $ac|b$-vel.

Könnyen látható, hogy pontosan ezt a két tulajdonságot kell tudnia egy ilyen $\mathscr{F}$ halmazrendszernek ahhoz, hogy a feladatot megoldja.

A 2. tulajdonságot vizsgáljuk meg jobban. Bármely $a, b, c \in [n]$ három különböző elemre kell lennie egy $ab|c$ vagy $ac|b$ halmaznak, egy $ba|c$ vagy

$bc|a$ halmaznak és egy $ca|b$ vagy $cb|a$ halmaznak. Ez ekvivalens azzal, hogy legalább kétféle van az $ab|c$, $bc|a$, $ca|b$ típusú halmazokból.

Most vegyük a duális halmazrendszert. Ez az a halmazrendszer, melynek M^T a mátrixa. Másképpen fogalmazva M sorai helyett az oszlopai alkotják a halmazrendszert. Nézzük, ebben mit jelent az előző két tulajdonság. Jelölje a duális halmazrendszert $\mathscr{G} = \{G_1, G_2, \dots G_n\} \subseteq 2^{[m]}$.

1. Bármely $A, B \in \mathscr{G}$ két különböző halmazra kell lennie egy $x \in [m]$-nek, hogy $x \in A$, de $x \notin B$. Vagyis $A \not\subseteq B$. Ennek a tulajdonságnak neve is van.

   8.2.1. Definíció. *Spernernek nevezünk egy $\mathscr{G}$ halmazrendszert, ha semelyik két különböző $A, B \in \mathscr{G}$ elemére nem teljesül, hogy $A \subseteq B$.[6]*

2. Bármely $A, B, C \in \mathscr{G}$ három különböző halmazra kell Az alábbi három közül legalább kettőnek teljesülnie kell:

   (a) Létezik $x \in [m]$, hogy $x \in A, B$, de $x \notin C$,

   (b) Létezik $y \in [m]$, hogy $y \in B, C$, de $y \notin A$,

   (c) Létezik $z \in [m]$, hogy $z \in C, A$, de $z \notin B$.

   Ezeket át lehet fogalmazni. Ekkor az alábbi három közül kell legalább kettőnek teljesülnie:

   (a) $A \cap B \not\subseteq C$,

   (b) $B \cap C \not\subseteq A$,

   (c) $C \cap A \not\subseteq B$.

   8.2.2. Definíció. *A $\mathscr{G}$ halmazrendszert angolul cancellative-nak nevezik, ha bármely $A, B, C \in \mathscr{G}$-re $A \cup B = A \cup C \Rightarrow B = C$.*

   8.2.3. Definíció. *A $\mathscr{G}$ halmazrendszert nevezzük metszet-cancellative-nak, ha bármely $A, B, C \in \mathscr{G}$-re $A \cap B = A \cap C \Rightarrow B = C$.*

   8.2.4. Állítás. *A $\mathscr{G} \subseteq 2^m$ halmazrendszer pontosan akkor metszet-cancellative, ha a $\mathscr{G}' = \{[m] \setminus A \mid A \in \mathscr{G}\}$ halmazrendszer cancellative.*

Bizonyítás. Tegyük fel, hogy $\mathscr{G}$ metszet-cancellative. Vezessük be a $\overline{A} = [m] \setminus A$ jelölést. Legyen $\overline{A}, \overline{B}, \overline{C} \in \mathscr{G}'$, amelyekre $\overline{A} \cup \overline{B} = \overline{A} \cup \overline{C}$. Ekkor $\overline{A \cap B} = \overline{A} \cup \overline{B} = \overline{A} \cup \overline{C} = \overline{A \cap C}$, és így $A \cap B = A \cap C$. A metszet-cancellative tulajdonság miatt így $B = C$, tehát $\overline{B} = \overline{C}$. Vagyis $\mathscr{G}'$ cancellative. A másik irányt ugyanígy be lehet látni. □

8.2.5. Állítás. *A $\mathscr{G}$ halmazrendszer pontosan akkor metszet-cancellative, ha bármely három különböző $A, B, C \in \mathscr{G}$-re az (a), (b), (c) közül legalább 3 teljesül.*

Bizonyítás. Rögzítsünk három különböző $A, B, C \in \mathscr{G}$ halmazt. Ezekre megmutatjuk, hogy (a), (b), (c) közül legalább 2 teljesülése ekvivalens azzal, hogy $A \cap B \neq A \cap C$, $B \cap C \neq B \cap A$ és $C \cap A \neq C \cap B$ mindegyike teljesül.

$A \cap B \neq A \cap C$ azt jelenti, hogy az $A \cap B \setminus C$ és $A \cap C \setminus B$ halmazok közül legalább az egyik nem üres. Hasonlóan a $B \cap C \setminus A$ és $B \cap A \setminus C$ halmazok közül is legalább az egyik nem üres, illetve a $C \cap A \setminus B$ és $C \cap B \setminus A$ halmazok közül legalább az egyik nem üres.

Vagyis $A \cap B \neq A \cap C$, $B \cap C \neq B \cap A$ és $C \cap A \neq C \cap B$ mindegyike teljesül pontosan akkor, ha $A \cap B \setminus C$, $B \cap C \setminus A$ és $C \cap A \setminus B$ halmazok közül legalább kettő nem üres.

$A \cap B \setminus C \neq \emptyset$ pedig pontosan azt jelenti, hogy $A \cap B \not\subseteq C$, ami pedig az (a) feltétel volt. Hasonlóan kijön a többi is, így ezzel beláttuk az állítást.

□

Vagyis beláttuk, hogy egy halmazrendszer akkor oldja meg a problémát, ha a duálisa Sperner és metszet-cancellative.

A továbbiakban bemutatom, hogy egy maximális cancellative halmaz méretéről mit tudunk.

8.3. Az asszimptotikusan pontos felső becslés

Ebben a fejezetben Frankl Péter és Füredi Zoltán cikkének [7] nekünk szükséges részét részletezem, illetve javítom ki.

8.3.1. Definíció. *Jelölje $G(n)$ egy maximális méretű $\mathscr{A} \subseteq 2^{[n]}$ cancellative halmazrendszer méretét. Továbbá jelölje $G_k(n)$ egy maximális méretű $\mathscr{A} \subseteq 2^{[n]}$ cancellative halmazrendszer méretét, melyben az összes részhalmaz mérete pontosan k. (Azaz $\mathscr{A} \subseteq \binom{[n]}{k}$, másképpen k-uniform.)*

8.3.2. Állítás. *Ha $\mathscr{A}$ cancellative, és $A \in \mathscr{A}$ egy maximális méretű eleme ($|A| = k$), akkor $|\mathscr{A}| \leq 2^{n-k} + 1$.*

Bizonyítás. $A \cup B \neq A \cup C$ miatt $B \cap \overline{A} \neq C \cap \overline{A}$ bármely két különböző $B, C \in \mathscr{A} \setminus \{A\}$-ra. Vagyis így $|\mathscr{A} \setminus \{A\}| \leq |\overline{A}| = 2^{n-k}$, tehát $|\mathscr{A}| \leq 2^{n-k}+1$. □

8.3.3. Állítás. *Ha $n \leq 2k$, akkor $G_k(n) = 2^{n-k}$.*

Bizonyítás. Egy k-uniform cancellative halmazredszer esetén $B \cap \overline{A} = \emptyset$ nem fordulhat elő semelyik $B \in \mathscr{A} \setminus \{A\}$-ra, különöben $B \subseteq A$ lenne, de mivel mindkettő elemszáma k, így mégis $A = B$ lenne. Így beláttuk, hogy $G_k(n) \leq 2^{n-k}$. Az egyenlőséghez pedig megadunk egy ilyen halmazrendszert.

Legyen $X_i = \{j \in [n] \mid j \equiv i \pmod{k}\}$ $(i = 1, 2, \ldots k)$. Ekkor $|X_1| = |X_2| = \cdots = |X_{n-k}| = 2$ és $|X_{n-k+1}| = \cdots = |X_k| = 1$, hiszen $k \leq n \leq 2k$.

Legyen $\mathscr{A} = \{A \subseteq [n] \mid \forall i \leq k : |A \cap X_i| = 1\}$. Ez könnyen láthatóan k-uniform, cancellative és mérete éppen 2^{n-k}.

□

8.3.4. Állítás. *Ha $n \geq 2k$, akkor $G_k(n) \leq \binom{n}{k} 2^k / \binom{2k}{k}$.*

Bizonyítás. Válasszunk véletlenszerűen egyenletes eloszlással egy $X \in \binom{[n]}{2k}$ $2k$-elemű halmazt. Legyen $\mathscr{A}_X = \mathscr{A} \cap \binom{X}{k}$.

Mivel $\mathscr{A}$-nak részhalmaza, ezért $\mathscr{A}_X$ is cancellative, és így alkalmazhatjuk az előző állítást, tehát $|\mathscr{A}_X| \leq 2^{2k-k} = 2^k$.

Ugyanakkor a várhatóérték kettős leszámlálással könnyen megkapható: $E(|\mathscr{A}_X|) = |\mathscr{A}| \binom{2k}{k} / \binom{n}{k}$.

Mivel a várhatóérték nem lehet nagyobb, mint a valószínűségi változó maximális értéke, így $|\mathscr{A}| \binom{2k}{k} / \binom{n}{k} \leq 2^k$, amit átrendezve megkapjuk a bizonyítandó állítást.

□

8.3.5. Lemma. $\binom{2k}{k} \geq \frac{2^{2k}}{2(2k)^{1/2}}$. [1]

[1] A cikkben[7] azt állítják, hogy $k \geq 7$ esetén $\binom{2k}{k} \geq \frac{2^{2k}}{(2k)^{1/2}}$, és ezt bizonyítják lényegében ugyanúgy, ahogy én itt leírtam, az indukciót $k = 7$-től kezdve. Sajnos azonban az állítás nem igaz se $k = 7$-re, se nagyobb k-ra. Így inkább ezt a rosszabb, de igaz becslést bizonyítom, és használom a továbbiakban. Mint látni fogjuk, nekünk elég ennyi is.

Bizonyítás. Ezt k szerinti indukcióval bizonyítjuk. $k = 1$-re mindkét oldal 2, tehát teljesül az egyenlőtlenség. Tegyük fel, hogy valamely k-ra teljesül, megmutatjuk, hogy ekkor $k+1$-re is fog. Bebizonyítjuk, hogy a bal oldalt egy nagobb számmal szorozzuk meg, mint a jobb oldalt, így az egyenlőtlenség továbbra is fenn fog állni:

A bal oldal ennyiszeresére nő: $\binom{2k+2}{k+1}/\binom{2k}{k} = \frac{(2k+2)(2k+1)}{(k+1)(k+1)} = \frac{4k+2}{k+1}$.

A jobb oldal pedig: $\frac{2^{2k+2}}{2(2k+2)^{1/2}}/\frac{2^{2k}}{2(2k)^{1/2}} = 2^2\frac{(2k)^{1/2}}{(2k+2)^{1/2}} = 4\frac{(k(k+1))^{1/2}}{k+1}$.

A számtani-mértani egyenlőtlenség miatt $(k(k+1))^{1/2} < k + \frac{1}{2}$, így $4\frac{(k(k+1))^{1/2}}{k+1} < 4\frac{k+\frac{1}{2}}{k+1} = \frac{4k+2}{k+1}$, és épp ezt akartuk megmutatni.

□

Végül ennyi felvezetés után már kimondhatjuk a tételt.

8.3.6. Tétel. $G(n) < 2n^{1/2}\left(\frac{3}{2}\right)^n$.

Bizonyítás. Legyen $\mathscr{A} \subseteq 2^{[n]}$ cancellative, és legyen $A \in \mathscr{A}$ egy maximális méretű eleme. Ha $|A| \geq \frac{n}{2}$, akkor az 8.3.2.-ss állítás jobb becslést biztosít, hiszen $2^{n/2} \leq \left(\frac{3}{2}\right)^n$, ugyanis $2^{1/2} = \sqrt{2} \approx 1,4142 < 1,5 = \frac{3}{2}$. Tehát feltehetjük, hogy $|A| < \frac{n}{2}$.

Legyen $\mathscr{A}_k = \mathscr{A} \cap \binom{[n]}{k}$ és $a_k = |\mathscr{A}_k|$. $a_0 > 0$ azt jelentené, hogy köztük van az üres halmaz, de akkor csak $|\mathscr{A}| \leq 2$ lehetne, így feltehető, hogy $a_0 = 0$. Ekkor tehát $|\mathscr{A}| = \sum_{k=1}^{\lfloor n/2 \rfloor} a_k$.

Mivel $\mathscr{A}_k$ egy k-uniform cancellative, így $a_k \leq G_k(n) \leq \binom{n}{k}2^k/\binom{2k}{k}$.

Felhasználva az előbbi lemmát: $a_k \leq \binom{n}{k}2^k/\binom{2k}{k} \leq \binom{n}{k}2^k/\frac{2^{2k}}{2(2k)^{1/2}} = \binom{n}{k}2^{-k}2(2k)^{1/2}$. Végül felhasználva, hogy $k < \frac{n}{2}$, azt kapjuk, hogy $a_k \leq \binom{n}{k}2^{-k}2(2k)^{1/2} < \binom{n}{k}2^{-k}2n^{1/2}$.

Így tehát $|\mathscr{A}| = \sum_{k=1}^{\lfloor n/2 \rfloor} a_k < \sum_{k=1}^{\lfloor n/2 \rfloor}\binom{n}{k}2^{-k}2n^{1/2} < 2n^{1/2}\sum_{k=0}^{n}\binom{n}{k}2^{-k} = 2n^{1/2}\left(\frac{3}{2}\right)^n$, és épp ezt akartuk belátni.

Az utolsó egyenlőség a binomiális tétel miatt teljesül: $\sum_{k=0}^{n}\binom{n}{k}2^{-k} = 2^{-n}\sum_{k=0}^{n}\binom{n}{k}1^k2^{n-k} = 2^{-n}(1+2)^n = \left(\frac{3}{2}\right)^n$.

□

Így tehát beláttuk, hogy egy $\mathscr{G} \subseteq 2^{[m]}$ cancellative halmazrendszer mérete legfeljebb $2m\left(\frac{3}{2}\right)^m$. Ám nekünk a duális probléma minimális megoldására van szükségünk. Vagyis, hogy melyik az a legkisebb m, hogy $n \leq 2m\left(\frac{3}{2}\right)^m$. Ezt nem tudjuk pontosan kiszámolni, de aszimptotikusan $m \approx \log_{3/2} n = \frac{1}{\log(3/2)}\log n \approx 1,7095 \log n$.

8.4. Az asszimptotikusan pontos alsó becslés

Most pedig megmutatom, hogy ez el is érhető. Ebben a fejezetben Ludo M. Tolhuizen cikkének[8] nekünk szükséges részét dolgozom fel. Ő a kódelmélet nyelvén fogalmazta meg és vizsgálta a problémát, én is így fogok tenni. Ehhez szükség lesz néhány újabb fogalom bevezetésére.

Az alábbi modellt *bináris szorzó csatornának* (angolul *binary multiplying channel*, röviden BMC) nevezzük. Alíz és Bob a csatorna két végén vannak, és szeretnének üzenetet váltani. $X, Y \subseteq \{0,1\}^n$ a két halmaz, melyekből kiválasztják a kódszavaiakat úgy, hogy Alíz választ egy $x \in X$, Bob egy $y \in Y$ elemet, egyszerre átküldik a csatornán, és mindketten megkapják az $x \cdot y$ *szorzatvektort*, melynek i-edik koordinátája x i-edik koordinátájának és y i-edik koordinátájának szorzata, vagyis $(x \cdot y)_i = x_i \cdot y_i$. A cél természetesen az, hogy ezután mindketten egyértelműen dekódolni tudják a másik üzenetét a saját elküldött üzenetük és a kapott üzenet segítségével. Ha ez megtehető, akkor egy ilyen (X, Y) párt *egyértelműen dekódolhatónak* (angolul *uniquely decodable*, röviden UD) nevezünk. Továbbá az (X, Y) pár *szimmetrikus*, amennyiben $X = Y$.

Egyáltalán mi köze van a BMC-nek a cancellative halmazredszerekhez?

8.4.1. Definíció. *Ha $a \in \{0,1\}^n$, akkor jelölje $supp(a) = \{i \in [n] \mid a_i = 1\}$ az a vektor tartóját.*

Ha $A \subseteq [n]$, akkor $\chi(A) \in \{0,1\}^n$ jelöli azt az egyértelmű vektor, amelynek A a tartója. $\chi(A)$-t az A karakterisztikus vektorának nevezzük.

8.4.2. Állítás. *Legyen az (X, X) szimmetrikus UD-pár. Ekkor $\mathscr{X} = \{supp(a) \mid a \in X\}$ egy metszet-cancellative halmazrendszer. És ugyanígy visszafelé, ha $\mathscr{Y}$ egy metszet-cancellative halmazrendszer, akkor (Y, Y) egy szimmetrikus UD-pár, ahol $Y = \{\chi(A) \mid A \in \mathscr{Y}\}$.*

Bizonyítás. Legyen $A, B, C \in \mathscr{X}$ három halmaz, melyekre $A = supp(a)$, $B = supp(b)$ és $C = supp(c)$.

Ekkor $A \cap B = supp(a) \cap supp(b) = \{i \in [n] \mid a_i = 1\} \cap \{i \in [n] \mid b_i = 1\} = \{i \in [n] \mid a_i = b_i = 1\} = \{i \in [n] \mid a_i \cdot b_i = 1\} = supp(a \cdot b)$. Hasonlóan $A \cap C = supp(a \cdot c)$.

Vagyis ha $A \cap B = A \cap C$, akkor $supp(a \cdot b) = supp(a \cdot c)$, vagyis $a \cdot b = a \cdot c$. Ez pedig azt jelenti, hogy ha Alíz az a üzenetet küldené, akkor nem tudná megkülönböztetni, hogy Bob a b-t vagy a c-t küldte, ami csak akkor történhet meg, ha $b = c$, vagyis így $B = supp(b) = supp(c) = C$, és épp ezt akartuk megmutatni.

A másik irány hasonlóan kijön.

□

8.4.3. Definíció. *Legyen $A \subseteq \{0,1\}^n$ egy kód. Az $I \subseteq [n]$ halmazt az A egy azonosító halmazának nevezzük, ha A bármely két elemének eltér legalább az egyik I-beli koordinátája.*

8.4.4. Állítás. *Legyen $A, B \subseteq \{0,1\}^n$ két kód, és jelölje $X(A,B) = \{a \in A \mid supp(a)$ a B egy azonosító halmaza$\}$. Ekkor $(X(A,B), X(B,A))$ egy UD-pár.*

Bizonyítás. Tegyük fel, hogy Alíz az $x \in X(A,B)$, Bob az $y \in X(B,A)$ üzenetet küldi el. Legyen $z = x \cdot y$. Ekkor minden $i \in supp(x)$-re $z_i = y_i$, vagyis Alíz (aki ismeri x-et és z-t) tudja ezeken a helyeken y értékét. Mivel $y \in B$, és B-nek azonosító halmaza $supp(x)$, így Alíz kiszámolhatja y-t. Ugyanígy Bob is meg tudja határozni y-ból és z-ből x-et.

□

Most tehát a célunk a célunk, hogy találjunk egy ilyen UD-párt viszonylag nagy számossággal. Ehhez a kódunk egy $[n,k]_2$-kód lesz.

8.4.5. Definíció. *Legyen q prímhatvány és jelölje $\mathbb{F}_q$ a q elemű véges testet. Ekkor az $[n,k]_q$ (lineáris) kódban a kódszavak az $\mathbb{F}_q^n$ (n-dimenziós) vektortér egy k-dimenzós alterét alkotják.*

Egy k elemű azonosító halmazt az $[n,k]_q$ kódhoz tartozó információs halmaznak nevezünk.

8.4.6. Lemma. *Az $\mathbb{F}_q$ feletti $k \times k$-as invertálható mátrixok száma pontosan $I_q(k) = \Pi_{i=0}^{k-1}(q^k - q^i)$.*

Bizonyítás. Építsük fel soronként a mátrixot. Az első sor a csupa nulla vektor kivételével bármi lehet, vagyis $q^k - 1$-féle lehet. Most tegyük fel, hogy az első i sort már kiválasztottuk. Ekkor az $i+1$-edik sor nem lehet az általuk kifeszített altérben, de egyébként bármi lehet, vagyis $q^k - q^i$ lehetőségünk van kiválasztani. Ezeket összeszorozva kapjuk $I_q(k)$ értékét.

□

8.4.7. Definíció. *Legyen $\gamma_q = \Pi_{i=1}^{\infty}(1 - q^{-i})$.*

8.4.8. Tétel. *Létezik olyan $[n,k]_q$ kód, melynek legalább $\gamma_q \binom{n}{k}$ információs halmaza van.*

Bizonyítás. Egy $G \in \mathbb{F}_q^{k\times n}$ mátrixhoz tartozzon a $C(G) = \{mG \mid m \in \mathbb{F}_q^k\}$ kód.

Egy $K \in \binom{[n]}{k}$ pontosan akkor információs halmaz a $C(G)$ kódhoz, ha invertálható a G_K $k \times k$-as részmátrixa G-nek, melyet úgy kapunk, hogy pontosan a K-beli indexű oszlopokat választjuk ki.

Egy adott $K \in \binom{[n]}{k}$-hoz pontosan $I_q(k)q^{k(n-k)}$ olyan G mátrix van, melyre G_K invertálható. Hiszen a K-beli oszlopokat láttuk, hogy ennyiféleképenn választhatjuk, a maradék $k(n-k)$ elemre pedig nincs semmi megkötés.

Most tekintsük a (G, K) párokat, ahol $G \in \mathbb{F}_q^{k\times n}$, $K \in \binom{[n]}{k}$ és G_K invertálható. Ezen párok száma $\binom{n}{k}I_q(k)q^{k(n-k)}$. Összesen q^{kn} mátrix van, így tehát van egy G mátrix, amelynek legalább $\binom{n}{k}I_q(k)q^{k(n-k)}/q^{kn} = \binom{n}{k}I_q(k)/q^{k^2} = \binom{n}{k}\Pi_{i=0}^{k-1}(1-q^{i-k}) \geq \binom{n}{k}\gamma_q$.

□

A továbbiakban $q = 2$, ekkor ki lehet számolni, hogy $\gamma_2 \approx 0,2888$, de úgyse fogjuk használni a pontos értékét.

8.4.9. Definíció. *A C $[n,k]_q$ kódhoz tartozó egy mellékosztály legyen egy $\{x + c \mid c \in C\}$ halmaz.*

Ilyen mellékosztályból nyilván 2^{n-k} van. Továbbá egy C-hez tartozó információs halmaz azonosító halmaza minden mellékosztálynak is.

8.4.10. Állítás. *Legyen C_i $[n,k_i]_2$ kód, amelynek M_i információs halmaza van ($i = 1,2$). Ekkor létezik egy A mellékosztálya C_1-nek és B mellékosztálya C_2-nek, hogy $|X(A,B)| \geq M_2/2^{n-k_1}$ és $|X(B,A)| \geq M_1/2^{n-k_2}$. Továbbá ha $C_1 = C_2$, akkor választható $A = B$-nek.*

Bizonyítás. C_1-nek van 2^{n-k_1} mellékosztálya, ezek együtt épp M_2 vektort tartalmaznak, melyeknek tartói mind információs halmazai C_2-nek. Emiatt van egy A mellékosztálya C_1-nek, hogy az legalább $M_2/2^{n-k_1}$ vektort tartalmaz, melyeknek a tartói továbbra is információs halmazok C_2-höz. Hasonlóan van egy B mellékosztálya C_2-nek, hogy abban legalább $M_1/2^{n-k_2}$ vektor van, és azok tartói mind információs halmazok C_1-hez. Ha $C_1 = C_2$, akkor látható, hogy választható $A = B$-nek.

Mivel a C_1-hez tatozó információs halmazok azonosító halmazai az A mellékosztálynak, így $|X(B,A)| \geq M_1/2^{n-k_2}$. Ugyanígy megmutatható, hogy $|X(A,B)| \geq M_2/2^{n-k_1}$.

□

Az előbbi állítás és az azt megelőző tétel nyilvánvaló következménye a következő állítás.

8.4.11. Következmény. *Tetszőleges $1 \leq k_1, k_2 \leq n$ három egész számhoz találhatunk egy olyan (X, Y) n-hosszú UD-párt, hogy $|X| \geq \gamma_2\binom{n}{k_2}/2^{n-k_1}$ és $|Y| \geq \gamma_2\binom{n}{k_1}/2^{n-k_2}$. Továbbá, ha $k_1 = k_2$, akkor választható $X = Y$-nak.*

8.4.12. Definíció. *Az (X, Y) n-hosszú UD-pár rátája az $(R(X), R(Y)) = \left(\frac{1}{n}\log|X|, \frac{1}{n}\log|Y|\right)$ pár.*

Az (r_1, r_2) ráta-pár elérhető, ha minden $\varepsilon > 0$-hoz létezik (X, Y) UD-pár, hogy $R(X) > r_1 - \varepsilon$ és $R(Y) > r_2 - \varepsilon$.

Az elérhető ráta-párok halmazát jelölje Z.

8.4.13. Tétel. *$\{(h(R_2) + R_1 - 1, h(R_1) + R_2 - 1) \mid 1/2 \leq R_1, R_2 < 1\} \subseteq Z$, ahol $h(p) = -p\log p - (1-p)\log(1-p)$ az entrópiafüggvény.*

Továbbá, ha $1/2 \leq R < 1$, akkor a $(h(R) + R - 1, h(R) + R - 1)$ pár elérhető szimmetrikus UD-párokkal.

Bizonyítás. Ez az előző következményből már könnyen látszik. Legyen $k_i = \lfloor nR_i \rfloor$. Ekkor a Stirling-formulát felhasználva és n-nel a végtelenbe tartva: $\frac{1}{n}\log\binom{n}{k_i} = \frac{1}{n}\left(\log\left(\frac{(n/e)^n}{(k_i/e)^{k_i}((n-k_i)/e)^{n-k_i}}\right) + \log(o(n))\right) =$
$\frac{1}{n}\left(n\log n - k_i\log k_i - (n-k_i)\log(n-k_i)\right) + o(1) = \log n - R_i(\log R_i + \log n) - (1-R_i)(\log(1-R_i) + \log n) + o(1) = -R_i\log R_i - (1-R_i)\log(1-R_i) + o(1) = h(R_i) + o(1)$.

Így tehát $n \to \infty$ esetén $R(X) = \frac{1}{n}\log\left(\gamma_2\binom{n}{k_1}/2^{n-k_1}\right) = h(R_2) - \frac{1}{n}\log 2^{n-k_1} + o(1) = h(R_2) + R_1 - 1 + o(1)$. Hasonlóan $R(Y) = h(R_1) + R_2 - 1 + o(1)$. És épp ezt akartuk megmutatni.

□

Végül nézzük meg a szimmetrikus esetben mi a legjobb becslés, amelyet kaphatunk. Ehhez deriváljuk R szerint az előbb kiszámolt függvényt: $(h(R) + R - 1)' = -(R\log R + (1-R)\log(1-R))' + 1 = -(R\log R + (1-R)\log(1-R))' + 1 = -\frac{1}{\ln 2}(R\ln R + (1-R)\ln(1-R))' + 1 = -\frac{1}{\ln 2}(\frac{R}{R} + \ln R - \frac{1-R}{1-R} - \ln(1-R)) + 1 = -\frac{1}{\ln 2}(\ln\frac{R}{1-R}) + 1 = -\log\frac{R}{1-R} + 1$. A számolás közben ln az e alapú logaritmust jelöli.

$0 = -\log\frac{R}{1-R} + 1 \Leftrightarrow 1 = \log\frac{R}{1-R} \Leftrightarrow 2 = \frac{R}{1-R} \Leftrightarrow 2(1-R) = R \Leftrightarrow 3R = 2 \Leftrightarrow R = \frac{2}{3}$. Könnyen ellenőrizhető, hogy itt a függvénynek maxmimua lesz, értéke pedig $h(\frac{2}{3}) + \frac{2}{3} - 1 = -\frac{2}{3}\log\frac{2}{3} - \frac{1}{3}\log\frac{1}{3} - \frac{1}{3} = -\frac{1}{3}(2(\log\frac{1}{3}+1) + \log\frac{1}{3}+1) =$

$-(\log\frac{1}{3}+1) = -\log\frac{2}{3} = \log\frac{3}{2}$. Vagyis azt kaptuk, hogy a legnagyobb rátapár, melyet így el tudunk érni az a $(\log\frac{3}{2}, \log\frac{3}{2})$. Vagyis tudunk nagyságrendileg $\left(\frac{3}{2}\right)^n$ méretű cancellative halmazrendszert találni, pontosabban:

8.4.14. Tétel. *$G(n) \geq cn^{-1/2}\left(\frac{3}{2}\right)^n$ alkalmas c konstanssal.*

Bizonyítás. Egy $\gamma_2\binom{n}{k}/2^{n-k}$ méretű halmazrendszert biztosít az előző konstrukció, ahol most $k = \left\lfloor\frac{2}{3}n\right\rfloor$ lesz. Az alábbi számolásban felhasználom az ismert közelítését $n!$-nak, miszerint $\sqrt{2\pi}\sqrt{n}\left(\frac{n}{e}\right)^n \leq n! \leq e\sqrt{n}\left(\frac{n}{e}\right)^n$. Továbbá a számolást könnyítendő feltesszük, hogy $\frac{2}{3}n$ egész szám (a különbség elnyelhető c-ben).

$$G(n) \geq \gamma_2\binom{n}{k}/2^{n-k} \geq \gamma_2\frac{\sqrt{2\pi}\sqrt{n}\left(\frac{n}{e}\right)^n}{e\sqrt{2n/3}\left(\frac{2n/3}{e}\right)^{2n/3}e\sqrt{n/3}\left(\frac{n/3}{e}\right)^{n/3}}/2^{n-2n/3} =$$

$$\gamma_2\frac{\sqrt{2\pi}}{e^2\sqrt{2/3}\sqrt{1/3}}\frac{1}{\sqrt{n}}\frac{n^n}{(2n/3)^{2n/3}(n/3)^{n/3}}\frac{1}{2^{n/3}} = cn^{-1/2}\left(\frac{1}{(2/3)^2(1/3)2}\right)^{n/3} = cn^{-1/2}\left(\frac{1}{8/27}\right)^{n/3}$$
$$= cn^{-1/2}\left(\frac{3}{2}\right)^n$$

□

Ez pedig már majdnem azt jelenti, hogy az eredeti számítógépes problémában az $\frac{1}{\log_{3/2}}$ konstans el is érhető. Ugyanis láttuk, hogy egy cancellative (és ugyanígy egy metszet-cancellative) halmazrendszernél ez a felső- és az alsóbecslés is. Ám mint láttuk, ennél többet is elvárunk a duális halmazrendszerünktől. Az is kell, hogy Sperner legyen. Ehhez nézzünk rá újra az előbbi konstrukciónkra. Egy $[n,k]_2$ kód mellékosztályából kerültek ki a halmazok. Semmi sem garantálja, hogy ezek között nem lesz kettő, hogy az egyik tartalmazza a másikat. Ám egy kicsit ritkíthatjuk, hogy alkalmas legyen. Mégpedig úgy, hogy egyforma méretű halmazokat veszünk. Ha két különböző halmaz mérete egyforma, akkor nyilván nem tartalmazhatja egyik a másikat. A konstrukcióban a halmazaink az $[n]$ részhalmazaiból kerültek ki. Ez azt jelenti, hogy mindegyik halmaz mérete 0 és n közé esik. Ez összesen $n+1$-féle méret. Vagyis kell lennie egy $0 \leq l \leq n$ számnak, hogy az l méretű halmazok száma legalább $\frac{1}{n+1}cn^{-1/2}\left(\frac{3}{2}\right)^n$. Az így kapott halmazrendszer Sperner, cancellative, és a nagyságrenden lényegesen nem rontottunk. És végül, hogy teljesen megoldjuk az eredeti problémát: ezen halmazoknak vegyük a komplementereit $[n]$-re nézve. Mint láttuk, ekkor metszet-cancellative lesz a halmazrendszer. És továbbra is Sperner, hiszen a halmazok mérete továbbra is megegyezik.

9. Tudatlan páciensek

Most vizsgáljuk a másik irányú problémát: nem az a célunk, hogy az elemek tudjanak mindent, hanem épp ellenkezőleg: a lehető legkevesebbet tudják. Például fel tudjuk-e úgy tenni a kérdéseket, hogy garantáltan egyik elem se tudja kitalálni, hogy ki a defektív azon tesztek eredményei alapján, melyekben benne volt, de az összes teszt eredménye alapján egy külső szemlélő (az orvos) meg tudja találni a defektívet (vagyis a kérdezett halmazrendszer szeparáló)?

9.0.1. Tétel. *Bárhogy is teszünk fel egy szeparáló halmazrendszer kérdéseit, nem tudjuk garantálni, hogy senki se tudja kitalálni, hogy ki a defektív.*

Bizonyítás. Tegyük fel, hogy mégis sikerült így feltenni egy $\mathscr{F} \subseteq 2^{[n]}$ kérdéssorozatot. Legyen $a \in [n]$ egy elem. Jelölje $\mathscr{F}_a \subseteq S$ azon feltett kérdések halmazát, melyekben a szerepelt, vagyis $\mathscr{F}_a = \{F \in \mathscr{F} \mid a \in F\}$.

Ha a lenne a defektív, akkor ezt nem tudhatja meg magáról. Ez azt jelenti, hogy kell lennie egy $b \in [n]$ elemnek is, aki szintén defektív lehet az ő ismeretei alapján. Ez csak úgy lehet, ha az összes kérdésben, melyben a szerepelt, b-nek is szerepelnie kellett. Vagyis $\mathscr{F}_a \subseteq \mathscr{F}_b$. Sőt, mivel $\mathscr{F}$ szeparáló, ezért létezik egy $F \in \mathscr{F}$, melyre $b \in F$, de $a \notin F$, vagyis $\mathscr{F}_a \subsetneq \mathscr{F}_b$ is teljesül.

Jelölje $a \preceq b$, ha $\mathscr{F}_a \subseteq \mathscr{F}_b$. Ekkor $([n], \preceq)$ egy részben rendezett halmaz. Hiszen reflexív ($\mathscr{F}_a \subseteq \mathscr{F}_a$ nyilván), tranzitív ($\mathscr{F}_a \subseteq \mathscr{F}_b \subseteq \mathscr{F}_c \Rightarrow \mathscr{F}_a \subseteq \mathscr{F}_c$ is triviális) és antiszimmetrikus ($\mathscr{F}_a \subseteq \mathscr{F}_b$ és $\mathscr{F}_b \subseteq \mathscr{F}_a$ esetén $\mathscr{F}_a = \mathscr{F}_b$, ez pedig $\mathscr{F}$ szeparálósága miatt csak $a = b$ esetén fordulhat elő).

Ráadásul ez a részben rendezett halmaz véges, tehát vehetünk egy $a \in [n]$ maximális elemét. Mint láttuk, ekkor létezik egy $b \in [n]$ elem, hogy $\mathscr{F}_a \subsetneq \mathscr{F}_b$, vagyis ekkor $a \prec b$, ami ellentmond a választásának. Ellentmondásra jutottunk, tehát nem lehet ilyen halmazrendszert találni.

□

Hivatkozások

[1] G.O.H. Katona, Combinatorial Search Problems, A survey of combinatorial theory (Ed. by J.N. Srivastava, North Holland/American Elsevier, Amsterdam/New York, 1973) 285-308.

[2] G. Katona, On separating systems of a finite set, J. Combin. Theory 1 (1966) 174-194.

[3] A. Feinstein, Foundations of Information Theory, Mc Graw-Hill, New York, 1958.

[4] Ding Zhu Du and Frank K. Hwang, Combinatorial group testing and its applications, World Scientific Publishing Co. Inc., River Edge, NJ, 1993.

[5] F. K. Hwang, A method for detecting all defective members in a population by group testing, J. Amer. Statist. Assoc. 67 (1972) 605-608.

[6] E. Sperner, Ein Satz über Untermegen einer endlichen Menge, Math. Z. 27 (1928) 544-548.

[7] P. Frankl and Z. Füredi, Union-fee hypergraphs and probability theory, Europ. J. Comb., vol. 5, 127-131, 1984.

[8] Ludo M. Tolhuizen, New Rate Pairs in the Zero-Error Capacity Region of the Binary Multiplying Channel Without Feedback, IEEE Transactions on Information Theory, vol 46., 1043-1046, 2000.