

**Válasz Katona Gyulának
az „Optimális térlefedő kódok kutatása” című
doktori értekezés opponensi bírálatára**

Mindenekelőtt szeretném megköszönni Katona Gyulának, az MTA rendes tagjának a támogató véleményét. A kritikai észrevételekre, megjegyzésekre és a feltett kérdésre a következőket szeretném válaszolni.

Először az opponensi bírálatnak „Az értekezés tartalma” szavakkal bevezetett részére (3. old.) szeretnék reagálni.

Amint az opponens is gondolta, valóban az volt a célom a hosszú bevezető részekkel, amelyek folyamatosan 37 oldalt kitöltenek már az értekezésem elején, hogy megkönnyítsem az értekezés olvashatóságát, figyelembe véve, hogy hazánkban tudomásom szerint senki sem foglalkozott behatóan ezzel a témával, ezért kevesen ismerhetik a szakterület zsargonját, speciális fogalmait, valamint a szakterületen korábban elért eredményeket. Ehhez a gondolathoz kapcsolódva mentegetőzni is szeretnék, hogy az értekezés túllépi az ajánlott (bár nem kötelezően előírt) 100 oldalnyi terjedelmet. Ha a maximum 100 oldalban ajánlott terjedelmet betartottam volna, akkor az említett kezdő 37 oldal, valamint a néhány további fejezet elejére írt hasonló jellegű szövegrész miatt túl kevés terjedelem maradt volna az eredmények ismertetésére.

Nagyon örülök, hogy az opponens humort is talált a dolgozatomban, a „normális és abnormális kód” definícióját és magyarázatát tartalmazó szövegrészben. Az opponens az értekezés alábbi mondatát idézi:

„Különösen hangsúlyozni szeretném, hogy az „abnormális” jelzőnek itt nincs pejoratív értelme, hanem csupán azt fejezi ki, hogy valamely kód nem rendelkezik egy meghatározott tulajdonsággal.”

Hogy jól értsük, miről is van itt szó, szeretném ezt a gondolatot kicsit jobban megmagyarázni.

Véleményem szerint a „normális kód” elnevezés egy tévedés következménye. Ennek magyarázatát az alábbiakban látom: A tapasztalatok szerint, valamint a térlefedő kódokra az utóbbi időszakban végzett klasszifikációs vizsgálatok szerint bináris kódok esetén vitathatatlanul az a normális viselkedés, amit a *normális kód* fenti definíciója kifejez; az optimális, ill. a lefedés szempontjából „jó” kódok túlnyomó többsége eleget tesz ennek az egyenlőtlenségnek. Amikor a *normális kód* fogalmát – először még csak bináris kódokra, a

$$d(x, C_0) + d(x, C_1) \leq 2R + 1 \quad (1)$$

egyenlőtlenséggel megfogalmazva – bevezették, akkor még senki nem gondolhatta, hogy a fogalom kézenfekvő általánosítása a nem bináris kódokra olyan

paradox helyzetet fog előidézni, hogy az optimális kódok zöme és valamennyi nem bináris perfekt kód a definíció kiterjesztése értelmében abnormálisnak fog bizonyulni. A tapasztalatok és a klasszifikációs vizsgálatok ugyanis azt is mutatják, hogy $q > 2$ esetén nagyon kevés, q értékét növelve arányukat tekintve egyre kevesebb a normális kód.

Ezek alapján határozottan az a véleményem, hogy szerencsésebb lett volna a fogalomra más elnevezést kitalálni a *normális kód* helyett, de mára az már annyira elterjedt a világon és annyira megszokottá vált a (főleg angol nyelvű) szakirodalomban, hogy ezen az elnevezésen nem hiszem, hogy jelenleg lehetne változtatni.

A bíráló 5. oldalának alján az opponens jogosan kifogásolja, hogy az értekezésben „nincs kellően megmagyarázva, miért érdekes” a normális kódok vizsgálata. Közvetve ugyan ez kiderül a dolgozatból, de valóban nem ártott volna ezt a kérdést kicsit direkter módon fejtegetni. Ennek pótlására írom a következő kb. 10-20 sort. (Ugyanezt a szövegrészt Győri Ervin opponensi véleményére adott válaszom is tartalmazza.)

Az értekezés 3.-7. fejezeteiben láttuk, hogy különböző konstrukciók segítségével normális kódok meghosszabbításával, ill. összetételével nagyobb méretű és adott elérési sugarú kódokat tudunk készíteni. (Ugyanezek a konstrukciók nem normális kódokra is néha, szerencsés esetben sikerre vezethetnek, de általában nem.) Ilyenek az ADS konstrukciók különböző változatai: bináris, ill. ternáris kódokra az egyszerűbb 3.3.3., ill. 4.2.3. konstrukciók, amelyek a bonyolultabb 3.4.2. ill. a ternáris kódokra alkalmazott hasonló általános ADS konstrukciók nagyon speciális esetei. Hasonló módszerek általános q -ra, valamint vegyes kódokra is alkalmazhatók (és a megfelelő fejezetek eredményeihez alkalmaztunk is azokat), ha a konstrukciókban részt vevő kódok legalább egy koordinátára nézve normálisak. Egy további érv az, hogy normális kódok vizsgálata alapján érdekes sejtéseket lehet megfogalmazni – így Cohen és szerzőtársai a [47] cikkben felvetett, a

$$K(n+2, R+1) \leq K(n, R)$$

egyenlőtlenség általános érvényűségére vonatkozó sejtését – és speciális esetekre bizonyítani. A sejtés helyessége jelenleg $R = 1$ -re van csak bebizonyítva.

A bíráló 6. oldalán az opponens a következő kérdést teszi fel:

„A 3.5 részben a szerző összefüggést mutat be a minimális bináris szűrjektív kódok és az optimális térlefedő kódok között. Ezután felhasználja, hogy a bináris szűrjektív kódok minimuma egy duális formában már ismert az extremális halmazrendszerek elméletéből. Az idézett Kleitman–Spencer [32] és a nem idézett Gargano–Körner–Vaccaro cikk (JCTA, 61 (1992), 173–192)

aszimptotikus eredményeket tartalmaz a páronként kvalitatíven független q részes particiók maximális számáról. Ez pedig lefordítható a q -szűrjektív kódok legkisebb méretére. Nem kapható ezek felhasználásával aszimptotikus eredmény a térlefedő kódokra?”

A kérdést, és így a választ is két részre bontanám: 1. Az idézett cikkek eredményei alapján milyen aszimptotikus eredmények adhatók meg a q -szűrjektív kódokra? 2. Ismerünk-e, vagy az 1. részre adott válasz alapján tudunk-e adni aszimptotikus eredményeket térlefedő kódokra?

Úgy érzem, a kérdés második fele a fontosabb, s mivel arra válaszolni is egyszerűbb, ezért a logikus sorrendet felrúgva, előbb a 2. részre szeretnék válaszolni.

Kleitman és Spencer, ill. Gargano és szerzőtársai exponenciális lefutású aszimptotikus eredményeket fogalmaznak meg (melyeket később részletesebben elmagyarázok), ezek a q -szűrjektív kódokra logaritmikus lefutású aszimptotikus görbéket eredményeznek. Azonban a megadott aszimptotikus formulák olyan konstansokat tartalmaznak, melyekre csak egymástól lényegesen eltérő alsó és felső korlátot tudnak megadni. A felső korlát általában legalább 4-szerese az alsó korlátnak. Egyetlen kivétel a $q = 3, k = 2$ eset, ahol a megadott legjobb alsó korlát 0.483..., a felső korlát pedig $2/3$, vagyis 0.666... Ebből érezhető, hogy ha tudnánk is térlefedő kódokra vonatkozó aszimptotikus eredményekre következtetni, a következtetési lánc és a konstansok bizonytalansága miatt ezek csak legfeljebb nagyon durva közelítések lennének. Ezért annak indoklásába már nem is mennék bele, hogy miért nem tudunk. Inkább annak illusztrálására térnék rá, hogy voltaképpen nincs is szükség ilyen aszimptotikus eredmények kidolgozására, mivel a téma klasszikus irodalmából nagyon jó aszimptotikus eredményeket tudunk megadni a térlefedő kódok méretét kifejező $K_q(n, R)$ függvényre.

Az $R = 1$ esetre és prím vagy prímhatvány q -ra a szférikus alsó korlát létezéséből és a Hamming-kódok (valamint az azokkal azonos paraméterű egyéb perfekt kódok) sorozatának az ismeretéből azonnal adódik, hogy

$$\liminf_{n \rightarrow \infty} \left(K_q(n, 1) \left/ \frac{q^n}{1 + n(q-1)} \right. \right) = 1.$$

Cohen és szerzőtársai [97] könyvének egy teljes fejezete (Chapter 12, pp. 319-353) aszimptotikus korlátokra vonatkozó eredményeket tárgyal tetszőleges elérési sugarú bináris térlefedő kódokra. Csak egy eredményt említenék az idézett könyvből, azt a szép eredményt, hogy $K_2(n, R)$ értékére logaritmikusan nemcsak alsó, hanem felső aszimptotikus korlátot is biztosít a szférikus alsó korlát, tehát adott R esetén

$$\lim_{n \rightarrow \infty} \left(\ln K_2(n, R) \left/ \ln \frac{2^n}{V_2(n, R)} \right. \right) = 1.$$

(Ez a könyv „Theorem 12.1.2” állításából következik.)

Rátérve a q -szűrjektív kódok aszimptotikus viselkedésének a kérdésére, ezt önmagában is érdekes kérdésnek találtam, amivel érdemes lehet behatóbban foglalkozni.

A választ az egyszerűbb $q = 2$ eset megfogalmazásával kezdem, amikor is kétrészes partíciókat tekintve egy halmaz részhalmazáiból álló rendszerrel és e részhalmazok komplementereivel fogalmazható meg a probléma. Valamely n elemű S halmaz $A_1, A_2, \dots, A_m$ részhalmazai (kvalitatíven) k -függetlenek, ha $m \geq k$ és e részhalmazok tetszőleges k halmazból álló $A_{i_1}, A_{i_2}, \dots, A_{i_k}$ rendszerére valamennyi

$$\bigcap_{j=1}^k B_{i_j}$$

halmaznak van legalább egy eleme, ahol

$$B_{i_j} = A_{i_j} \text{ vagy } B_{i_j} = S \setminus A_{i_j}.$$

Az ilyen metszethalmazok száma 2^k .

A matematikusokat régóta foglalkoztatja az a kérdés, hogy adott n méret esetén mi az a lehető legnagyobb m érték, amelyre létezik m halmazból álló k -független halmazrendszer. Jelöljük m -nek ezt a maximális értékét $f_2(n, k)$ -val.

Érdekes módon körülbelül 40 évvel ezelőtt nagyjából egy időben több publikációban (köztük az opponens egyik publikációjában) jelent meg annak megállapítása és bizonyítása, hogy

$$f_2(n, 2) = \binom{n-1}{\lfloor n/2 \rfloor - 1}.$$

Az általánosabb esetben az S halmaz részhalmazai és azok komplementerei helyett q részes partíciókat vizsgálunk. A k -független halmazrendszer definícióját értelemszerűen ki lehet terjeszteni k -független q -részes partíciókra. Az előbbiekhez hasonlóan az utóbbiakra is feltehető az a kérdés, hogy mekkora m méretig létezik m számú k -független q -részes partícióból álló partíció-rendszer. Jelöljük m -nek ezt a maximális értékét $f_q(n, k)$ -val.

Az értekezésben, más megfogalmazásban, azzal a hasonló, bizonyos értelemben duális, problémával foglalkozom, amikor m értéke adott és keressük az S halmaznak azt a lehető legkisebb n méretét, amelyre létezik m halmazból álló k -független halmazrendszer, ill. az általánosabb esetben partíció-rendszer. Jelöljük ezt a legkisebb méretet az egyszerűség kedvéért $g_q(m, k)$ -val (Az értekezésben $\sigma_q(m, k)$ -val történt ennek jelölése, s lényegében ugyanennek a

mennyiségnek a jelölésére a „covering arrays” témájú munkák a $CAN(k, m, q)$ jelölést használják.)

Az $f_q(n, k)$ és $g_q(m, k)$ függvények definíciójából egyszerűen adódik, hogy közöttük az alábbi kapcsolat van:

$$g_q(m, k) = \min\{n : f_q(n, k) \geq m\}$$

és

$$f_q(n, k) = \max\{m : g_q(m, k) \leq n\}.$$

Rögzített q és k esetén az $f_q(n, k)$ függvény n -nek, a $g_q(m, k)$ függvény pedig m -nek monoton nemcsökkenő függvénye. Szigorú értelemben monoton függvények esetén a fenti egyenlőségek azt jelentenék, hogy $f_q(n, k)$ és $g_q(m, k)$ egymás inverzei lennének.

Ezért vezessük be az $f_q^*(n, k)$ és $g_q^*(m, k)$ függvényeket úgy, hogy ezek értelmezési tartománya legyen

$$D_f^* = \{n : n \geq q^k, \quad q^k \leq n_1 < n \implies f_q(n_1, k) < f_q(n, k)\},$$

ill.

$$D_g^* = \{m : m \geq k, \quad m_1 > m \implies g_q(m_1, k) > g_q(m, k)\},$$

értékük pedig az így megritkított értelmezési tartományukon legyen egyenlő $f_q(n, k)$, ill. $g_q(m, k)$ értékével.

Az így értelmezett $f_q^*(n, k)$ és $g_q^*(m, k)$ függvények már pontosan egymás inverzei, tehát elvi akadálya nincs, hogy az $f_q^*(n, k)$ függvényre vonatkozó aszimptotikus eredményből az inverz $g_q^*(m, k)$ függvényre kapjunk aszimptotikus eredményt.

Kleitman és Spencer idézett cikke szerint léteznek $c_{2,k}$ konstansok úgy, hogy

$$c_{2,k} = \lim_{n \rightarrow \infty} \frac{\ln f_2(n, k)}{n},$$

tehát

$$f_2(n, k) = e^{n(c_{2,k} + o(1))}.$$

A g függvényre átfogalmazva:

$$g_2(m, k) = \ln m \cdot \left(\frac{1}{c_{2,k}} + o(1) \right),$$

azaz

$$\lim_{m \rightarrow \infty} \frac{g_2(m, k)}{\ln m} = \frac{1}{c_{2,k}}.$$

Az idézett cikk egy-egy képletet is ad a $c_{2,k}$ konstansok alsó, ill. felső korlátjára, tetszőleges 2-nél nagyobb k egészre. Táblázatot ad $k = 3, 4, 5, 6, 10$ -re. Mivel ők 2 alapú logaritmust használnak, néhányat felírok természetes logaritmusra átszámítva:

$$0.04450 \dots \leq c_{2,3} \leq 0.2157 \dots$$

$$0.01608 \dots \leq c_{2,4} \leq 0.1017 \dots$$

$$0.00635 \dots \leq c_{2,5} \leq 0.0490 \dots$$

$$0.00262 \dots \leq c_{2,6} \leq 0.0239 \dots$$

Tetszőleges $q \geq 3$ esetére (de csak $k = 2$ -re) Poljak és Tuza bizonyítják, hogy vannak olyan $c_{q,2}$ konstansok, melyekre

$$c_{q,2} = \limsup_{n \rightarrow \infty} \frac{\ln f_q(n, k)}{n},$$

ebből viszont a $g_q(m, k)$ függvény aszimptotikus viselkedésére vonhatunk le következtetést.

Gargano és szerzőtársai cikke a $q = 3$ speciális esettel foglalkozik, és a $c_{3,2}$ konstansra ad meg a korábban ismertnél jobb alsó korlátot, amely nemcsak az $f_3(n, 2)$, hanem következésképpen a $g_3(m, 2)$ függvény aszimptotikus becslését is finomítja.

Budapest, 2011. 11. 16.

Kéri Gerzson