

Kéri Gerzson

Optimális térlefedő kódok című MTA doktori értekezésének értékelése

Bevezető elmélkedés

Egy véges ábécé feletti n hosszúságú sorozatokból válasszunk ki minél többet úgy, hogy bármely két sorozat d helyen különbözzék. Ez a kódelmélet legismertebb és legelterjedtebb feladata, amit hírközlési és elektronikai alkalmazások motiválnak. Az ilyen kódokat (optimális) hibajavító kódoknak nevezzük.

A jelen dolgozat feladata más, fogalmazzuk meg azonnal pontosan. A $0, 1, \dots, q - 1$ elemekből álló n hosszúságú sorozatok egy C halmazát itt is kódnak nevezzük, ennek elemei a kódszavak. Két sorozat (Hamming) távolsága azon helyek száma, ahol a két sorozat különbözik. C -t R -sugarú térlefedő kódnak nevezzük, ha bármely (ezen ábécéből készített) sorozat távolsága a kód valamely elemétől legfeljebb R . Ez úgy is fogalmazható, hogy a C kódbeli kódszavak köré írt R sugarú gömbök lefedik az egész teret, azaz az összes, az ábécéből készített sorozat benne van a gömbök uniójában. Az ilyen tulajdonságú kódokat nevezzük térlefedő kódoknak. Míg a hibajavító kódoknál a kódszavak maximális számát keressük, itt a kódszavak minimumát. Ezt a minimumot a dolgozatban $K_q(n, R)$ jelöli, és ennek meghatározása a témakör fő feladata.

Bár a hibajavító kódok elmélete fejlettebb, a térkitöltő kódoknak is sok alkalmazása, és kiterjedt irodalma van. Már az 1960-as években születtek benne említésre méltó eredmények.

Sem (az adott paraméterek melletti) legnagyobb hibajavító kódok legnagyobb, sem a térkitöltő kódok legkisebb méretét nem lehet pontosan meghatározni általában, ezért a kutatás reális célja a jó alsó és felső becslések keresése. Egy — a feltételeket kielégítő — konkrét, adott kód alsó becslést ad a hibajavító kódoknál, és felsőt a térlefedőknél. Az alkalmazások elsősorban a konkrét, kis paraméterekre adott konstrukciókat igénylik. Persze azért még a mérnököt is érdekli, hogy „nincs-e jobb?”, ezért a kis értékekre vonatkozó — másik oldali — becslésekkel is sokan foglalkoznak. A nagy értékekre vonatkozó általános, vagy aszimptotikus alsó-felső becslések megtalálása nagyon nehéz, messze vannak az igazságtól, az alkalmazások nem kényszerítik ki, így az irodalom jelentős része a kis paraméterek esetével foglalkozik. Az már általános jellegű eredménynek számít, ha a paraméterek csupán egyike is végigfut a természetes számokon.

Tehát — például adott paraméterek mellett — a kutatás a következőképpen folyik. Meg kell adni egy kevés szóból álló térlefedő kódot. Ezután bizonyítani kellene, hogy kisebb nincs. Szerencsés esetben ez sikerülhet összefüggések, lemmák segítségével, de sokszor csak az a lehetőség marad, hogy számítógéppel kell sok esetet végigpróbálni. Ha az összes esetet akarunk végigpróbálni, azok száma olyan nagy, hogy a számítógép is kudarcot vall. Egyes kis lemmák, állítások segítségével az esetek száma annyira lecsökkenthető, hogy a számítógép már képes végezni a feladattal. Sajnos a kis állítások annyira specifikusak, hogy nincs szép általánosításuk, egyáltalán nem látványosak, pedig megtalálásuk komoly szellemi erőfeszítést igényelhet.

Régebben a kódelméleti monográfiák az elméleti alapok, általános eredmények után hosszú táblázatokban adták meg a legjobb értékeket. (Sokszor csak alsó és felső becsléseket.) Az újabb, és újabb kiadásokban beírva a javított értékeket. Manapság már jól karbantartott internetes táblázatok vették át ezt a szerepet. A kutatók között pedig igen nagy verseny folyik, ki, mit tud megjavítani.

Mindezekből látszik, hogy bár a feladat tisztán kombinatorikus, a terület igen messze áll a „magyar” kombinatorikai iskola stílusától. Vannak a matematikának más hasonló területei. Például a statisztikai kísérlettervezésben használt dizájnok, vagy az óriási primszámok keresése. De bizonyos geometriai feladatok is hasonlóak, amikor a gömb felszínén kell kiválasztani adott számú pontot úgy, hogy a legnagyobb távolság minimális legyen. Ezek a feladatok részben az informatika problémaköréhez hasonlítanak. Ezért értékeléséhez figyelembe kell vennünk az informatikai munkák értékelésére korábban kidolgozott elveket is.

A dolgozatban — természetesen — vannak a klasszikus kombinatorikai értelemben vett szép eredmények is. Azonkívül olyan pontos értékek, vagy becslések, ahol egy vagy több paraméter a végtelenbe fut. Sokszor ezek is összefüggésben vannak a „munkás” eredményekkel. Többször is a számítógéppel talált, kis, adott paraméterekre vonatkozó kódot jól használja a szerző egy, paraméterek végtelen halmazára érvényes konstrukció készítésére.

Szinte törvényszerű, hogy Kéri Gerzson rátalált erre a témára. Hiszen már első, 1964-ben megjelent, sok hivatkozással rendelkező cikke is hasonló volt: meghatározta az $R(6, 3) = 18$ Ramsey számot. Élete későbbi szakaszában lineáris programozási feladatokkal foglalkozott, ami hasonló gondolkodást igényelt.

Az értekezés tartalma

Az első 37 oldal, a 3.1-3.4 részek egy nagyon alapos bevezetőt tartalmaznak. A szerző nyilvánvalóan figyelembe vette, hogy hazánkban senki sem foglalkozik a témával főfoglalkozásként, sőt kevesen is ismerik az eredményeket. Ezután a bevezető után bárki jó eséllyel indul a megértés fele.

A világosan fogalmazott bevezetőben még humor is van. Idézem: „Különösen hangsúlyozni szeretném, hogy az ‚abnormális’ jelzőnek itt nincs pejoratív értelme, hanem csupán azt fejezi ki, hogy valamely kód nem rendelkezik egy meghatározott tulajdonsággal.”

De van a bevezető részben egy definíció, az r -sugarú szűrjektív kódoké, ami a szerzőtől származik, és fontos szerepet játszik módszereiben.

A 3.5 rész már tartalmaz új eredményeket. Az Östergårddal közös 3.7 tétel azt mondja ki, hogy a $2R + 4$ hosszú bináris sorozatok tere nem fedhető le 9-nél kevesebb R sugarú gömbbel. Eddig a 7 volt csak ismeretes. Ez a tétel azért különösen kedves a bírálónak, mert az extremális halmazrendszerek elméletének egy régi tételét használja. A 3.7 tétel segítségével azt is megtudják pontosan mondani, hogy $K(n, R)$ mikor lehet 7 illetve 8. Ezt eddig csak a 2,3,4,5,6 értékekre tudták.

A 3.6 rész a bináris térlefedő kódok jellemzésével, felsorolásával, osztályozásával foglalkozik. Az Östergårddal közös 3.12 tétel felsorolja az összes olyan bináris térlefedő kódot, amik a $2R + 3$ hosszú sorozatokat 7 darab R sugarú gömbbel fedik le. A 3.13 tétel megadja a számukat is egy szép — generátorfüggvényes — formában. A 3.16, 17 és 18 tételek más paraméterek mellett adnak nagyszámú konstrukciót térlefedő kódokra, de itt nem sikerül a teljes felsorolást megadni.

A 3.7 rész Kéri (Östergård nélkül) azon kutatási eredményeit tartalmazza, amelyek a 2-szűrjektív bináris kódokra vonatkoznak. Azt a speciális esetet tekinti, amikor a kódhossz

$$\binom{m}{\lfloor \frac{m-1}{2} \rfloor} + 1,$$

ahol m kettőhatvány. A 3.21 Tétel pontosan megadja a lefedéshez szükséges R sugár minimumát a minimális méretű 2-szűrjektív bináris kódok között. Valószínűleg ez a dolgozat legjobb bizonyítása, ugyanis a problémát a Baranyai-tételre vezeti vissza.

A 3.8 rész összefoglalja, hogy mit lehet tudni az 1, 2 és 3 sugárú térlefedő kódokról.

A negyedik fejezet a ternáris térlefedő kódokkal foglalkozik, mikben 3 jelet használunk. A 4.1-4.3 részek itt is bevezető jellegűek. A 4.4 rész viszont a fő kérdéssel, az adott R sugárú ternáris térlefedő kódok minimális méretével foglalkozik. Itt használja fel a szerző az általa bevezetett r -sugarú szűrjektív kódokat, megmutatva, hogy szorosan összefüggenek az itt tárgyalt fő problémával (4.2 Lemma és 4.3-4.5 Következmények). Ezek segítségével az Östergårddal közös 4.6 és 4.7 tételek pontosan megadják azon n és R értékeket, amelyekre $K_3(n, R)$ éppen 4, 5, 6, 7 vagy 8. A 4.8 tétel a 9-es értékre ad végtelen sok esetet lefedő elégséges feltételt.

A 4.5 részben a ternáris kódok leírására vonatkozó eredmények találhatók. A 4.9 Állítás általános q -elemű ábécére vonatkozik: pontosan leírja a $K_q(n, R) = q$ egyenlőségnek megfelelő optimális kódokat. A 4.10 Tétel viszont megadja a $K_3(n, R) = 3$ esetben optimális térlefedő kódok számát egy generátorfüggvénnyel. A 4.6 rész összefoglalja, felsorolja, mit lehet tudni a szerző eredményei után az 1, ..., 7 elérési sugárú ternáris térlefedő kódokról.

Az 5-ik fejezet a nagyobb ábécék esetével foglalkozik. A bevezető 5.1 és 5.2 részek után az 5.3 rész az Östergårddal közösen elért új felső becsléseket tartalmazza $K_q(n, 1)$ -re, ahol $n = 8, 9$ illetve 10, q viszont a mod 7, 8 illetve 9 egy maradékosztályán fut végig (tehát egy r paramétretől függ).

Az 5.4 rész a szűrjektív kódokkal való szoros kapcsolatra mutat rá. Az Östergårddal közös 5.3 tétel és az 5.4 Következmény egy nagyon általános felső becslést ad $K_q(n, R)$ -re szűrjektív kódok minimális méreteinek segítségével.

Az 5.5 részben lévő 5.5 Tétel szerint

$$K_q(4, 2) = \left\lceil \frac{q^2}{3} \right\rceil$$

teljesül, ha $9 \leq q \leq 15$ vagy $21 \leq q$. Ennek konstrukciós részét Rodemich már 1970-ben megadta, de csak most sikerült Kérinek bebizonyítania, hogy a konstrukció nem javítható.

Az 5.7, 5.8 és 5.9 részek az optimális és rekorder kódokat tekintik át $q = 4$ -re, $q = 5$ -re illetve $6 \leq q \leq 10$ -re.

A 6-ik fejezet olyan kódokkal foglalkozik, amelyekben adott számú helyen lehet 0,1 illetve 0,1,2. A 6.1-6.3 részek a szükséges előismereteket tartalmazzák.

A 6.4 rész foglalkozik $K(t, b; R)$ értékével. (Minimális, R sugarú térlefedő kód, ami t ternáris és b bináris jelből álló kódszavakat tartalmaz.) Az Östergård-dal közös 6.12, 6.15, 6.18 és 6.23 tételek pontosan jellemzik azon t, b párokat, amelyekre $K(t, b; R)$ 4, 5, 6 illetve 7. Ezek bizonyításai a dolgozat leghosszabbjai, összesen 12 oldalt foglalnak el. A 6.24 és 6.25 tételben megadnak végtelen sok t, b párt, amikor $K(t, b; R)$ 8 illetve 9, de itt nem tudják, hogy ezek az összes-e. Végül a 6.28 tétel a szerző által számítógép segítségével bizonyított $K(3, 6; 3) = 12$ és $K(1, 8; 2) = 20$ új állításokat tartalmazza.

A 6.5 rész a szerző által bizonyított, a ternáris-bináris vegyes esetre vonatkozó klasszifikációs eredményeket tartalmazza. A 6.29-6.34 tételek bizonyos paraméterek mellett.

A 6.6 rész ismét a konkrét esetekre vonatkozó eredmények áttekintését adja.

A 7-ik fejezet $K(q, t, b; R)$ -rel foglalkozik, azaz a b helyen 0,1-et, t helyen 0,1,2-öt, q helyen 0,1,2,3-at tartalmazó kódszavakból álló R sugarú térlefedő kódok minimális méretével. A 7.7 tételben a szerző egy 6 oldalas bizonyítással adja meg annak szükséges és elégséges feltételét, hogy $K(q, t, b; R)$ pontosan 4 legyen. Az itteni további tételek végtelen paramétersereget adnak meg, amikor az érték pontosan 5, 6 illetve 8, de ezekben az esetekben nem biztos, hogy az összes ilyen paraméter-együttes fel van sorolva. A 7.2 fejezet néhány klasszifikációs eredményt mutat be, és táblázatokat ad a legjobb konkrét eredményekre, amelyeket a szerző számítógép segítségével bizonyított.

A 8-ik fejezet a normális kódokkal foglalkozik. Ezek definíciója egy képlettel van megadva a 17. oldalon. Ez azt fejezi ki, hogy van a kódban egy olyan irány, amelyre vetítve a kapott kódok összlefedési sugara is kicsi. A dolgozat egy kis hiányossága, hogy nincs kellően megmagyarázva, miért érdekes ezen kódok vizsgálata. Persze az alapos olvasó megtalálja később, hogy normális és optimális kódokból jól lehet hosszabb és nagyobb sugarú kódokat csinálni. Tulajdonképpen ez van összefoglalva a 8.1 részben.

A 8.2 részbeli 8.2 Tétel egy egyszerű észrevétel, a normális kód fedési sugara és a minimális kódtávolság közötti viszonyt kifejező egyenlőtlenség. Azonban megmagyarázza, miért normálisak többnyire az optimális bináris térlefedő kódok, míg ugyanez nagyobb q -kra nem igaz.

A 8.3 rész a normális, minimális, R -sugarú térlefedő kódok méreteit adja meg a ternáris-bináris esetben kis t és b értékekre. A számítógépes eredmények több mint két oldalt foglalnak el. Ezek segítségével azután már egyparaméteres végtelen halmazokra tud jó konstrukciókat, azaz felső becsléseket adni $K(t, b; R)$ -re. A 8.3 Tétel ilyen típusú becsléseket tartalmaz: $K(3u+1, 4; 2u+1) \leq 10$.

A 9-ik fejezet a számítógépes algoritmusokat és a szerző által készített implementációkat írja le.

Egy kérdés

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 extrémális 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 kvalitatívan független q -részes partíciók maximális számáról. Ez pedig lefordítható a q -szűrjektív kódok legkisebb méretére. Nem kapható ezek felhasználásával aszimptotikus eredmény a térlefedő kódokra?

Értékelés

A dolgozat jelentős hozzájárulás a térlefedő kódok elméletéhez. Az eredmények egy kisebbik része szépnek nevezhető, érdekes kapcsolatokat mutat ki a kombinatorika más területeivel (3.7, 3.21, 5.5 Tételek). Más részük a kódelmélet számára fontos, viszont sok munkát és kisebb ötletek seregét igényelte (3.12, 3.13, 3.16, 3.17, 3.18, 4.6, 4.7, 4.8, 4.9, 5.3, 6.24, 6.25, 8.2, 8.3 Tételek, az 5.3 rész eredményei, az 5.4 Következmény). A 6.12, 6.15, 6.18, 6.18, 6.23 és 7.7 Tételeknek, hosszabb, nehezebb bizonyításuk van. A szerző érdeme az r -sugarú szűrjektív kódok fogalmának bevezetése és használata. A konkrét, kis paraméterekre vonatkozó eredmények seregét lehetetlen felsorolni. A munka egy része ismert, erős matematikusokkal közös. A cikkek jó

nevű folyóiratokban jelentek meg. Az eredményeket a nemzetközi honlapi táblázatok valóban számontartják.

Javaslom az értekezés nyilvános vitára bocsátását és a jelöltnek az MTA doktora cím odaítélését.

Budapest, 2011. október 10.

Katona Gyula