

Optimális térlefedő kódok kutatása

Kéri Gerzson

Akadémiai doktori értekezés

Budapest, 2009

Az értekezés tagolódása

Nyomtatott anyagrészek a függelék nélkül

Az értekezés bevezetése és kilenc fejezete tartozik ide. Az első két fejezet előkészítő célzatú; e fejezetekben a jelölések és a használt fogalmak kifejtésére, ill. a térlefedő kódok történetének ismertetésére kerül sor. Előkészítő jellegűek még több fejezet elején az adott fejezetben használt fogalmak, ill. szinte már fogalom számba menő standard konstrukciós technikák ismertetését tartalmazó 3.1–3.4, 4.1–4.3, 5.1–5.2, 6.1–6.3 szakaszok. Ezek tehát új eredményt nem tartalmaznak. A szerző új eredményei az értekezés 3.5–3.8, 4.4–4.6, 5.3–5.9, 6.4–6.6, 7.1–7.2, 8.1–8.3 szakaszaiban találhatók. Az új eredmények három csoportba sorolhatók.

1. Társszerzővel (Patric Östergård) közösen készített és a [129], [135], [139], [145], [155] cikkekben publikált eredmények. Ezeket az értekezés 3.5–3.6., 4.4. és 6.4. szakaszai tárgyalják.
2. Egyedül készített és a [143], [154] cikkekben publikált eredmények. Ilyenek az értekezésben a 3.7. és a 7.1. szakaszban tárgyalt eredmények.
3. Egyedül készített és még nem publikált eredmények. Ilyenek a 3.16., 3.17., 3.18., 4.10., 4.11., 5.5., 5.6., 6.30., 6.31., 7.10., 7.11., 8.2. tételekben megfogalmazott eredmények az értekezés 3.6–3.7., 4.5., 5.5–5.6, 6.4–6.5 szakaszaiban, ill. a 7. és 8. fejezetében. Zömmel ide sorolható további új eredmények számos egyedi esetre vonatkozó alsó vagy felső korlátnak, ill. az inekvivalens megoldások számának a meghatározására vonatkozó, nagyrészt számítógép segítségével kapott eredmények, melyekre a 3.8., 4.6., 5.7.–5.9. és 6.6. szakaszokban elhelyezett hivatkozások utalnak.

Függelék

Szigorúan nem tartoznak a térlefedő kódok kategóriái közé, de azokhoz több szálon is kapcsolódnak a szűrjektív kódok. Ezt a felemás helyzetet úgy szándékoztam megoldani, hogy a szűrjektív kódok tanulmányozásával kapcsolatos anyagrészt nem fejezetként, hanem függeléként csatoltam az értekezéshez. Felhasználási célból azonban a szűrjektív kódokra vonatkozó egyes eredmények megjelennek már az értekezés 3.5, 4.4, 5.4, 6.4 és 7.1 szakaszaiban, a 3.7 szakasz pedig, bár teljes egészében szűrjektív kódokról szól, mégis inkább a bináris térlefedő kódokról szóló fejezetbe kívánczik, nem pedig a függelékbe. A szűrjektív kódokra vonatkozó új eredmények két közleményben: [161] és [166] (mindkettő társszerzős) kerültek ill. várnak publikálásra.

Irodalomjegyzék

Az irodalomjegyzék struktúrájáról az alábbi rövid magyarázatot szeretném elmondani. Először a hivatkozott (vagy esetleg egyébként releváns) cikkeket és könyveket soroltam fel időrendi sorrendben. Ezt a felsorolást zárja [167] sorszámmal az értekezésnél bővebb terjedelmű, vele azonos tárgyú monográfia. Az erre történő hivatkozásokkal a jelen munka során kapott eredményeket jelzem. A cikkek és könyvek listáját követik az értekezés szerzője és mások által folyamatosan karbantartott hivatkozott internetes táblázatok, melyekhez nem lehet konkrét évszámot rendelni.

Tartalomjegyzék

A fejezetek és a függelék kezdő oldalszámát mutató rövid tartalomjegyzék az értekezés végén található.

Interneten tárolt melléklet és monográfia verzió

Eredeti tervem szerint az értekezés CD mellékletét képezte volna az ismert (beleértve a szerző által talált) optimális és rekord-tartó térlefedő kódok gazdag tára a tárgyalt különböző kód kategóriák szerint csoportosítva. Arra törekedtem, hogy a melléklet csaknem minden, a konkrét térlefedő kódokra vonatkozó ismeretet tartalmazzon, tehát a térlefedő kódoknak minél komplexebb tára legyen. A CD melléklet elkészült, viszont az értekezéshez történő illesztése különböző gyakorlati problémákba ütközött. Ezért a teljes CD mellékletet inkább az értekezéssel párhuzamosan készített, „A térlefedő kódok (covering codes) története, módszertana, rendszerezése” című [167] monográfia tartozékául szánom.

Az értekezéshez képest kibővített és sok példával kiegészített monográfia elektronikus formában (pdf típusú fájlként) megtalálható a <http://www.sztaki.hu/~keri/codes-hu> webhelyen, mérete kb. 1 Mbyte. Ugyanitt megtalálható az említett CD mellékletnek egy szintén kb. 1 Mbyte méretű demo változata. (A CD-n lévő anyagok teljes összmérete több mint 50 Mbyte, ezért a CD teljes tartalmának a SZTAKI serverén történő elhelyezése nem volna szerencsés.)

Az értekezés szövegében a CD mellékletre történő utalások alatt az előbb elmondottak alapján a [167] monográfia mellékletét vagy az interneten található mellékletet kell érteni.

A szerkesztés lezárása

Az értekezés fő részeinek szerkesztését 2009. augusztus 28-án zártam le. A monográfiának (valamint a CD teljes és demo változatának) szerkesztését minden egyes újabb eredmény vagy információ rendelkezésre állása esetén napra készre módosítom a kézirat nyomdába kerüléséig.

Bevezetés

A térlefedő kódok (angolul: covering codes) alapproblémája: Hamming terekben, vagyis adott hosszúságú bináris, ternáris stb. jelek sorozatai által alkotott terekben előírt elérési sugarú és lehetőleg minél kisebb számosságú kódok keresése. Matematikai megfogalmazásban a legáltalánosabb esetben keressük a $Z_{q_1}^{n_1} Z_{q_2}^{n_2} \cdots Z_{q_m}^{n_m}$ Hamming térnek egy (vagy összes) lehető legkisebb elemszámú olyan részhalmazát, melyeknek a tér tetszőleges pontjától való Hamming távolsága nem halad meg egy adott R értéket.

Az ilyen kérdésekre adandó válaszok általában nagyon nehéz optimalizálási problémáknak a megoldását vagy a megoldás megközelítését igénylik. A tárgyalt problémák kezelésére általános módszer nem ismeretes, szinte minden eset külön megfontolást igényel. Az alkalmazott módszertan kombinatorika, kombinatorikus optimalizálás, lineáris algebra, egészértékű programozás, játékelmélet módszerei mellett sajátos kódelméleti módszerek széles skáláját öleli fel. Hatékony számítógépek igénybevétele egyre inkább elkerülhetetlen új eredmények eléréséhez e területen, mivel esetenként akár több millió objektum tulajdonságainak a vizsgálatára is szükség lehet.

Az optimális kódok méretének pontos értéke csak kevés esetben ismert, ezért a legtöbb esetben meg kell elégednünk a fenti értelemben vett legkisebb elemszámmal, azaz az optimális kód méretének jelölésére használatos $K_{q_1, q_2, \dots, q_m}(n_1, n_2, \dots, n_m; R)$ kifejezés jó alsó, ill. felső korlátjának a meghatározásával. A felső korlát bizonyítása szinte minden esetben konstrukció bemutatásával történik, amely sok esetben az adott feladatnak nem optimális, de az adott időpontban a legjobb ismert megoldása. A felső korlátok helyessége ennél fogva viszonylag egyszerűen ellenőrizhető. Az alsó korlátok helyességének ellenőrzése sokkal problematikusabb, mivel ezek (gyakran igen bonyolult) bizonyításának valamennyi mozzanatát végig kell követni. Számítógép segítségével bizonyított alsó korlátok esetén viszont vagy az alkalmazott gépi program helyességét kell ellenőrizni, vagy másik (számítógéppel vagy anélkül végzett) bizonyítást találni az adott alsó korlát bizonyítására.

Esetenként nehéz és érdekes probléma egy-egy konkrétan megadott kód elérési sugarának a meghatározása is, de ilyen kérdésekre csak a példák között térünk ki, továbbá olyankor, amikor az elérési sugár kiszámítására az optimalitás bizonyítása céljából van szükség.

Alkalmazási lehetőségek. Térlefedő kódokat az informatika és a műszaki tudományok számos területén sikerrel alkalmaztak. Ilyenek: adattömörítés kötetlen sorrend esetén, tömörítés torzítással, hiba és adatvesztés dekódolása, műsorszórás összekapcsolt hálózatokban, egyszer írható memória, beszéd kódolása, sejt elvén alapuló távközlés, Berlekamp–Gale játék. Minderről részletesebben angol nyelven a [97] könyv 12-14. oldalain, magyar nyelven (az előbbi kissé rövidítve) a [167] monográfia kéziratban olvas-

hatunk. Az előbb felsoroltakon kívül az alábbi újabb keletű alkalmazási lehetőségeket találtam.

Kielégíthetőség vizsgálata (k -SAT). Egyszerűbb és kifinomultabb algoritmusok egyaránt léteznek annak eldöntésére, hogy logikai változók valamely formulája esetén a változókhoz lehet-e olyan értékeket rendelni, amely értékek mellett a formula kiértékelése a TRUE (igaz) értéket eredményezi. Dantsin és szerzőtársai [115] térlefedő kódokat alkalmaznak egy ebbe a kategóriába tartozó (a cikkben k -SAT-nak nevezett) probléma gyorsabb algoritmusának kidolgozására.

Szteganográfiai alkalmazások. A rejtett üzenetek beágyazásának hatékonyságát Zhang és szerzőtársai [151] bináris és ternáris térlefedő kódok alkalmazásával javítják a publikáció ismertetője szerint. Térlefedő kódok szteganográfiai alkalmazása a témája Bierbrauer és Fridrich [152] dolgozatának is. A közelmúltban pedig már sorra jelentek meg a térlefedő kódok szteganográfiai alkalmazását tárgyaló további cikkek.

Nagyobb q alapszámú térlefedő kódok a fehérjék szerkezetének kutatásával, vegyes térlefedő kódok pedig bonyolult döntési problémákkal hozhatók kapcsolatba. Az előbbi összefüggés abból adódik, hogy az ismert 20 fehérjeépítő aminosav adott n hosszúságú sorozatai (láncai) a Z_{20}^n Hamming tér pontjait alkotják, e fehérjék viszont egy négyelemű kódábécén (U = uracil, C = citozin, A = adenin, G = guanin) értelmezett triplettek, tehát a Z_4^3 Hamming tér pontjainak tekinthetők. A szerves kémiai/biológiai/genetikai kapcsolatot részletesebben fejti ki Golomb és Posner a [15] cikkben.

Végül a térlefedő kódok egy lehetséges alkalmazásaként képzeljünk el egy olyan döntési problémát, ahol a figyelembe veendő döntési alternatívák m számú paraméterrel írhatók le, s ezen paraméterek mindegyike véges sok, rendre $q_1, q_2, \dots, q_m$ különböző értéket vehet fel, vagy ennyi különböző állapottal jellemezhető. Ekkor a lehetséges alternatívák a $Z_{q_1} Z_{q_2} \dots Z_{q_m}$ Hamming tér pontjainak feleltethetők meg, ha feltételezzük, hogy e Hamming térben egymáshoz közeli pontoknak olyan alternatívák felelnek meg, amelyek közül egyiknek vagy másiknak a választása közel azonos eredményhez vezet. (A konkrét alkalmazástól függ, hogy ez a feltételezés helytálló-e.) Ebben az esetben az összes lehetséges alternatíva hatásának előzetes értékelése helyett – ami ezek túl nagy száma esetén reménytelenül túl nagy feladatot jelentene –, célszerű az alternatívák Hamming terének valamely olyan részhalmazára korlátozni az értékelést, amelytől a tér bármely pontja adott R Hamming távolságon belül van. Ez azt jelenti, hogy a szóban forgó vegyes Hamming térben térlefedő kódot kell keresnünk R elérési sugárral és lehetőleg minél kevesebb elemszámmal.

Szemléltető példák.

Sakktábla. Egy nagyon egyszerű példa térlefedő kódra a sakktáblával szemléltethető: Tekintsük azt a közismert feladatot, melyben bástyákat kell elhelyezni a sakktáblán oly módon, hogy a sakktábla minden mezőjét uralják, vagyis minden olyan mezőt, amin nem áll bástya, az elhelyezett bástyák valamelyike egy lépéssel elérje. Ez még nagyon könnyű feladat, nyilvánvalóan 8 bástyával a feladat megoldható, 8-nál kevesebb bástyával viszont nem. Ha azonban áttesszük a feladatot a síkból a térbe, akkor már kicsit nehezebbé válik, a dimenzió további növelése esetén pedig már négy dimenziós térben is mindmáig megoldatlan a minimálisan szükséges bástyák számának problémája. A három dimenziós térbeli feladat megoldásához tekintsük az (x_1, x_2, x_3) számhármassokat, ahol x_1, x_2, x_3

mindegyike az 1, 2, 3, 4, 5, 6, 7, 8 értékeket veheti fel. Ezek száma $8^3 = 512$, és az ilyen számhármások egyértelműen megfeleltethetők a 3 dimenziós sakktábla 512 mezőjének. Ha most a bástyákat az

(1, 1, 1)	(3, 1, 3)	(5, 5, 5)	(7, 5, 7)
(1, 2, 4)	(3, 2, 2)	(5, 6, 8)	(7, 6, 6)
(1, 3, 3)	(3, 3, 1)	(5, 7, 7)	(7, 7, 5)
(1, 4, 2)	(3, 4, 4)	(5, 8, 6)	(7, 8, 8)
(2, 1, 4)	(4, 1, 2)	(6, 5, 8)	(8, 5, 6)
(2, 2, 3)	(4, 2, 1)	(6, 6, 7)	(8, 6, 5)
(2, 3, 2)	(4, 3, 4)	(6, 7, 6)	(8, 7, 8)
(2, 4, 1)	(4, 4, 3)	(6, 8, 5)	(8, 8, 7)

számhármásokkal megadott térbeli mezőkbe helyezzük, akkor belátható, hogy a további 480 mező bármelyikébe el tudunk jutni úgy, hogy a felsorolt 32 mező valamelyikében egy koordináta értékét megváltoztatjuk.

Számzár. Következő példaként tekintsünk egy négyjegyű számzárát, olyat, amelyet például aktatászkák biztonságos zárására, nyitására használnak. Képzeljük el a számzárnak azt a különleges esetét, amikor a 4 számjegy közül 3 számjegy helyes beállítása esetén a zár, ha nehézkesebben is, de nyitható. Nem tudom, műszakilag megvalósítható-e az ilyen konstrukció, de a megvalósíthatóság lehetőségétől vagy lehetetlenségétől függetlenül jó példa térlefedő kódra az alábbi kérdésfeltevés esetén: Hogyan lehet a lehető legkevesebb próbálkozással kinyitni a zárat, ha elfelejtettük a bekódolt négyjegyű számot? Nem nehéz észrevenni, hogy lényegében ugyanazzal a feladattal állunk szemben, mint egy 4 dimenziós sakktábla esetén, ha a sakktábla méretét mindhárom irányban 8-ról 10-re növeljük. E feladat optimális megoldását a megadott konkrét esetben nem ismerjük, a legjobb ismert megoldás 352 négyjegyű szám kipróbálása. Ez lényegesen kisebb számhalmaz, mint az összes négy jeggyel írható szám halmaza, melynek elemszáma 10000. A megoldás 352 elemű számhalmazának listáját itt nem adjuk meg, a mellékelt CD lemezről viszont ez a lista kikereshető. Ha gondolatban tovább gyengítjük a számzár erejét, és feltesszük, hogy 4 közül 2 számjegy helyes beállítása esetén a zár már kinyitható, akkor mindössze 34 próbára van szükség, és az is bebizonyítható, hogy ennél kevesebb próba nem elég. A módosított feladat egy megoldása:

0000	2021	4444	6466	8788
0111	2130	4556	6545	8897
0222	2203	4665	6654	8979
0333	2312	5455	7777	9799
1013	3032	5564	7889	9878
1102	3123	5646	7998	9987
1231	3210			
1320	3301			

Bármely négyjegyű szám esetén található a megadottak között olyan, amelytől az csak két (vagy még kevesebb) helyen különbözik. Ezt úgy fejezzük ki, hogy az utóbbi példánál az elérési sugár 2. (A sakktáblás és az első számzáras példa esetén az elérési sugár 1 volt.)

Nem ellentmondás, mégcsak következetlenségnek sem szabad tekinteni, hogy az első példánál a nyolcelemű alaphalmaz számozását 1-gyel, a második példánál a tízelemű alaphalmaz számozását 0-val kezdtük. Elméleti szempontból ugyanis teljesen lényegtelen, hogy mi az alaphalmaz, és nemcsak számokból, hanem bármilyen szimbólumokból állhat. A lehetséges szimbólumok halmaza – a kódábécé – állhat akár színekből, kételemű alaphalmaz esetén pl. a fehér és fekete színből, háromelemű alaphalmaz esetén a kódábécé állhat az 1, x, 2 szimbólumokból. Totó kombinációra irányuló alkalmazás során – aminek két nagyon egyszerű esetét a következő példában mutatjuk be – ez az utóbbi a természetes kódábécé.

Totó. Az alábbi példában egy totószelvény négy mérkőzését ragadjuk ki; tegyük fel, hogy ezek kimenetelében vagyunk a legbizonytalanabbak, a többi totómeccs eredményét illetően viszont határozott elképzelésünk van. Kérdés: hány tipposzlopot kell kitölteni, hogy a kiválasztott négy mérkőzés közül legalább hármat biztosan eltaláljunk valamelyik oszlopban. A helyes válasz 9 tipposzlop, egy lehetséges megoldás pedig a következő:

hazai csapat 1 – vendég csapat 1	x	x	x	1	1	1	2	2	2
hazai csapat 2 – vendég csapat 2	x	1	2	x	1	2	x	1	2
hazai csapat 3 – vendég csapat 3	x	1	2	1	2	x	2	x	1
hazai csapat 4 – vendég csapat 4	x	1	2	2	x	1	1	2	x

Ebben az esetben 1 elérési sugárral (totós szóhasználat: 1 hibaponttal) kerestünk megoldást. Ugyanezekre a mérkőzésekre 2 elérési sugárral (2 hibaponttal) nagyon egyszerű a megoldás három tipposzloppal:

hazai csapat 1 – vendég csapat 1	x	1	2
hazai csapat 2 – vendég csapat 2	x	1	2
hazai csapat 3 – vendég csapat 3	x	1	2
hazai csapat 4 – vendég csapat 4	x	1	2

Az első esetben a ternáris (azaz 3 elemű kódábécére épülő) Hamming kód, a második esetben a négy hosszúságú ternáris ismétléses kód használatával kaptunk egy optimális megoldást.

Most térjünk vissza a többdimenziós sakktábla példájára, de csökkentsük a tábla méretét minden irányban először 3-ra, azután pedig 2-re. A 3×3 méretű közönséges síkbeli sakktábla esetén ez a tábla nyilván 3 bátyával uralható. Ismerjük az optimális megoldás pontos értékét 3, 4 és 5 dimenziós, 3 élhosszúságú sakktábla esetén is, ezekben az esetekben 5, 9, ill. 27 bátyára van szükség, 6 dimenzió esetén azonban már csak azt tudjuk, hogy a szükséges bátyák száma legalább 71 és legfeljebb 73. Nem nehéz észrevenni, hogy az n dimenziós, 3 élhosszúságú sakktáblára megfogalmazott probléma szoros kapcsolatban áll az n totó-mérkőzésre adandó 1 hibapontos totó-kombináció problémájával, ugyanis mindkettő ugyanazzal a kódelméleti problémával modellezhető.

Hiperkocka. A 2 élhosszúságú sakktáblákra vonatkozó kérdés frappánsabban fogalmazható meg, ha sakktábla mezői helyett az n dimenziós kocka (n -kocka vagy más elnevezéssel hiperkocka) csúcsaival értelmezzük lényegében ugyanazt a feladatot. Tekintsük

tehát az n dimenziós tér egységkockáját. Ez a hiperkocka a térnek azokat a pontjait tartalmazza, melyekben minden koordináta értéke 0 vagy 1. A lehetséges variációk száma 2^n , tehát ennyi a hiperkocka csúcsainak száma, továbbá minden csúcsban n él fut össze. Feladat: Küldjünk öröket a hiperkocka bizonyos csúcsaiba úgy, hogy ezek az örök együttesen a kocka valamennyi csúcsát őrizni tudják. Minden ör természetesen azt a csúcsot is őrizi, amelyre állították, de ezen kívül őrizi a saját posztjával szomszédos (azaz éllel összekötött) további n csúcsot is. Azt a célt tűzzük ki, hogy a hiperkocka csúcsai őrzésének a feladatát minél kevesebb örrel lássuk el. A szükséges örök száma a négyzettől az $n = 9$ dimenziós hiperkockáig ismert (2, 2, 4, 7, 12, 16, 32, ill. 62 ör), 10 dimenzió esetén már csak azt tudjuk, hogy a $2^{10} = 1024$ csúcs őrzéséhez az örök szükséges létszáma legalább 107 és legfeljebb 120.

Kapcsolótábla. Az alkalmazások között már idézett *Berlekamp–Gale játék* példáját szeretném további gondolatokkal és újabb információkkal kiegészíteni.

Tegyük fel, hogy adva van egy kapcsolótábla, amelyhez rögzítve n^2 villanyégő helyezkedik el n sorban és n oszlopban, rácsszerű elrendezésben, amint az alábbi bal oldali ábra mutatja $n = 3$ esetén. Számozzuk meg a táblára rögzített égőket sorfolytonosan, a jobb oldali ábra szerint mutatott módon.

o	o	o
o	o	o
o	o	o

1	2	3
4	5	6
7	8	9

A tábla hátulján elhelyezett n^2 kapcsolóval az égők egyenként ki- vagy bekapcsolhatók. A tábla fedelén elől is található $2n$ kapcsoló, amelyek az egy sorban, ill. egy oszlopban elhelyezett n égő ki- vagy bekapcsolt állapotának az ellentétes állapotra változtatását teszik lehetővé.

Adott két játékos, egyikük csak a hátul elhelyezett n^2 kapcsolót, a másik viszont csak az elől elhelyezett $2n$ kapcsolót használhatja. Mindketten csak egyszer léphetnek, de ekkor tetszőleges számú kapcsolási műveletet végezhetnek a számukra rendelkezésre álló kapcsolókkal. A hátsó kapcsolót kezelő játékos kezd, neki az a célja, hogy a játék végén minél több égő világítson. Amikor az első játékos jelzi, hogy befejezte a kapcsolási műveleteket, ezt követően a másik játékos csak az elől elhelyezett kapcsolók használatával arra törekszik, hogy a játék végén minél kevesebb égő világítson. Kérdés: Hány égő fog világítani a játék végén, ha mindkét játékos hiba nélkül játszik, vagyis a létező legjobb stratégiát választja.

A probléma matematikai megoldásához tekintsük át, hogy az összes égő kikapcsolt állapotából elindulva, az elől lévő kapcsolók használatával milyen lehetséges állapotokat lehet létrehozni. Mivel e kapcsolókból álló rendszer szabadsági foka $2n - 1$, a használatukkal elérhető különböző lehetséges állapotok száma 2^{2n-1} . A lehetséges állapotok n^2 hosszúságú bináris vektorokkal írhatók le, amelyekben az i -edik koordináta értéke 1, ill. 0, annak megfelelően, hogy az i sorszámú égő világít, vagy nem világít. Az alábbiakban $n = 3$ esetére a lehetséges állapotoknak a felét, 16 állapotot, pontosabban az ezekhez tartozó vektorokat soroljuk fel. A további 16 állapotot leíró vektort ezek komplementének képzésével, vagyis a 0-k és 1-esek felcserélésével kapjuk meg.

(0 0 0 0 0 0 0 0 0)
 (0 0 0 1 1 1 0 0 0)
 (0 0 0 0 0 0 1 1 1)
 (0 0 0 1 1 1 1 1 1)
 (0 1 1 0 1 1 0 1 1)
 (0 1 1 1 0 0 0 1 1)
 (0 1 1 0 1 1 1 0 0)
 (0 1 1 1 0 0 1 0 0)

(0 1 0 0 1 0 0 1 0)
 (0 1 0 1 0 1 0 1 0)
 (0 1 0 0 1 0 1 0 1)
 (0 1 0 1 0 1 1 0 1)
 (0 0 1 0 0 1 0 0 1)
 (0 0 1 1 1 0 0 0 1)
 (0 0 1 0 0 1 1 1 0)
 (0 0 1 1 1 0 1 1 0)

Minthogy az

(1 0 0 0 1 0 0 0 0)

vektor a felsoroltak és komplementeik mindegyikétől legalább 2 koordináta-helyen különbözik, ezért az 1-es és az 5-ös számú égő bekapcsolása esetén az elől elhelyezett kapcsolókkal a világító égők száma nem csökkenthető 2 alá.

Ez a példa abban különbözik az előzőektől, hogy itt nem a feltételeknek megfelelő legjobb tulajdonságú struktúrát (térlefedő kódot) keressük, mint a sakktáblás, számozás, totós és hiperkockás példák esetén, hanem adott egy térlefedő kód struktúrája, és az adott kód elérési sugarának a meghatározása a feladat. Nagyobb méretű kódok esetén ez sem könnyű. Az ismertett játékos kapcsolótáblás problémát Berlekamp 10×10 égőre fogalmazta meg még az 1960-as években, és jó 40 évvel később 2004-ben Carlson és Stolarski [131] adott rá helyes megoldást, amely szerint legfeljebb 35 villanyégőt lehet egyenként úgy bekapcsolni, hogy ez a szám az elől lévő kapcsolók használatával ne legyen csökkenthető. Ugyanebben a cikkben a szerzők a 11×11 és 12×12 méretű hasonló probléma megoldását is megadták. A probléma nehézségét mutatja, hogy az említett két időpont között megjelent egy (neves szerzők által készített) cikk, amely a megoldást tévesen 34-ben adta meg 10×10 méret esetére. (Viszont minden ennél kisebb méretre megadták a korrekt megoldást.) Az ismert eredmények számértéke 2×2 -től 12×12 méretig: 1, 2, 4, 7, 11, 16, 22, 27, 35, 43, 54.

Köszönetnyilvánítás

Matematikus pályára állításomért, ill. tudományos tevékenységem szakmai támogatásáért több évtized távlatából ezúton mondok köszönetet egykori tanárainknak, közülük kiemelten Autheried Éva gimnáziumi tanárnak, valamint Reiman István, T. Sós Vera és Prékopa András egyetemi tanároknak, továbbá munkahelyi szakmai vezetőimnek és valamennyi eddigi munkatársamnak.

Jelölések

Az alkalmazott jelölések megegyeznek a konvencionális matematikai jelölésekkel, ezért az alábbiakban csak azokat a jelöléseket soroljuk fel, amelyeknek a használata ritkábban fordul elő vagy nem egységes a matematikai szakirodalomban. Ilyenek a következők:

$A \subseteq B$	Halmaz tartalmazás; az A halmaz része a B halmaznak, vagy azonos vele.
$A \subset B$	Szigorú halmaz tartalmazás; az A halmaz része a B halmaznak, az azonosság kizárt.
$A \cup B$	Két halmaz egyesítése.
$A \cap B$	Két halmaz metszete.
$A \setminus B$	Két halmaz különbsége.
$\lfloor x \rfloor$	Alsó egész rész, floor (padló) függvény, a legnagyobb x -nél kisebb vagy vele egyenlő egész szám.
$\lceil x \rceil$	Felső egész rész, ceiling (mennyezet) függvény, a legkisebb x -nél nagyobb vagy vele egyenlő egész szám.
$wt(x)$	Bináris szó súlya, az 1 értékű koordináták száma.
x^T, A^T	Az x vektor, ill. az A mátrix transzponáltja.
$ x y $	Vektorok (szavak) összefűzése (konkatenációja), a $z = x y $ vektor koordinátáit úgy kapjuk, hogy x koordinátáinak a sorát y összes koordinátájával folytatjuk.
$ C D $	Kódok összefűzése (konkatenációja) szavanként, csak azonos számú kódszóból álló kódokra értelmezhető.
$C \oplus D$	Két kód direkt összege.
$C \equiv D$	Két kód ekvivalenciájának jelölése.
$\{\text{lista}\}$	Kód v. tetszőleges halmaz megadása a kódszavak/elemek felsorolásával.
$\text{GF}(q)$	Egy q elemszámú véges test; alternatív jelölése: F_q .

1. fejezet

Definíciók, fogalmak

Itt azokat a fogalmakat tárgyaljuk, amelyeket több fejezetben is használni fogunk, ill. bizonyosakat közülük már a bevezetés példáiban is használtunk. A csak egy-egy fejezetben használandó fogalmakat a megfelelő fejezet elején fogjuk ismertetni. Mivel a definíciókat koncentráltan helyezzük el ebben a fejezetben és néhány további fejezet első szakaszában, ezért a matematikai munkákban megszokott gyakorlattól eltérően nem tesszük oda eléjük a *Definíció* szót.

1.1. Kódelméleti alapfogalmak

Kódábécé és szimbólumok

A kódábécé egy tetszőleges q elemszámú halmaz lehet, amit a továbbiakban Z_q -val jelölünk. A Z_q kódábécé elemeit szimbólumoknak nevezzük. Ezek lehetnek például az 1-től q -ig, vagy a 0-tól $q-1$ -ig terjedő egész számok, lehetnek egymástól különböző színek, vagy tetszőleges egymástól különböző dolgok. E munka során többnyire a $Z_q = \{0, 1, \dots, q-1\}$ kódábécét használjuk, amikor tehát a kódábécé a 0-tól $q-1$ -ig terjedő egész számokból áll. Tekintsük most mindazon $(x_1, x_2, \dots, x_n)$ n -esek halmazát, melyekre minden egyes x_i a kódábécé valamelyik szimbóluma, tehát $x_1, x_2, \dots, x_n \in Z_q$, és jelöljük az így definiált halmazt Z_q^n -nel. A példák ismertetése során említettem, hogy a szimbólumoknak nem kötelező számoknak lenniük, és 0-tól kezdődniük, mégis az egyöntetűség kedvéért a továbbiakban a Z_q halmazokat általában a

$$Z_q = \{0, 1, \dots, q-1\}$$

képlettel értelmezzük, kivéve, ha külön megjegyezzük, hogy adott esetben eltérünk ettől a konvenciótól. A Z_q^n halmaz elemeit szavaknak hívjuk, melyekre esetenként használjuk a geometriában megszokott pont vagy vektor elnevezést is. Ezzel már közel jutottunk a Hamming tér fogalmához is, melynek pontjai (vektorai) a Z_q^n halmaz elemeiből állnak. A Z_q^n halmaz úgy lesz valójában Hamming tér, ha egy speciális metrikát (Hamming metrika) is értelmezzünk rajta.

Hamming távolság, Hamming metrika, Hamming tér

Két szó, $x, y \in Z_q^n$ Hamming távolsága alatt azon koordináták számát értjük, melyek az adott két szóban különböznek egymástól. A Hamming távolság szokásos jelölése $d(x, y)$. Könnyű belátni, hogy a Hamming távolság a Z_q^n halmazon egy metrikát valósít meg, ez a Hamming metrika. Ezek alapján Hamming térnek nevezzük a Hamming metrikával felruházott Z_q^n halmazt.

Kód, kódszó, hibajavító kód, térlefedő kód

Itt adjuk meg a kód általunk használt matematikai definícióját: A Hamming tér egy tetszőleges nem üres részhalmazát kódnak, e halmaz elemeit kódszavaknak nevezzük. Matematikai értelemben tetszőleges kódot tekinthetünk akár hibajavító kódnak, akár térlefedő kódnak. Az utóbbi elnevezések arról tájékoztatnak, hogy a kódot milyen célra akarjuk használni. Bármely így definiált kód esetén értelmezzük a kód legkisebb távolságát és elérési sugarát. Hibajavító kód vagy térlefedő kód (vagy egyszerűen kód) alatt tehát tetszőleges nem üres

$$C \subseteq Z_q^n$$

halmazt értünk. A különbség az, hogy egy hibajavító kód annál jobb, minél nagyobb e kód legkisebb távolsága, egy térlefedő kód pedig annál jobb, minél kisebb az elérési sugara.

Gömb a Hamming térben és szférikus korlát

Az $x \in Z_q^n$ középpontú, R sugarú gömböt a

$$B_R(x) = \{y \in Z_q^n : d(x, y) \leq R\}$$

képlettel értelmezzük. Ez az értelmezés analóg a geometriai gömb fogalmával, de lényeges különbség, hogy a Hamming térben a gömb véges, mégpedig

$$V_q(n, R) = \sum_{i=0}^R \binom{n}{i} (q-1)^i$$

számú pontból áll.

Mivel egy térlefedő kód bármely kódszava a Hamming tér $V_q(n, R)$ számú pontját fedi, ebből azonnal adódik az úgynevezett szférikus korlát:

$$K_q(n, R) \geq \left\lceil \frac{q^n}{V_q(n, R)} \right\rceil.$$

Ezért a

$$\left\lceil \frac{q^n}{V_q(n, R)} \right\rceil = \left\lceil \frac{q^n}{\sum_{i=0}^R \binom{n}{i} (q-1)^i} \right\rceil$$

kifejezést a $K_q(n, R)$ kifejezés *prompt alsó korlátjának* is nevezzük.

Legkisebb távolság (kódtávolság)

Egy $C \subseteq Z_q^n$ kód legkisebb távolsága, vagy más elnevezéssel kódtávolsága alatt a kódszavak közötti Hamming távolságok minimumát értjük. Képlettel

$$d_{\min}(C) = \min\{d(x, y) : x, y \in C, x \neq y\}.$$

A legkisebb távolság definíciójából következik, hogy a $c \in C$ kódszavakhoz tartozó $e = \lfloor (d_{\min}(C) - 1)/2 \rfloor$ sugarú $B_e(c)$ gömbök páronként diszjunktak.

Elérési sugár

Egy $C \subseteq Z_q^n$ kód elérési sugara az a legkisebb R egész, melyre teljesül, hogy a Z_q^n Hamming tér tetszőleges eleme legalább egy kódszótól legfeljebb R távolságra van. Képlettel

$$R = \max_{x \in Z_q^n} d(x, C).$$

Az x pont és a C halmaz távolsága alatt a szokásos módon x -nek és C pontjai közül a hozzá legközelebbi pontnak a távolságát értjük, képlettel

$$d(x, C) = \min_{y \in C} d(x, y).$$

Az elérési sugár definíciójából következik, hogy a $c \in C$ kódszavakhoz tartozó R sugarú $B_R(c)$ gömbök egyesítése kiadja a teljes Z_q^n teret. Ennélfogva $e \leq R$, tehát a kódtávolság és az elérési sugár között mindig fennáll a

$$d_{\min}(C) \leq 2R + 1 \quad (1.1)$$

összefüggés.

Kód mérete, alapszáma, dimenziója

Egy $C \subseteq Z_q^n$ kód mérete alatt a kódszavak számát (vagyis a véges C halmaz számosságát, elemeinek a számát), alapszáma alatt a q egészet, dimenziója alatt a tér dimenzióját, vagyis az n egészet értjük.

Megjegyzések:

1. A kód dimenzióját tekintve a fenti értelmezés szerint eltértünk a dimenzióknak a lineáris kódok esetében szokásosan használt fogalmától, mivel a főleg lineáris kódokat tárgyaló kódelméleti publikációkban a dimenziót a lineáris kód mint altér dimenziójaként értelmezik. Mivel e munkában főleg nem-lineáris kódokról lesz szó, célszerű ettől eltérni, ugyanis körülményes lenne a koordináták számára más szót használni, mint a dimenzió szót. Inkább a lineáris kód mint altér dimenzióját fogjuk másképp kifejezni ott, ahol szükség lesz annak használatára.

2. A kód fenti definíciója szerint alapértelmezésben ugyanaz a kódszó egy kódon belül nem ismétlődhet. Néha ezt a követelményt kénytelenek leszünk feloldani (elsősorban kódok összefűzése esetén), anélkül, hogy erre külön felhívnánk a figyelmet. Ezért itt jegyezzük meg, hogy a kódok méretére (kódszavak számára) vonatkozó állításokon kívül minden egyéb tételünk és egyéb állításunk érvényes abban az esetben is, ha a kódszavak ismétlődését megengedjük.

$\{c_1, c_2, \dots, c_M\}$

séma mintájára adjuk meg. Amennyiben a $c_i = (c_{i1}, c_{i2}, \dots, c_{in})$ kódszavak koordinátáit is konkrétan meg akarjuk adni, akkor a kód részletes sémája

[illegible]

$$\begin{array}{cccc} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \dots & \dots & \dots & \dots \\ c_{M1} & c_{M2} & \dots & c_{Mn} \end{array}$$

Adott paraméterekkel rendelkező kód jelölése

Optimális hibajavító kód, optimális térlefedő kód

Adott q alapszám, n dimenzió és R elérési sugár esetén a q, n, R paraméterekhez tartozó optimális térlefedő kódok mindazok a kódok, melyek elérési sugara legfeljebb R és a kódszavak száma a lehető legkisebb.

A q, n, R paraméterekhez tartozó optimális térlefedő kódok méretére a $K_q(n, R)$ jelölést használjuk. Más szavakkal: $K_q(n, R)$ a q alapszámhoz tartozó n dimenziós, legfeljebb R elérési sugárral rendelkező kódok méretének (kódszavai számának) a minimuma. Bináris kód ($q = 2$) esetén a q alsó indexet el lehet hagyni, tehát $K_2(n, R)$ és $K(n, R)$ ugyanazt jelenti.

15

Rekord-tartó kód

Egy térlefedő kódot rekord-tartónak nevezünk, ha az adott időpontban a legjobb ismert kód az adott q , n , R paraméterekre. Ha egy rekord-tartó térlefedő kód M kódszóból áll, akkor tehát $K_q(n, R) \leq M$. Míg egy optimális kód örökre optimális marad, egy rekord-tartó kód általában csak időlegesen rekord-tartó, ha ugyanis annál jobb kódot talál valaki, akkor a talált új kód lép a korábbi rekord-tartó kód helyére.

Perfekt kód

Egy $(n, M)_q R$ kód perfekt, ha a Z_q^n tér tetszőleges x pontja egy és csak egy kódszóból érhető el R sugarú gömbbel. Nyilvánvaló, hogy perfekt kód csak páratlan $d_{\min}$ kódtávolság esetén létezik és perfekt kód esetén (1.1) egyenlőséggel teljesül, vagyis az elérési sugár és a legkisebb távolság között fennáll a $d_{\min} = 2R + 1$ összefüggés, továbbá minden perfekt kód egyszerre optimális hibajavító kód és optimális térlefedő kód.

Ha létezik perfekt $(n, M)_q R$ kód, akkor az egyszeres fedés következtében

$$K_q(n, R) = \frac{q^n}{V_q(n, R)}. \quad (1.3)$$

Az ellenkező esetben viszont, vagyis ha nem létezik perfekt $(n, M)_q R$ kód, akkor az átfedések miatt

$$K_q(n, R) > \frac{q^n}{V_q(n, R)}.$$

Ismétléses kód

Ismétléses kód tetszőleges $n, q \geq 2$ esetén a Z_q^n tér azonos koordinátájú pontjaiból álló kód (az első kódszó csupa 0, a második kódszó csupa 1 stb.). Egy ismétléses kód elérési sugara a skatulya elv alapján könnyen bizonyíthatóan

$$R = \left\lfloor \frac{n(q-1)}{q} \right\rfloor = \left\lceil \frac{(n-1)(q-1)}{q} \right\rceil. \quad (1.4)$$

Térlefedő kódok konstrukciója szempontjából elsősorban azok az ismétléses kódok érdekesek, melyekre $n = q + 1$ és ennél fogva $R = q - 1$. Ezek ugyanis normális kódok a következő szakasz elején adott definíció értelmében.

Vegyes kódok

Vegyes kód alatt legáltalánosabban a $Z_{q_1}^{n_1} Z_{q_2}^{n_2} \dots Z_{q_m}^{n_m}$ tér valamely nem üres részhalmazát értjük, ahol $m \geq 1$, $n_i \geq 0$, $\sum_{i=1}^m n_i \geq 1$ és $q_i \geq 2$. Értelmezésünkben a vegyes kód nem alternatívája a tiszta (fix alapszámú) kódnak, hanem annál általánosabb. Így például a vegyes ternáris/bináris kódok közé értjük akár a tisztán ternáris, akár a tisztán bináris kódokat. A $K_q(n, R)$ kifejezéshez hasonlóan használjuk vegyes kódok esetén a $K_{q_1, q_2, \dots, q_m}(n_1, n_2, \dots, n_m; R)$ kifejezést.

Könnyen verifikálható, hogy az előbbieken értelmezett fogalmak jó része értelemszerűen átvihető vegyes kódok esetére is.

Ekvivalens és inekvivalens kódok

Tetszőleges Hamming tér esetén két kódot ekvivalensnek nevezünk, ha a koordináták alkalmas permutációjával, majd koordinátánként a szimbólumok (koordinátánként egymástól független) permutációjával egyikből a másik megkapható. Ha ily módon nem kaphatók meg egymásból, akkor a két kód inekvivalens. Vegyes Hamming tér esetén természetesen a koordinátákra alkalmazható permutációik halmazát értelemszerűen szűkíti az a megszorítás, hogy csak azonos rendű koordináták cserélhetők fel egymással, vagyis csak olyan koordináták, melyek ugyanahhoz a $Z_{q_i}^{n_i}$ -hez tartoznak.

1.2. Speciális fogalmak

Normális és abnormális kód

Legyen C egy $(n, M)_q R$ kód, i pedig egy tetszőleges index ($1 \leq i \leq n$). Jelölje C_j azon kódszavak halmazát, melyekben az i -edik koordináta-helyen a j érték áll ($0 \leq j \leq q-1$). Azt mondjuk, hogy a C kód normális az i -edik koordinátára vonatkozóan (röviden: az i -edik koordinátában), ha tetszőleges $x \in Z_q^n$ esetén fennáll

$$\sum_{j=0}^{q-1} d(x, C_j) \leq qR + q - 1. \quad (1.5)$$

Valamely C kód definíció szerint abnormális, ha egyetlen koordinátában sem normális.

Megjegyezzük, hogy a fenti definíció értelmében normális tulajdonság a tapasztalatok szerint bináris kód esetén az optimális, ill. térlefedés szempontjából „jó” kódok túlnyomó többségét jellemzi, $q > 2$ esetén viszont sajnos ezzel éppen ellentétesek a tapasztalatok, és azt mutatják, hogy $q = 3$ vagy ennél nagyobb alapszám esetén nagyon kevés a normális kód.

Különösen hangsúlyozni szeretném, hogy az „abnormális” jelzőnek itt nincs pejoratív értelme, hanem csupán azt fejezi ki, hogy valamely kód nem rendelkezik egy meghatározott tulajdonsággal. Ismeretes, hogy a nem bináris perfekt kódok kivétel nélkül mind abnormálisak a fenti definíció értelmében, holott ezek a létező legököltelesebb kódoknak tekinthetők.

Az $R = 1$ elérési sugarú *bináris* perfekt kódok viszont bizonyítottan normálisak, hiszen [62] (Theorem 1) szerint $n \geq 3$ esetén minden 1 elérési sugarú bináris optimális térlefedő kód normális minden koordinátában. Ugyanebből a cikkből (Theorem 6, ill. Theorem 7) azt is megtudjuk, hogy ha C egy bináris $(n, M)_1$ kód, melyre $M \leq 95$ vagy $n \leq 8$, akkor C normális kód.

Normális kódra legegyszerűbb példa tetszőleges q esetén az $n = q+1$ dimenziós ismétléses kód.

Kiegyensúlyozott és kiegyensúlyozatlan kód

Egy $C \subseteq Z_q^n$ kód kiegyensúlyozott, ha valamennyi $i \in \{1, 2, \dots, n\}$ koordinátára fennáll, hogy az i -edik koordináta-helyen tetszőleges $j \in \{0, 1, \dots, q-1\}$ szimbólum a kódszavakban együttesen $\lfloor n/q \rfloor$ vagy $\lceil n/q \rceil$ alkalommal fordul elő. Ellenkező esetben a C kód kiegyensúlyozatlan.

Szűrjektív és általánosított szűrjektív kód

Valamely $C \subseteq Z_q^n$ kód s -szűrjektív, ha a tér koordinátáinak tetszőleges $\{a_1, a_2, \dots, a_s\}$ halmazára, tetszőleges $(b_1, b_2, \dots, b_s) \in Z_q^s$ választása esetén létezik legalább egy olyan $(c_1, c_2, \dots, c_n) \in C$ kódszó, melyre fennáll $c_{a_i} = b_i$ minden i ($1 \leq i \leq s$) esetén.

Valamely $C \subseteq Z_q^n$ kód r sugárral s -szűrjektív, ha a tér koordinátáinak tetszőleges $\{a_1, a_2, \dots, a_s\}$ halmazára, tetszőleges $(b_1, b_2, \dots, b_s) \in Z_q^s$ választása esetén létezik legalább egy olyan $(c_1, c_2, \dots, c_n) \in C$ kódszó, melyre fennáll $c_{a_i} = b_i$ legalább $s - r$ számú i ($1 \leq i \leq s$) esetén.

Az utóbbi – adott r sugárral s -szűrjektív kód – általam ([129],[135]) bevezetett fogalma egyszerre általánosítása a hagyományos értelemben vett szűrjektív kódnak ($r = 0$ esetén) és a térlefedő kódnak ($s = n$ esetén).

Mindkét fajta szűrjektív kód fogalma igen hasznosnak bizonyult térlefedő kódok méretének vizsgálatához.

A $\sigma_q(n, s)$, $\sigma_q(n, s; r)$ kifejezések értelmezése

Jelölje $\sigma_q(n, s)$ a q alapszámhoz tartozó n dimenziós s -szűrjektív kódok méretének a minimumát, $\sigma_q(n, s; r)$ pedig a q alapszámhoz tartozó n dimenziós, legfeljebb r sugárral s -szűrjektív kódok méretének a minimumát.

Szavak és kódok összefűzése

Az $x \in Z_{q_1}^{n_1}$ és $y \in Z_{q_2}^{n_2}$ szavak összefűzésének eredménye az az $|x|y| \in Z_{q_1}^{n_1} Z_{q_2}^{n_2}$ szó, melyben x komponensei után y komponensei következnek. (Itt q_1 és q_2 lehet akár egyenlő, akár különböző.)

Legyenek $x_1, x_2 \in Z_{q_1}^{n_1}$ és $y_1, y_2 \in Z_{q_2}^{n_2}$, ekkor a Hamming távolság definíciója alapján nyilvánvalóan fennáll

$$d(|x_1|y_1|, |x_2|y_2|) = d(x_1, x_2) + d(y_1, y_2). \quad (1.6)$$

Két azonos méretű $C = \{c_1, c_2, \dots, c_M\} \subseteq Z_{q_1}^{n_1}$ és $D = \{d_1, d_2, \dots, d_M\} \subseteq Z_{q_2}^{n_2}$ kód összefűzésének eredménye (konkaténáltja) a

$$|C|D| = \{|c_1|d_1|, |c_2|d_2|, \dots, |c_M|d_M|\} \subseteq Z_{q_1}^{n_1} Z_{q_2}^{n_2}$$

kód.

Legyen C elérési sugara $R(C)$, D elérési sugara pedig $R(D)$, ekkor az összefűzéssel nyert $|C|D|$ kód $R(|C|D|)$ elérési sugarára (1.6) következtében fennáll

$$R(|C|D|) \geq R(C) + R(D). \quad (1.7)$$

1.3. Véges testek és lineáris kódok

Mivel e munkában konkrétan előállított formában csak legfeljebb 10 alapszámú kódok fordulnak elő, a véges testek közül is csak a 10-nél nem több elemből álló véges testeket tekintjük át. Ezek struktúrájának és műveleti szabályainak leírását igyekszem – a véges testek szokásos tárgyalásmódjától eltérően – olyan módon kifejteni, hogy az algebrai struktúrák területén kevésbé jártas olvasó számára is érthető, és számítógépen könnyen programozható legyen nemcsak prím, hanem prímhatvány alapszám esetén is.

Véges test fogalma

Egy $q \geq 2$ elemű véges F_q halmazt véges testnek nevezünk, ha tetszőleges két eleme között értelmezve van két művelet: összeadás és szorzás, és ezek rendelkeznek a következő tulajdonságokkal:

1. F_q az összeadásra nézve kommutatív csoport, azaz F_q az összeadás műveletre kommutatív, asszociatív és zárt, továbbá van nulleleme (0_q), és minden elemnek van ellentettje.
2. A 0_q nullelem nélkül F_q elemei a szorzásra nézve kommutatív csoportot alkotnak, azaz, $F_q \setminus \{0_q\}$ a szorzási műveletre kommutatív, asszociatív és zárt, továbbá van egységeleme (1_q), és 0_q kivételével minden elemnek van a szorzásra nézve inverze.
3. Tetszőleges $x, y, z \in F_q$ esetén fennállnak a disztributivitást kifejező

$$x(y + z) = xy + xz, (x + y)z = xz + yz$$

egyenlőségek.

Ismeretes, hogy q elemű véges test csak prím vagy prímhatvány q esetén létezik. A véges test angol elnevezése finite field vagy Galois field, gyakori jelölése az utóbbi kifejezés kezdőbetűi alapján $GF(q)$, de szokásos a fent használt F_q jelölés is.

Prím elemszámú véges test

Ha p prímszám, akkor a p szerinti maradékosztályok, vagy ha jobban tetszik, a $0, 1, 2, 3, \dots, p-1$ egészek, a közönséges értelemben vett összeadás és szorzás eredményét modulo p véve, p elemű véges testet alkotnak. Ha precízek akarunk lenni, akkor annak jelzésére, hogy a műveleteket nem a közönséges aritmetika szerint végezzük, a p elemű véges test elemeit a p indexszel ellátva, a $GF(p)$ testben a műveleteket a következőképpen definiáljuk:

$$a_p + b_p = (a + b \pmod{p})_p,$$

és a szorzásra hasonlóan

$$a_p \cdot b_p = (a \cdot b \pmod{p})_p.$$

Prímhatvány elemszámú véges test

Prímhatvány $q = p^k$ elemszám esetén a $GF(q)$ véges test elemeit $GF(p)$ elemeiből vett komponensek által alkotott k dimenziós vektorokként értelmezhetjük, melyek összeadását komponensenként, a $GF(p)$ -ben értelmezett aritmetika szerint végezhetjük, a szorzást azonban – p és k értékétől függő – sajátos előírás szerint kell értelmeznünk ahhoz, hogy

valóban véges testhez jussunk. Megadjuk a $q = 4, 8$ és 9 elemű véges testek elemei szorzásának egy lehetséges módját.

1. Ha $x = (x_1, x_2)$ és $y = (y_1, y_2)$ a $\text{GF}(4)$ test elemei, ahol tehát $x_1, x_2, y_1, y_2 \in \text{GF}(2)$, akkor legyen

$$xy = (x_1y_1 + x_1y_2 + x_2y_1, x_1y_1 + x_2y_2),$$

ahol a jobb oldalon álló vektor komponenseire a műveleteket a $\text{GF}(2)$ -ben érvényes aritmetikai szerint végezzük.

2. Ha $x = (x_1, x_2, x_3)$ és $y = (y_1, y_2, y_3)$ a $\text{GF}(8)$ test elemei, akkor elvileg hasonló módon, azonban az erre az esetre vonatkozó alábbi szorzási szabállyal számolhatunk:

$$xy = (x_1y_1 + x_1y_3 + x_2y_2 + x_3y_1, x_1y_1 + x_1y_2 + x_2y_1 + x_2y_3 + x_3y_2, x_1y_2 + x_2y_1 + x_3y_3).$$

3. Ha $x = (x_1, x_2)$ és $y = (y_1, y_2)$ a $\text{GF}(9)$ test elemei, ahol tehát $x_1, x_2, y_1, y_2 \in \text{GF}(3)$, akkor legyen

$$xy = (x_1y_1 + x_1y_2 + x_2y_1, x_1y_1 + x_2y_2),$$

ahol a jobb oldalon álló vektor komponenseire a műveleteket a $\text{GF}(3)$ -ra érvényes aritmetikai szerint végezzük.

Egyszerű, bár a két utóbbi esetben kézzel kicsit hosszadalmas számolással be lehet látni, hogy a fent megadott módon valóban véges testhez jutunk, melyek zérus eleme $0_4 = (0_2, 0_2)$, $0_8 = (0_2, 0_2, 0_2)$, ill. $0_9 = (0_3, 0_3)$, egység eleme pedig $1_4 = (0_2, 1_2)$, $1_8 = (0_2, 0_2, 1_2)$, ill. $1_9 = (0_3, 1_3)$.

A továbbiakban a szabatos definíció kedvéért bevezetett, de nehézkes, az egész számok és a véges testek elemei megkülönböztetésére használt alsó indexeket elhagyjuk.

Lineáris kód

Egy $C \subset Z_q^n$ kód lineáris kód, ha Z_q véges test, és teljesül, hogy bármely két kódszó összege és bármely kódszónak a Z_q test elemeivel vett szorzata kódszót eredményez, ahol az összeadást, ill. szorzást koordinátánként végezzük a Z_q véges test műveleti szabályai szerint.

Lineáris kód tehát csak azokra a q alapszámokra értelmezhető, melyekre létezik q elemszámú véges test, tehát q prím vagy prímhatvány.

Egy lineáris kód leírásához elég a kódszavaknak egy maximális lineárisan független rendszerét megadni, ennek elemei a generáló kódszavak. Az utóbbiak a Z_q térnek egy alterét generálják, melynek pontjai egyúttal a lineáris C kód kódszavai.

Generátor mátrix és paritás-ellenőrző mátrix

Legyen Z_q egy q elemű véges test, $C \subset Z_q^n$ pedig a $g_1, g_2, \dots, g_k$ kódszavak által generált lineáris kód. A generáló kódszavakból mint sorvektorokból álló $k \times n$ méretű G mátrixot a C kód generátor mátrixának nevezzük. A generátor mátrixból tehát a C kód a

$$C = \{vG : v \in Z_q^k\} \quad (1.8)$$

formulával adódik.

Ugyanezen C kód paritás-ellenőrző mátrixa bármely olyan $(n - k) \times n$ méretű mátrix, melyre fennáll

$$C = \{x : Hx^T = 0\}. \quad (1.9)$$

Gyakran a generátor mátrix megadható úgy, hogy tartalmazza a $k \times k$ méretű I_k egységmátrixot, tehát $G = (I_k \ A)$ alakban particionálható, ahol A egy $(n - k) \times k$ méretű mátrix. Ebben az esetben az (1.8) formula a kód

$$C = \{(v \ vA) : v \in Z_q^k\} \quad (1.10)$$

előállítását eredményezi. Ekkor a $H = (-A^T \ I_{n-k})$ mátrixra és az (1.10) képletben szereplő $x = (v \ vA)$ vektorra fennáll (1.9). Ha viszont valamely $x = (x_1 \ x_2)$ vektorra (ahol $x_1 \in Z_q^k$ és $x_2 \in Z_q^{n-k}$) és a $H = (-A^T \ I_{n-k})$ mátrixra teljesül az (1.9)-ben megadott egyenlőség, tehát $-A^T x_1^T + x_2^T = 0$, akkor ebből $x_2 = x_1 A$ adódik, és következésképpen az $(x_1 \ x_2)$ vektor eleme az (1.10) jobb oldalán álló halmaznak. Ezzel megmutattuk, hogy a $H = (-A^T \ I_{n-k})$ mátrix paritás-ellenőrző mátrixa a $G = (I_k \ A)$ mátrixszal generált lineáris kódnak.

Mellékosztály, szindróma

Legyen Z_q továbbra is véges test, $C \subset Z_q^n$ lineáris kód, $x \in Z_q^n$ pedig a Hamming tér tetszőleges pontja. Ekkor az

$$\{x + c : c \in C\} \quad (1.11)$$

halmazt az x pont által meghatározott mellékosztálynak nevezzük. Nyilvánvalóan bármely lineáris kód esetén a Z_q^n tér a mellékosztályok diszjunkt egyesítése, ahol x_1 és x_2 akkor és csak akkor van ugyanabban a mellékosztályban, ha $x_1 - x_2 \in C$.

Ha a C kód $k \times n$ méretű G mátrixszal generálható, akkor a mellékosztályok száma $q^n/q^k = q^{n-k}$, mivel (1.11) szerint minden mellékosztály ugyanannyi elemet tartalmaz. A mellékosztályok egyike maga a C kód.

Adott $C \subset Z_q^n$ lineáris kód, H paritás-ellenőrző mátrix és tetszőleges $x \in Z_q^n$ pont esetén az x pont szindrómájának nevezzük a Hx^T oszlopvektort. Az (1.9) formula alapján látható, hogy minden kódszó szindrómája a zéró vektor, továbbá két vektor akkor és csak akkor van ugyanabban a mellékosztályban, ha szindrómájuk megegyezik.

2. fejezet

A térlefedő kódok rövid története

Ebben a fejezetben a térlefedő kódok területén elért eredmények történetét általánosabb vonásaiban ismertetjük, ez azonban nem zárja ki egyes lényegesebb konkrét példák említését. Adott paraméter értékekhez tartozó optimális vagy rekord-tartó kódok méretére, ill. annak alsó és felső korlátjára vonatkozó állandóan fejlődő, gyarapodó ismeretek történetét a tárgyalásra kerülő kód kategóriák körébe tartozó kódok áttekintését szolgáló részekben ismertetjük. Így bináris kódokra a 3.8, ternáris kódokra a 4.6, magasabb rendű kódokra a 5.7–5.9, vegyes kódokra pedig a 6.6 szakasz is félig-meddig történeti célzatú, de egyúttal konkrét egyedi kódok, kód-csoportok jellegzetességeinek egyes részleteit is tartalmazza.

2.1. Kezdetek

A térlefedő kódok elmélete és módszerei a XX. század első felében, döntően az alábbi három eredet mentén alakultak ki: 1. A hibajavító és hibafelismerő kódok kutatása, melynek első lényegesebb eredményei R. Hamming és M. Golay nevéhez fűződnek. 2. Algebrai kódelméleti kutatások és perfekt kódokra vonatkozó további eredmények. 3. Hatékony totó-kombinációk világszerte kibontakozott kutatása.

2.1.1. Hibajavító és hibafelismerő kódok kutatása

A hibajavító kód és a hibafelismerő kód kifejezés differenciáltabban fejezi ki azt a fogalmat, amit az 1.1 szakaszban hibajavító kódként értelmeztünk. Ha a C kód $d_{\min}(C)$ kódtávolsága páratlan, akkor bármely kódszót legfeljebb $(d_{\min}(C) - 1)/2$ hiba esetén ki tudunk javítani, ha viszont páros, akkor bármely kódszót legfeljebb $d_{\min}(C)/2$ hiba esetén fel tudunk ismerni. Ezért a 2 kódtávolságú kódokat 1-hibafelismerő kódnak, a 3 kódtávolságú kódokat 1-hibajavító kódnak, a 4 kódtávolságú kódokat 2-hibafelismerő kódnak, az 5 kódtávolságú kódokat 2-hibafelismerő kódnak nevezik stb.

A hibajavító és hibafelismerő kódoknak fontos gyakorlati jelentősége van a számítógéptudományban, a távközlésben és az információelméletben, s igen nagy lökést adott ezek

fejlődésének, amikor Golay [4] 1949-ben, ill. Hamming [5] 1950-ben ismertette a később az ő nevükről elnevezett kódok alkalmazásának módját az említett szakterületeken. Mivel ezek mind perfekt kódok, kézenfekvő volt felismerni ezek alkalmazásának lehetőségét térlefedő kódok gyanánt is. Az utóbbiak iránt is érdeklődő kutatók ezt követően meghatározták más, később felfedezett hibajavító kódok elérési sugarát, és ezáltal újabb térlefedő kódokat teremtettek. Később azonban kiderült, hogy a (nem perfekt) jó hibajavító kódok általában nem túl jók térlefedési célra (és ez fordítva is fennáll: a jó térlefedő kódok általában nem túl jók hibajavítási célra).

2.1.2. Algebrai kódelméleti kutatások és további perfekt kódok felfedezése

Egy érdekes lefedési problémát csoportelméleti megfogalmazásban vetett fel Taussky és Todd [3] 1948-ban: Legyen G egy n báziselemet tartalmazó Abel csoport, ahol minden báziselem rendje d . Jelöljük S -sel a báziselemek $n(d-1)+1$ különböző hatványának a halmazát. A szerzők feltették azt a kérdést, hogy mennyi az a legkisebb $\sigma = \sigma(n, d)$ egész szám, melyre létezik G -nek σ elemből álló H részhalmaza úgy, hogy $G = HS$? (HS alatt a $\{hs : h \in H, s \in S\}$ halmaz értendő.) Mindjárt megmutatták egyebek között, hogy $\sigma(4, 3) = 9$ és $\sigma(7, 2) = 16$. Ebből a jelenleg használt jelölésekkel az adódik, hogy $K_3(4, 1) = 9$ és $K(7, 1) = 16$.

Az [3] cikkekre reagálva, Mattioli [6] 1950-ben, ugyancsak algebrai megfogalmazásban, bebizonyította, hogy ha p prím és $k \geq 2$ egész, akkor

$$K_p\left(\frac{p^k - 1}{p - 1}, 1\right) = p^{\frac{p^k - 1}{p - 1} - k}.$$

Mattiolitól függetlenül ugyanezt az eredményt találta Mauldon [7] szintén 1950-ben és Zaremba [8] 1951-ben, amit aztán Zaremba [9] 1952-ben prímről prímszámokra általánosított. Az említett publikációkban tehát a szerzők felfedezték a tetszőleges prím, ill. prímszám alapszámú lineáris perfekt kódokat.

Végül itt említjük meg Fontaine és Peterson [11] 1959-ben megjelent publikációját, amelyben a szerzők lineáris kóddal bizonyítják a $K(14, 3) \leq 64$ felső korlátot, amely jelenleg is az ismert legjobb felső korlát.

2.1.3. Hatékony totó-kombinációk kutatása

Mivel a mai totóhoz hasonló sportfogadásokat már a 19. században is szerveztek, feltételezhető, bár nincs rá bizonyíték, hogy ugyanabban az időszakban már egyes totó-kombinációk is készültek, amik egyúttal térlefedő kódokat valósítottak meg. Az 1940-es évektől kezdve viszont már totó magazinok is kiadásra kerültek a skandináv országokban, Olaszországban, Görögországban és talán még másutt is, melyekben sok érdekes totó-kombinációs struktúra kinyomtatásra került, így például bináris kódok esetére a $K(7, 1) \leq 16$ egyenlőtlenséget bizonyító struktúra (Hamming kód), amit [168] szerint

egy bizonyos Ericson már 1936-ban, tehát jóval Hamming felfedezése előtt ismert és alkalmazott. Ugyanezen forrás szerint a $K(5, 1) \leq 7$ és $K(6, 1) \leq 12$ egyenlőtlenséget bizonyító struktúrát Di Nasso 1950-ben alkotta meg.

Ternáris esetre pl. a $K_3(3, 1) \leq 5$ egyenlőtlenséget bizonyító totó célú struktúrát a dán Weikel 1943-ban, a $K_3(6, 2) \leq 17$ egyenlőtlenséget bizonyító struktúrát ugyancsak Weikel 1960-ban, a $K_3(5, 2) \leq 8$ egyenlőtlenséget bizonyító struktúrát a svéd Himberg 1970-ben, a $K_3(10, 1) \leq 3645$ egyenlőtlenséget bizonyító struktúrát egymástól függetlenül az olasz Cercone De Lucia 1962-ben és a finn Heikkonen 1967-ben találta és ismertette. A felsorolt esetekre vonatkozó felső korlátoknál ma sem ismerünk jobbat.

A $K_3(11, 2) \leq 729$ egyenlőtlenséget bizonyító, tehát a Golay kóddal ekvivalens struktúrát a finn Virtakallio totó-kombináció formájában már 1947-ben publikálta, és így vitathatatlanul megelőzte Golay felfedezését, de nem gondolt arra, hogy e felfedezést hibajavítási célra is alkalmazni lehetne. Ugyanez a finn férfiú a bináris esetre vonatkozó $K(11, 1) \leq 192$ egyenlőtlenséget bizonyító struktúrát 1946-ban találta.

Még több, már az 1940-es, 1950-es években felfedezett totó célú struktúrát lehetne felsorolni a vegyes ternáris/bináris esetre. Csak néhányat említve, a $K(2, 6; 1) \leq 64$ egyenlőtlenséget bizonyító struktúrát Stene 1947-ben, a $K(1, 4; 1) \leq 8$ és a $K(2, 2; 1) \leq 6$ egyenlőtlenséget bizonyító struktúrát Di Nasso 1950-ben, a $K(6, 4; 1) \leq 864$ egyenlőtlenséget bizonyító struktúrát Cavallaro 1963-ban találta.

A jelenlegi időszakban is születnek sportfogadási eredetű rekord-javító térlefedő kódok. A legutóbbiak közé tartozó érdekesebb eredmények a Rivas Soriano által 2009. január hónapban készített, a ternáris esetre a $K_3(13, 4) \leq 340$ egyenlőtlenséget, ill. a vegyes ternáris/bináris esetre a $K(9, 1; 3) \leq 91$ egyenlőtlenséget bizonyító kód, valamint a Bertolo, Di Pasquale és Santisi által 2008. december hónapban készített, a $K(9, 3; 2) \leq 1184$ egyenlőtlenséget bizonyító kód.

2.2. 1967–1975 közötti eredmények

2.2.1. Rodemich egyenlőtlenségei

Ezekben az években több jelentős cikk jelent meg a térlefedő kódok témaköréből. Ide kapcsolható Golomb és Posner [15] cikke, amely ugyan valamivel korábban, 1964-ben jelent meg, és amely a latin négyzeteknek a Hamming terekre való alkalmazhatóságát elemzi. A [15] cikk hatással volt Rodemich [24] munkájára, aki ebben az 1970-ben megjelent cikkben több jelentős, ma is gyakran idézett általános egyenlőséget és egyenlőtlenséget bizonyított. Ilyenek az 5.5 szakasz (g) pontjában felírt egyenlőség, ill. az ugyanabban a szakaszban felhasznált $K_q(n, n-2) \geq \frac{q^2}{n-1}$ általános egyenlőtlenség, valamint ennek párja, a $K_q(n, 1) \geq \frac{q^{n-1}}{n-1}$ általános egyenlőtlenség. Rodemich egyenlőtlenségeiből adódhatnak konkrétan, egyebek között a [135] cikkben megadott $K_7(4, 1) \geq 115$, $K_8(4, 1) \geq 171$, $K_6(4, 2) \geq 13$, $K_7(4, 2) \geq 17$, $K_8(5, 3) \geq 17$, $K_9(5, 3) \geq 21$ alsó korlátok, melyeket az utóbbi cikk megjelenésétől (2005) máig senkinek nem sikerült megjavítania.

2.2.2. Kalbfleisch, Stanton és szerzőtársaik publikációi

Horton, Kalbfleisch, Stanton és Weiland 1969 és 1971 között több cikkben [17, 18, 19, 20, 21, 22, 25] foglalkoztak térlefedő kódok konstrukciójával, és egyúttal az alsó korlátokat is vizsgálták. Bebizonyították a $K_q(3, 1) = \left\lceil \frac{q^2}{2} \right\rceil$ általános egyenlőséget, ehhez először ők használták szűrjektív kódok egyesítését térlefedő kódok konstrukciója céljából. Megalkották az adjungált kódok módszerét, amit hatékonyan alkalmaztak elsősorban 1 elérési sugarú perfekt kódokra, és ők bizonyították be először, hogy $K(6, 1) = 12$ és $K_4(4, 1) = 24$. Az első publikált klasszifikációs eredmények is tőlük származnak, nevezetesen bebizonyították a $K(5, 1) = 7$ és $K_3(4, 1) = 9$ egyenlőséghez tartozó optimális térlefedő kód unicitását, továbbá megadták a $K(4, 1) = 4$ egyenlőséghez tartozó optimális kódokat.

2.2.3. Kamps és van Lint publikációi

Kamps és van Lint két cikkben [16] és [23] foglalkozott térlefedő kódokkal. Az első, 1967-ben megjelent cikkben még csak egy konkrét esettel foglalkoztak és bebizonyították a $K_3(5, 1) = 27$ egyenlőséget, melynél a nehézséget annak bizonyítása jelentette, hogy $K_3(5, 1)$ értéke nem lehet 27-nél kevesebb. A másik, 1970-ben megjelent cikkükben bevezették az ún. mátrix módszert, ami máig igen hatékony eljárásnak bizonyult – viszonylag nagyobb méretek esetén is – térlefedő kódok konstrukciójára.

2.2.4. Helgert konstrukciója és Johnson egyenlőtlensége a szférikus alsó korlát élesítésére (1972)

1972-ből két publikációt lehet említeni, melyek egy-egy konkrét esettel foglalkoznak. Helgert [28] cikke a $K(14, 3) \leq 64$ egyenlőtlenséget bizonyító kódra ad egy konstrukciót. (Igaz, hogy a már említett [11] publikációban lényegében ugyanez az eredmény már korábban közlésre került.) Johnson [29] cikke alsó korlátokra vonatkozó formulákat ad meg ugyancsak a bináris esetre. Ezek egyikéből, a páros n esetre bizonyított $K(n, 1) \geq \frac{2^n}{n}$ egyenlőtlenségből, amely a szférikus alsó korlát egy speciális esetének élesítése, következik a $K(2^h, 1) = 2^{2^h-h}$ egyenlőség. Ezeket az összefüggéseket később, nem ismerve a [29] cikket, van Wee [52] újra felfedezte és közölte.

2.2.5. Delsarte és Goethals, ill. Lindström eredményei perfekt kódokra (1975)

1972 és 1983 között egy évtizednyi szünet következett a kimondottan térlefedő kódok témában megjelent publikációk közlésében, viszont e témához is érdekes új ismereteket szolgáltatottak a perfekt kódokra vonatkozó 1975-ben megjelent alábbi eredmények: Delsarte és Goethals [36] bebizonyították a 23 bináris koordinátát tartalmazó 3 elérési sugarú perfekt kód és a 11 ternáris koordinátát tartalmazó 2 elérési sugarú perfekt kód unicitását, vagyis azt, hogy minden ilyen kód ekvivalens a megfelelő Golay kóddal.

Lindström [37] munkája vegyes perfekt kódok konstrukciójára ad egy csoportelméleten alapuló érdekes módszert, és bár explicit módon nem mondja ki, mégis az általa adott konstrukcióból következik egyebek között pl. a $K_{4,2}(1, 4; 1) = 8$ és a $K_{4,2}(1, 12; 1) = 1024$ egyenlőség.

2.3. 1983–1990 közötti eredmények

2.3.1. Weber, Fernandes és Rechtschaffen, Blokhuis és Lam, Graham és Sloane, valamint Cohen, Lobstein és Sloane eredményei

Weber [40], valamint Fernandes és Rechtschaffen [41] cikke (mindkettő 1983-ban jelent meg) ternáris térlefedő kód esetére közöl új eredményt, nevezetesen Weber cikke $K_3(6, 1)$ értékére, a kétszerzős cikk pedig $K_3(7, 1)$ és $K_3(8, 1)$ értékére adja az akkor új 79, 225, ill. 567 felső korlátot az addig ismert legjobb 81, 243, ill. 729 felső korlát helyett. Ám ezt követően nagyon hamar még jobb korlátok bizonyítására került sor más szerzők által.

Blokhuis és Lam 1984-ben megjelent [42] cikke újra tárgyalja és magyarázza, példákkal illusztrálja a [23] cikkben bevezetett mátrix módszert, továbbá néhány érdekes, rekurziót eredményező egyenlőtlenséget bizonyít. Így pl. a szerzők megmutatják, hogy $K_{tq}(n, 1) \leq t^{n-1}K_q(n, 1)$, és hogy itt egyenlőség áll fenn abban az esetben, ha q prím vagy prímhatvány és $n = q + 1$. Ekkor az egyenlőtlenségből egyenlőséggé váló képlet jobb oldala a $t^q q^{q-1}$ kifejezéssé egyszerűsödik.

Graham és Sloane 1985-ben megjelent [43] cikkének egyik érdeme, hogy a lineáris bináris térlefedő kódok optimális méretének korlátaira komoly terjedelmű táblázatot is megad. Eredményeik között jelenleg két olyan korlát van, amely a nemlineáris térlefedő kódok körében is a jelenleg ismert legjobb korlát, nevezetesen $K(13, 2) \leq 128$ és $K(14, 3) \leq 64$.

Cohen, Lobstein és Sloane [46] cikke (1986) bináris térlefedő kódokkal foglalkozik, ezekre nagyon érdekes egyedi kód-konstrukciókat ismertet, valamint igen sok új általános és konkrét egyenlőséget, alsó és felső korlátot bizonyít. A cikkben közölt általános formulák pl. a $K(2R + 2, R) = 4$, $K(2R + 3, R) = 7$ egyenlőségek, valamint a $7 \leq K(2R + 4, R) \leq 12$ egyenlőtlenség. Egy nagyon szép konstrukció a $K(11, 1) \leq 192$ felső korlát bizonyítására e cikkben megadott konstrukció, amely az $S(5, 6, 12)$ Steiner rendszeren alapuló önkomplementer kód.

2.3.2. Wille, Honkala, Härmäläinen, Chen, Laarhoven, Aarts, van Lint és van Wee eredményei

Ebben az időszakban és az ezt követő évtizedekben a szerzők már számítógépes módszerek alkalmazását, valamint olyan heurisztikus módszerek alkalmazását is említik, mint a „simulated annealing” és a „tabu search” módszer. Ma is igen gyakran e két módszer valamelyikének segítségével készülnek a rekord-javító térlefedő kódok, elsősorban $R = 1$

elérési sugár esetén. A „simulated annealing” eljárást dokumentáltan Wille alkalmazta először a [49] (1987) cikkben 6 ternáris koordinátát tartalmazó rekord-javító kód készítésére, és ennek alapján bebizonyította a $K_3(6, 1) \leq 74$ korlátot.

Honkala több cikkében foglalkozik konstrukciókkal és alsó korlátok bizonyításával egyaránt. A Hämäläinen-nel közös [51] (1988) cikkben egy új, különleges módszert ismeretnek, melynek alapján új felső korlátokat találnak. A [50] cikkben a szerző néhány bináris alsó korlát javítását adja, ám jelenleg már azoknál jobb alsó korlátokat ismerünk. A Chen-nel közös [57] (1990) cikkben néhány viszonylag bonyolult formulát adnak meg a nembináris esetre a szférikus alsó korlátok javítására. Ezek alapján igen sok konkrét esetre – mind ternáris, mind magasabb alapszámú kódok ($q = 4$ és $q = 5$) esetére – közöltek olyan alsó korlátot, amely jelenleg is a legjobb ismert alsó korlát.

Ebből az időszakból származó további érdekesebb cikkek felső korlátok javítására vonatkozóan Laarhoven, Aarts, van Lint és Wille [54] (1989) és Wille [58] (1990) cikke, alsó korlátok javítására vonatkozóan pedig van Wee [52] (1988) cikke. Foglalkoznak már a szerzők a normalitás témakörével is, lásd Lobstein és van Wee [55] (1989) cikkét.

Az ebben az időszakban megjelent cikkek egy részében a szerzők táblázatba gyűjtik $K(n, R)$, ill. $K_3(n, R)$ addig ismert legjobb alsó és felső korlátját. Cohen, Lobstein és Sloane [46] (1986) cikke az $1 \leq n \leq 23$, $1 \leq R \leq 4$ tartományra adta meg $K(n, R)$ ismert legjobb korlátait, van Wee [52] (1988) ezt kiterjesztette az $1 \leq n \leq 33$, $1 \leq R \leq 10$ tartományra, az általa talált új korlátok megadásával. Chen és Honkala [57] (1990) cikke a ternáris esetre és további két alapszám esetére vonatkozó alsó és felső korlátokat gyűjti össze, mégpedig $K_3(n, R)$ korlátait a $2 \leq n \leq 14$, $1 \leq R \leq 9$ tartományban, $K_4(n, R)$ korlátait a $2 \leq n \leq 10$, $1 \leq R \leq 7$ tartományban, $K_5(n, R)$ korlátait pedig a $2 \leq n \leq 9$, $1 \leq R \leq 7$ tartományban.

2.4. 1990–2000 közötti eredmények

Az 1991-től kezdődő évtizedben, az előző évtizedekkel összehasonlítva, azokhoz képest lényegesen több térlefedő kódokról szóló cikk jelent meg, és ezek nagy része olyan nívós folyóiratokban került publikálásra, mint az IEEE Transactions on Information Theory ([61, 62, 64, 65, 67, 70, 71, 80, 85, 90, 95, 103]), Journal of Combinatorial Theory, Series A ([60, 63, 66, 77, 82, 87, 93, 96]), Designs, Codes and Cryptography ([74, 102, 114]), Journal of Combinatorial Designs ([75, 101, 118]). Ebben az időszakban, 1997-ben jelent meg „Covering Codes” címmel Cohen, Honkala, Litsyn és Lobstein 20 fejezetből álló nagyszerű munkája is, amely az első monográfiája ebben a témában. Erről külön szakaszban szólunk néhány szót az alábbiakban.

2.4.1. Cohen, Honkala, Litsyn és Lobstein könyve

A könyv tárgyát elsősorban a bináris térlefedő kódok képezik. Ezekre vonatkozó konstrukciók, külön fejezetben a lineáris konstrukciók, bináris kódokra vonatkozó normalitási kérdések, $K(n, R)$ alsó, ill. felső korlátainak képzésére vonatkozó módszerek, aszimptotikus korlátok vizsgálata, a hibajavító kódok területéről ismert néhány kód típus elérési

sugarának meghatározása stb. töltik ki a könyv első 14 fejezetét, bár a 6. fejezetben már nembináris kódok vizsgálatára is sor kerül, és az e fejezet végén lévő $-K_q(n, R)$ alsó, ill. felső korlátaira vonatkozó – táblázatok $q = 2, 3, 4$ -re és 5-re készítették el a szerzők. Két nembináris alsó korlát: $K_3(6, 3) \geq 6$ és $K_4(4, 2) \geq 7$ első bizonyítása is e könyvben található meg. A 15. fejezet vegyes ternáris/bináris kódokkal foglalkozik, a hátralévő fejezetek pedig néhány speciális témával, köztük komplexitási vizsgálatokkal foglalkoznak.

2.4.2. Hämäläinen és Rankinen közös publikációban megjelent eredményei

A két szerző [60] (1991) cikke az első olyan munka, amely egy meghatározott tartományra vonatkozóan teljeskörűen ismerteti a t ternáris, b bináris koordinátát tartalmazó, R elérési sugarú vegyes ternáris/bináris, optimális, ill. a cikk készítésének időszakában rekordtartó térlefedő kódokat. Nyolc különböző módszert sorolnak fel (a)-(h)-ig címkézve, alkalmazzák – bár elméleti megalapozás nélkül – a későbbi ADS módszernek nevezett eljárás egyszerűbb eseteit, és elkészítik a $K(t, b; R)$ kifejezés felső korlátainak a táblázatát a $0 < t + b \leq 13$, $0 < R \leq 3$ tartományban.

2.4.3. Honkala és szerzőtársai, valamint van Lint és van Wee újabb eredményei

Honkala ebben az időszakban megjelent cikkei egyrészt alsó korlátokkal ([61] és [83]) és a normalitás kérdésével foglalkoznak (a Hämäläinnel közösen készített [62] cikk). Új konstrukciós módszereket tárgyal viszont Hämäläinen, Honkala, Kaikkonen és Litsyn [74] (1993) cikke.

Van Lint és van Wee az 1991-ben megjelent [63] cikkben párhuzamosan tárgyalja és táblázatba foglalja a vegyes ternáris/bináris hibajavító, ill. térlefedő kódokat 1, 2 és 3 kitöltési sugár, ill. elérési sugár esetére. Van Wee [66] (1991) cikkében általános alsó korlátokat fogalmaz meg $K_q(n, 1)$ -re és $K_q(n, R)$ -re, majd később a [80] (1993) cikkben további hasonló korlátokat.

2.4.4. Östergård kódelméleti tevékenysége

Östergård tevékenysége különösen kiemelkedő és akár külön fejezetet is érdemelhetne a térlefedő kódok történetének ismertetésében. A [64] (1991) cikkben a $K(10, 1) \leq 120$ felső korlátot bizonyítja konstrukcióval. A [65] (1991) cikk a nembináris esetekkel foglalkozik, konstrukciós módszereket tárgyal, a normalitás kérdését is érinti, és végül az általa kapott új eredmények beillesztésével felfrissíti az [57] (1990) cikkben található három táblázatot. Ezeket az eredményeket egészítik ki a hasonló tárgyú későbbi [113] (1999) cikk eredményei. A [86] (1994) cikkben néhány tételt fogalmaz meg az általános vegyes térlefedő kódokra, és több módszert fejt ki ilyen kódok konstrukciójára. Mellesleg a bináris esetre és $K_q(n, R)$ néhány speciális esetére is közöl e cikkben új eredményeket,

nevezetesen a $K(12, 2) \leq 78$, $K_q(4, 2) \leq 4q - 9$ ($3 \leq q \leq 9$), $K_q(5, 3) \leq 5q - 16$ ($4 \leq q \leq 9$) felső korlátokat. A [87] (1994) cikkben $K_3(11, 1)$ -re és $K_3(12, 1)$ -re ad javított felső korlátot, a [93] cikkben pedig új bizonyítást $K_3(6, 1)$ ismert felső korlátjára. A [101] (1997) cikkben „tabu search” heurisztika segítségével talál rekord-javító konstrukciót 9 ternáris koordináta és $R = 1$ esetére.

Cock és Östergård [96] (1997) cikkében a már [87]-ben is tárgyalt két esetre adnak a szerzők újabb, hibajavító kódokon (ternáris BCH kódokon) alapuló konstrukciót.

Kaikkonen és Östergård [107] (1998) cikkében a szerzők összefoglalják a bináris térlefedő kódokra addig ismert eredmények jó részét, azokat sok új további eredménnyel egészítik ki, és táblázatba gyűjtik a $K(n, R)$ -re vonatkozó akkor ismert legjobb felső korlátokat egészen $n \leq 64$ -ig.

Östergård és Härmäläinen [102] (1997) cikke a vegyes ternáris/bináris térlefedő kódokra vonatkozó korábbi és a szerzők által talált módszereknek és eredményeknek a komplex összefoglalása táblázattal, valamint az optimális és a cikk készítésének idején rekord-tartó kódok jelentős részének az ismertetésével.

2.4.5. Alsó korlátokat tárgyaló publikációk

Ebben az időszakban nagyon intenzívvé vált az alsó korlátok javítására irányuló módszerek kutatása. Zhang két, 1991-ben, ill. 1992-ben megjelent cikkében ([67, 71], ezek közül a második Lo-val közösen készített cikk) a szerzők lineáris egyenlőtlenség-rendszerek vizsgálata alapján határoznak meg új alsó korlátokat. Később azonban az e cikkekben megadott konkrét alsó korlátok helyett mások kifinomultabb módszerekkel, vagy számítógép segítségével jobb alsó korlátokat bizonyítottak, egy kivétellel, mivel a Zhang és Lo cikkében megadott $K(12, 3) \geq 18$ alsó korlátnál ma sem ismerünk jobbat. Li és Chen [85] (1994) szférikus alsó korlátokat javító újabb formulákat ad meg. Az e formulákból adódó konkrét $K(13, 3) \geq 28$ és $K(14, 3) \geq 44$ korlátoknál jelenleg sem ismerünk jobbat. Habsieger [82] (1994), [91] (1996), [100], (1997), Habsieger és Plagne [116] (2000), valamint Haas [117] (2000) cikke, valamint Blass és Litsyn 3 közös cikke: [103, 104] (1998), [110] (1999) is alsó korlátokkal foglalkozik.

Bhandari és Durairajan [90] (1996) munkája új konstrukciókat és új alsó korlátokat is közöl, elsősorban $q = 5$ esetére. Egyik észrevételükre, az alapján véve egyszerű, és mégis ötletes

$$K_q(n_1 + n_2, R_1 + R_2 + 1) \geq \min(K_q(n_1, R_1), K_q(n_2, R_2))$$

egyenlőtlenségre később többen is hivatkoztak. ADS konstrukcióval bizonyították egyebek között a $K_3(14, 6) \leq 81$, $K_5(8, 3) \leq 325$ felső korlátokat. Alsó korlátra vonatkozó eredményeik közül is csak néhányat említünk; ilyenek a $K_3(6n, 4n - 1) \geq 6$, $K_4(9, 5) \geq 8$, $K_5(6, 3) \geq 13$ alsó korlátok.

2.4.6. Kolev és szerzőtársai publikációi

Kolev [75, 76] (1993), [88] (1995), [106] (1998), Kolev és Landgev [84] (1994), Kolev és Hill [112] (1999) munkáinak főbb eredményei: A $K_3(5, 1) = 27$ esethez tartozó optimális

térlefedő kódok karakterizálása a [75] cikkben, lásd a 4.5 szakasz (e) esetére vonatkozó magyarázatot. [84]-ben a szerzők bebizonyították, hogy általánosan fennáll $K(2, 2R - 1; R) = 4$, $K(1, 2R + 1; R) = 6$, $K(2, 2R; R) = 6$ és $K(3, 2R - 2; R) = 5$. [76]-ben Koley határozta meg először a $K(1, 4; 1) = 8$ esethez tartozó inekvivalens optimális kódok számát. [88]-ben, számítógépes program segítségével is igénybe véve, bebizonyította, hogy $K(4, 2; 1) = 36$. [112]-ben a szerzők $K(9, 1)$ korábbi alsó korlátját javították meg.

2.5. A 2000 utáni eredmények összefoglalása

Az ezredforduló utáni fejlődésről és eredményekről csak globálisan és rövidebben szövel néhány mondatot. Gyakran úgy tűnik, hogy minden olyan eredményt, ami látványosan szép a térlefedő kódok elméletében, az előző időszakokban már megtaláltak a kutatók. Bizonyos mértékig valóban így lehet, de ennek ellenére találhatók olyan eredmények, amelyek kissé rácăfolnak az előző megállapításra. Dejter és Phelps [120] (2001) egy ternáris Hamming kód alapján nagyon szép konstrukciót ír le a 13 koordinátát tartalmazó 1 elérési sugarú bináris – jelenleg is rekord-tartó – kódra 704 kódszóval. Di Pasquale és Östergård [127] (2003), valamint Bertolo, Östergård és Weakley [130] (2004) az ekvivalens kódok automorfizmusainak vizsgálata alapján nagyon érdekes új konstrukciós módszereket vezet be ternáris és vegyes kódokra. Haas, Schlage-Puchta és Quistorff a [158] (2009) cikkben partíciós mátrixokat alkalmazva, Haas, Halupczok és Schlage-Puchta pedig a [164] (2009) cikkben játékelméleti megközelítést alkalmazva, igen sok esetre nyer az eddig ismertnél jobb alsó korlátot. Legyen szabad az utóbbi évekből származó szép eredmények között említeni még egy társszerzővel elért saját eredményt is, nevezetesen az optimális $(2R + 3, 7)R$ kódok klasszifikációját K. és Östergård [139] (2006) cikkében.

A legutóbbi időszakot jellemzi, hogy a számítógépes módszerek egyre jobban elterjednek. A növekvő méretű esetek vizsgálata, diszkussziója gyakorlatilag lehetetlen számítógép segítségével az igénybe vétele nélkül. Sajnos, a folyóiratok szerkesztőinek és a cikkek bírálataira felkért szakértőknek egy része a számítógép segítségével kapott eredmények, bizonyítások értékét nem ismeri el. Az egyik szerzőtől kapott információ szerint Bertolo és szerzőtársai [130] cikke azért nem jelenhetett meg abban a folyóiratban, ahová a szerzők először elküldték, mert sok számítógépes eredmény van benne. Pedig bonyolult rendszer esetén a gép kevésbé siklik át olyan részleteken, amiken az emberi agy esetleg könnyen átsiklik, kiflejt a gondolatmenetből. Jó példa erre, hogy a bevezető részben ismertetett Berlekamp féle kapcsolótáblás feladat megoldását, amely egy nagyobb méretű lineáris kód elérési sugarának a meghatározását jelentette, Fishburn és Sloane egy 1989-ben közölt cikkben tévesen adták meg, és ez csak 15 évvel később derült ki Carlson és Stolarski [131] cikkéből, melynek szerzői számítógép igénybevétele segítségével a helyes megoldást határozták meg.

Az ezredfordulót követően felgyorsult a klasszifikációs eredmények közlése, lásd [118] (2000), [126] (2002), [129] (2003) ($K_4(4, 2) = 7$ klasszifikációja), [130] (2004) ($K(9, 2) = 16$ klasszifikációja), [138] (2006), [139] (2006), [145] (2006) ($K(3, 1; 1) = 9$ és $K(6, 1; 3) = 9$ klasszifikációja), [155] (2008), és végül sok új klasszifikációs eredmény közlése a [171] web lapon és a jelen munkában [167].

3. fejezet

Bináris térlefedő kódok

3.1. Csak a 3. fejezetben használt fogalmak

Önkomplementer kód

Egy bináris C kód önkomplementer, ha bármely $c \in C$ kódszó esetén c komplemente (c -ből a 0 és 1 értékek felcserélésével kapott bináris vektor) szintén kódszó.

Nyilvánvalóan minden bináris önkomplementer kód kiegyensúlyozott, melyben a kódszavak száma páros.

Bináris szó súlya

Tetszőleges $x \in Z_2^n$ esetén x súlyának nevezzük és $wt(x)$ -szel jelöljük x koordinátáinak összegét, vagyis az 1 értékű koordináták számát.

Hipergráf, független hipergráf

A hipergráf olyan (V, E) pár, ahol V bizonyos – csúcsoknak nevezett – elemek nem üres halmaza, E pedig – hiperéleknek (vagy röviden éleknek) nevezett – elemek halmaza, ahol a hiperélek V -nek egymástól különböző nem üres részhalmazai.

A (V, E) hipergráf független hipergráf, ha bármely két $e_i, e_j \in E$ él esetén az $e_i \cap e_j$, $e_i \cap e_j^c$, $e_i^c \cap e_j$, $e_i^c \cap e_j^c$ halmazok közül ezek egyike sem üres, ahol e^c -vel az e él komplementjét jelöljük, vagyis $e^c = V \setminus e$.

Hipergráf csúcsának foka

Hipergráfban egy v csúcs fokának nevezzük és $\delta(v)$ -vel jelöljük a v -t tartalmazó élek számát.

Uniform hipergráf, reguláris hipergráf

Egy hipergráf k -uniform, ha minden él számossága azonosan k . Egy k -uniform (V, E) hipergráf teljes, ha E tartalmazza V valamennyi k elemű részhalmazát. Egy hipergráf t -reguláris, ha minden csúcs foka azonosan t .

Szakaszonként konstans súlyú kód

A $C \subseteq Z_2^n$ kód szakaszonként konstans súlyú, ha C előállítható $C = |C_1|C_2|\dots|C_k|$ alakban úgy, hogy ha egy $c = |c_1|c_2|\dots|c_k|$ kódszó esetén $wt(c_1) = w_1$, $wt(c_2) = w_2, \dots$, $wt(c_k) = w_k$, akkor C kódszavai között az összes többi ugyanilyen tulajdonságú szó is megtalálható.

3.2. Egyszerű konstrukciók

Az egyszerű jelzőt itt nem abban az értelemben használjuk, hogy ezek minden esetben könnyen kiötölhető konstrukciók, hanem inkább abban az értelemben, hogy ezeket nem más kódok konstrukciójából származtatjuk.

3.2.1. Bináris ismétléses kódok

A Z_2^n térben értelmezett bináris ismétléses kódok formája:

$$C = \{ (0, 0, \dots, 0), \\ (1, 1, \dots, 1) \},$$

és a C kód elérési sugara nyilván $R = \lfloor n/2 \rfloor$ – v.ö. (1.4). Könnyen látható, hogy a bináris ismétléses kód az előbbi n, R paraméterekhez tartozó optimális térlefedő kód, tehát $K(n, \lfloor n/2 \rfloor) = 2$, vagyis az egész rész jelölés használata nélküli képletté átformálva

$$K(2R, R) = K(2R + 1, R) = 2.$$

Az ilyen optimális térlefedő kódok különösen páratlan n esetén érdekesek, mivel a páratlan n -hez tartozó bináris ismétléses kódokra fennáll (1.3), tehát ezek perfekt kódok.

3.2.2. Bináris Hamming kódok

Tetszőleges $h \geq 2$, egész és $n = 2^h - 1$ esetén létezik a Z_2^n térben perfekt lineáris kód; $h = 2$ esetén ez egy ismétléses kód, a következő legegyszerűbb eset a $h = 3$ -hoz tartozó $H_7 \subset Z_2^7$ kód, amely perfekt $(7, 16)_1$ kód és a következő négy kódszóval generálható:

$$\begin{aligned} h_1 &= (0, 0, 0, 1, 1, 1, 0), \\ h_2 &= (0, 0, 1, 0, 0, 1, 1), \\ h_3 &= (0, 1, 0, 0, 1, 0, 1), \\ h_4 &= (1, 0, 0, 0, 1, 1, 1). \end{aligned}$$

Az összes kódszó a h_1, h_2, h_3, h_4 generáló kódszavak valamennyi lehetséges lineáris kombinációját képezve adódik, és így

$$H_7 = \{ 0, h_1, h_2, h_1 + h_2, h_3, h_1 + h_3, h_2 + h_3, h_1 + h_2 + h_3, h_4, h_1 + h_4, h_2 + h_4, \\ h_1 + h_2 + h_4, h_3 + h_4, h_1 + h_3 + h_4, h_2 + h_3 + h_4, h_1 + h_2 + h_3 + h_4 \}, \quad (3.1)$$

az összeadást az alaptest műveleti szabályai szerint értelmezve, ami bináris esetben modulo 2 értelmezett összeadást jelent, tehát páros számú 1-es összege 0, páratlan számú 1-es összege 1.

A H_7 Hamming kód létezéséből, konstrukciójából adódik az alábbi egyenlőség:

$$K(7, 1) = 16.$$

A nagyobb méretű bináris Hamming kódok konstrukcióját illetően lásd pl. [39] vagy [97]. Ilyen kódok létezéséből következik általánosan a

$$K(2^h - 1, 1) = 2^{2^h - h - 1},$$

konkrétan tehát a $K(15, 1) = 2^{11}$, $K(31, 1) = 2^{26}$ stb. egyenlőség.

3.2.3. Egyéb konstrukciók lineáris kódokkal

A térlefedő kódok lehető legkisebb méretére vonatkozó első táblázatokban az ezeket tartalmazó publikációk szerzői lineáris kódokra szorítkoztak. Ilyen táblázatok találhatók Graham és Sloane [43], később Cohen, Litsyn, Lobstein és Mattson [98] cikkében, az utóbbi azonban már a nemlineáris térlefedő kódokra is közöl táblázatokat.

3.3. Folytatólagos konstrukciók és kapcsolatos egyenlőtlenségek

Az itt tárgyalt konstrukciókat lehetne rögtön általánosan, tetszőleges q alapszám esetére ismertetni, azonban a bizonyítások, a konstrukciók tulajdonságainak a megindoklása a bináris esetben sokkal könnyebben fogalmazható meg és ezért könnyebben is érthető. Az ezekhez szükséges gondolatmenetek lényege bináris, ternáris, ill. az általános esetben is azonos, azonban általános q alapszám esetén nehezebb a megfogalmazásuk. Ezért a bináris kód-konstrukciókat részletezzük bővebben, a ternáris és magasabb rendű esetekre vonatkozó analóg konstrukciókat pedig a megfelelő fejezetekben röviden és bizonyítások nélkül fogjuk tárgyalni.

A konstrukciók tárgyalása során az elérési sugár értékének vagy felső korlátjának meghatározásán kívül kitérünk a normalitás öröklődésének a vizsgálatára is. Ez főleg olyankor érdekes, ha az elkészített kódot újabb folytatólagos vagy összetételes konstrukció kiindulási kódjaként kívánjuk használni, mivel néhány konstrukció teljes bizonyossággal csak normál kódokra alkalmazható.

A normalitás öröklődésére vonatkozó bizonyítások esetén nem fogalmazom meg tételként a bizonyításra kerülő állításokat, mivel ezek nem tekinthetők újaknak. Ezek már korábban meglévő ismeretek, melyeket sokan felhasználtak, bizonyításukat azonban sehol nem láttam leírva.

3.3.1. 1-gyel növelt dimenzió és elérési sugár, változatlan méret

Legyen $C \subset Z_2^n$ egy M kódszóból álló, R elérési sugarú kód. Egészítsük ki C kódszavait egy-egy tetszőleges értékű $(n+1)$ -edik koordinátával. Az eredményül kapott C' kód R' elérési sugarára nyilvánvalóan fennáll $R \leq R' \leq R+1$, és következésképpen

$$K(n+1, R+1) \leq K(n, R) \leq K(n+1, R). \quad (3.2)$$

Az $R' \geq R$ egyenlőtlenség az összefűzéssel nyert kód elérési sugarára vonatkozó (1.7) egyenlőtlenségből következik. $R' \leq R+1$ bizonyításához legyen $x' = |x|x_{n+1}|$ a Z_2^{n+1} tér tetszőleges pontja. Ekkor van olyan $c \in C$ kódszó, melyre $d(x, c) \leq R$, és így tetszőleges c_{n+1} érték esetén (1.6) szerint

$$d(|x|x_{n+1}|, |c|c_{n+1}|) = d(x, c) + d(x_{n+1}, c_{n+1}) \leq d(x, c) + 1 \leq R+1.$$

A normalitás öröklődésének a vizsgálatához tegyük fel, hogy a C kód normális valamelyik koordinátában, és az e koordináta szerinti felbontás $C = C_0 \cup C_1$. Legyen a megnövelt $C' = |C|v|$ kód ennek megfelelő felbontása $C' = C'_0 \cup C'_1$, ahol $C'_0 = |C_0|v_0|$, $C'_1 = |C_1|v_1|$ és $v = v_0 \cup v_1 \subset Z_2$. C normalitása miatt tetszőleges $x' = |x|x_{n+1}| \in Z_2^{n+1}$ esetén létezik két olyan $c_0 \in C_0$ és $c_1 \in C_1$ kódszó, melyekkel fennáll

$$d(x, c_0) + d(x, x_1) \leq 2R+1.$$

Mivel (1.6) szerint $d(|x|x_{n+1}|, c'_0) \leq d(x, c_0) + 1$ és hasonlóan $d(|x|x_{n+1}|, c'_1) \leq d(x, c_1) + 1$, következésképpen

$$d(|x|x_{n+1}|, c'_0) + d(|x|x_{n+1}|, c'_1) \leq 2R+3.$$

A kapott eredmény szerint kimondhatjuk, hogy ha C' elérési sugara $R+1$ (és véletlenül nem kisebb), akkor C' normális minden olyan koordináta szerint, amelyek szerint C normális.

3.3.2. 1-gyel növelt dimenzió, változatlan elérési sugár, kétszeres méret

Legyen $C \subset Z_2^n$ egy M kódszóból álló, R elérési sugarú kód. Egészítsük ki C kódszavait először 0 értékű, majd 1 értékű $(n+1)$ -edik koordinátával. Az eredményül kapott

$$C'' = \{|c|0| : c \in C\} \cup \{|c|1| : c \in C\}$$

kód elérési sugara megegyezik C elérési sugarával, és következésképpen

$$K(n+1, R) \leq 2K(n, R). \quad (3.3)$$

A konstrukció eredményeként kapott kód $C'' = |C|v_0| \cup |C|v_1|$ alakban is írható, ahol v_0 csupa 0-ból, v_1 pedig csupa 1-esből tevődik össze. Ekkor tetszőleges $x'' = |x|x_{n+1}| \in Z_2^{n+1}$ esetén $d(x'', |C|v_0|) = d(x, C)$, ha $x_{n+1} = 0$ és $d(x'', |C|v_1|) = d(x, C)$, ha $x_{n+1} = 1$, következésképpen mindkét esetben $d(x'', C'') \leq R$. Ez bizonyítja, hogy C'' elérési sugara legfeljebb R . Az viszont, hogy R -nél kisebb nem lehet az elérési sugár, legegyszerűbben

úgy bizonyítható, hogy a $|C|v_0| \cup |C|v_1|$ egyesítést egyetlen konkatenációnak tekintve, alkalmazzuk rá az (1.7) egyenlőtlenséget.

A normalitás öröklődésének a vizsgálatához tegyük fel megint, hogy a C kód normális valamelyik koordinátában, és az e koordináta szerinti felbontás $C = C_0 \cup C_1$. Legyen a megnövelt kód ennek megfelelő felbontása $C'' = C_0'' \cup C_1''$, ahol $C_0'' = |C_0|v_{00}| \cup |C_0|v_{01}|$ és $C_1'' = |C_1|v_{10}| \cup |C_1|v_{11}|$, továbbá v_{00} és v_{10} csupa 0-ból, v_{01} és v_{11} pedig csupa 1-esből tevődik össze.

Tetszőleges $x'' = |x|x_{n+1}| \in Z_2^{n+1}$, $c_0 \in C_0$, $c_1 \in C_1$ esetén

$$d(x'', |c_0|x_{n+1}|) = d(x, c_0) \text{ és } d(x'', |c_1|x_{n+1}|) = d(x, c_1), \quad (3.4)$$

és következésképpen C'' is normális ugyanazokban a koordinátákban, mint amelyekben C . Ehhez most az elérési sugárra vonatkozó plusz feltételre sincs szükség, mivel C és C'' elérési sugara mindig megegyezik. Az (3.4) egyenlőségekkel az is bizonyítható, hogy ha valamely koordinátában C nem normális, akkor C'' sem.

A konstrukció minden esetben normális kódot eredményez az $(n+1)$ -edik koordinátára nézve. Legyen ugyanis ismét $x'' = |x|x_{n+1}| \in Z_2^{n+1}$ tetszőleges pont, ekkor pl. $x_{n+1} = 0$ esetén $d(x'', |C|v_0|) \leq R$ és $d(x'', |C|v_1|) \leq R+1$.

E konstrukció alkalmazásával jön létre pl. a 3.8.1 szakaszban a $K(3, 1) = 2$ esetre megadott optimális kódból az ugyanott a $K(4, 1) = 4$ esetre megadott (1) jelű optimális kód.

3.3.3. 2-vel növelt dimenzió, 1-gyel növelt elérési sugár, változatlan méret

Legyen $C \subset Z_2^n$ egy M kódszóból álló, R elérési sugarú, az utolsó koordinátában normális kód. Bontsuk fel C -t két kód, C_0 és C_1 egyesítésére úgy, hogy C_0 tartalmazza C -nek azokat a kódszavait, melyeknek az utolsó koordinátája 0, C_1 pedig C -nek azokat a kódszavait, melyeknek az utolsó koordinátája 1. Egészítsük ki C_0 minden kódszavát két további 0 értékű koordinátával, C_1 minden kódszavát pedig két további 1 értékű koordinátával. Az így létrehozott

$$\overline{C} = \{|c|00| : c \in C_0\} \cup \{|c|11| : c \in C_1\}$$

kód elérési sugara legfeljebb $R+1$.

Legyen $\overline{C}_0 = \{|c|00| : c \in C_0\}$ és $\overline{C}_1 = \{|c|11| : c \in C_1\}$. Megmutatjuk, hogy tetszőleges $\overline{x} \in Z_2^{n+2}$ esetén

$$d(\overline{x}, \overline{C}_0) + d(\overline{x}, \overline{C}_1) \leq 2R + 3; \quad (3.5)$$

ebből az előbbi állítás már következik.

A két utolsó koordináta értékétől függően $\overline{x} = |x|00|$ vagy $\overline{x} = |x|01|$ vagy $\overline{x} = |x|10|$ vagy $\overline{x} = |x|11|$. Mivel C -ről feltételeztük, hogy az utolsó koordináta szerint normális, van olyan $c_0 \in C_0$, ill. $c_1 \in C_1$ kódszó, melyekre $d(x, c_0) + d(x, c_1) \leq 2R + 1$. Ekkor az $\overline{x}$ pontnak a kibővített kód $\overline{c}_0 = |c_0|00|$, $\overline{c}_1 = |c_1|11|$ kódszavaitól való távolsága a

két utolsó koordináta értékétől függően $d(\bar{x}, \bar{c}_0) = d(x, c_0)$, $d(x, c_0) + 1$, $d(x, c_0) + 1$, ill. $d(x, c_0) + 2$ és $d(\bar{x}, \bar{c}_1) = d(x, c_1) + 2$, $d(x, c_1) + 1$, $d(x, c_1) + 1$, ill. $d(x, c_1)$. Ezekből az összefüggésekből mind a négy esetben megkapjuk a (3.5) egyenlőtlenséget, melyből az $\bar{C}$ kód elérési sugarára vonatkozó állításon túl az is következik, hogy ha a $\bar{C}$ kód elérési sugara pontosan $R + 1$, akkor ez a kód normális a három azonos utolsó koordinátában.

A fentiekből az is következik, hogy ha létezik Z_2^n -ben M kódszóból álló, R elérési sugarú normális kód, akkor $K(n + 2, R + 1) \leq M$.

Az e pontban tárgyalt konstrukció alkalmazásával jön létre pl. a 3.8.1 szakaszban a $K(5, 1) = 7$ esetre megadott optimális kódból a $K(7, 2) = 7$ esethez tartozó (1) jelű optimális kód, azzal az eltéréssel, hogy nem az utolsó, hanem az első koordinátát ismételtük háromszor minden kódszóban.

3.4. Összetételes konstrukciók és kapcsolatos egyenlőtlenségek

Az előző szakasz bevezetésében mondtak az itt ismertetésre kerülő konstrukciókra is érvényesek, tehát mindaz, amit a bináris esetre megfogalmazunk, analóg módon megfogalmazható tetszőleges q alapszám esetére is.

3.4.1. Két kód direkt összege (DS konstrukció)

Legyenek $C \subset Z_2^{n_1}$ és $D \subset Z_2^{n_2}$ tetszőleges kódok, jelölje ezek kódszavainak számát M_1 , ill. M_2 , elérési sugarát R_1 , ill. R_2 . Képezzük a megadott két kód szavaiból a

$$C \oplus D = \{|c|d| : c \in C, d \in D\}$$

kódot.

Ekkor tetszőleges $x \in Z_2^{n_1}, y \in Z_2^{n_2}$ esetén valamely $c_1 \in C$, $c_2 \in D$ kódszavakra $d(x, c_1) \leq R_1$, $d(x, c_2) \leq R_2$, és ennél fogva

$$d(|x|y|, |c_1|c_2|) = d(x, c_1) + d(y, c_2) \leq R_1 + R_2.$$

Az összetétel eredményeként kapott, $M_1 M_2$ kódszóból álló, $C \oplus D \subset Z_2^{n_1+n_2}$ kód elérési sugara tehát legfeljebb $R_1 + R_2$, és következésképpen

$$K(n_1 + n_2, R_1 + R_2) \leq K(n_1, R_1)K(n_2, R_2). \quad (3.6)$$

A normalitás öröklődésének kérdéséhez tegyük fel megint, hogy a C kód normális valamilyen koordinátában, és az e koordináta szerinti felbontás $C = C_0 \cup C_1$. Ekkor tetszőleges $x \in Z_2^{n_1}$, $y \in Z_2^{n_2}$ esetén találhatóak $c_0 \in C_0$, $c_1 \in C_1$, ill. $c_2 \in D$ kódszavak úgy, hogy $d(x, c_0) + d(x, c_1) \leq 2R_1 + 1$, $d(x, c_2) \leq R_2$, és ennél fogva

$$d(|x|y|, |c_0|c_2|) + d(|x|y|, |c_1|c_2|) = d(x, c_0) + d(x, c_1) + 2d(y, c_2) \leq (2R_1 + 1) + 2R_2.$$

Eszerint, ha $C \oplus D$ elérési sugara pontosan $R_1 + R_2$, akkor $C \oplus D$ normális mindazokban a koordinátákban, amelyek szerint C (és hasonlóan: amelyek szerint D) normális.

3.4.2. Amalgám direkt összeg (ADS konstrukció)

Az előző pontban tárgyalt direkt összeghez valamelyest hasonlóan járunk el, két lényeges eltéréssel.

Legyenek $C \subset Z_2^{n_1}$ és $D \subset Z_2^{n_2}$ megint egyelőre tetszőleges kódok R_1 , ill. R_2 elérési sugárral; bontsuk fel őket a kódszavak utolsó koordinátáinak értéke szerint a C_0 és C_1 , ill. D_0 és D_1 kódok egyesítésére. Tekintsük most külön-külön a $C_0 \oplus D_0$ és $C_1 \oplus D_1$ direkt összegeket. Hagyjuk el ezután D_0 -ból és D_1 -ből a kódszavak utolsó koordinátáit, hiszen azok a direkt összegben ismétlést eredményeznének. Az így keletkező D'_0 és D'_1 kódok használatával adódó

$$C^\bullet = (C_0 \oplus D'_0) \cup (C_1 \oplus D'_1)$$

kódra bizonyos feltételek fennállása esetén teljesül, hogy elérési sugara legfeljebb $R_1 + R_2$. Ennek elégséges – de nem szükséges – feltétele, hogy C és D mindegyike az utolsó koordinátában normális kód legyen.

Bizonyítás. A $C^\bullet$ kód a $Z_2^{n_1+n_2-1}$ tér részhalmaza. E tér tetszőleges vektora $|x|y|0|$ vagy $|x|y|1|$ alakú, ahol $x \in Z_2^{n_1-1}$ és $y \in Z_2^{n_2-1}$. C és D normalitása miatt létezik c_1, c_2, d_1, d_2 úgy, hogy

$$d(|x|0|, c_0) + d(|x|0|, c_1) \leq 2R_1 + 1, \quad (3.7)$$

$$d(|y|0|, d_0) + d(|y|0|, d_1) \leq 2R_2 + 1.$$

Vezessük be a c_i, d_i szavakból az utolsó koordináta elhagyásával keletkező részre a c_i^-, d_i^- jelöléseket. Ekkor

$$\begin{aligned} d(|x|0|, c_0) &= d(x, c_0^-), \\ d(|x|0|, c_1) &= d(x, c_1^-) + 1, \\ d(|y|0|, d_0) &= d(y, d_0^-), \\ d(|y|0|, d_1) &= d(y, d_1^-) + 1. \end{aligned} \quad (3.8)$$

Az (1.6) egyenlőség többszörös alkalmazásával kapjuk, hogy

$$\begin{aligned} d(|x|y|0|, |c_0^-|d_0^-|0) &= d(x, c_0^-) + d(y, d_0^-), \\ d(|x|y|0|, |c_1^-|d_1^-|1) &= d(x, c_1^-) + d(y, d_1^-) + 1. \end{aligned} \quad (3.9)$$

Végül, a (3.7)-(3.9) relációkból következik, hogy

$$d(|x|y|0|, |c_0^-|d_0^-|0) + d(|x|y|0|, |c_1^-|d_1^-|1) \leq 2R_1 + 2R_2 + 1, \quad (3.10)$$

tehát a bal oldalon álló összeg legalább egyik tagja kisebb vagy egyenlő mint $R_1 + R_2$. A hasonló gondolatmenetet az $|x|y|1|$ alakú vektorokra is elvégezve, arra a következtetésre jutunk, hogy $C^\bullet$ elérési sugara legfeljebb $R_1 + R_2$. Ha az elérési sugár pontosan $R_1 + R_2$, akkor az (3.10) egyenlőtlenség azt is mutatja, hogy $C^\bullet$ normális kód arra a koordináta-helyre nézve, amelyen a C és D kódokat összekapcsoltuk. $\square$

Megjegyezzük, hogy az ADS konstrukció egy speciális eseteként, D -nek a 3 dimenziós bináris ismétléses kódot választva, a 3.3.3 pontban tárgyalt méretnövelő konstrukcióhoz jutunk.

3.4.3. Blokk direkt összeg (BDS konstrukció)

Hasonló, mint az amalgám direkt összeg konstrukció. Az eltérés csak annyi, hogy C és D közül az egyik vagy mindkét kódot nem valamelyik koordináta értéke alapján, hanem más módon bontjuk fel két kód egyesítésére.

3.5. Bináris térlefedő kódok mérete

Az optimális bináris térlefedő kódok pontos méretét, azaz $K(n, R)$ értékét az alábbi esetekben ismerjük:

- (a) $R = 0$ esetén;
- (b) $n = 2^h - 1$ és $n = 2^h$, mindkét esetben $R = 1$, ahol $h \geq 3$, egész;
- (c) $n = 23, R = 3$ esetén;
- (d) $R > 0, n \leq 2R + 3$ fennállása esetén;
- (e) $n \leq 9$ esetén;
- (f) $n = 10, R = 3$ esetén.

A 3.1. táblázatban $\bullet$ jelek mutatják az optimális bináris térlefedő kódok méretének ismert eseteit a $2 \leq n \leq 33, 1 \leq R \leq 9$ tartományban. Az értelmezhetetlen mezőket $\circ$ jellel láttuk el, és ezáltal az üresen hagyott mezők szemléletesen mutatják a megoldatlan eseteket.

Megjegyezzük, hogy (a), (b), (c), (d) és (f) egymást kizáró feltételek, az (e) eset feltétele viszont teljesülhet az (a), (b), ill. (d) feltétel teljesülésével egyidejűleg. Az (a) esetben nyilvánvaló, hogy

$$K(n, 0) = 2^n,$$

ugyanis 0 sugarú térlefedő kódnak a tér minden pontját tartalmaznia kell.

A (b) és (c) esetekhez tartozó optimális kódok a bináris Hamming kódok, valamint ezekből származtatott térlefedő kódok, ill. a bináris Golay kód, melyek méretei ismeretének alapján kapjuk az

$$(i) K(2^h - 1, 1) = 2^{2^h - h - 1}, \quad (ii) K(2^h, 1) \leq 2^{2^h - h}, \quad (iii) K(23, 3) = 4096$$

egyenlőségeket, ill. egyenlőtlenségeket. Az (i) és (iii) esetben az optimális kódok perfektek, a (ii) esetben nem, ezért az optimális kódok konstrukciója alapján erre az esetre csak a fenti felső korlátot lehet bizonyítani. Viszont a szférikus alsó korlát élesítéséből ([29, 52]) adódóan ebben az esetben is fennáll az egyenlőség, lásd 2.2.4. szakasz.

A (d) esetben $K(n, R)$ értéke 1, 2, 4 vagy 7 lehet, mégpedig $K(n, R) = 1, 2, 4$, ill. 7 akkor és csak akkor, ha $n = R, R < n < 2R + 2, n = 2R + 2$, ill. $n = 2R + 3$.

$n \setminus R$	1	2	3	4	5	6	7	8	9	$n \setminus R$	1	2	3	4	5	6	7	8	9
2	•	•	◦	◦	◦	◦	◦	◦	◦	18								•	•
3	•	•	•	◦	◦	◦	◦	◦	◦	19								•	•
4	•	•	•	•	◦	◦	◦	◦	◦	20									•
5	•	•	•	•	•	◦	◦	◦	◦	21									•
6	•	•	•	•	•	•	◦	◦	◦	22									
7	•	•	•	•	•	•	•	◦	◦	23			•						
8	•	•	•	•	•	•	•	•	◦	24									
9	•	•	•	•	•	•	•	•	•	25									
10			•	•	•	•	•	•	•	26									
11				•	•	•	•	•	•	27									
12					•	•	•	•	•	28									
13					•	•	•	•	•	29									
14						•	•	•	•	30									
15	•					•	•	•	•	31	•								
16	•						•	•	•	32	•								
17							•	•	•	33									

3.1. táblázat. Optimális bináris térlefedő kódok megoldott esetei

Itt az 1 méretű kódokra vonatkozó állítás triviális, hiszen egyetlen kódszóból álló kód elérési sugara a tér dimenziójával, n -nel egyenlő, és fordítva, $R = n$ sugárral történő fedés a tér egyetlen (tetszőleges) pontjával megvalósítható. A 2 és 4 méretre vonatkozó állításokat Chen és Honkala [57], ill. Cohen, Lobstein és Sloane [46] bizonyította. Az utóbbi cikk szerzői arra is rámutattak, hogy 3, 5 vagy 6 kódszóból álló bináris optimális térlefedő kód nem létezik. Bebizonyították továbbá, hogy $K(n, R) = 7$, ha $n = 2R + 3$ és R pozitív egész. Azonban akkor még nyitott kérdés maradt, hogy van-e ezenkívül más olyan eset, melyre $K(n, R) = 7$. Erre a kérdésre a [145] cikk adta meg a választ.

Az (e) feltételnek megfelelő, de az (a), (b) vagy (d) feltételek egyikének sem megfelelő esetek az alábbiak:

$$K(6, 1) = 12, \quad K(8, 2) = 12, \quad K(9, 1) = 62, \quad K(9, 2) = 16.$$

Az utóbbi 4 egyenlőség bizonyítása Stanton és Kalbfleisch [18], Blass és Litsyn [110], Östergård és Weakley [118], ill. Östergård és Blass [121] publikációjában található. A kisebb vagy egyenlő relációt – sok más esethez hasonlóan – ezekben az esetekben is már jóval régebben ismert totó-kombinációk bizonyították, például a $K(6, 1) \leq 12$ egyenlőtlenséget bizonyító konstrukció [168] szerint Di Nasso (1950), a $K(9, 1) \leq 62$ egyenlőtlenséget bizonyító konstrukció Fagioli (1984) nevéhez kapcsolható. (Sok hasonló, régóta ismert konstrukció szerzője homályban maradt, például [168] szerint a $K(8, 2) \leq 12$ és a $K(9, 2) \leq 16$ egyenlőtlenséget bizonyító konstrukció szerzője ismeretlen. Más esetekben a prioritás eldöntése problematikus, ezért előfordul, hogy ugyanarra a konstrukcióra vonatkozóan az olasz kiadványok olasz szerzőt, a skandináv kiadványok pedig skandináv szerzőt jelölnek meg.)

Az (f) esetre vonatkozó

$$K(10, 3) = 12$$

állításnak a kisebb vagy egyenlő részét Rankinen (1975) konstrukcióval igazolta. A 12 alsó korlátot és egyúttal a pontos értéket számítógépes módszerrel Östergårddal külön-külön bizonyítottuk, és az eredményt közösen publikáltuk a [155] cikkben.

A bináris térlefedő kódok körében ezzel az egyetlen esettel tudtuk kibővíteni az optimális térlefedő kódok pontos méretére már korábban is ismert eseteket. Az alsó korlátot még egy konkrét bináris esetben tudtuk bizonyítani szintén számítógép segítségével, és ezzel a $K(11, 3)$ korábban ismert legjobb alsó korlátját az ismert felső korláttól egy egységre közelítettük meg. Megjegyzem, hogy a térlefedő kódok kategóriái közül hagyományosan a bináris kódok alkotják a legintenzívebben kutatott kategóriát, így ezekre ma jóval nehezebb új eredményeket találni és bizonyítani, mint más kód kategóriákra.

Egy általánosabb esetben, a $K(n, R) = 7$ egyenlőséget kielégítő optimális kódok problémájára vonatkozóan Östergårddal közösen végzett kutatásunk során nemcsak azt mutattuk meg, hogy nincs más további eset azokon kívül, amelyeket Cohen és szerzőtársai [46]-ben megadtak, hanem azt is, hogy a triviális $K(3, 0) = 8$ eseten kívül nincs más 8 méretű bináris optimális térlefedő kód sem. Ehhez a $K(n, R)$ függvény monotonitása miatt azt kellett már csak bizonyítani, hogy $K(2R + 4, R) \geq 9$, ha $R \geq 1$. A bizonyításhoz szükség volt a 8 kódszóból álló bináris 2-szűrjektív kódok áttekintésére és elérési sugaruk kiszámítására 35 dimenzióig. A vizsgált inekvivalens kódok milliós nagyságrendje miatt ezt csak számítógép segítségével lehetett elvégezni. A bizonyításhoz felhasználtuk a $K_q(n, R)$ és a $\sigma_q(n, s)$ függvények monotonitására vonatkozó, az elérési sugár, ill. a szűrjektív kód definíciója alapján nyilvánvaló

$$K_q(n, R + 1) \leq K_q(n, R) \quad (3.11)$$

és

$$\sigma_q(n + 1, s) \geq \sigma_q(n, s) \quad (3.12)$$

egyenlőtlenségeket, az ezekkel rokon (3.2) egyenlőtlenség-párt, valamint a következő lemmát és annak következményeit:

3.1. Lemma. *(K. és Östergård [155], Theorem 12)*

Ha C bináris kód, melynek elérési sugara R , és C nem 2-szűrjektív, akkor a 00, 01, 10, 11 értékpárok mindegyikét nem tartalmazó bármely két koordináta törlésével olyan kódhoz jutunk, melynek elérési sugara legfeljebb $R - 1$.

Bizonyítás. A koordináták permutációja után, $C = |C_1|C_2|$ konkatenációként írható fel, ahol C_2 a kódszavak 2 törölt koordinátájából álló kód, C_1 pedig a törlés által adódó kód. Legyen C_1 , ill. C_2 elérési sugara R_1 , ill. R_2 . A törölt koordináták választása folytán $R_2 \geq 1$, és így az (1.7) egyenlőtlenséget is alkalmazva kapjuk, hogy $R_1 \leq R - R_2 \leq R - 1$.

□

A 3.1. lemmában foglalt állítás sok esetben meggyorsítja az elérési sugár számítógép segítségével végzett meghatározásának időigényes műveletét; olyan esetekben, amikor számítógép nélküli módszer alkalmazása teljesen reménytelennek látszik.

Bizonyos esetekben közvetlenebbül alkalmazhatók a 3.1. lemma alábbi következményei:

3.2. Következmény. (Cohen és szerzőtársai [46] Theorem 5, K. és Östergård [155], Theorem 11)

Bármely az $M < K(n, R)$ egyenlőtlenséget kielégítő bináris $(n + 2, M)R + 1$ kód 2-szűrjektív.

3.3. Következmény.

Ha $n \geq 3$, $R \geq 1$ és $K(n, R) < K(n - 2, R - 1)$, akkor az n, R paraméterekhez tartozó bármely optimális térlefedő kód bináris 2-szűrjektív kód.

Az utóbbi állításból viszont következik a csupán egy képletből álló következő forma:

3.4. Következmény. (K. és Östergård [129], Theorem 2 speciális esete)

$$K(n, R) \geq \min\{\sigma_2(n, 2), K(n - 2, R - 1)\}.$$

Mivel $\sigma_2(n, 2)$ -re ismert a

$$\sigma_2(n, 2) = \min \left\{ M : n \leq \binom{M-1}{\lfloor (M-2)/2 \rfloor} \right\} \quad (3.13)$$

formula (lásd [27, 30, 31, 32]), ezt az előző képletbe behelyettesítve egy újabb formát kaphatnánk, amely azonban a két – ráadásul különböző módon használt – 'min' függvény egymásba ágyazása miatt eléggé áttekinthetetlen lenne. Ez a probléma áthidalható a következő újabb átfogalmazással:

3.5. Következmény.

Ha $K(n - 2, R - 1) > M$ és $\sigma_2(n, 2) > M$, akkor $K(n, R) > M$.

Viszont a $\sigma_2(n, 2)$ értékeire felírt formula szerint $\sigma_2(n, 2) > M$ akkor és csak akkor áll fenn, ha $n > \binom{M-1}{\lfloor (M-2)/2 \rfloor}$. Ily módon megkapjuk az alábbi állítást:

3.6. Következmény.

Ha $K(n - 2, R - 1) > M$, ahol $n > \binom{M-1}{\lfloor (M-2)/2 \rfloor}$, akkor $K(n, R) > M$.

Visszatérve a $K(2R + 4, R) \geq 9$ alsó korlát kérdésére, kimondjuk a következő tételt, amelyben megadott általános felső korlát bizonyítása [46]-ben, az általános alsó korlát bizonyítása pedig [145]-ben került közlésre.

3.7. Tétel. (felső korlát Cohen és szerzőtársai [46] (33), alsó korlát K. és Östergård [145], Theorem 8)

$9 \leq K(2R + 4, R) \leq 12$ fennáll tetszőleges pozitív egész R esetén.

Bizonyítás. A felső korlát régóta ismert, ezért itt csak az alsó korlát bizonyításával foglalkozunk. Az alsó korlátra megadott egyenlőtlenség $R = 0$ esetén is nyilvánvalóan fennáll, ugyanis $K(4, 0) = 16$. (Tudjuk azt is – de nem használjuk fel a bizonyításhoz – hogy $K(6, 1) = K(8, 2) = 12$.) Indukcióval, indirekt lépésekkel bizonyítjuk, hogy a tétel állítása fennáll minden pozitív egész R esetén is. Tegyük fel, hogy igaz az állítás valamely $(R - 1)$ -re, de nem igaz R -re, azaz $K(2R + 2, R - 1) \geq 9$, de $K(2R + 4, R) = 7$ vagy $K(2R + 4, R) = 8$. (Hiszen $K(2R + 3, R) = 7$, és ennél kisebb $K(2R + 4, R)$ sem lehet.) Ekkor a 3.2. következmény szerint a $K(2R + 4, R)$ értékét meghatározó, 7 vagy 8 kódszóból álló bármely optimális kód 2-szürjektív.

A (3.13) formula szerint $\sigma_2(n, 2) \geq 9$ ha $n \geq 36$, ilyen n -ek esetén tehát 9-nél kevesebb kódszóból álló 2-szürjektív kód egyáltalán nem létezik. A $2 \leq n \leq 35$ intervallumban a 7, ill. 8 kódszóból álló bináris 2-szürjektív kódok összegyűjtése és elérési sugaruk kiszámítása folytán pedig bebizonyosodott, hogy 2-szürjektív $(2R + 4, M)R$ kód nem létezik, ha $M \in \{7, 8\}$ és $0 \leq R \leq 15$, ezáltal ellentmondáshoz jutunk az indukciós gondolatmenetben. (A 2-szürjektív kódok összegyűjtése és vizsgálata során megengedtük ugyanannak a kódszónak az ismétlődését az egyes kódokban.) A 7, ill. 8 kódszóból álló bináris 2-szürjektív kódok lehetséges elérési sugarainak a táblázatát a [145] cikk tartalmazza, ezt terjedelmi okból az értekezésbe teljes egészében nem másoltam át, azonban az $n \geq 16$ esetére ezeket az adatokat a Függelék A.2 táblázata mutatja. $\square$

A 3.7. tétel egyenlőtlenség-párjával a [46]-ben megadott hasonló egyenlőtlenség-pár (lásd 2.3.1 szakasz) alsó egyenlőtlenségében 2 egységnyit javítottunk.

A (d) esetre vonatkozó korábbi, az előbb tárgyalt ismeretek alapján a legfeljebb 6 kódszóból álló optimális térlefedő kódok méretét a következőképpen foglalhatjuk össze:

3.8. Állítás.

$K_2(n, R) = 2$ akkor és csak akkor áll fenn, ha $R < n < 2R + 2$;

$K_2(n, R) = 3$ nem lehetséges;

$K_2(n, R) = 4$ akkor és csak akkor áll fenn, ha $n = 2R + 2$;

$K_2(n, R) = 5$ nem lehetséges;

$K_2(n, R) = 6$ nem lehetséges.

Láttuk, hogy $K_2(n, R) \leq 7$ minden olyan esetben, amikor $n \leq 2R + 3$. Ha ezt az ismeretet kombináljuk a 3.7. tétel állításával, akkor megkapjuk a 3.8. állítás 8 kódszóig történő kiterjesztését eredményező következő tételt.

3.9. Tétel. (K. és Östergård [145])

$K_2(n, R) = 7$ akkor és csak akkor áll fenn, ha $R > 0$ és $n = 2R + 3$;

$K_2(n, R) = 8$ akkor és csak akkor áll fenn, ha $R = 0$ és $n = 3$.

3.6. Klasszifikációs eredmények bináris térlefedő kódokra

Klasszifikáció alatt adott paraméterekkel bíró matematikai objektumok izomfiaosztályai egy-egy reprezentánsának a megadását értjük. Az adott objektum-típustól függően sok esetben az ekvivalencia-osztályok markánsabb tulajdonságai alapján történő csoportosítást is érdemes elvégezni, de ezt a teendőt eleve nem értjük bele a klasszifikáció fogalmába. (Az izomfia és ekvivalencia szavakat itt egymás szinonimájaként használjuk.)

Először röviden összefoglaljuk az optimális bináris térlefedő kódokra vonatkozó klasszifikációs eredményeket.

(a) Tetszőleges n pozitív egész és $R = 0$ esetén az inekvivalens optimális térlefedő kódok száma 1.

(b_1) $n = 2^h - 1$, $R = 1$, $h = 3$, ill. $h = 4$ esetén az inekvivalens optimális térlefedő kódok száma 1, ill. 5983, a 4-nél nagyobb h esetre vonatkozó hasonló kérdés megoldatlan, nehéz probléma, $h = 4$ -re is csak nemrég sikerült Östergårdnak és Pottónennek megadnia a választ.

(b_2) $n = 2^h$, $R = 1$, $h = 3$ esetén az inekvivalens optimális térlefedő kódok száma 10, a 3-nál nagyobb h esetre vonatkozó hasonló kérdés megoldatlan probléma.

(c) $n = 23$, $R = 3$ esetén az inekvivalens optimális térlefedő kódok száma 1.

(d_1) Minden olyan esetben, amikor $K(n, R) = 2$, az inekvivalens optimális térlefedő kódok száma $2R - n + 2$.

(d_2) Minden olyan esetben, amikor $K(n, R) = 4$, az inekvivalens optimális térlefedő kódok száma $\lfloor (\frac{R}{2} + 1)^2 \rfloor$.

(d_3) Minden olyan esetben, amikor $K(n, R) = 7$, az inekvivalens optimális térlefedő kódok számát megadja az $1/((1-x)^3(1-x^2)^2(1-x^3))$ kifejezés végtelen polinom kifejtésében x^{R-1} együtthatója.

(e) A $K(6, 1) = 12$, $K(8, 2) = 12$ esetekhez tartozó inekvivalens optimális térlefedő kódok száma 2, ill. 277. A $K(9, 2) = 16$ esethez tartozó inekvivalens optimális térlefedő kódok száma 4. Az optimális kódok számának kérdése az $n = 9$, $R = 1$ esetben megoldatlan.

(f) A $K(10, 3) = 12$ egyenlőségnek megfelelő inekvivalens optimális térlefedő kódok száma 11481.

Folytatjuk a felsorolt esetek részletesebb kifejtésével. Az (a) esethez nincs mit hozzátenni. Egy zéró elérési sugarú kód a Hamming tér összes pontját tartalmazza, amiből az ilyen kódok unicitása is következik.

A (b_1) esetben $n = 7$, $R = 1$, $K(n, R) = 16$, amely a Hamming kóddal megvalósítható. Az optimális kód unicitását elsőként Zaremba [9] bizonyította, később még sokan

megegerősítették. A $K(15, 1) = 2048$ egyenlőséghez tartozó inekvivalens perfekt optimális kódok számának meghatározásáról a [157] cikk számol be.

A 4-nél nagyobb h értékekhez tartozó $n = 2^h - 1$ dimenziós $R = 1$ elérési sugarú perfekt optimális kódokról annyit tudunk, hogy h növelésével ezek száma robbanásszerűen növekszik. Ide vonatkozó részeredmények Weakley [141] munkájában találhatók.

A (b_2) esetben $n = 8$, $R = 1$, $K(n, R) = 32$, az ezen értékeknek megfelelő optimális térlefedő kódok száma 10, leírásuk megtalálható a [118] publikációban. A 10 optimális kód mindegyike 2-szürjektív, 4 közülük önkomplementer.

Az $n = 2^h$ dimenziós, $R = 1$ elérési sugarú optimális kódok számát $h > 3$ esetén nem ismerjük.

(c) $n = 23$, $R = 3$ esetén az egyetlen optimális térlefedő kód a bináris Golay kód. Az unitás első bizonyítása Snover [33] PhD disszertációjában található, folyóiratban megjelent egyszerűbb bizonyítást adott rá Delsarte és Goethals [36].

(d₁) Láttuk, hogy $K(n, R) = 2$ akkor és csak akkor áll fenn, ha $R < n < 2R + 2$. A megfelelő inekvivalens kódok száma $2R - n + 2$ (lásd [118]), ezek úgy képezhetők, hogy legfeljebb $2R - n + 1$ koordinátahelyen a két kódszóban azonos, a többi koordinátahelyen a két kódszóban különböző értéket helyezünk el.

(d₂) Minden olyan esetben, amikor $K(n, R) = 4$, az inekvivalens optimális térlefedő kódok száma $\lfloor (\frac{R}{2} + 1)^2 \rfloor$ (ismét lásd [118]).

Az optimális $(2R + 2, 4)R$ kódok válfajainak bemutatására egy olyan konstrukciót alkalmazunk, melyhez hasonló konstrukciót a $(2R + 3, 7)R$, $(2R + 4, 12)R$, $(2R + 5, 16)R$ kódokra is alkalmazni fogunk, a két utóbbi esetben azonban nem tudjuk ily módon az összes inekvivalens kódot előállítani, továbbá a két utóbbi eset annyiban is eltér az első kettőtől, hogy a $K(2R + 2, R) = 4$ és $K(2R + 3, R) = 7$ egyenlőségek bizonyítottan fennállnak minden pozitív egész R esetén, a $K(2R + 4, R) = 12$ és $K(2R + 5, R) = 16$ egyenlőségek általános érvényűségének a kérdése viszont jelenleg még nyitott probléma.

A konstrukció bemutatásához a kódokra sematikus, táblázatos jelölést alkalmazunk, ahol minden oszlophoz egy-egy kódszó és a kódszavak minden koordinátájához egy-egy oszlop tartozik. A szerkezet szemléltetésének kedvéért a táblázatban esetleg vízszintes és/vagy függőleges választó vonalakat helyezünk el. Eleinte használni fogjuk a táblázatos jelölés mellett a hagyományos, kódszavak halmazaként megadott jelölést is, amelynél az egyszerűség kedvéért a kódszavak befoglaló zárójeleit elhagyjuk, és a koordinátákat szóköz vagy más szeparátor nélkül soroljuk fel.

A 4 szóból álló optimális kódok tárgyalásához induljunk ki a $K(2, 0) = 4$ egyenlőséghez tartozó

$$\begin{array}{|c|c|} \hline 0 & 0 \\ \hline 0 & 1 \\ \hline 1 & 0 \\ \hline 1 & 1 \\ \hline \end{array} = \{00, 01, 10, 11\}$$

optimális térlefedő kódból, amely a Z_2^2 térben egy $(2, 4)0$ kód. Következő lépésként egészítsük ki e kód szavait egy paritás bittel. Ezáltal a

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} = \{000, 011, 101, 110\}$$

kódhoz jutunk. Végül tekintsük azokat a $C(n_1, n_2, n_3)$ kódokat, amelyeket úgy kapunk, hogy a fenti, paritás bittel kiegészített, kód oszlopait rendre n_1, n_2, n_3 -szor megismétljük. A n_1, n_2, n_3 értékek között a 0-t is megengedjük. Ekkor a következőt állítjuk:

3.10. Állítás.

$C(n_1, n_2, n_3)$ akkor és csak akkor optimális térlefedő kód, ha az n_1, n_2, n_3 nemnegatív egészek között pontosan egy páros értékű fordul elő. Továbbá: bármely $(2R + 2, 4)R$ kód ekvivalens egy, az előző feltételt teljesítő $C(n_1, n_2, n_3)$ kóddal.

A 3.10. állítás (más megfogalmazásban), és annak bizonyítása megtalálható a [118] publikációban. Ezért a bizonyítást nem ismertetem, hanem csak annyit szeretnék megjegyezni, hogy tetszőleges n -re az inekvivalens kódok képzéséhez tekinthetjük az $n = 2R + 2$ páros egész azon $n_1 + n_2 + n_3 = n$ partícióit, melyekre $n_1 \geq n_2$, mindkettő páratlan, n_3 pedig páros. A két legegyszerűbb eset a következő:

$n = 2, R = 0$ esetén egyetlen ilyen partíció van: $n_1 = n_2 = 1, n_3 = 0$. (Ebben az esetben visszajutottunk ahhoz a kódhoz, amiből kiindultunk.)

$n = 4, R = 1$ esetén a megfelelő partíciók száma 2: $n_1 = 3, n_2 = 1, n_3 = 0$, ill. $n_1 = n_2 = 1, n_3 = 2$.

Az $n + 2$ -höz tartozó megfelelő partíciókat megkaphatjuk úgy, hogy az n -re már összegyűjtött partíciók mindegyikében n_3 értékét 2-vel megnöveljük és az így kapott halmazt kibővítjük az $n_3 = 0$ rögzítésével képezhető megfelelő partíciókkal.

(d_3) A $K(n, R) = 7$ egyenlőséghez tartozó inekvivalens optimális térlefedő kódok képzéséhez az előzőhöz hasonló konstrukciót lehet alkalmazni. Az erre az esetre vonatkozó, a következőkben megfogalmazott állításokat és bizonyításokat lényegesebb változtatás nélkül a [139] cikkből vettem át.

Ezúttal induljunk ki a $K(5, 1) = 7$ egyenlőséghez tartozó

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

optimális térlefedő kódból. Megint a táblázat sorai alkotják a kódszavakat, de itt és a továbbiakban már nem írjuk fel azokat explicit módon. Ezt megint – az előző konstrukcióhoz hasonlóan – paritás bittel kiegészítve a következő kódot kapjuk:

0	0	0	0	0	0
0	0	1	1	1	1
0	1	0	1	1	1
1	0	0	1	1	1
1	1	1	0	0	1
1	1	1	0	1	0
1	1	1	1	0	0

Ez a kód ugyan nem optimális térlefedő kód, de – mint látható – szép szimmetrikus struktúrával rendelkezik, és hamarosan ki fog derülni, hogy segítségével az összes hét szóból álló optimális térlefedő kód leírható. Jelöljük az egyes oszlopok által meghatározott 1 dimenziós kódokat C_i -vel ($i = 1, 2, \dots, 6$), vagyis legyen

$$\begin{aligned} C_1 &= \{0, 0, 0, 1, 1, 1, 1\}, \\ C_2 &= \{0, 0, 1, 0, 1, 1, 1\}, \\ C_3 &= \{0, 1, 0, 0, 1, 1, 1\}, \\ C_4 &= \{0, 1, 1, 1, 0, 0, 1\}, \\ C_5 &= \{0, 1, 1, 1, 0, 1, 0\}, \\ C_6 &= \{0, 1, 1, 1, 1, 0, 0\}. \end{aligned}$$

Az előbbi esethez hasonlóan bevezetjük a $C(n_1, n_2, n_3, n_4, n_5, n_6)$ kódokat is, melyeket megint úgy kapunk, hogy a paritás bittel kiegészített kód oszlopait $n_1, n_2, \dots, n_6$ -szor ismételjük. Ekkor $C(1, 1, 1, 1, 1, 0)$ visszaadja a kiindulási kódot, $C(3, 1, 1, 1, 1, 0)$, $C(1, 1, 1, 3, 1, 0)$ és $C(1, 1, 1, 1, 1, 2)$ pedig előállítja a $K(7, 2) = 7$ egyenlőséghez tartozó 3 inekvivalens optimális kódot. Ezekre a legegyszerűbb 7 szavas optimális kódokra, $n = 5, R = 1$, ill. $n = 7, R = 2$ esetre vonatkozó klasszifikációs eredmény Stanton és Kalbfleisch [18], ill. Östergård és Weakley [118] munkájában található.

Ugyanezek a kódok az elemi C_i kódokkal a következőképpen fejezhetők ki: Az egyetlen $(5, 7)1$ kód a $|C_1|C_2|C_3|C_4|C_5|$ kód, a három inekvivalens $(7, 7)2$ kód pedig az előbbihez a $|C_1|C_1|$, $|C_4|C_4|$, ill. $|C_6|C_6|$ kódot hozzáfűzve adódik. Az $(5, 7)1$ és $(7, 7)2$ kódok szerkezetének ismeretében egyszerűen adódik a következő állítás:

3.11. Állítás. (*K. és Östergård [139], Corollary 2.1*)

Bármely a csupa 0-ból álló kódszót tartalmazó és $|C_1|C_2|C_3|C_4|C_5|D|$ alakban felírt $(7, 7)2$ kód esetén $D = |C_i|C_j|$, ahol $i = j$, vagy $i = 6$, vagy $j = 6$.

Az általános esetre bebizonyítjuk a következő tételt:

3.12. Tétel. (*K. és Östergård [139], Theorem 2.2*)

$C = C(n_1, n_2, n_3, n_4, n_5, n_6)$ akkor és csak akkor optimális térlefedő kód, ha az $n_1, n_2, \dots, n_6$ nemnegatív egészek között pontosan egy páros értékű fordul elő. Továbbá: bármely optimális $(2R + 3, 7)R$ kód ekvivalens egy, az előző feltételt teljesítő $C(n_1, n_2, n_3, n_4, n_5, n_6)$ kóddal.

Bizonyítás. Tudjuk, hogy $K(n, R) = 7$ akkor és csak akkor áll fenn, ha $n = 2R + 3$. Ezért a tétel első állítását úgy is fogalmazhatjuk, hogy C elérési sugara akkor és csak akkor $(n-3)/2$, ahol $n = \sum_{i=1}^6 n_i$, ha az $n_1, n_2, \dots, n_6$ nemnegatív egészek között pontosan egy páros értékű van. Ennek bizonyításához tegyük fel először, hogy pontosan egy páros érték fordul elő. Szimmetria miatt elég azt az egy esetet vizsgálni, amikor n_1, n_2, n_3, n_4, n_5 páratlan, n_6 pedig páros. Legyen $x = |x_1|x_2|x_3|x_4|x_5|x_6|$ a bináris Z_2^n Hamming tér tetszőleges pontja, ahol $x_i \in Z_2^{n_i}$ és x_i a $C(n_1, n_2, n_3, n_4, n_5, n_6)$ kód szerkezete szerint particionált. Jelölje c_i e kód i -edik szavát, w_i pedig az x_i vektor súlyát, vagyis a benne szereplő 1 értékű komponensek számát. Ekkor

$$\begin{aligned} d(x, c_1) &= w_1 + w_2 + w_3 + w_4 + w_5 + w_6, \\ d(x, c_2) &= w_1 + w_2 + (n_3 - w_3) + (n_4 - w_4) + (n_5 - w_5) + (n_6 - w_6), \\ d(x, c_3) &= w_1 + (n_2 - w_2) + w_3 + (n_4 - w_4) + (n_5 - w_5) + (n_6 - w_6), \\ d(x, c_4) &= (n_1 - w_1) + w_2 + w_3 + (n_4 - w_4) + (n_5 - w_5) + (n_6 - w_6), \\ d(x, c_5) &= (n_1 - w_1) + (n_2 - w_2) + (n_3 - w_3) + w_4 + w_5 + (n_6 - w_6), \\ d(x, c_6) &= (n_1 - w_1) + (n_2 - w_2) + (n_3 - w_3) + w_4 + (n_5 - w_5) + w_6, \\ d(x, c_7) &= (n_1 - w_1) + (n_2 - w_2) + (n_3 - w_3) + (n_4 - w_4) + w_5 + w_6, \end{aligned}$$

és következésképpen

$$d(x, C) \leq \frac{2d(x, c_1) + \sum_{i=2}^7 d(x, c_i)}{8} = \frac{4 \sum_{i=1}^6 n_i}{8} = n/2.$$

Tegyük fel, hogy $d(x, C) > (n-3)/2$. Ekkor $d(x, C) = (n-1)/2$ (mivel n páratlan és $d(x, C) \leq n/2$). Az n_i -k paritására tett feltételből következik, hogy $d(x, c_1)$, $d(x, c_6)$, $d(x, c_7)$ paritása azonos, és hasonlóan $d(x, c_2)$, $d(x, c_3)$, $d(x, c_4)$, $d(x, c_5)$ paritása is azonos, de az előző három paritástól eltérő. A $d(x, c_1)$, $d(x, c_2)$, $\dots$, $d(x, c_7)$ távolságokat tekintve, közülük az elsőt kétszer véve láttuk, hogy e nyolc távolság összege $4n$, s tudjuk, hogy mindegyik legalább $(n-1)/2$, továbbá négy-négy távolság páros, ill. páratlan egész. Ez csak úgy lehetséges, ha közülük négynek az értéke $(n-1)/2$, szintén négynek az értéke pedig $(n+1)/2$. Mindezek alapján $d(x, c_1) = d(x, c_6) = d(x, c_7)$ és $d(x, c_2) = d(x, c_3) = d(x, c_4) = d(x, c_5)$. Ekkor

$$\begin{aligned} 3n &= d(x, c_1) + 2d(x, c_4) + d(x, c_5) + d(x, c_6) + d(x, c_7) \\ &= 5n_1 - 4w_1 + 3n_2 + 3n_3 + 3n_4 + 3n_5 + 3n_6 \\ &= 3n + (2n_1 - 4w_1), \end{aligned}$$

amiből az adódna, hogy n_1 páros. Mivel kiindulásképpen feltettük, hogy páratlan, ellentmondáshoz jutottunk, amiből következik, hogy tetszőleges $x \in Z_2^n$ esetén $d(x, C) \leq (n-3)/2$.

Egy olyan x vektort véve, melyre $w_i = \lceil \frac{n_i}{2} \rceil$ valamennyi $i = 1, 2, \dots, 6$ indexre, rövid számolással azt kapjuk, hogy $d(x, C) = (n-3)/2$, tehát a vizsgált kód elérési sugara pontosan $(n-3)/2$.

A szükségesség bizonyításához tegyük fel, hogy $C(n_1, n_2, n_3, n_4, n_5, n_6)$ optimális térlefedő kód, melyre a páros n_i -k száma 1-nél nagyobb. Tudjuk, hogy $K(n, R) = 7$ csak páratlan n esetén lehetséges, ezért csak azzal a két esettel kell foglalkoznunk, amikor a páros n_i -k száma 3 vagy 5. Szimmetria miatt elég a két esetnek azokat a rész-eseteit nézni amikor n_1, n_2, n_3 , vagy n_1, n_2, n_4 , vagy n_1, n_2, n_3, n_4, n_5 páratlan, a hátralévő n_i -k

pedig párosak. Minden ilyen esetben legyen $w_i = \lfloor \frac{n_i}{2} \rfloor$, ha $i = 1, 2, 3, 5$, és $w_i = \lceil \frac{n_i}{2} \rceil$, ha $i = 4, 6$, ahol w_i , mint korábban is, x_i súlyát jelenti egy tetszőleges $x = |x_1|x_2|x_3|x_4|x_5|x_6|$ vektor esetén. Mindegyik esetben azt kapjuk, hogy $d(x, C) \geq (n-1)/2$, tehát a C kód elérési sugara nem lehet $(n-3)/2$.

A 3.12. tétel második állításának a bizonyításához legyen $C = C^{(R)}$ egy tetszőleges $(2R+3, 7)R$ kód, ahol $R \geq 1$. $R = 1$ esetén egyetlen $(5, 7)1$ kód létezik (lásd [18]), ez szükségképpen ekvivalens azzal a kóddal, melyből a $C = C(n_1, n_2, n_3, n_4, n_5, n_6)$ kód konstrukciójához kiindultunk. $R \geq 2$ esetén a $C^{(R)}$ kód nem lehet 2-szürjektív (lásd [31] az $R > 6$ esetre, ill. [145], Table 1 az $R \leq 6$ esetre), ezért $C^{(R)} \equiv |C^{(R-1)}|X|$, ahol $C^{(R-1)}$ dimenziója $2R+1$, X dimenziója pedig 2, és az utóbbi elérési sugara 0-nál nagyobb. Mivel egy particionált kód elérési sugara nem lehet kisebb, mint a rész-kódok elérési sugarainak az összege, lásd (1.7), ezért a $C^{(R-1)}$ kód elérési sugara $R-1$, az X kód elérési sugara pedig 1. A gondolatmenet ismételt alkalmazásával azt kapjuk, hogy

$$C^{(R)} \equiv |C^{(1)}|X^{(1)}|X^{(2)}|\dots|X^{(R-1)}|,$$

ahol $C^{(1)}$ egy $(5, 7)1$ kód, $|C^{(1)}|X^{(1)}|$ pedig egy $(7, 7)2$ kód. Mivel a $C^{(R)}$ kódot az $X^{(i)}$ kódok tetszőlegesen permutált sorrendjében képezhetjük a rekurzió során, ezért minden egyes $|C^{(1)}|X^{(i)}|$ kód szintén $(7, 7)2$ kód.

A $C^{(1)}$ kód választható úgy, hogy azonos legyen a $|C_1|C_2|C_3|C_4|C_5|$, vagyis a $C(1, 1, 1, 1, 1, 0)$ kóddal, ennek megfelelően szükség esetén az $X^{(i)}$ kódokban is permutálva a sorokat, majd ezt követően, ugyancsak szükség esetén, oszlopok komplementálásával elérhető, hogy az első kódszó csupa 0-ból álljon. Ezáltal olyan, az $X^{(i)}$ kódokkal ekvivalens $Y^{(i)}$ kódokhoz jutunk, melyekkel fennáll

$$C^{(R)} \equiv |C^{(1)}|Y^{(1)}|Y^{(2)}|\dots|Y^{(R-1)}|,$$

ahol $|C^{(1)}|Y^{(i)}|$ egy $(7, 7)2$ kód minden i -re, továbbá az összefűzött $|C^{(1)}|Y^{(1)}|Y^{(2)}|\dots|Y^{(R-1)}|$ kód is tartalmazza a csupa zéróból álló kódszót. Ekkor pedig a 3.11. állítás szerint $Y^{(i)}$ azonos egy $|C_j|C_k|$ kóddal, tehát $C^{(R)} \equiv C(n_1, n_2, n_3, n_4, n_5, n_6)$ az n_i nemnegatív egészek valamely értékrendszerével. Mivel ez a kód optimális, az $n_1, n_2, n_3, n_4, n_5, n_6$ egészek között pontosan egy páros értékű van. $\square$

Az inekvivalens optimális kódok számára a következő formula adható:

3.13. Tétel. (*K. és Östergård [139], Theorem 3.3*)

Tetszőleges pozitív R esetén az inekvivalens $(2R+3, 7)R$ kódok számát megadja x^{R-1} együtthatója az

$$\frac{1}{(1-x)^3(1-x^2)^2(1-x^3)}$$

függvény kifejtésében.

Az együtthatók sorozatát a *The on-line encyclopedia of integer sequences* [175] A002625 sorszámával tartalmazza; a sorozat első tíz eleme 1, 3, 8, 17, 33, 58, 97, 153, 233, 342.

Bizonyítás. A 3.12. tétel és az előző szakasz eredményei szerint egy 7 kódszóból álló bináris kód akkor és csak optimális térlefedő kód, ha ekvivalens egy

$$C(2m_1 + 1, 2m_2 + 1, 2m_3 + 1, 2m_4 + 1, 2m_5 + 1, 2m_6)$$

alakú kóddal, ahol $m_1, m_2, m_3, m_4, m_5, m_6$ nemnegatív egészek és $\sum_{i=1}^6 m_i = R - 1$. Egy ilyen kód viszont akkor és csak akkor ekvivalens egy másik, ugyanilyen alakban írható

$$C(2m'_1 + 1, 2m'_2 + 1, 2m'_3 + 1, 2m'_4 + 1, 2m'_5 + 1, 2m'_6)$$

kóddal, ha $\{m_1, m_2, m_3\} = \{m'_1, m'_2, m'_3\}$, $\{m_4, m_5\} = \{m'_4, m'_5\}$ és $m_6 = m'_6$. Az utóbbi állítás helyessége a szóban forgó kódok szerkezetéből látszik. Eszerint az inekvivalens optimális $(2R + 3, 7)R$ kódok $Q(R)$ számát megadja az

$$\begin{aligned} m_1 + m_2 + m_3 + m_4 + m_5 + m_6 &= R - 1, \\ m_1 &\geq m_2 \geq m_3 \geq 0, \\ m_4 &\geq m_5 \geq 0, \\ m_6 &\geq 0 \end{aligned}$$

feltételrendszer különböző egészértékű megoldásainak a száma. A [38]-ban alkalmazott módszertant követve azt kapjuk, hogy

$$Q(R) = \sum_{\substack{N_1 + N_2 + N_3 = R - 1 \\ N_1, N_2, N_3 \geq 0}} P(N_1, 1)P(N_2, 2)P(N_3, 3),$$

ahol $P(N, t)$ az N egész legfeljebb t pozitív tagból álló partícióinak a számát jelöli, melyre a

$$\sum_{N=0}^{\infty} P(N, t)x^N = \prod_{j=1}^t \frac{1}{1 - x^j}.$$

formula ismeretes. Az utóbbi két képletből következik, hogy

$$\sum_{R=1}^{\infty} Q(R)x^{R-1} = \frac{1}{(1-x)^3(1-x^2)^2(1-x^3)}.$$

□

A $(2R + 4, 12)R$ kódok vizsgálatára rátérve, először összefoglaljuk az $R \leq 3$ esetre vonatkozó ismereteket. Ezekben az esetekben tudjuk, hogy $K(2R + 4, R) = 12$.

3.14. Állítás.

A $K(6, 1) = 12$ egyenlőséghez tartozó inekvivalens optimális kódok száma 2, mindkettő kiegyensúlyozott és 2-szűrjektív. A két optimális kód közül az egyik ezenkívül önkomplementer és 3-szűrjektív.

A $K(8, 2) = 12$ egyenlőséghez tartozó inekvivalens optimális kódok száma 277, ezek közül kiegyensúlyozott 155 kód, önkomplementer mindössze 1 kód. A 155 kiegyensúlyozott optimális kód közül 2-szűrjektív 137 kód, a 122 kiegyensúlyozatlan optimális kód közül pedig 2-szűrjektív 113 kód.

A fenti két esetre az egyenlőséget Stanton és Kalbfleisch [18], ill. Blass és Litsyn [110] bizonyították, az inekvivalens optimális kódok számának meghatározása mindkét esetre Östergård és Weakley [118] eredménye. Az optimális kódok kiegyensúlyozottság és szűrjektivitás szerinti megoszlását már én tettem hozzá.

A következő tételben megfogalmazott esetre az egyenlőség bizonyítása és a klasszifikációs eredmény egyaránt K. és Östergård [155] eredménye.

3.15. Tétel. *(K. és Östergård [155], Theorem 6)*

$K(10, 3) = 12$ és az ehhez az esethez tartozó inekvivalens optimális kódok száma 11481, melyek közül kiegyensúlyozott 5543 kód, önkomplementer 3 kód. Az 5543 kiegyensúlyozott optimális kód közül 2-szűrjektiv 1490 kód, az 5938 kiegyensúlyozatlan optimális kód közül pedig 2-szűrjektiv 1589 kód.

Bizonyítás. Számítógéppel végzett klasszifikáció. □

A $(2R+4, 12)R$ kódokat átfogóbban vizsgálva azt tapasztaljuk, hogy a viszonylag egyszerűbb $(2R+2, 4)R$, $(2R+3, 7)R$ kódok esetére alkalmazott módszerrel az összes inekvivalens optimális kódot nem tudjuk ugyan előállítani, de olyan konstrukciót tudunk találni, melynek segítségével számos $(2R+4, 12)R$ kód előállítható.

Az egyik optimális $(6, 12)1$ kódból kiindulva, azt paritás bittel kiegészítve, az alábbi táblázattal megadott kódhoz jutunk:

0	0	0	0	0	1	1
0	0	0	0	1	0	1
0	0	0	1	0	0	1
0	0	1	1	1	1	0
0	1	0	1	1	1	0
1	0	0	1	1	1	0
1	1	1	0	1	1	1
1	1	1	1	0	1	1
1	1	1	1	1	0	1
0	1	1	0	0	0	0
1	0	1	0	0	0	0
1	1	0	0	0	0	0

A korábbi esetekhez hasonló módon bevezetett $C(n_1, n_2, n_3, n_4, n_5, n_6, n_7)$ kódra $n = \sum_{i=1}^7 n_i$ jelöléssel a következőt lehet állítani:

3.16. Tétel.

Ha $n \geq 6$ és az $n_1, n_2, \dots, n_7$ nemnegatív egészek között pontosan egy páros értékű van, akkor a $C(n_1, n_2, n_3, n_4, n_5, n_6, n_7)$ kód elérési sugara $\frac{n-4}{2}$.

Bizonyítás. A 3.12. tétel bizonyításához hasonló módon indulunk el, az ott bevezetett jelöléseket alkalmazva. Legyen $x = |x_1|x_2|x_3|x_4|x_5|x_6|x_7|$ a Z_2^n tér tetszőleges pontja. Írjuk fel megint ennek a particionált formában megadott x pontnak a kódszavaktól való távolságát.

$$\begin{aligned}
d(x, c_1) &= w_1 + w_2 + w_3 + w_4 + w_5 + (n_6 - w_6) + (n_7 - w_7), \\
d(x, c_2) &= w_1 + w_2 + w_3 + w_4 + (n_5 - w_5) + w_6 + (n_7 - w_7), \\
d(x, c_3) &= w_1 + w_2 + w_3 + (n_4 - w_4) + w_5 + w_6 + (n_7 - w_7), \\
d(x, c_4) &= w_1 + w_2 + (n_3 - w_3) + (n_4 - w_4) + (n_5 - w_5) + (n_6 - w_6) + w_7, \\
d(x, c_5) &= w_1 + (n_2 - w_2) + w_3 + (n_4 - w_4) + (n_5 - w_5) + (n_6 - w_6) + w_7, \\
d(x, c_6) &= (n_1 - w_1) + w_2 + w_3 + (n_4 - w_4) + (n_5 - w_5) + (n_6 - w_6) + w_7, \\
d(x, c_7) &= (n_1 - w_1) + (n_2 - w_2) + (n_3 - w_3) + w_4 + (n_5 - w_5) + (n_6 - w_6) + (n_7 - w_7), \\
d(x, c_8) &= (n_1 - w_1) + (n_2 - w_2) + (n_3 - w_3) + (n_4 - w_4) + w_5 + (n_6 - w_6) + (n_7 - w_7), \\
d(x, c_9) &= (n_1 - w_1) + (n_2 - w_2) + (n_3 - w_3) + (n_4 - w_4) + (n_5 - w_5) + w_6 + (n_7 - w_7), \\
d(x, c_{10}) &= w_1 + (n_2 - w_2) + (n_3 - w_3) + w_4 + w_5 + w_6 + w_7, \\
d(x, c_{11}) &= (n_1 - w_1) + w_2 + (n_3 - w_3) + w_4 + w_5 + w_6 + w_7, \\
d(x, c_{12}) &= (n_1 - w_1) + (n_2 - w_2) + w_3 + w_4 + w_5 + w_6 + w_7,
\end{aligned}$$

és ennél fogva

$$d(x, C) \leq \frac{\sum_{i=1}^{12} d(x, c_i)}{12} = \frac{6 \sum_{i=1}^7 n_i}{12} = n/2.$$

Tegyük fel, hogy $d(x, C) > (n-4)/2$. Ekkor $d(x, c_j) \geq (n-2)/2$ minden kódszóra, mivel n most páros. Ebből az $y_i = 2w_i - n_i$ változók bevezetésével a következő egyenlőtlenség-rendszert kapjuk:

$$\begin{aligned}
& y_1 + y_2 + y_3 + y_4 + y_5 - y_6 - y_7 + 2 \geq 0 \\
& y_1 + y_2 + y_3 + y_4 - y_5 + y_6 - y_7 + 2 \geq 0 \\
& y_1 + y_2 + y_3 - y_4 + y_5 + y_6 - y_7 + 2 \geq 0 \\
\\
& y_1 + y_2 - y_3 - y_4 - y_5 - y_6 + y_7 + 2 \geq 0 \\
& y_1 - y_2 + y_3 - y_4 - y_5 - y_6 + y_7 + 2 \geq 0 \\
- & y_1 + y_2 + y_3 - y_4 - y_5 - y_6 + y_7 + 2 \geq 0 \\
\\
- & y_1 - y_2 - y_3 + y_4 - y_5 - y_6 - y_7 + 2 \geq 0 \\
- & y_1 - y_2 - y_3 - y_4 + y_5 - y_6 - y_7 + 2 \geq 0 \\
- & y_1 - y_2 - y_3 - y_4 - y_5 + y_6 - y_7 + 2 \geq 0 \\
\\
& y_1 - y_2 - y_3 + y_4 + y_5 + y_6 + y_7 + 2 \geq 0 \\
- & y_1 + y_2 - y_3 + y_4 + y_5 + y_6 + y_7 + 2 \geq 0 \\
- & y_1 - y_2 + y_3 + y_4 + y_5 + y_6 + y_7 + 2 \geq 0
\end{aligned}$$

Az y_i változó paritása n_i paritásával azonos, tehát közöttük egy és csak egy a páros értékű egész, viszont az y_i -k negatív értékűek is lehetnek. Megmutatjuk, hogy az egyenlőtlenség-rendszer feltételi halmaza korlátos, mégpedig $|y_i| \leq 2$ minden lehetséges i index esetén. Legegyszerűbben y_7 korlátossága bizonyítható, ugyanis

$$\frac{n-2}{2} \leq d(x, C) \leq \frac{d(x, c_1) + d(x, c_9)}{2} = \frac{n + n_7 - 2w_7}{2},$$

amiből $y_7 \leq 2$, és hasonlóan

$$\frac{n-2}{2} \leq d(x, C) \leq \frac{d(x, c_4) + d(x, c_{12})}{2} = \frac{n + 2w_7 - n_7}{2},$$

amiből $y_7 \geq -2$. A többi y_i korlátosságának bizonyításához kicsit csúnyább súlyozott átlagra van szükség, például

$$\begin{aligned} \frac{n-2}{2} \leq d(x, C) &\leq \\ &\leq \frac{3d(x, c_1) + d(x, c_2) + d(x, c_3) + 2d(x, c_4) + 2d(x, c_5) + 2d(x, c_9) + 3d(x, c_{10})}{14} = \\ &= \frac{7n + 10w_1 - 5n_1}{14}, \end{aligned}$$

amiből $y_1 \geq -2$. A hátralévő $y_1 \leq 2$ és $-2 \leq y_i \leq 2$ ($i = 2, 3, \dots, 6$) korlát igazolásához elég az egyenlőtlenség-rendszer szimmetriájára hivatkozni.

Ismerve az $|y_i| \leq 2$ korlátokat, most már nagyon egyszerű számítógépes vizsgálattal megmutatható, hogy az y_i -kre felírt egyenlőtlenség-rendszernek nincs olyan egész értékű megoldása, melyre valamelyik, de csak az egyik y_i páros, az összes többi pedig páratlan. Ezzel bizonyítást nyer, hogy $d(x, C) \leq (n-4)/2$.

A fordított $d(x, C) \geq (n-4)/2$ egyenlőtlenség bizonyításához most választhatunk akár olyan x vektort, melyre $w_i = \lfloor \frac{n_i}{2} \rfloor$ minden $i = 1, 2, \dots, 7$ indexre, akár olyat, melyre $w_i = \lceil \frac{n_i}{2} \rceil$ minden i -re. Mindkét esetben azt kapjuk, hogy $d(x, C) = (n-4)/2$, tehát a vizsgált kód elérési sugara pontosan $(n-4)/2$. $\square$

Megmutatható, hogy $R = 1, 2, 3, 4$, $n = 2R+4$ esetén a 3.16. tétel alapján konstruálható inekvivalens kódok száma 2, 6, 17, 39, továbbá tetszőleges R esetén az ilyen inekvivalens kódok számát megadja x^{R-1} együtthatója a

$$\frac{2 + 3x^2 + 2x^3 + 3x^4 + 2x^5 + x^6 + x^7}{(1-x)^3(1-x^2)(1-x^3)(1-x^4)(1-x^6)}$$

függvény kifejtésében. Ebből az önkomplementer ($n_7 = 0$) kódok száma az

$$\frac{1 - x + x^2 + x^4}{(1-x)^2(1-x^2)(1-x^3)(1-x^4)(1-x^6)}$$

függvény kifejtése alapján, a nem önkomplementer kódok száma páros értékű pozitív n_7 esetén az

$$\frac{x(1 - x + x^2 + x^4)}{(1-x)^3(1-x^2)(1-x^3)(1-x^4)(1-x^6)}$$

függvény, páratlan értékű n_7 esetén az

$$\frac{1}{(1-x)^4(1-x^2)^2(1-x^3)}$$

függvény kifejtése alapján adódik a partíciókra vonatkozó formulából levezetve.

Tudjuk, hogy az inekvivalens $(6, 12)_1$ kódok száma 2. Ezeket még maradéktalanul megadja a 3.16. tétel konstrukciója. Könnyen belátható, hogy ezek éppen a 3.16. tételben szereplő $C(1, 1, 1, 1, 1, 1, 0)$ és $C(1, 1, 1, 1, 1, 0, 1)$ kódok. Viszont $R = 2$ és $R = 3$ esetén nem kapjuk meg az összes optimális $(2R + 4, 12)_R$ kódot ezzel a konstrukcióval, hiszen ezek száma 277, ill. 11481, tehát jóval több, mint a 3.16. tétel konstrukciója szerint adódó 6, ill. 17 kód. Ha pedig $R \geq 4$, akkor már $K(12, 4)$ pontos értékét sem ismerjük.

A vizsgált kérdéskör nehézségére utal a talált inekvivalens kódok számának gyors növekedése mellett az is, hogy a 2-szűrjektív $(8, 12)_2$ kódok közül 24 kód a két optimális $(6, 12)_1$ kód kiterjesztése, 226 kód viszont nem kapható meg ezek kiterjesztéseként, továbbá, hogy az optimális $(2R + 4, 12)_R$ térlefedő kódok között $R = 2$ -től már kiegyensúlyozatlan kódok is megjelennek. Az önkomplementer kódokra szorítkozva viszont azt találtuk, hogy egyetlen önkomplementer $(8, 12)_2$ kód és 3 önkomplementer $(10, 12)_3$ kód van, tehát nincs más ilyen kód, mint a 3.16. tétel konstrukciója alapján is megkapható $C(3, 1, 1, 1, 1, 1, 0)$, ill. $C(5, 1, 1, 1, 1, 1, 0)$, $C(3, 3, 1, 1, 1, 1, 0)$, $C(3, 1, 1, 3, 1, 1, 0)$ kódok.

Ezzel az (e) és (f) esetekhez tartozó optimális kódok áttekintésével majdnem végeztünk, már csak (e) -ből a $K(9, 2) = 16$ eset van hátra. Ismét általánosabban a $(2R + 5, 16)_R$ kódokat tanulmányozzuk, ennek megfelelően a $(7, 16)_1$ Hamming kódból indulunk el, annak kódszavait kibővítjük egy paritás bittel. A korábbi esetekhez hasonló táblázatos jelölést alkalmazzuk, de lineáris kódról lévén szó, csak annyi sort veszünk fel a táblázatba, amennyi a generáló kódszavak száma, vagyis négyet.

A paritás bittel kibővített kód generáló kódszavai ekkor a következő táblázattal adhatók meg:

0	0	0	1	0	1	1	1
0	0	1	0	1	0	1	1
0	1	0	0	1	1	0	1
1	0	0	0	1	1	1	0

Függőleges irányú elválasztó vonalat itt azért nem alkalmazunk, mert – mint ismeretes – a paritás bittel kibővített $(8, 16)_2$ Hamming kód mind a nyolc koordinátában szimmetrikus.

A korábbi esetekhez hasonlóan értelmezzük a $C(n_1, n_2, n_3, n_4, n_5, n_6, n_7, n_8)$ kódot, melyet a generáló kódszavak koordinátáinak többszörözésével képezünk. Ez szintén lineáris kód, négy generáló kódszóval. Legyen $n = \sum_{i=1}^8$, ekkor a következőt állítjuk:

3.17. Tétel.

Ha $n \geq 7$ és az $n_1, n_2, \dots, n_8$ nemnegatív egészek között pontosan egy páros értékű van (következésképpen n páratlan), akkor a $C(n_1, n_2, n_3, n_4, n_5, n_6, n_7, n_8)$ kód elérési sugara $\frac{n-5}{2}$.

Bizonyítás. Az $x = |x_1|x_2|x_3|x_4|x_5|x_6|x_7|x_8|$ particionált formában megadott pontnak a kódszavaktól való távolságát a szokásos módon felírva, majd az $y_i = 2w_i - n_i$ változókat

bevezetve, a 3.16. tétel bizonyításához analóg gondolatmenet szerint elég azt belátni, hogy az

$$\begin{array}{rcl}
y_1 + y_2 + y_3 + y_4 + y_5 + y_6 + y_7 + y_8 + 3 & \geq & 0 \\
y_1 + y_2 + y_3 - y_4 + y_5 - y_6 - y_7 - y_8 + 3 & \geq & 0 \\
y_1 + y_2 - y_3 + y_4 - y_5 + y_6 - y_7 - y_8 + 3 & \geq & 0 \\
y_1 + y_2 - y_3 - y_4 - y_5 - y_6 + y_7 + y_8 + 3 & \geq & 0 \\
y_1 - y_2 + y_3 + y_4 - y_5 - y_6 + y_7 - y_8 + 3 & \geq & 0 \\
y_1 - y_2 + y_3 - y_4 - y_5 + y_6 - y_7 + y_8 + 3 & \geq & 0 \\
y_1 - y_2 - y_3 + y_4 + y_5 - y_6 - y_7 + y_8 + 3 & \geq & 0 \\
y_1 - y_2 - y_3 - y_4 + y_5 + y_6 + y_7 - y_8 + 3 & \geq & 0 \\
- y_1 + y_2 + y_3 + y_4 - y_5 - y_6 - y_7 + y_8 + 3 & \geq & 0 \\
- y_1 + y_2 + y_3 - y_4 - y_5 + y_6 + y_7 - y_8 + 3 & \geq & 0 \\
- y_1 + y_2 - y_3 + y_4 + y_5 - y_6 + y_7 - y_8 + 3 & \geq & 0 \\
- y_1 + y_2 - y_3 - y_4 + y_5 + y_6 - y_7 + y_8 + 3 & \geq & 0 \\
- y_1 - y_2 + y_3 + y_4 + y_5 + y_6 - y_7 - y_8 + 3 & \geq & 0 \\
- y_1 - y_2 + y_3 - y_4 + y_5 - y_6 + y_7 + y_8 + 3 & \geq & 0 \\
- y_1 - y_2 - y_3 + y_4 - y_5 + y_6 + y_7 + y_8 + 3 & \geq & 0 \\
- y_1 - y_2 - y_3 - y_4 - y_5 - y_6 - y_7 - y_8 + 3 & \geq & 0
\end{array}$$

egyenlőtlenség-rendszernek nincs olyan egész értékű megoldása, melyben az y_i változók értéke között pontosan egy páros érték van.

Ennek bizonyítását ismét kézi számolással kezdjük és számítógéppel fejezzük be. A kézi számolás most abból áll, hogy megmutatjuk az $|y_i| \leq 3$ egyedi korlátok teljesülését. Valóban, az egyenlőtlenség-rendszer felső nyolc, ill. alsó nyolc sorát összegezve kapjuk, hogy $|y_1| \leq 3$, a többi változóra vonatkozó hasonló egyenlőtlenség pedig következik a változók szimmetriájából.

A $d(x, C) \geq (n - 5)/2$ egyenlőtlenség bizonyításához tekintsünk egy olyan x vektort, melyre $w_i = \lceil \frac{n_i}{2} \rceil$ egyetlen i indexre (amelyhez tartozó n_i páratlan értékű) és $w_i = \lfloor \frac{n_i}{2} \rfloor$ az összes többi i indexre. Akár kézi, akár gépi számítással megmutatható, hogy egy ilyen x vektorra $d(x, C) = (n - 5)/2$, tehát a vizsgált kód elérési sugara $(n - 5)/2$. $\square$

Ismét alkalmazva a partíciós módszertant, megkapjuk, hogy a 3.17. tétel alapján konstruálható inekvivalens kódok száma az

$$\frac{1}{(1-x)^2(1-x^2)(1-x^3)(1-x^4)(1-x^5)(1-x^6)(1-x^7)} = \\
1 + 2x + 4x^2 + 7x^3 + 12x^4 + 19x^5 + \dots$$

függvény kifejtésében x^{R-1} együtthatója. Eszerint $R = 2$ esetén két különböző lineáris $(9, 16)_2$ kódot kapunk, melyek $C(3, 1, 1, 1, 1, 1, 1, 0)$ és $C(1, 1, 1, 1, 1, 1, 1, 2)$. Bertolo és szerzőtársai [130] publikációjából kiderül, hogy a lineáris kódok körében nincs más $(9, 16)_2$ kód, mint az előbbi kettő, azonban létezik két nemlineáris $(9, 16)_2$ kód is. A 4 inekvivalens $(9, 16)_2$ kódra [130]-ben ismertett konstrukció adja azt az ötletet, hogy tekintsünk inkább $C(n_1, n_2, n_3, n_4, n_5, n_6, n_7, n_8, n_9)$ alakban partíciónált kódokat. Mivel ekkor már nemcsak lineáris kódokról lesz szó, ezúttal nem spórolhatjuk meg mind a 16

kódszó megadását a séma felírásakor, amely most az

0	0	0	0	0	0	0	0	0
0	0	0	1	0	1	1	1	0
0	0	1	0	1	0	1	1	0
0	0	1	1	1	1	0	0	1
0	1	0	0	1	1	0	1	0
0	1	0	1	1	0	1	0	1
0	1	1	0	0	1	1	0	1
0	1	1	1	0	0	0	1	1
1	0	0	0	1	1	1	0	1
1	0	0	1	1	0	0	1	1
1	0	1	0	0	1	0	1	1
1	0	1	1	0	0	1	0	0
1	1	0	0	0	0	1	1	1
1	1	0	1	0	1	0	0	0
1	1	1	0	1	0	0	0	0
1	1	1	1	1	1	1	1	0

alakot ölti. A függőleges vonal itt a lineáris részt választja el a nemlinearitást eredményező utolsó koordinátától.

Bebizonyítható a következő tétel állítása.

3.18. Tétel.

Ha $n \geq 7$ és az $n_1, n_2, \dots, n_9$ nemnegatív egészek valamennyien páratlan értékek, vagy pedig pontosan két páros értékű van közöttük, és ezek egyike n_9 , akkor a $C(n_1, n_2, n_3, n_4, n_5, n_6, n_7, n_8, n_9)$ kód elérési sugara $\frac{n-5}{2}$.

Bizonyítás. Az előző tétel bizonyításához hasonlóan járunk el. A fenti kódséma egyúttal megadja az aktuális egyenlőtlenség-rendszerben az y_i változók együtthatóinak a sémáját. Ez mindössze abban különbözik a 3.17. tétel bizonyításában felírt egyenlőtlenség-rendszertől, hogy minden egyes sor kiegészül egy további, az y_9 változót $+1$ vagy -1 együtthatóval tartalmazó taggal, rendre $+, +, +, -, +, -, -, -, -, -, -, +, -, +, +, +$ előjellel.

Az előző (8 változót tartalmazó) egyenlőtlenség-rendszerhez hasonlóan adódik, hogy $|y_i| \leq 3$ fennáll valamennyi változóra, de itt már nem elég ezt egy i indexre belátni. Ez a tulajdonság azon múlik, hogy az egyenlőtlenség-rendszer mátrixában bármely két oszlopot kiválasztva, a kiválasztott két oszlopban az előjelek lehetséges $(+, +)$, $(+, -)$, $(-, +)$, $(-, -)$ variációi egyaránt három-három sorban fordulnak elő.

A bizonyítás folytatása az előző tétel bizonyításával analóg módon géppel végzett számításon alapul. $\square$

Az ezzel a konstrukcióval felépíthető kódok számának meghatározásához a partíciós módszertant követve először kiszámítjuk a csupa páratlan n_i -hez tartozó inekvivalens kódok számát, amire azt kapjuk, hogy megegyezik x^{R-1} együtthatójával az

$$\frac{x}{(1-x)^2(1-x^2)(1-x^3)(1-x^4)(1-x^5)(1-x^6)(1-x^7)(1-x^8)} =$$

$$x + 2x^2 + 4x^3 + 7x^4 + 12x^5 + \dots$$

függvény kifejtésében. Hasonlóan, a páros tagokat is tartalmazó kódok száma x^{R-1} együtthatója az

$$\frac{1}{(1-x)^3(1-x^2)(1-x^3)(1-x^4)(1-x^5)(1-x^6)(1-x^7)} =$$

$$1 + 3x + 7x^2 + 14x^3 + 26x^4 + 45x^5 + \dots$$

függvény kifejtésében. Az utóbbi két kifejezés összege adja végeredményként az

$$\frac{x + (1-x^8)/(1-x)}{(1-x)^2(1-x^2)(1-x^3)(1-x^4)(1-x^5)(1-x^6)(1-x^7)(1-x^8)} =$$

$$1 + 4x + 9x^2 + 18x^3 + 33x^4 + 57x^5 + \dots$$

függvényt. A felírt tagok együtthatóiból látszik, hogy a 3.18. tétel konstrukciójával $n = 9$ -re megkapjuk mind a négy inekvivalens optimális $(9, 16)_2$ kódot, $n = 11$ -re pedig 9 inekvivalens $(11, 16)_3$ kódot kapunk, melyek közül négy kód lineáris, öt pedig nem. Az $n = 11$ esetre kapott kódokról viszont egyelőre nem tudjuk, hogy optimálisak-e, mivel $K(11, 3)$ pontos értéke jelenleg még nem ismeretes. Az inekvivalens $(11, 16)_3$ kódok klasszifikációja is megoldatlan, mert jelenleg nem tudjuk, hogy nincs-e más ilyen kód azokon kívül, amelyek a 3.18. tétel konstrukciójával megkaphatók.

3.7. Extrém bináris 2-szűrjektív kódok elérési sugara

A $\sigma_2(n, 2)$ értékét meghatározó (3.13) képlet állítása úgy is megfogalmazható, hogy ha az n_i ($i = 4, 5, \dots$) sorozat elemeit az $n_i = \binom{i-1}{\lfloor (i-2)/2 \rfloor}$ binomiális együtthatókkal értelmezzük, akkor az i számú kódszóval megadható lehető leghosszabb bináris 2-szűrjektív kódok hossza (dimenziója, vagyis a kódszavak koordinátáinak a száma) legfeljebb n_i lehet. Ezért az ilyen i kódszóból álló n_i dimenziós bináris 2-szűrjektív kódokra az extrém jelzővel utalhatunk.

A 3.7. tételben a 9 alsó korlát bizonyításához az adott méretekhez tartozó bináris 2-szűrjektív kódok lehetséges elérési sugarára kapott adatokat használtuk. Ezeket az adatokat 8 kódszóig és $n_8 = 35$ dimenzióig tudtuk kiszámítani. $K(2R + 4, R)$ pontos értékének a meghatározása vagy akár az általános érvényű 9 alsó korlát további javítása nagyon nehéz problémának látszik. Talán kicsit közelebb visz a megoldás felé, de ettől függetlenül is érdekes lehet, ha legalább az extrém bináris 2-szűrjektív kódokra ki tudjuk számítani azok lehetséges elérési sugarát tetszőleges i számú kódszó és a megfelelő dimenziók n_i sorozatának minden esetére. Segíti a számítást és a bizonyítást a bináris kódok hipergráf reprezentációjának a használata.

Egy C bináris kódhoz – bizonyos megkötések mellett – természetes módon hozzárendelhető egy (V, E) hipergráf, és fordítva, hipergráfhoz is hozzárendelhető bináris kód oly

módon, hogy a C kódszavaiból álló mátrix a (V, E) hipergráf incidencia mátrixa legyen. Más szavakkal: a C kód i -edik kódszavában a j -edik koordináta értéke akkor és csak akkor legyen 1, ha $v_i \in e_j$. A megkötés az, hogy a kódszavakból álló mátrixban ne legyen csupa azonos értékből (csupa 0-ból vagy csupa 1-ből) álló oszlop, és e mátrixnak ne legyen két azonos oszlopa. (Bináris 2-szűrjektív kódokra ez szükségszerűen teljesül.)

A megfeleltetésből nyilvánvaló, hogy bináris 2-szűrjektív C kódnak független (V, E) hipergráf felel meg, és a fordított irányú hasonló következtetés is igaz.

Tetszőleges $m \geq 2$ és $1 \leq k < m$ esetén jelölje $\mathcal{G}_k^{(m)}$ az m csúcsot tartalmazó teljes k -uniform hipergráfot, $\mathbf{B}_k^{(m)}$ annak incidencia mátrixát, $D_k^{(m)}$ pedig azt a bináris kódot, melynek kódszavai a $\mathbf{B}_k^{(m)}$ mátrix sorai.

További vizsgálatunk tárgya az a $\mathcal{G}_k^{(m)}$ -ből származtatott $(k+1)$ -uniform $\mathcal{F}_{k+1}^{(m+1)}$ hipergráf, melynek $\mathbf{A}_{k+1}^{(m+1)}$ incidencia mátrixát úgy kapjuk, hogy a $\mathbf{B}_k^{(m)}$ mátrixot megtoldjuk egy csupa 1-esből álló sorral. Ezáltal a $(k+1)$ -uniform $\mathcal{F}_{k+1}^{(m+1)}$ hipergráfnak egy olyan $C_{k+1}^{(m+1)}$ kód felel meg, melynek kódszavai a megtoldott $\mathbf{A}_{k+1}^{(m+1)}$ mátrix sorai.

Szögezzük le, hogy az $\mathcal{F}_{k+1}^{(m+1)}$ hipergráfnak $m+1$ csúcsa és $\binom{m}{k}$ éle, az $\mathbf{A}_{k+1}^{(m+1)}$ mátrixnak $m+1$ sora és $\binom{m}{k}$ oszlopa van, a $C_{k+1}^{(m+1)} \subset Z_2^{\binom{m}{k}}$ kód pedig $m+1$ kódszóból áll. A fenti konstrukcióból az is eléggé nyilvánvalóan következik, hogy $k = \lfloor (m-1)/2 \rfloor$ esetén $C_{k+1}^{(m+1)}$ extrém 2-szűrjektív kód. A továbbiakban csak ilyen esetekkel foglalkozunk, és célul tűzzük ki ezekben az esetekben a $C_{k+1}^{(m+1)}$ kód $R(C_{k+1}^{(m+1)})$ elérési sugarának meghatározását. A [27, 30, 31, 32] cikkek lényegében ezzel a konstrukcióval bizonyítják a (3.13) formula fennállását. A [31] cikkben adott bizonyításból az is kiderül, hogy tetszőleges $i \geq 4$ egész esetén az i kódszóból álló $n_i = \binom{i-1}{\lfloor (i-2)/2 \rfloor}$ dimenziós extrém bináris 2-szűrjektív kód ekvivalenciától eltekintve egyértelmű.

A célul kitűzött $R(C_{k+1}^{(m+1)})$ elérési sugár meghatározására két különböző megoldást találtam. Az elsőként talált megoldás Baranyai l -faktorizációs tételét használja. A később talált második bizonyítást használva általánosabban, tetszőleges m, k párra – a $k = \lfloor (m-1)/2 \rfloor$ megkötés nélkül – meghatározható a fenti alakú kódok elérési sugara. Ehhez a bizonyításhoz Billington [45] cikkének egyik állításában megadott formulát használjuk, amely az adott foksám-sorozattal rendelkező k -uniform hipergráfok rekurzív kezelését teszi lehetővé. Mivel a [154] cikk az utóbbi bizonyítást tartalmazza, azért itt a Baranyai-tételre alapuló eddig még nem publikált bizonyítást ismertetem. A Baranyai-tétel megfogalmazásával kezdem, majd egy több részből álló egyszerűbb állítással, továbbá egy reguláris hipergráfra vonatkozó egzisztencia tétel megfogalmazásával és bizonyításával folytatom az elérési sugár meghatározásának az előkészítését.

Baranyai l -faktorizációs tétele. Legyen $m \geq 3$, $1 \leq k < m$ és $l = \frac{k}{(k,m)}$, ahol (k, m) a legnagyobb közös osztót jelenti. Ekkor

$$\frac{1}{k} \cdot lm \text{ és } \frac{1}{l} \cdot \binom{m-1}{k-1} \text{ egészek,}$$

a teljes k -uniform $\mathcal{G}_k^{(m)} = (V, E)$ hipergráf pedig l -faktorizálható, ami alatt azt értjük, hogy létezik az E élhalmaznak $\frac{1}{l} \cdot \binom{m-1}{k-1}$ számú páronként diszjunkt E_i halmazra történő felbontása, amely csupa l -reguláris (V, E_i) hipergráfot eredményez.

3.19. Állítás.

- (i) $\binom{2^p}{2^{p-1}-1}$ páros minden $p \geq 2$ esetén;
- (ii) $\binom{2^p-1}{2^{p-1}-1}$, $\binom{2^p-1}{2^{p-1}-2}$ és $\binom{2^p-2}{2^{p-1}-2}$ páratlan minden $p \geq 2$ esetén;
- (iii) $\binom{2^p-3}{2^{p-1}-3}$ páratlan minden $p \geq 3$ esetén;
- (iv) $\binom{m}{\lfloor (m-1)/2 \rfloor}$ páros minden $m \geq 3$ esetén, kivéve, ha $m = 2^p - 1$ vagy $m = 2^p - 2$ alakú;
- (v) $\binom{m-1}{\lfloor (m-3)/2 \rfloor}$ páros minden $m \geq 3$ esetén, az előbbi, valamint az $m = 2^p$ kivételekkel;
- (vi) $\binom{2^j}{j}$ páros minden pozitív j -re;
- (vii) $\binom{2^j}{j}$ akkor és csak akkor osztható 4-gyel, ha j nem 2 hatvány.

A felsorolt állítások elemi úton bizonyíthatóak.

3.20. Tétel.

Legyen $m \geq 3$, $k = \lfloor \frac{m-1}{2} \rfloor$,

$$i = \begin{cases} \frac{\binom{m}{k}-m}{2} & \text{ha } m = 2^p \text{ vagy } m = 2^p - 1, \\ \frac{\binom{m}{k}-\frac{m}{2}}{2} & \text{ha } m = 2^p - 2, \\ \frac{\binom{m}{k}}{2} & \text{egyébként,} \end{cases} \quad (3.14)$$

legyen továbbá $t = \frac{ik}{m}$, $l = \frac{k}{(k,m)}$. Ekkor i , t és t/l egészek és létezik m csúcsból álló és i élt tartalmazó k -uniform t -reguláris $\mathcal{G}^*$ hipergráf.

Bizonyítás. A 3.19. állítás sorai segítségével mutatható meg, hogy i minden esetben egész. Hasonlóan adódik, hogy t is minden esetben egész, de ehhez előbb azt kell észrevenni, hogy t -re a (3.14) formula sorainak megfelelően a következő képlet érvényes:

$$t = \begin{cases} \frac{\binom{m-1}{k-1}-k}{2} & \text{ha } m = 2^p \text{ vagy } m = 2^p - 1, \\ \frac{\binom{m-1}{k-1}-\frac{k}{2}}{2} & \text{ha } m = 2^p - 2, \\ \frac{\binom{m-1}{k-1}}{2} & \text{egyébként.} \end{cases} \quad (3.15)$$

Rátérünk l és t/l vizsgálatára. Mivel páros m -re $m = 2k + 2$, páratlan m -re pedig $m = 2k + 1$, ezért csak $(k, m) = 2$ vagy $(k, m) = 1$ lehetséges attól függően, hogy $m \equiv 2 \pmod{4}$ vagy sem, és következésképpen

$$l = \frac{k}{(k, m)} = \begin{cases} k & \text{ha } m \not\equiv 2 \pmod{4}, \\ k/2 & \text{ha } m \equiv 2 \pmod{4}. \end{cases} \quad (3.16)$$

A folytatás során intenzíven használjuk a binomiális együtthatóknak – a Baranyai tételben is megfogalmazott – ismert tulajdonságát, hogy

$$\frac{(k, m)}{k} \cdot \binom{m-1}{k-1} = \frac{(k, m)}{m} \cdot \binom{m}{k}$$

mindig egész, ha $m > k \geq 1$. Mindezek alapján már viszonylag egyszerűen következik t/l egészértékűsége, ami az egyes esetekre a következőképpen látható be:

(a) Legyen $m = 2^p$ vagy $m = 2^p - 1$. Ekkor $k = 2^{p-1} - 1$, $l = k$, és így a 3.19. állítás szerint $\binom{m-1}{k-1} = \binom{m-1}{2^{p-1}-2}$ páratlan egész. Ebből viszont következik, hogy $\frac{(k, m)}{k} \cdot \binom{m-1}{k-1} = \frac{1}{k} \cdot \binom{m-1}{k-1}$ is páratlan egész, amiből pedig végül az adódik, hogy $\frac{t}{l} = \frac{1}{2} \cdot \frac{1}{k} \cdot \binom{m-1}{k-1} - \frac{1}{2}$ egész.

(b) Legyen $m = 2^p - 2$, ekkor $\binom{m-1}{k-1} = \binom{2^p-3}{2^{p-1}-3}$ páratlan, $l = k/2 = 2^{p-2} - 1$ páratlan, és következésképpen $\frac{(k, m)}{k} \cdot \binom{m-1}{k-1} = \frac{1}{k/2} \cdot \binom{m-1}{k-1}$ szintén páratlan, amiből következik, hogy $\frac{t}{l} = \frac{1}{k} \cdot \binom{m-1}{k-1} - \frac{1}{2}$ egész.

(c) Legyen $m = 2k + 1$, ahol $m \neq 2^p - 1$. Ekkor $l = k$, és így a 3.19. állítás szerint $\frac{(k, m)}{k} \cdot \binom{m-1}{k-1} = \frac{1}{k} \cdot \binom{2k}{k-1} = \frac{1}{2} \cdot \frac{1}{2k+1} \cdot \binom{2k+2}{k+1}$ páros egész, amiből következik, hogy t/l egész.

(d) Legyen $m = 2k + 2$, ahol k páratlan és $m \neq 2^p$. Ekkor $l = k$, és így a 3.19. állítás szerint $\frac{(k, m)}{k} \cdot \binom{m-1}{k-1} = \frac{1}{k} \cdot \binom{2k+1}{k-1} = \frac{1}{2} \cdot \frac{1}{k+2} \cdot \binom{2k+2}{k+1}$ páros egész, amiből ismét következik, hogy t/l egész.

(e) Legyen $m = 2k + 2$, ahol k páros és $m \neq 2^p - 2$. Ekkor $l = k/2$ és $\frac{(k, m)}{k} \cdot \binom{m-1}{k-1} = \frac{1}{k/2} \cdot \binom{2k+1}{k-1} = \frac{1}{2} \cdot \frac{1}{2k+3} \cdot \binom{2k+4}{k+2}$ páros egész, tehát t/l ebben az esetben is egész.

A t/l hányados egész értékűségének ismeretében most már a Baranyai-tétel alkalmazásával közvetlenül adódik a 3.20. tétel állítása szerinti $\mathcal{G}^*$ hipergráf létezésének bizonyítása. Legyen ugyanis E^* a Baranyai-tétel szerint garantált páronként diszjunkt E_i élhalmazok közül tetszőleges t/l számú élhalmaz egyesítése. Ekkor (V, E^*) k -uniform t -reguláris hipergráf. $\square$

Most $n = \binom{m}{k}$ jelöléssel legyenek $i = 0, 1, \dots, n$ -re

$$W_i = \{x \in Z^n : wt(x) = i\}$$

a Z_2^n Hamming tér azonos súlyú pontjaiból álló halmazok.

Tekintsük ismét a $\mathcal{G}_k^{(m)} = (V, E)$ teljes k -uniform hipergráfot abban a speciális esetben, ha $k = \lfloor (m-1)/2 \rfloor$. Legyen $n = \binom{m}{k}$, továbbá $V = \{v_1, v_2, \dots, v_m\}$ és $E = \{e_1, e_2, \dots, e_n\}$.

Legyen ezután $i \in \{0, 1, \dots, m\}$, $x \in W_i$, $E(x) = \{e_h \in E : x_h = 1\}$, $\mathcal{G}_k^{(m)}(x) = (V, E(x))$, és jelölje $\delta_j(x)$ a v_j csúcs fokát a $\mathcal{G}_k^{(m)}(x)$ hipergráfban.

Tekintsük azt az esetet, amikor i azonos a 3.20. tételben megadott értékkel, $\mathcal{G}_k^{(m)}(x)$ pedig az ugyanott megadott $\mathcal{G}^*$ hipergráffal. (Az utóbbi előírás persze szűkíti x lehetséges értékeit a W_i halmazon belül.) Ekkor a $\mathcal{G}^*$ hipergráf regularitása miatt tetszőleges csúcsának a foka a 3.20. tételben megadott t értékkel azonos.

A hipergráfoknak megfeleltetett kódok terminológiájában kifejezve $\delta_j(x)$ azoknak a koordináta-helyeknek a száma, ahol x -ben is, valamint a d_j kódszóban is egyaránt 1-es áll. Következésképpen azoknak a koordináta-helyeknek a száma, ahol x és d_j különbözik egymástól

$$d(x, d_j) = \binom{m-1}{k-1} + i - 2\delta_j(x). \quad (3.17)$$

Jelölje x^* azt a W_i -beli vektort, melyre $\mathcal{G}_k^{(m)}(x^*) = \mathcal{G}^*$. A (3.17) kifejezés jobb oldalára a 3.20. tételben megadott i érték és $\mathcal{G}^*$ hipergráf esetére (amikor is j választásától függetlenül $\delta_j(x^*) = t = ik/m$), elemi számítási műveletekkel adódik, hogy

$$d(x^*, d_j) = \begin{cases} \frac{\binom{m}{k}}{2} - \frac{m-2k}{2} = \begin{cases} \frac{n-2}{2} & \text{ha } m = 2^p, k = 2^{p-1} - 1, \\ \frac{n-1}{2} & \text{ha } m = 2^p - 1, k = 2^{p-1} - 1, \end{cases} \\ \frac{\binom{m}{k}}{2} - \frac{m-2k}{4} = \frac{n-1}{2} & \text{ha } m = 2^p - 2, k = 2^{p-1} - 2, \\ \frac{\binom{m}{k}}{2} = \frac{n}{2} & \text{egyébként.} \end{cases} \quad (3.18)$$

A továbbiakban bebizonyítjuk, hogy a (3.18) soraiban álló kifejezések a $C_{k+1}^{(m+1)}$ kód elérési sugarát is mindig megadják, tehát $R(C_{k+1}^{(m+1)}) = d(x^*, d_j)$.

A (3.18) formulából látható, hogy minden esetben $d(x^*, d_j) \leq n/2$. A $C_{k+1}^{(m+1)}$ kód a d_j kódszavakon kívül még a csupa 1-esből álló kódszót tartalmazza, amelytől az x^* vektor (3.14) szerint legalább $n/2$ távolságra van. Következésképpen $d(x^*, C_{k+1}^{(m+1)}) = d(x^*, d_j)$. Ebből viszont következik, hogy

$$R(C_{k+1}^{(m+1)}) \geq d(x^*, d_j).$$

A fordított egyenlőtlenség bizonyításához megmutatjuk, hogy tetszőleges $x \in Z_2^n$ esetén

$$d(x, C_{k+1}^{(m+1)}) \leq d(x^*, d_j). \quad (3.19)$$

Tetszőleges i súly és $x \in W_i$ vektor esetén, mivel (3.17) változatlanul érvényes, a

$$\sum_{j=1}^m \delta_j(x) = ik \quad (3.20)$$

összeg értéke pedig nem függ attól, hogy melyik x vektort választottuk W_i -ből, ezért

$$\max_{1 \leq j \leq m} \delta_j(x) \geq \left\lceil \frac{ik}{m} \right\rceil,$$

tehát

$$\min_{1 \leq j \leq m} d(x, d_j) \leq \binom{m-1}{k-1} + i - 2 \cdot \left\lceil \frac{ik}{m} \right\rceil,$$

és így

$$d(x, C_{k+1}^{(m+1)}) \leq \min \left(\binom{m-1}{k-1} + i - 2 \cdot \left\lceil \frac{ik}{m} \right\rceil, \binom{m}{k} - i \right).$$

Rögzített m és $k = \lfloor (m-1)/2 \rfloor$ esetén az $U_i = \binom{m-1}{k-1} + i - 2 \cdot \lfloor \frac{ik}{m} \rfloor$ és $V_i = \binom{m}{k} - i$ véges ($i = 0, 1, \dots, m$) sorozatok elemzésével adódik, hogy valóban fennáll (3.19). Megkönnyíti az elemzést, ami ezáltal elemi módszerekkel elvégezhető, ha észrevesszük, hogy az U_i sorozatnak külön a páros és külön a páratlan sorszámú elemei monoton nemcsökkenő részsorozatokat képeznek, V_i -ről pedig ránézésre látszik, hogy monoton csökkenő sorozat. Ezzel bebizonyítottuk a következő tételt:

3.21. Tétel. (*K. [154], Theorem 6*)

Legyen $m \geq 3$, továbbá $k = \lfloor \frac{m-1}{2} \rfloor$ és $n = \binom{m}{k}$. E jelölésekkel a $C_{k+1}^{(m+1)}$ kód elérési sugarára fennáll

$$R\left(C_{k+1}^{(m+1)}\right) = \begin{cases} n/2 - 1 & \text{ha } m = 2^p, (p \text{ egész}), \\ \lfloor n/2 \rfloor & \text{egyébként.} \end{cases} \quad (3.21)$$

3.8. A bináris térlefedő kódok áttekintése

Ebben a szakaszban egyenként bemutatjuk, az ismeretek fejlődését követve, a bináris térlefedő kódok leginkább vizsgált konkrét eseteire ($n \leq 14, R \leq 3$) vonatkozó ismeretanyagot. Mivel a 3-nál nagyobb elérési sugarú nem-triviális bináris optimális, ill. rekord-tartó kódok $n \leq 14$ -ig 3 elérési sugarú hasonló kódokból származtathatóak, ezért bináris kódok esetén megállunk az $R = 3$ elérési sugárnál. Minden egyes konkrét esetben $K(n, R)$ értékének, annak ismerete hiányában pedig az ismert legjobb alsó és felső korlátjának a megadásával kezdjük. Amennyiben az optimális kódok száma ismert, akkor azok számát (értsd: az *inekvivalens* optimális kódok számát) is mindjárt itt adjuk meg. Ezt követően – általában csak legfeljebb hét szavas optimális kódok esetében – az előző szakaszban adott általános leírások alapján felsoroljuk az adott esethez tartozó optimális kódokat. A hét szónál hosszabb optimális, ill. rekord-tartó kódoknak a konkrét esettől függően egy, néhány vagy összes változatát a mellékelt CD lemezen adjuk meg. Ugyanitt megtalálható az optimális $(8, 4)_3$ és $(9, 7)_3$ kódok listája is.

Minden egyes esetre – a triviális kétszavas optimális kódok ($n \leq 2R + 1$) esetei kivételével – megadunk egy-egy prompt (azaz könnyen verifikálható) alsó és felső korlátot. A *prompt alsó korlát* kifejezést szinonimaként használjuk a korábban már értelmezett *szférikus korláttal* azonos értelemben. A *prompt felső korlátokat* a (3.3) összefüggésnek az ismétléses kódokra és a Hamming kódra való alkalmazásával, ill. néhány esetben egy normális $(n, M)_R$ kód ismerete esetén fennálló $K(n+2, R+1) \leq K(n, R)$ egyenlőtlenség (lásd 3.3.3 szakasz) alkalmazásával kapjuk, nevezetesen:

$K(3, 1) = 2$ adja a $K(4, 1) \leq 4$, $K(5, 1) \leq 8$ és $K(6, 1) \leq 16$ prompt felső korlátokat;

$K(5, 2) = 2$ adja a $K(6, 2) \leq 4$, $K(7, 2) \leq 8$ és $K(8, 2) \leq 16$ prompt felső korlátokat;

$K(7, 3) = 2$ adja a $K(8, 3) \leq 4$, $K(9, 3) \leq 8$ és $K(10, 3) \leq 16$ prompt felső korlátokat;

$K(7, 1) = 16$ adja a $K(8, 1) \leq 32$, $K(9, 1) \leq 64$, $K(10, 1) \leq 128$, $K(11, 1) \leq 256$, $K(12, 1) \leq 512$, $K(13, 1) \leq 1024$ és $K(14, 1) \leq 2048$ prompt felső korlátokat;

$K(7, 1) = 16$ adja a $K(9, 2) \leq 16$, és $K(11, 3) \leq 16$ prompt felső korlátokat;

$K(9, 2) \leq 16$ adja a $K(10, 2) \leq 32$, $K(11, 2) \leq 64$, $K(12, 2) \leq 128$, $K(13, 2) \leq 256$, és $K(14, 2) \leq 512$ prompt felső korlátokat;

$K(11, 3) \leq 16$ adja a $K(12, 3) \leq 32$, $K(13, 3) \leq 64$ és $K(14, 3) \leq 128$ prompt felső korlátokat.

A prompt alsó, ill. felső korlát megadását követően nyomon követjük ezek fokozatos javításának a menetét, ami általában néhány évtized hosszúságú időtartam alatt ment végbe. Itt adjuk meg – amennyiben megfelelő adat rendelkezésre áll – az adott esethez tartozó valamely kóddal ekvivalens, de kifejezetten totó-kombináció céljára készített konstrukció szerzőjének a nevét és a konstrukció felfedezésének a tényleges vagy valószínű évszámát. Ezekre a továbbiakban röviden, a *totókód* megjelöléssel utalunk. (Bizonyos esetekben az ilyen totókódok szerzőnek csak az álnevét ismerjük, mint „ARIC”, „SEPPO” stb.) Az ide vonatkozó, néha homályos vagy pontatlan információkat javarészt az [168] hivatkozású web lapról, kisebb arányban az [60] publikációból vettem, ezeket úgy adom tovább, ahogy ott is megtalálhatóak, és e forrásadatokat nem óhajtom magyarázni vagy kritika alá vonni. A források szerint előfordul, hogy a matematikai szakirodalomban több évvel később kerül ismertetésre a korábban más személy, ill. néha ugyanazon szerző által totókódként közölt konstrukció. Az is érdekes, hogy sok esetben az eredetileg – gyakran már évtizedekkel ezelőtt – totó-kombinációnak készült kód ma is a legjobb ismert térlefedő kód, bár ez nem annyira a bináris, mint inkább a ternáris és vegyes kódok esetében figyelhető meg. Ha ismert a lap neve, amelynek valamelyik számában az idézett totó-konstrukció megjelent, akkor a lap megnevezését szögletes zárójelben adom meg.

Minden elemzett és a mellékelt lemezen található kód esetén ellenőriztem (de erre a szövegezésben csak néhány esetben utalok), hogy nincsenek-e a kódszavak között elemi négyzetek, vagyis olyan négyes kódszó-csoportok, amelyek csak két koordináta-helyen különböznek, de ott mind a 4 variáció előfordul. E tulajdonságnak totó célú alkalmazásnál van jelentősége, ilyen konstrukciók esetén ugyanis a tippek egy részét vagy egészét kombinációs szelvényeken összevontan meg lehet adni.

A következő három szakaszban és később a további fejezetekben sorra kerülő, a ternáris, magasabb rendű és vegyes optimális és rekord-tartó kódokra vonatkozó hasonló részletezés során az ismertetett jellegzetességek (kiegyensúlyozottság vagy kiegyensúlyozatlanság, bináris kódok esetén önkomplementaritás, nembináris kódok esetén normalitás) általában a mellékelt lemezen megadott kódokra vonatkoznak. További optimális (rekord-tartó) kódok létezése esetén azok tulajdonságai eltérhetnek a megadott kódok jellegzetességeitől. A normalitási tulajdonságot minden tárgyalásra kerülő térlefedő kód esetén koordinátánként is meghatároztam, de ebben az anyagban mindig csak a globális normalitást adom meg, vagyis azt, hogy a tárgyalt optimális, ill. rekord-tartó kódok normálisak vagy abnormálisak-e. A bináris esetben ettől is eltekintünk, mivel kiderült, hogy a konkrétan tárgyalt bináris kódok valamennyien normálisak (és többségük minden koordinátában normális).

3.8.1. $R = 1$ elérési sugarú kódokra vonatkozó eredmények

$K(2, 1) = 2$ és az alábbi 2 optimális kód létezik, melyek közül az első önkomplementer.

$$(1) \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \quad (2) \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$K(3, 1) = 2$ és egyetlen optimális kód létezik (önkomplementer).

$$(1) \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

$K(4, 1) = 4$ és az alábbi 2 optimális kód létezik. Prompt alsó és felső korlát: egyaránt 4. Pontos érték igazolása: [3, 46, 52]. Klasszifikáció: [18]. Az első kód önkomplementer, a második csak kiegyensúlyozott.

$$(1) \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \quad (2) \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

$K(5, 1) = 7$ és az alábbi egyetlen optimális kód létezik (amely kiegyensúlyozott és 2-szűrjektív). Prompt alsó és felső korlát: 6, ill. 8. Pontos érték igazolása: [3, 76]. Klasszifikáció (ami itt az unicitás bizonyítását jelenti): [18]. Totókód 7 kódszóval: Di Nasso R. (1950).

$$(1) \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

$K(6, 1) = 12$ és 2 optimális kód létezik, egyikük önkomplementer és 3-szűrjektív, a másik csak kiegyensúlyozott és 2-szűrjektív. Prompt alsó és felső korlát: 10, ill. 16. Pontos érték igazolása: [18]. Klasszifikáció: [118]. Totókód 12 kódszóval: Di Nasso R. (1950).

$K(7, 1) = 16$ és egyetlen optimális kód létezik. Prompt alsó és felső korlát: egyaránt 16 (perfekt kód). Pontos érték igazolása: [3, 5, 6, 7, 8]. Klasszifikáció (ami itt az unicitás bizonyítását jelenti): [9]. Totókód 16 kódszóval: Ericson A. „ARIC” (1936). Az optimális kód lineáris, perfekt, önkomplementer és 2-szűrjektív.

$K(8, 1) = 32$ és 10 optimális kód létezik. Prompt alsó és felső korlát: 29, ill. 32. Az alsó korlát javítása 31-re [18], 32-re [22]. Klasszifikáció: [118]. Totókód 32 kódszóval: Ericson A. „ARIC” (1936). Valamennyi optimális kód kiegyensúlyozott, de közülük csak 4 önkomplementer, és valamennyien 2-szűrjektivék.

$K(9, 1) = 62$. Prompt felső korlát 64. A felső korlát javítása 62-re [78, 95]. Prompt alsó korlát: 52. Az alsó korlát javítása 54-re [18, 46], 55-re [82], 56-ra [112], 57-re [103], 62-re [121]. Klasszifikáció: Megoldatlan (nehéz) probléma. Totókód 62 kódszóval: Fagioli C. (1984). Mindkét ismert konstrukció kiegyensúlyozatlan (és 2-szűrjektiv). Külön említést érdemel a Wille-féle konstrukciónak ([95]) az a jellegzetessége, hogy a kódszavak között találhatók olyan 4-es csoportok, amelyek a bináris Hamming térben elemi négyzetet képeznek, azaz két koordináta kivételével azonosak, a két kivételes koordináta-helyen pedig mind a 4 variáció előfordul. Ilyen elemi négyzetet alkotnak a szóban forgó kódban pl. a

$$\begin{aligned} c_2 &= (000001010) \\ c_7 &= (000101010) \\ c_9 &= (001001010) \\ c_{13} &= (001101010) \end{aligned}$$

kódszavak.

$107 \leq K(10, 1) \leq 120$. Prompt felső korlát 128. A felső korlát javítása 120-ra [58, 64]. Prompt alsó korlát: 94. Az alsó korlát javítása 96-ra [18], 97-re [46], 103-ra [52], 105-re [67], 107-re [130]. Totókód 120 kódszóval: Fagioli C. (1975). Az ismert rekord-tartó konstrukció kiegyensúlyozatlan (és 2-szűrjektiv).

$180 \leq K(11, 1) \leq 192$. Prompt felső korlát 256. A felső korlát javítása 224-re [42], 192-re [46]. Prompt alsó korlát: 171. Az alsó korlát javítása 174-re [46], 176-ra [52], 177-re [80, 85], 178-ra [83, 97, 100], 180-ra [103]. Totókód 192 kódszóval: Virtakallio J. (1946). Az ismert rekord-tartó konstrukció önkomplementer és 2-szűrjektiv.

$342 \leq K(12, 1) \leq 380$. Prompt felső korlát 512. A felső korlát javítása 448-ra [42], 384-re [46, 60], 380-ra Exoo, lásd [78], valamint [95, 102]. Prompt alsó korlát: 316. Az alsó korlát javítása 342-re [52]. Totókód 382 kódszóval: ismeretlen szerző [Vi Tippa], 380 kódszóval: Fagioli C. (1977). Mindkét ismert rekord-tartó konstrukció kiegyensúlyozott, 2-szűrjektiv, egyikük önkomplementer, a másik nem.

$598 \leq K(13, 1) \leq 704$. Prompt felső korlát 1024. A felső korlát javítása 768-ra [46], a 750 kódszavas totó-konstrukciós megoldást ismerteti [60], javítás 736-ra [102], 704-re [114, 120]. Prompt alsó korlát: 586. Az alsó korlát javítása 598-ra [46]. Totókód 750 kódszóval: Hämäläinen H. [Veikkaus-Lotto] (1986), 704 kódszóval: Östergård P. (1996). Az ismert rekord-tartó konstrukció önkomplementer és 2-szűrjektiv.

$1172 \leq K(14, 1) \leq 1408$. Prompt felső korlát 2048. A felső korlát javítása 1536-ra [46], 1460-ra Hämäläinen és Rankinen (1991), amit azonban nem publikáltak, 1408-ra [102, 113, 120]. Prompt alsó korlát: 1093. Az alsó korlát javítása 1171-re [52], 1172-re [100]. Totókód 1408 kódszóval: Östergård P. (1996). Mindkét ismert rekord-tartó konstrukció önkomplementer és 2-szűrjektiv.

3.8.2. $R = 2$ elérési sugarú kódokra vonatkozó eredmények

$K(3, 2) = 2$ és 3 optimális kód létezik:

$$(1) \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix} \quad (2) \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \quad (3) \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$K(4, 2) = 2$ és 2 optimális kód létezik:

$$(1) \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \quad (2) \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

$K(5, 2) = 2$ és egyetlen optimális kód létezik:

$$(1) \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$K(6, 2) = 4$ és az alábbi 4 optimális kód létezik. Prompt alsó és felső korlát: 3, ill. 4. Az alsó korlát javítása 4-re, azaz a pontos érték igazolása: [46]. Klasszifikáció: [118]. Totókód 4 kódszóval: „ARIC” v. Weikel (1947). Mind a négy optimális kód kiegyensúlyozott, (1) és (3) önkomplementer, (2) és (4) nem.

$$\begin{array}{cc} (1) \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} & (2) \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix} \\ (3) \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} & (4) \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix} \end{array}$$

$K(7, 2) = 7$ és az alábbi 3 optimális kód létezik. Prompt alsó és felső korlát: 5, ill. 8. Pontos érték igazolása: [46]. Klasszifikáció: [118]. Totókód 7 kódszóval: „ARIC” v. Weikel (1947). Mindhárom optimális kód kiegyensúlyozott.

$$\begin{array}{ccc} (1) \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix} & (2) \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix} & (3) \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix} \end{array}$$

$K(8, 2) = 12$ és 277 optimális kód létezik. Prompt felső korlát 16. A felső korlát javítása 12-re [46]. Prompt alsó korlát: 7. Az alsó korlát javítása 9-re [46], 10-re [50], 11-re [67], 12-re [110]. Klasszifikáció: [118]. Totókód 12 kódszóval: „ARIC” v. Weikel (1947).

$K(9, 2) = 16$ és 4 optimális kód létezik. Prompt alsó és felső korlát 12, ill. 16. Az alsó korlát javítása 13-ra [46], 14-re [52], 15-re [85], 16-ra [118]. Klasszifikáció: [130]. Totókód 16 kódszóval: „ARIC” v. Weikel (1940). Valamennyi optimális kód kiegyensúlyozott, kettő közülük önkomplementer, egyikük 2-szűrjektív.

$24 \leq K(10, 2) \leq 30$. Prompt felső korlát 32. A felső korlát javítása 30-ra [60]. Prompt alsó korlát: 19. Az alsó korlát javítása 20-ra [46], 21-re [52], 22-re [61], 23-ra [67], 24-re [116]. Totókód 30 kódszóval: Hämäläinen H. [Veikkaus-Lotto] (1989). Az ismert rekord-tartó konstrukció kiegyensúlyozatlan, 2-szűrjektív kód.

$37 \leq K(11, 2) \leq 44$. Prompt felső korlát 64. A felső korlát javítása 56-ra [46], 44-re [51]. Prompt alsó korlát: 31. Az alsó korlát javítása 35-re [61], 36-ra [67], 37-re [116]. Totókód 44 kódszóval: Weikel (1959) és ismeretlen szerző [Valiosysteemit] (1970). Az ismert rekord-tartó konstrukció önkomplementer, 2-szűrjektív kód.

$62 \leq K(12, 2) \leq 78$. Prompt felső korlát 128. A felső korlát javítása 96-ra [46], 88-ra [51], 80-ra [60], 78-ra [86]. Prompt alsó korlát: 52. Az alsó korlát javítása 61-re [52], 62-re [116]. Totókód 80 kódszóval: ismeretlen szerző [Valiosysteemit] (1970), 78 kódszóval Östergård P. (1990). Az ismert rekord-tartó konstrukció kiegyensúlyozatlan, 2-szűrjektív kód.

$97 \leq K(13, 2) \leq 128$. Prompt felső korlát 256. A felső korlát javítása 128-ra [43]. Prompt alsó korlát: 90. Az alsó korlát javítása 91-re [46], 96-ra [52], 97-re [61]. Totókód 128 kódszóval: „SEPPPO” (1967). Az ismert rekord-tartó konstrukció önkomplementer, 2-szűrjektív kód.

$159 \leq K(14, 2) \leq 248$. Prompt felső korlát 512. A felső korlát javítása 256-ra [43], 248-ra (totókód gyanánt) Bertolo R., Di Pasquale F. és Santisi F. (2006). Prompt alsó korlát: 155. Az alsó korlát javítása 157-re [46], 159-re [156]. Az ismert rekord-tartó konstrukció kiegyensúlyozatlan, 2-szűrjektív kód.

3.8.3. $R = 3$ elérési sugarú kódokra vonatkozó eredmények

$K(4, 3) = 2$ és 4 optimális kód létezik:

$$(1) \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \quad (2) \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \quad (3) \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \quad (4) \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$K(5, 3) = 2$ és 3 optimális kód létezik:

$$(1) \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} \quad (2) \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix} \quad (3) \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

$K(6, 3) = 2$ és 2 optimális kód létezik:

$$(1) \begin{array}{cccccc} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{array} \quad (2) \begin{array}{cccccc} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \end{array}$$

$K(7, 3) = 2$ és egyetlen optimális kód létezik:

$$(1) \begin{array}{cccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}$$

$K(8, 3) = 4$ és 6 optimális kód létezik. Prompt alsó és felső korlát: 3, ill. 4. Az alsó korlát javítása 4-re, azaz a pontos érték igazolása: [46]. Klasszifikáció: [118]. Totókód 4 kódszóval: ismeretlen szerző (1963). Mind a hat optimális kód kiegyensúlyozott, kettő közülük önkomplementer.

$K(9, 3) = 7$ és 8 optimális kód létezik. Prompt alsó és felső korlát: 4, ill. 8. A pontos érték igazolása: [46]. Klasszifikáció: [138]. Totókód 7 kódszóval: Weikel (1974). Mind a 8 optimális kód kiegyensúlyozott.

$K(10, 3) = 12$ és 11481 optimális kód létezik. Prompt felső korlát 16. A felső korlát javítása 12-re [46]. Prompt alsó korlát: 6. Az alsó korlát javítása 9-re [67], 11-re [130], 12-re [155]. Klasszifikáció: [155]. Totókód 12 kódszóval: Rankinen S. (1975).

$15 \leq K(11, 3) \leq 16$. Prompt alsó és felső korlát 9, ill. 16. Az alsó korlát javítása 10-re [46], 11-re [50], 12-re [67], 14-re [130], 15-re [155]. Totókód 16 kódszóval: ismeretlen szerző (1954). Az ismert rekord-tartó konstrukciók mindegyike kiegyensúlyozott, néhány közülük önkomplementer.

$18 \leq K(12, 3) \leq 28$. Prompt felső korlát 32. A felső korlát javítása 30-ra [60], 28-ra [74], valamint Exoo, lásd [107]. Prompt alsó korlát: 14. Az alsó korlát javítása 15-re [46], 16-ra [50], 17-re [52], 18-ra [71]. Totókód 28 kódszóval: Hämäläinen H. (1990). Az ismert rekord-tartó konstrukció önkomplementer, 2-szűrjektív kód.

$28 \leq K(13, 3) \leq 42$. Prompt felső korlát 64. A felső korlát javítása 56-ra [46], 44-re [51], 42-re [74]. Prompt alsó korlát: 22. Az alsó korlát javítása 25-re [52], 26-ra [61], 27-re [71], 28-ra [85]. Totókód 42 kódszóval: Hämäläinen H. (1990). Az ismert rekord-tartó konstrukció kiegyensúlyozatlan, 2-szűrjektív kód.

$44 \leq K(14, 3) \leq 64$. Prompt felső korlát 128. A felső korlát javítása 64-re [11, 28, 43]. Prompt alsó korlát: 35. Az alsó korlát javítása 36-ra [46], 38-ra [52], 42-re [61], 44-re [85]. A rekord-tartó konstrukció lineáris kód, amely figyelemre méltóan szép struktúrával rendelkezik. A [43] hivatkozás e kódot az alábbi generátor mátrixszal adja meg.

$$\begin{array}{c|c|c|c|c} \begin{array}{c} 0 & 1 \\ 1 & 0 \end{array} & \begin{array}{c} 0 & 0 & 1 \\ 0 & 1 & 0 \end{array} & \begin{array}{c} 0 & 0 & 1 \\ 0 & 1 & 0 \end{array} & \begin{array}{c} 0 & 0 & 1 \\ 0 & 1 & 0 \end{array} & \begin{array}{c} 0 & 0 & 1 \\ 0 & 1 & 0 \end{array} \\ \hline \begin{array}{c} 1 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{array} & \begin{array}{c} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{array} & \begin{array}{c} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{array} & \begin{array}{c} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{array} & \begin{array}{c} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{array} \end{array}$$

4. fejezet

Ternáris térlefedő kódok

4.1. Egyszerű konstrukciók

4.1.1. Ternáris ismétléses kódok

Az n dimenziós

$$\{ (0, 0, \dots, 0), \\ (1, 1, \dots, 1), \\ (2, 2, \dots, 2) \}$$

ternáris ismétléses kód elérési sugara (1.4) szerint $R = \lfloor 2n/3 \rfloor$. A bináris esethez hasonlóan a ternáris ismétléses kódok is optimális n dimenziós kódok. (Lásd a 4.4 szakasz (d_2) állítását vagy az általánosabban megfogalmazott 4.9. állítást.) Következésképpen $K_3(n, \lfloor 2n/3 \rfloor = 3)$, így pl.

$$K_3(3R + 1, 2R) = 3.$$

A bináris esettől eltérően a ternáris ismétléses kódok között nincsenek perfekt kódok, mivel $2R + 1 = 2 \cdot \lfloor 2n/3 \rfloor + 1$ mindig nagyobb a $d_{\min} = n$ kódtávolságnál.

4.1.2. Ternáris Hamming kódok

A bináris Hamming kódokkal analóg módon tetszőleges $h \geq 2$ egész és $n = \frac{3^h - 1}{2}$ esetére találhatóak ternáris perfekt kódok. Ezek között vannak a ternáris Hamming kódok: H_4 , H_{13} , $H_{40}, \dots$ Megadjuk a két legkisebb méretű ilyen lineáris kódnak egy-egy lehetséges generátor rendszerét. H_4 esetén generáló kódszavaknak választhatjuk a

$$\begin{aligned} h_1 &= (0, 1, 1, 1), \\ h_2 &= (1, 0, 1, 2) \end{aligned}$$

kódszavakat, H_{13} esetén pedig a

$$\begin{aligned}
h_1 &= (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1), \\
h_2 &= (0, 0, 0, 0, 0, 0, 0, 0, 1, 2, 0, 2, 1), \\
h_3 &= (0, 0, 0, 0, 0, 0, 0, 1, 0, 2, 0, 1, 2), \\
h_4 &= (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1), \\
h_5 &= (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 2, 2), \\
h_6 &= (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 2, 0), \\
h_7 &= (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1), \\
h_8 &= (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 2), \\
h_9 &= (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 2), \\
h_{10} &= (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)
\end{aligned}$$

kódszavakat.

4.1.3. A ternáris Golay kód

A ternáris Golay kód perfekt lineáris kód a Z_3^{11} térben, melynek 2 az elérési sugara, és ennek megfelelően 5 a kódtávolsága. Generáló kódszavaknak választhatjuk az alábbiakat:

$$\begin{aligned}
g_1 &= (0, 0, 0, 0, 0, 1, 0, 1, 2, 2, 1), \\
g_2 &= (0, 0, 0, 0, 1, 0, 1, 0, 1, 2, 2), \\
g_3 &= (0, 0, 0, 1, 0, 0, 2, 1, 0, 1, 2), \\
g_4 &= (0, 0, 1, 0, 0, 0, 2, 2, 1, 0, 1), \\
g_5 &= (0, 1, 0, 0, 0, 0, 1, 2, 2, 1, 0), \\
g_6 &= (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1).
\end{aligned}$$

4.1.4. Mellékosztályok módszere (mátrix módszer)

Kamps és van Lint [23] alkalmazta először a később mátrix módszernek elnevezett konstrukciót, amely a mellékosztályok használatával röviden a következőképpen fogalmazható meg:

Ha $C \subset Z_3^n$ lineáris kód, $x_1, x_2, \dots, x_t \in Z_3^n$ pedig C különböző mellékosztályaihoz tartozó pontok, akkor az x_i pontok ügyes választása esetén az általuk definiált mellékosztályok egyesítése jó térlefedő kódot eredményezhet.

Blokhuis és Lam [42] (Theorem 2.1) elégséges feltételt adtak arra, hogy a konstrukció $R = 1$ elérési sugarú kódot eredményezzen. A tételt tetszőleges q alapszámra fogalmazták meg. Mások ezt később általánosították 1-nél nagyobb elérési sugár, ill. vegyes kód esetére. A bizonyításokra és a módszer alkalmazásaira vonatkozóan lásd még Laarhoven és szerzőtársai [54], Östergård (és Hämäläinen) [86, 87, 102], Davies és Royle [99] cikkét. A növekvő méretekre való alkalmazások már számítógép használatát igényelték, melynek során a rekord-tartó kódok méretének csökkentéséhez a szerzők „simulated annealing”, ill. „tabu search” heurisztikát alkalmaztak a C kód és az x_i vektorok minél jobb választásának a megtalálására.

4.2. Folytatólagos konstrukciók és kapcsolatos egyenlőtlenségek

Az itt tárgyalt konstrukciók teljes mértékben a bináris esettel analóg módon tárgyalhatók, ezért a bizonyításokat mellőzzük. A normalitás öröklődésére is minden esetben érvényes a hasonló bináris konstrukciónak megfelelő analóg állítás. Ismét hangsúlyozzuk azonban azt a lényeges különbséget, hogy a ternáris esetben az optimális és rekord-tartó kódok között sokkal kisebb a normális kódok aránya, mint a bináris esetben.

4.2.1. 1-gyel növelt dimenzió és elérési sugár, változatlan méret

Legyen $C \subset Z_3^n$ egy M kódszóból álló, R elérési sugarú kód. Egészítsük ki C kódszavait egy-egy tetszőleges értékű $(n+1)$ -edik koordinátával. Az eredményül kapott C' kód R' elérési sugarára nyilvánvalóan fennáll $R \leq R' \leq R+1$, és következésképpen

$$K_3(n+1, R+1) \leq K_3(n, R) \leq K_3(n+1, R). \quad (4.1)$$

4.2.2. 1-gyel növelt dimenzió, változatlan elérési sugár, háromszoros méret

Legyen $C \subset Z_3^n$ egy M kódszóból álló, R elérési sugarú kód. Egészítsük ki C kódszavait először 0 értékű, majd 1 értékű, és végül 2 értékű $(n+1)$ -edik koordinátával. Az eredményül kapott

$$C'' = \{|c|0| : c \in C\} \cup \{|c|1| : c \in C\} \cup \{|c|2| : c \in C\}$$

kód elérési sugara megegyezik C elérési sugarával, és következésképpen

$$K_3(n+1, R) \leq 3K_3(n, R). \quad (4.2)$$

4.2.3. 3-mal növelt dimenzió, 2-vel növelt elérési sugár, változatlan méret

Legyen $C \subset Z_3^n$ egy M kódszóból álló, R elérési sugarú, az utolsó koordinátában normális kód. Bontsuk fel C -t a C_i ($i = 0, 1, 2$) kódok egyesítésére úgy, hogy C_i tartalmazza C -nek azokat a kódszavait, melyeknek az utolsó koordinátája i . Egészítsük ki mindegyik C_i minden kódszavát három további i értékű koordinátával. A kapott

$$\overline{C} = \{|c|000| : c \in C_0\} \cup \{|c|111| : c \in C_1\} \cup \{|c|222| : c \in C_2\}$$

kód elérési sugara legfeljebb $R+2$.

$n \setminus R$	1	2	3	4	5	6	7	8	9
2	•	•	◦	◦	◦	◦	◦	◦	◦
3	•	•	•	◦	◦	◦	◦	◦	◦
4	•	•	•	•	◦	◦	◦	◦	◦
5	•	•	•	•	•	◦	◦	◦	◦
6			•	•	•	•	◦	◦	◦
7				•	•	•	•	◦	◦
8				•	•	•	•	•	◦
9					•	•	•	•	•
10						•	•	•	•
11		•				•	•	•	•
12							•	•	•
13	•							•	•
14								•	•

4.1. táblázat. Optimális ternáris térlefedő kódok megoldott esetei

4.3. Összetételes konstrukciók

A bináris kódok tárgyalása során már említett DS, ADS és BDS konstrukcióhoz analóg módon tárgyalhatóak és lényeges változtatások nélkül átvihetők a bináris esetre megfogalmazott állítások, tulajdonságok és bizonyítások.

4.4. Ternáris térlefedő kódok mérete

A ternáris optimális térlefedő kódok pontos méretét, azaz $K_3(n, R)$ értékét az alábbi esetekben ismerjük:

- (a) $R = 0$ esetén;
- (b) $n = \frac{3^h - 1}{2}$ és $R = 1$ esetén, ahol $h \geq 2$, egész;
- (c) $n = 11, R = 2$ esetén;
- (d) $R > 0, n \leq \lfloor \frac{3R+4}{2} \rfloor$ fennállása esetén;
- (e) $n \leq 5$ esetén.

A felsorolásban, amennyire lehetett, a bináris kódokra korábban felírt esetek menetét követtük. Megint (a), (b), (c) és (d) egymást kizáró feltételek, de ezek nem zárják ki az (e) feltétel egyidejű fennállását.

A bináris esethez hasonló sematikus 4.1. táblázattal szemléltetjük – de már csak a $2 \leq n \leq 14$ intervallumban – a megoldott (• jellel jelölt), értelmezhetetlen (◦ jellel jelölt), ill. megoldatlan (üresen hagyott mezőkhöz tartozó) esetek tartományát. Az (a) esetben a

bináris kódok hasonló esetével analóg

$$K_3(n, 0) = 3^n.$$

egyenlőség érvényes. A (b) és (c) esetekhez tartozó optimális kódok a ternáris Hamming kódok, ill. a ternáris Golay kód, melyek ismeretével kapjuk a

$$K_3\left(\frac{3^h-1}{2}, 1\right) = 3^{\frac{3^h-1}{2}-h}, \quad K_3(11, 2) = 729$$

egyenlőségeket.

A (d) esetben $K_3(n, R)$ értéke 1, 3, 5, 6, 8 vagy 9 lehet.

Ezek közül a két legkisebb méret esetére nyilvánvaló a következő állítás.

4.1. Állítás.

$K_3(n, R) = 1$ akkor és csak akkor, ha $n = R$;

$K_3(n, R) = 2$ nem lehetséges;

$K_3(n, R) = 3$ akkor és csak akkor, ha $R < n < \frac{3R+3}{2}$.

A 3-nál nagyobb méretek vizsgálatához szükségünk van a bináris esetre vonatkozó 3.3. következményben megfogalmazott állítás analógiájára, amit ugyanazzal az erővel lehet rögtön általánosan, tetszőleges q alapszámra bizonyítani. Az állítást a következő lemmában mondjuk ki.

4.2. Lemma.

Ha $n \geq s+1$, $R \geq r+1$ és $K_q(n, R) < K_q(n-s, R-r-1)$, akkor az n, R paraméterekhez tartozó bármely q alapszámú optimális térlefedő kód s -szürjektív r sugárral.

Bizonyítás. Tegyük fel indirekten, hogy valamely M kódszóból álló és R elérési sugarú optimális $C \subset Z_q^n$ kód nem s -szürjektív r sugárral. Ekkor, esetleg a koordináták permutációja után, $C = |C_1|C_2|$ konkatenációként írható fel, ahol C_1 egy $(n-s, M)_q R_1$ kód, C_2 pedig egy $(s, M)_q R_2$ kód, és $R_2 \geq r+1$. Mivel C elérési sugara nem lehet C_1 és C_2 elérési sugarai összegénél kisebb, vagyis $R_1 + R_2 \leq R$, ezért $R_1 \leq R - R_2 \leq R - r - 1$, amiből viszont következik, hogy $K_q(n-s, R-r-1) \leq M$, tehát $K_q(n, R) \geq K_q(n-s, R-r-1)$. $\square$

Megfogalmazzuk még a bebizonyított lemmának egy közvetlenül adódó következményét, majd annak egy speciális esetét.

4.3. Következmény. (K . és Östergård [129], Theorem 2)

Ha $K_q(n-s, R-r-1) > M$ és $\sigma_q(n, s; r) > M$, akkor $K_q(n, R) > M$. Ennélfogva fennáll

$$K_q(n, R) \geq \min\{\sigma_q(n, s; r), K_q(n-s, R-r-1)\}. \quad (4.3)$$

Az $s = q$, $r = q - 2$ speciális esetre megfogalmazva:

4.4. Következmény. Ha $K_q(n - q, R - q + 1) > M$ és $\sigma_q(n, q; q - 2) > M$, akkor $K_q(n, R) > M$. Ennélfogva fennáll

$$K_q(n, R) \geq \min\{\sigma_q(n, q; q - 2), K_q(n - q, R - q + 1)\}.$$

Ebből a ternáris esetre specifikálva kapjuk a következő állítást.

4.5. Következmény.

Ha $K_3(n - 3, R - 2) > M$ és $\sigma_3(n, 3; 1) > M$, akkor $K_3(n, R) > M$. Ennélfogva fennáll

$$K_3(n, R) \geq \min\{\sigma_3(n, 3; 1), K_3(n - 3, R - 2)\}. \quad (4.4)$$

A továbbiakban a (4.4) egyenlőtlenséget sorozatosan felhasználjuk a 4.1. állítás folytatását szolgáló tételek bizonyítására.

4.6. Tétel. (*K. és Östergård [129], Theorem 11 és [145] Theorem 3, 5 és 10*)

$K_3(n, R) = 4$ nem lehetséges;

$K_3(n, R) = 5$ akkor és csak akkor, ha $n = 3$ és $R = 1$;

$K_3(n, R) = 6$ akkor és csak akkor, ha $R \geq 3$, páratlan és $n = \frac{3R+3}{2}$;

$K_3(n, R) = 7$ nem lehetséges.

Bizonyítás. A tételben foglalt állítások egyes részletei korábbról ismertek. A $K_3(3, 1) = 5$ egyenlőséget először Taussky és Todd [3] bizonyították, később Blokhuis és Lam [42] általánosították tetszőleges q esetére, bebizonyítva, hogy $K_q(3, 1) = \left\lceil \frac{q^2}{2} \right\rceil$.

Az $R \geq 3$, páratlan, $n = \frac{3R+3}{2}$ esetre vonatkozó $K_3(n, R) \leq 6$ egyenlőtlenséget Östergård [65] bizonyította, a fordított egyenlőtlenséget az Östergårddal közösen írt [129] cikkben bizonyítottuk. Az utóbbi bizonyítás lényege, hogy $K_3(6, 3) = 6$ (lásd Cohen, és szerzőtársai [97], Example 6.7.5) és $\sigma_3(4, 3; 1) = 6$ (lásd [129], Theorem 7) ismeretében ismételtén alkalmazzuk a (4.4) egyenlőtlenséget.

A tétel állításai szükségességének a bizonyításához abból indulunk ki, hogy a 4.1. állításból következően $n < \frac{3R+3}{2}$ esetén $K_3(n, R)$ értéke nem lehet 3-nál nagyobb. Most tekintsük át rendre az $n = \frac{3R+3}{2}$, $n = \frac{3R+4}{2}$ stb. eseteket, minden lépés során a jobb oldalon lévő tört értékét $\frac{1}{2}$ -del növelve.

Ha $n = \frac{3R+3}{2}$, akkor R szükségképpen páratlan, és így éppen a 4.6. tételben szereplő esetekhez jutunk.

Az $n = \frac{3R+4}{2}$ esetre bebizonyítjuk, hogy ilyenkor $K_3(n, R) \geq 8$. Ennek bizonyításához (amikor is R szükségképpen páros), már számítógép segítségére volt szükségünk.

Gépi programmal végzett vizsgálatokkal [145]-ben megmutattuk, hogy $K_3(8, 4) = 9$ és $\sigma_3(11, 3; 1) = 8$. (Az utóbbi adat a Függelék A.6 táblázatából, vagy a CD mellékleten a $\sigma_3(n, s; r)$ korlátaira megadott táblázatból is kiolvasható.) Most a (4.4) egyenlőtlenség ismételt alkalmazásával adódik, hogy $K_3(n, R) \geq 8$, ha $R \geq 4$, páros és $n = \frac{3R+4}{2}$. $R = 2$ -re viszont nagyon rég óta ismert a $K_3(5, 2) = 8$ egyenlőség.

Az $n = \frac{3R+5}{2}$ esetre vonatkozóan (amikor is R szükségképpen páratlan) elég a nyilvánvaló $K_q(n, R) \geq K_q(n+1, R+1)$ egyenlőtlenségre hivatkozni, melynek alapján azt kapjuk, hogy $K_3(\frac{3R+5}{2}, R) \geq K_3(\frac{3R+7}{2}, R+1) = K_3(\frac{3S+4}{2}, S)$, ahol $S = R+1$.

Itt megállhatunk, mivel n értékének további növelésével, változatlanul hagyott R érték mellett nyilván még inkább legalább 8 adódik $K_q(n, R)$ értékeként. $\square$

4.7. Tétel. (*K. és Östergård [145], Theorem 10*)

$K_3(n, R) = 8$ akkor és csak akkor, ha $n = 5$ és $R = 2$.

Bizonyítás. A feltétel elégségességét, vagyis a $K_3(5, 2) = 8$ egyenlőséget Östergård és Härmäläinen [78, 102], valamint tőlük függetlenül Kolev és Landgev [84] bizonyították.

A szükségesség bizonyítását az alábbi észrevétellel kezdjük: A 4.1. állítás és a 4.6. tétel egyesítése mutatja, hogy $n \leq \frac{3R+3}{2}$ esetén $K_3(n, R)$ értéke nem lehet 6-nál nagyobb.

Ha $n = \frac{3R+4}{2}$, akkor az $R = 2$ esetre már tudjuk, hogy $K_3(5, 2) = 8$.

Ha $n = \frac{3R+4}{2}$ és $R \geq 4$, páros, akkor minden ilyen esetre bebizonyítjuk, hogy $K_3(n, R) \geq 9$. Ehhez ismét szükségünk van az előző tétel bizonyításához is felhasznált $K_3(8, 4) = 9$ egyenlőség ismeretére, valamint az 1 sugárral 3-szűrjektív kódokra vonatkozó, a [145] cikkben elvégzett klasszifikáció eredményére, melynek során gépi programmal az összes ilyen kód elérési sugarát is kiszámítottuk. Az említett cikkből átvett, az értekezés függelékében található A.6 táblázat alapján megállapítható, hogy nincs sem olyan $(11, 8)_3$ kód, sem olyan $(14, 8)_3$ kód, amely 3-szűrjektív 1 sugárral.

Ha tehát feltesszük, hogy $K_3(11, 6) = 8$, akkor a 4.2. lemmát $n = 11, R = 6, s = 3, r = 1$ -re alkalmazva, $K_3(8, 4) = 9$ ismeretében arra következtethetünk, hogy a feltételezett 8 szavas optimális $(11, 8)_3$ kódok 3-szűrjektívek 1 sugárral. Az előbb viszont megállapítottuk, hogy ilyen kód nem létezik. Következésképpen $K_3(11, 6) \geq 9$. A gondolatmenet megismétlésével adódik, hogy $K_3(14, 8) \geq 9$. Idáig eljutva, a folytatáshoz lehet már a 4.5. következményt alkalmazni, mely szerint

$$K_3(17, 10) \geq \min\{\sigma_3(17, 3; 1), K_3(14, 8)\} \geq 9.$$

Ezzel eljutottunk annak bizonyításáig, hogy $K_3(n, R) \geq 9$, ha $4 \leq R \leq 10$, R páros és $n = \frac{3R+4}{2}$.

A 4.5. következmény ismételt alkalmazásával kapjuk, hogy innentől kezdve a 9 alsó korlát öröklődik minden olyan n, R párra, amelyre $R \geq 12$, R páros és $n = \frac{3R+4}{2}$ és $R \geq 12$

Ha $n = \frac{3R+5}{2}$, akkor $R = 1$ esetén $K_3(4, 1) = 9$ a ternáris Hamming kód bizonyítja a $K_3(4, 1) = 9$ egyenlőséget. Ha viszont $n = \frac{3R+5}{2}$ és $R \geq 3$, páratlan, akkor majdnem

szóról szóra megismételhetjük az előző tétel bizonyításának két utolsó bekezdését úgy, hogy a 8 számot 9-re cseréljük a bizonyítás végén. $\square$

4.8. Tétel. (*K. és Östergård [145], Theorem 9*)

$K_3(n, R) = 9$, ha $n = 4$, $R = 1$, vagy pedig $R \geq 4$, páros és $n = \frac{3R+4}{2}$.

Bizonyítás. Az első esetet a már az előző tétel bizonyításában is említett Hamming kód bizonyítja, a második esetként megfogalmazott kód családra pedig az előző bizonyításban már megmutattuk, hogy $K_3(n, R) \geq 9$. A fordított egyenlőtlenség viszont nagyon egyszerűen következik a 4.1. állításból adódó $K_3(\frac{3R+2}{2}, R) \leq 3$ egyenlőtlenségből és a (4.2) összefüggésből. $\square$

Szükséges és elégséges feltételt 9 kódszó esetére nem tudunk bizonyítani, de a 4.8. tételben megadott feltételek szükségessége nagyon valószínűnek látszik. Ahhoz ugyanis, hogy az ott megadott eseteken kívül legyen még más olyan eset, melyre $K_3(n, R) = 9$, egyenlőséggel kellene teljesülnie a $K_3(n+1, R+1) \leq K_3(n, R)$ egyenlőtlenségnek valamely páratlan R és $n = \frac{3R+5}{2}$ esetén.

Végül az egyetlen hátralévő, eddig még nem magyarázott (*e*) esetben egyetlen olyan értékpár van, amelyet még nem tárgyaltunk: $n = 5$, $R = 1$. Ebben az esetben $K_3(5, 1) = 27$, melynek bizonyítása Kamps és van Lint [16] cikkében található.

4.5. Klasszifikációs eredmények ternáris térlefedő kódokra

Klasszifikációs eredményről a következő esetekben tudunk beszámolni:

(a) Tetszőleges n pozitív egész és $R = 0$ esetén az inekvivalens optimális térlefedő kódok száma 1.

(b) $n = \frac{3^h-1}{2}$, $R = 1$ és $h = 2$ esetén az inekvivalens optimális térlefedő kódok száma 1. (2-nél nagyobb h esetére nincs klasszifikációs eredmény.)

(c) $n = 11$, $R = 2$ esetén az inekvivalens optimális térlefedő kódok száma 1.

A (d_1) eset érdektelen, mivel bármely két 1-szavas kód ekvivalens egymással.

(d_2) Minden olyan esetben, amikor $K_3(n, R) = 3$, az inekvivalens optimális térlefedő kódok számát megadja az $1/((1-x)^3(1-x^2)(1-x^3))$ kifejezés végtelen polinom kifejtésében $x^{3R-2n+2}$ együtthatója.

(d_3) $n = 3$, $R = 1$ esetén az inekvivalens optimális térlefedő kódok száma 1.

(d_4) $n = 6$, $R = 3$ esetén az inekvivalens optimális térlefedő kódok száma 28.

(d_5) $n = 5, R = 2$ esetén az inekvivalens optimális térlefedő kódok száma 1.

(e) $n = 5, R = 1$ esetén az inekvivalens optimális térlefedő kódok száma 17.

Részletek.

Az (a) esetben az egyetlen optimális kód az egész tér.

A (b) $K_3(4, 1) = 9$, (c) $K_3(11, 2) = 729$, (d_3) $K_3(3, 1) = 5$, ill. (d_5) $K_3(5, 2) = 8$ esetekre az optimális kód unicitását Kalbfleisch és Stanton [17], Delsarte és Goethals [36], Östergård [94], ill. Bertolo és szerzőtársai [130] bizonyították.

A (d_2) esetre vonatkozó klasszifikációt látszólag könnyű feladatnak gondolhatnánk, azonban az eddigi szakirodalomból nem ismerünk erre az esetre klasszifikációs eredményt. Kivétel ez alól az $n = 2$ eset, amelyre vonatkozó eredmény következik egy, a $K_q(2, 1) = q$ egyenlőséget teljesítő optimális térlefedő kódokra megfogalmazott általánosabb klasszifikációs eredményből, lásd Kaski és Östergård [138], Theorem 7.32.

A tetszőleges n értékre vonatkozó klasszifikációs tételhez (4.10. tétel) szükségünk van a 3 kódszóból álló optimális térlefedő kódok karakterizálására, amit általánosabban, q -adrendű kódábécé és q kódszó esetére következő állításban fogalmazunk meg.

4.9. Állítás.

$K_q(n, R) = q$ akkor és csak akkor, ha $R < n < \frac{qR+q}{q-1}$. Az adott egyenlőtlenség-pár fennállása esetén az optimális kódok azok és csak azok a q szóból álló kódok, melyek kódszavaiban legalább $q(n - R - 1) + 1$ koordináta-helyen a $0, 1, \dots, q - 1$ szimbólumok mindegyike előfordul.

Megjegyezzük, hogy bizonyos esetekben jobban használható az állításban szereplő egyenlőtlenség-párnak olyan átalakítása, ahol R értékét szorítjuk két kifejezés közé:

$$K_q(n, R) = q \text{ akkor és csak akkor áll fenn, ha } \frac{(q-1)(n-1)}{q} \leq R < n.$$

Bizonyítás. Az állítás első fele közismert, bizonyítása a skatulya elven alapul. Az állítás második felének bizonyításához először tegyük fel, hogy egy q kódszóból álló $C \subset Z_q^n$ kód szavaiban legalább $q(n - R - 1) + 1$ koordináta-helyen fordul elő a $0, 1, \dots, q - 1$ szimbólumok mindegyike. Tekintsük C -nek a koordináták szerinti $|C_1|C_2|$ felbontását, ahol C_1 az előbbi $q(n - R - 1) + 1$ koordináta-helyhez, C_2 pedig a további $n - q(n - R - 1) - 1$ koordináta-helyhez tartozó kód. Ekkor C_1 egy ismétléses kóddal ekvivalens, tehát elérési sugara $\left\lfloor \frac{(q(n - R - 1) + 1)(q - 1)}{q} \right\rfloor = (n - R - 1)(q - 1)$. E kódot további $n - q(n - R - 1) - 1$ koordinátával kibővítve, az elérési sugár is legfeljebb $n - q(n - R - 1) - 1$ -gyel növekedhet, tehát nem lehet nagyobb, mint $(n - R - 1)(q - 1) + n - q(n - R - 1) - 1 = R$.

Fordítva, tegyük fel, hogy egy q kódszóból álló $C \subset Z_q^n$ kód szavaiban legfeljebb $q(n - R - 1)$ koordináta-helyen fordul elő a $0, 1, \dots, q - 1$ szimbólumok mindegyike. Tekintsük megint C -nek a koordináták szerinti $|C_1|C_2|$ felbontását, ahol C_1 dimenziója most $q(n - R - 1)$, C_2 -é pedig $n - q(n - R - 1)$. Ekkor C_1 elérési sugara legalább

akkora, mint a vele azonos dimenziós ismétléses kód elérési sugara, vagyis legalább $(n - R - 1)(q - 1)$, C_2 elérési sugara $n - q(n - R - 1)$, így a kettő összefűzésével képzett C kód elérési sugara legalább $(n - R - 1)(q - 1) + n - q(n - R - 1) = R + 1$, tehát nem R . $\square$

4.10. Tétel.

Minden olyan esetben, amikor $K_3(n, R) = 3$ – tehát $R < n < \frac{3R+3}{2}$ – az inekvivalens optimális térlefedő kódok számát megadja az

$$\frac{1}{(1-x)^3(1-x^2)(1-x^3)} = 1 + 3x + 7x^2 + 14x^3 + 25x^4 + 41x^5 + \dots$$

kifejezés végtelen polinom kifejtésében $x^{3R-2n+2}$ együtthatója.

E polinom együtthatóinak sorozata a *The on-line encyclopedia of integer sequences* [175] összeállításban A057524 azonosítóval jelölt sorozat.

Bizonyítás. A 4.9. állítást $q = 3$ -ra specifikálva, optimális kódok azok a 3 szavas kódok, melyek kódszávaiban legalább $3n - 3R - 2$ koordináta-helyen előfordul a 0, 1, 2 szimbólumok mindegyike. Ez azt jelenti, hogy a kód $3n - 3R - 2$ koordinátát tartalmazó része ekvivalenciától eltekintve kötött, ekvivalens egy ismétléses kóddal, a további $3R - 2n + 2$ koordináta-helyen pedig bármi állhat a kódszavakban. Ebből már látszik, hogy az inekvivalens optimális kódok száma csak $3R - 2n + 2$ értékétől függ. Csoportosítsuk a nem kötött koordinátákat aszerint, hogy az előforduló különböző szimbólumok száma 1, 2, vagy 3. Három azonos szimbólum esetén feltehetjük, hogy azonosan 0-k; két különböző szimbólum esetén feltehetjük, hogy két kódszóban fordul elő a 0, egy kódszóban az 1-es, de mindhárom lehetséges sorrendet figyelembe kell venni; végül három különböző szimbólum esetén feltehetjük, hogy ezek mindig 0, 1, 2 sorrendben következnek a három kódszóban. A kérdés tehát úgy is feltehető, hogy az 1 dimenziós

$$\begin{aligned} C_1 &= \{0, 0, 0\}, \\ C_2 &= \{0, 0, 1\}, \\ C_3 &= \{0, 1, 0\}, \\ C_4 &= \{1, 0, 0\}, \\ C_5 &= \{0, 1, 2\} \end{aligned}$$

kódokból ismétlést is megengedő összefűzéssel hány $N = 3R - 2n + 2$ dimenziós inekvivalens kódot tudunk felépíteni. Jelöljük n_i -vel a C_i kód ismétléseinek számát. Mivel C_2, C_3 és C_4 felépítése a kódszavak sorrendjétől eltekintve megegyezik, ezért a célból, hogy csak inekvivalens kódokat vegyünk figyelembe, feltesszük, hogy $n_2 \geq n_3 \geq n_4$. Így tehát az N egész olyan 5 nemnegatív egész tagból álló partícióinak a számát kell meghatároznunk, melyekre

$$\begin{aligned} n_1 + n_2 + n_3 + n_4 + n_5 &= N, \\ n_1 &\geq 0, \\ n_2 &\geq n_3 \geq n_4 \geq 0, \\ n_5 &\geq 0. \end{aligned}$$

Ebből a korábbi hasonló jellegű partíciókra alkalmazott módszerrel adódik, hogy a partíciók számát x^N együtthatója mutatja a tétel állításában megadott függvény

polinom kifejtésében. □

A (d_4) $K_3(6, 3) = 6$ esetre számítógép segítségével, a 9. fejezetben ismertetésre kerülő algoritmus és program alkalmazásával kaptam a következő klasszifikációs eredményt.

4.11. Tétel.

A $K_3(6, 3) = 6$ egyenlőséghez tartozó inekvivalens optimális térlefedő kódok száma 28.

Megjegyzés. A klasszifikációs eredmények felhasználási lehetőségére mutatunk rá az alábbi gondolatmenettel. A 4.11. tétel esetéhez tartozó inekvivalens optimális kódok ismerete alapján nem nehéz olyan általánosított szűrjektív kódot találni, amely bizonyítja, hogy $\sigma_3(7, 6; 3) = 6$. Ha mind a hét inekvivalens ilyen kódot összegyűjtjük, akkor pedig ezek vizsgálata alapján megmutatható, hogy $\sigma_3(8, 6; 3) = 7$. Mindez számítógép nélkül elvégezhető, azonban gépi program használatával kényelmesebben lehet ezeket a következtetéseket is levonni.

Az (e) $K_3(5, 1) = 27$ esetre vonatkozóan Kolev [75] meghatározta az optimális kódok szerkezetét, megmutatva, hogy minden optimális kód előállítható úgy, hogy három (nem feltétlenül különböző), a $(4, 9)_3$ Hamming kóddal ekvivalens, perfekt kód egyikének minden kódszavát 0-val, a másiknak minden kódszavát 1-essel, a harmadiknak minden kódszavát 2-essel megtoldjuk. Az optimális $(5, 27)_3$ térlefedő kódok e tulajdonságának ismeretében Östergård és Weakley [126] leírta az inekvivalens optimális kódokat, megmutatva, hogy ezek száma 17.

4.6. A ternáris térlefedő kódok áttekintése

A bináris kódokra összeállított 3.8 szakaszhoz hasonlóan járunk el, azonban most 3-nál nagyobb elérési sugárhoz tartozó eseteket is vizsgálunk, és ennél fogva az $n \leq 14, R \leq 7$ tartományra ismertetjük a rendelkezésre álló eredményeket és egyéb közölni valókat. Megint csak néhány esetben adjuk meg az optimális kódok kódszavait a nyomtatott anyagban, viszont minden esetben megadjuk ezeket, valamint esetenként legalább egy rekord-tartó kódot a mellékelt lemezen.

Ismét megadjuk a prompt (azaz triviális vagy majdnem triviális) korlátokat. A prompt alsó korlátra most is a szférikus korlátot használjuk. A prompt felső korlátok képzéséhez 3 szavas kódok, valamint a Hamming kódok és a Golay kód ismert méretéből kiindulva, elsősorban a (4.2) egyenlőtlenséget használjuk. Ily módon

$K_3(2, 1) = 3$ alapján kapjuk a $K_3(3, 1) \leq 9$ prompt felső korlátot;

$K_3(4, 2) = 3$ alapján kapjuk a $K_3(5, 2) \leq 9$, $K_3(6, 2) \leq 27$, $K_3(7, 2) \leq 81$, $K_3(8, 2) \leq 243$ és $K_3(9, 2) \leq 729$ prompt felső korlátokat;

$K_3(5, 3) = 3$ alapján kapjuk a $K_3(6, 3) \leq 9$, $K_3(7, 3) \leq 27$, $K_3(8, 3) \leq 81$, $K_3(9, 3) \leq 243$ és $K_3(10, 3) \leq 729$ prompt felső korlátokat;

$K_3(4, 1) = 9$ (Hamming kód) alapján kapjuk a $K_3(5, 1) \leq 27$, $K_3(6, 1) \leq 81$, $K_3(7, 1) \leq 243$, $K_3(8, 1) \leq 729$, $K_3(9, 1) \leq 2187$, $K_3(10, 1) \leq 6561$, $K_3(11, 1) \leq 19683$ és $K_3(12, 1) \leq 59049$ prompt felső korlátokat;

$K_3(13, 1) = 59049$ (Hamming kód) alapján kapjuk a $K_3(14, 1) \leq 177147$ prompt felső korlátot;

$K_3(11, 2) = 729$ (Golay kód) alapján kapjuk a $K_3(12, 2) \leq 2187$, $K_3(13, 2) \leq 6561$ és $K_3(14, 2) \leq 19683$ prompt felső korlátokat.

A Golay kódnál tartva néhány esetben jobban járunk, ha a $K_3(n, R)$ függvény (4.1)-ben megadott monotonitási tulajdonságait használjuk fel a prompt felső korlátok képzéséhez:

$K_3(11, 2) = 729$ alapján kapjuk a $K_3(10, 2) \leq 729$, $K_3(11, 3) \leq 729$, és $K_3(12, 3) \leq 729$ prompt felső korlátokat;

Végül visszatérve az alap-értelmezett prompt felső korlát képzéshez:

$K_3(12, 3) \leq 729$ alapján kapjuk a $K_3(13, 3) \leq 2187$ és $K_3(14, 3) \leq 6561$ prompt felső korlátokat.

Itt említjük meg a ternáris kódok történetének egy vitatott részletét. Még 1992-ben elkészült és szűk körben terjesztésre került Lo és Zhang [69] kézírata, amelyben a szerzők több, az addig ismertnél jobb alsó korlát létezését állították. E kéziratra három azóta már megjelent cikk hivatkozik: [92], [98] és [104], de a [69] kéziratnak folyóiratban vagy cikkgyűjteményben való közlése máig sem történt meg. Ezért a szakma nem fogadja el bizonyítottaknak a [69]-ben adott új alsó korlátokat. Ezek között már csak egy olyan eset fordul elő, amelyre azóta sem sikerült jobbat találni, mégpedig a $K_3(11, 3)$ -re vonatkozó megkérdőjelezett 119 alsó korlát.

4.6.1. $R = 1$ elérési sugarú kódokra vonatkozó eredmények

$K_3(2, 1) = 3$ és 3 optimális kód létezik:

$$\begin{array}{ccc} & \begin{matrix} 0 & 0 \\ 1 & 1 \\ 2 & 2 \end{matrix} & \begin{matrix} 0 & 0 \\ 0 & 1 \\ 1 & 2 \end{matrix} & \begin{matrix} 0 & 0 \\ 0 & 1 \\ 0 & 2 \end{matrix} \\ (1) & & (2) & (3) \end{array}$$

$K_3(3, 1) = 5$ és az alábbi egyetlen optimális kód létezik. Prompt alsó és felső korlát: 4, ill. 9. Pontos érték igazolása: [3, 17]. Klasszifikáció (ami itt az unicitás bizonyítását jelenti): [94]. Totókód 5 kódszóval: Weikel G. (1943). Az optimális kód kiegyensúlyozott, abnormális kód.

$$\begin{array}{ccc} & 0 & 0 & 0 \\ & 1 & 1 & 1 \\ (1) & 1 & 2 & 2 \\ & 2 & 1 & 2 \\ & 2 & 2 & 1 \end{array}$$

$K_3(4, 1) = 9$ és az alábbi egyetlen optimális kód létezik. Prompt alsó és felső korlát: egyaránt 9 (perfekt kód). Pontos érték igazolása: [3, 6, 7, 8]. Klasszifikáció (ami itt az unicitás bizonyítását jelenti): [17]. Totókód 9 kódszóval: ismeretlen szerző (1946). Az optimális kód lineáris, perfekt, kiegyensúlyozott, abnormális kód.

$$(1) \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 1 & 2 & 0 & 1 \\ 2 & 0 & 2 & 1 \\ 2 & 1 & 0 & 2 \\ 2 & 2 & 1 & 0 \end{pmatrix}$$

$K_3(5, 1) = 27$ és 17 optimális kód létezik. Prompt alsó és felső korlát: 23, ill. 27. Az alsó korlát javítása 26-ra [20], 27-re [16, 75]. Klasszifikáció: [126]. Totókód 27 kódszóval: ismeretlen szerző (1946), [Valiosysteemit] (1970). Valamennyi optimális kód kiegyensúlyozott, normális kód.

$71 \leq K_3(6, 1) \leq 73$. Prompt felső korlát 81. A felső korlát javítása 79-re [40], 74-re [49], 73-ra [54, 93]. Prompt alsó korlát: 57. Az alsó korlát javítása 60-ra [82], 63-ra [40], 65-re [125], 71-re [147, 148]. (Az utóbbi eredmény érdekessége, hogy szokatlanul nagy, figyelemre méltó ugrást tartalmaz a 65 alsó korlátról 71-re, a bizonyítás azonban óriási mennyiségű gépidőt, számítógép-hálózat használatával a szerzők szerint összesítve 140 CPU-évet vett igénybe.) Totókód 73 kódszóval: D'Agostino F. (1984). Az ismert rekord-tartó konstrukció kiegyensúlyozatlan, abnormális kód. Található benne hat olyan kódszó-hármas, amelyekhez tartozó három-három kódszó csak egy koordináta-helyen tér el egymástól. Az ilyen tulajdonságnak, a bináris kódok esetén két koordináta-helyen eltérő kódszó-négyesekhez hasonlóan, totó célú alkalmazásnál van jelentősége.

$156 \leq K_3(7, 1) \leq 186$. Prompt felső korlát 243. A felső korlát javítása 225-re [41], 216-ra [42], 186-ra [54]. Prompt alsó korlát: 146. Az alsó korlát javítása 147-re [57], 150-re [82], 153-ra [91], 156-ra [144]. Totókód 189 kódszóval: Himberg [Valiosysteemit] (1970), 186 kódszóval: D'Agostino F. (1985). Az ismert rekord-tartó konstrukció kiegyensúlyozatlan, abnormális kód. Találhatóak benne egy koordináta-helyen eltérő hármas, valamint két koordináta-helyen eltérő négyes kódszó-csoportok.

$402 \leq K_3(8, 1) \leq 486$. Prompt felső korlát 729. A felső korlát javítása 567-re [41], 486-ra [54]. Prompt alsó korlát: 386. Az alsó korlát javítása 389-re [57], 390-re [66], 393-ra [80], 397-re [92], 398-ra [116], 402-re [144]. Totókód 546 kódszóval: ismeretlen szerző [Valiosysteemit] (1970), 486 kódszóval: Bruno G. (1988). Az ismert rekord-tartó konstrukció kiegyensúlyozott, normális kód.

$1060 \leq K_3(9, 1) \leq 1269$. Prompt felső korlát 2187. A felső korlát javítása 1458-ra [23], 1431-re [77], 1356-ra [78], 1341-re [101], 1269-re [127]. Prompt alsó korlát: 1036. Az alsó korlát javítása 1043-ra [66], 1044-re [82], 1048-ra [80], 1060-ra [92]. Totókód 1269 kódszóval: Di Pasquale F. (2000). Az ismert rekord-tartó konstrukció kiegyensúlyozott, abnormális kód.

$2854 \leq K_3(10, 1) \leq 3645$. Prompt felső korlát 6561. A felső korlát csökkentése 3645-re [42]. Prompt alsó korlát: 2812. Az alsó korlát javítása 2814-re [57], 2818-ra [82], 2835-re [117], 2854-re [124]. Totókód 3645 kódszóval: Cercione De Lucia F. (1962) és Heikkonen [Veikkaja] (1967). Az ismert rekord-tartó konstrukció kiegyensúlyozott, abnormális kód.

$7832 \leq K_3(11, 1) \leq 9477$. Prompt felső korlát 19683. A felső korlát javítása 10935-re [60], 10530-ra Hämmäläinen, lásd [65], 9477-re [87, 96]. Prompt alsó korlát: 7703. Az alsó korlát javítása 7734-re [57], 7736-ra [66], 7767-re [80], 7822-re [92], 7832-re [116]. Az ismert rekord-tartó konstrukció kiegyensúlyozott, abnormális kód.

$21531 \leq K_3(12, 1) \leq 27702$. Prompt felső korlát 59049. A felső korlát csökkentése 29889-re [60], 27702-re [87, 96]. Prompt alsó korlát: 21258. Az alsó korlát javítása 21329-re [66], 21395-re [80], 21531-re [116]. Totókód 29889 kódszóval: ismeretlen szerző [Veikkaja] (1949). Az ismert rekord-tartó konstrukció kiegyensúlyozatlan, normális kód. Találhatóak benne egy koordináta-helyen eltérő hármas, valamint két koordináta-helyen eltérő négyes kódszó-csoportok.

$K_3(13, 1) = 59049$. Prompt alsó és felső korlát: egyaránt 59049 (perfekt kód). Pontos érték igazolása: [6, 7, 8]. Klasszifikáció: megoldatlan (nehéz) probléma. Minden optimális kód lineáris, perfekt, kiegyensúlyozott, abnormális kód.

$166610 \leq K_3(14, 1) \leq 177147$. Prompt alsó és felső korlát: 164930, ill. 177147. Az alsó korlát javítása 163351-re [57], 165365-ra [66], 165775-re [80], 166526-re [92], 166610-re [116]. Konstrukció: Az egy koordinátával rövidebb perfekt kódra alkalmazzuk a 4.2.2 szakaszban ismertetett módszert.

4.6.2. $R = 2$ elérési sugarú kódokra vonatkozó eredmények

$K_3(3, 2) = 3$ és az alábbi 7 optimális kód létezik.

$$\begin{array}{cccc}
 & \begin{array}{ccc} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 2 & 2 & 2 \end{array} & & \begin{array}{ccc} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 2 & 2 \end{array} & & \begin{array}{ccc} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 2 & 2 \end{array} & & \begin{array}{ccc} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 2 \end{array} \\
 (1) & & (2) & & (3) & & (4) & \\
 & & & & & & & \\
 & & \begin{array}{ccc} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 2 \end{array} & & \begin{array}{ccc} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 2 \end{array} & & \begin{array}{ccc} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 2 \end{array} & & \\
 & & (5) & & (6) & & (7) &
 \end{array}$$

$K_3(4, 2) = 3$ és az alábbi egyetlen optimális kód létezik, amely kiegyensúlyozott, normális kód.

$$\begin{array}{c}
 \begin{array}{cccc} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 \end{array} \\
 (1)
 \end{array}$$

$K_3(5, 2) = 8$ és az alábbi egyetlen optimális kód létezik. Prompt felső korlát 9. A felső korlát javítása 8-ra [60]. Prompt alsó korlát: 5. Az alsó korlát javítása 6-ra [55, 57], 8-ra [78, 84, 102]. Klasszifikáció (ami itt az unicitás bizonyítását jelenti): [130]. Totókód 8 kódszóval: Himberg [Valiosysteemit] (1970). Az egyetlen optimális kód kiegyensúlyozott, abnormális kód.

$$(1) \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 2 & 2 & 2 \\ 1 & 2 & 1 & 2 & 2 \\ 1 & 2 & 2 & 0 & 0 \\ 2 & 1 & 1 & 0 & 1 \\ 2 & 1 & 1 & 1 & 0 \\ 2 & 2 & 2 & 2 & 2 \end{pmatrix}$$

$15 \leq K_3(6, 2) \leq 17$. Prompt felső korlát 27. A felső korlát javítása 17-re [60]. Prompt alsó korlát: 10. Az alsó korlát javítása 11-re [55], 12-re [57], 14-re [104], 15-re [130]. Totókód 17 kódszóval: Weikel (1960) és ismeretlen szerző [Veikkaja] (1961). Az ismert rekord-tartó konstrukció kiegyensúlyozatlan, abnormális kód.

$26 \leq K_3(7, 2) \leq 34$. Prompt felső korlát 81. A felső korlát javítása 34-re [60, 78, 102]. Prompt alsó korlát: 23. Az alsó korlát javítása 24-re [55], 25-re [66], 26-ra [57]. Totókód 34 kódszóval: Östergård P. [Veikkaus-Lotto] (1988). Az ismert rekord-tartó konstrukció kiegyensúlyozott, abnormális kód.

$54 \leq K_3(8, 2) \leq 81$. Prompt felső korlát 243. A felső korlát csökkentése 81-re [60]. Prompt alsó korlát: 51. Az alsó korlát javítása 52-re [80], 54-re [104]. Totókód 81 kódszóval: „ARIC” (1936). Az ismert rekord-tartó konstrukció kiegyensúlyozott, abnormális kód.

$130 \leq K_3(9, 2) \leq 219$. Prompt felső korlát 729. A felső korlát csökkentése 219-re [60, 65]. Prompt alsó korlát: 121. Az alsó korlát javítása 128-ra [57, 66], 130-ra [92]. Totókód 219 kódszóval: Östergård P. [Veikkaus-Lotto] (1989). Az ismert rekord-tartó konstrukció kiegyensúlyozatlan, abnormális kód. Találhatóak benne egy koordináta-helyen eltérő hármas kódszó-csoportok.

$323 \leq K_3(10, 2) \leq 555$. Prompt felső korlát 729. A felső korlát javítása 558-ra [65], 555-re [130]. Prompt alsó korlát: 294. Az alsó korlát javítása 322-re [66], 323-ra [57]. Totókód 555 kódszóval: D’Agostino F. (1996). Az ismert rekord-tartó konstrukció kiegyensúlyozatlan, abnormális kód.

$K_3(11, 2) = 729$ és egyetlen optimális kód létezik. Prompt alsó és felső korlát: egyaránt 729 (perfekt kód). Pontos érték igazolása: [4]. Klasszifikáció (ami itt az unicitás bizonyítását jelenti): [36]. Totókód 729 kódszóval: Virtakallio (1947). Az egyetlen optimális kód a ternáris Golay kód, amely perfekt, kiegyensúlyozott, abnormális kód, 5 legkisebb távolsággal.

$1919 \leq K_3(12, 2) \leq 2187$. Prompt alsó és felső korlát: 1839, ill. 2187. Az alsó korlát javítása 1915-re [66], 1919-re [57]. Konstrukció: Az egy koordinátával rövidebb perfekt kódra alkalmazzuk a 4.2.2 szakaszban ismertetett módszert. Az ismert rekord-tartó konstrukció kiegyensúlyozott, normális kód. A konstrukció folytán egy koordináta-helyen eltérő hármas kódszó-csoportokra tagolható.

$5062 \leq K_3(13, 2) \leq 6561$. Prompt alsó és felső korlát: 4704, ill. 6561. Az alsó korlát javítása 5048-ra [66], 5062-re [57]. Konstrukció: A 4.2.2 szakaszban ismertetett módszer kétszeres alkalmazása. Az ismert rekord-tartó konstrukció kiegyensúlyozott, normális kód. A konstrukció folytán két koordináta-helyen eltérő kilences kódszó-csoportokra tagolható.

$12204 \leq K_3(14, 2) \leq 19683$. Prompt alsó és felső korlát: 12171, ill. 19683. Az alsó korlát javítása 12193-ra [80], 12204-re [92].

4.6.3. $R = 3$ elérési sugarú kódokra vonatkozó eredmények

$K_3(4, 3) = 3$ és 14 optimális kód létezik:

(1)	0 0 0 0 1 1 1 1 2 2 2 2	(2)	0 0 0 0 0 1 1 1 1 2 2 2	(3)	0 0 0 0 0 1 1 1 0 2 2 2	(4)	0 0 0 0 0 0 1 1 1 1 2 2
(5)	0 0 0 0 0 1 1 1 1 0 2 2	(6)	0 0 0 0 0 0 1 1 0 1 2 2	(7)	0 0 0 0 0 0 1 1 0 0 2 2	(8)	0 0 0 0 0 0 0 1 1 1 1 2
(9)	0 0 0 0 0 0 1 1 1 1 0 2	(10)	0 0 1 0 0 1 0 1 1 0 0 2	(11)	0 0 0 0 0 0 0 1 0 1 1 2		
(12)	0 0 0 0 0 0 1 1 0 1 0 2	(13)	0 0 0 0 0 0 1 1 0 0 0 2	(14)	0 0 0 0 0 0 0 1 0 0 0 2		

$K_3(5, 3) = 3$ és az alábbi 3 optimális kód létezik. Az első optimális kód kiegyensúlyozott, a másik kettő kiegyensúlyozatlan.

(1)	0 0 0 0 0 1 1 1 1 1 2 2 2 2 2	(2)	0 0 0 0 0 0 1 1 1 1 1 2 2 2 2	(3)	0 0 0 0 0 0 1 1 1 1 0 2 2 2 2
-----	-------------------------------------	-----	-------------------------------------	-----	-------------------------------------

$K_3(6, 3) = 6$ és 28 optimális kód létezik. Prompt felső korlát 9. A felső korlát csökkentése 6-ra [60]. Prompt alsó korlát: 4. Az alsó korlát javítása 6-ra: Honkala (nem publikált, lásd [57]; erre az adatra [90] is hivatkozik), valamint [97] (1997), Example 6.7.5. Klasszifikáció: 4.11. tétel. Totókód 6 kódszóval: „SEPPO” (1975). Az optimális kódok között kiegyensúlyozott és kiegyensúlyozatlan, normális és abnormális kódok is találhatóak.

$11 \leq K_3(7, 3) \leq 12$. Prompt felső korlát 27. A felső korlát javítása 12-re [60]. Prompt alsó korlát: 6. Az alsó korlát javítása 7-re [55], 9-re [104], 10-re [130], 11-re [167]. Totókód 12 kódszóval: Weikel (1975). Az ismert rekord-tartó konstrukció kiegyensúlyozatlan, normális kód.

$14 \leq K_3(8, 3) \leq 27$. Prompt felső korlát 81. A felső korlát javítása 27-re [60]. Prompt alsó korlát: 12. Az alsó korlát javítása 13-ra [55, 57], 14-re [104]. Totókód 27 kódszóval: „ARIC” (1972). Az ismert rekord-tartó konstrukciók (DS vagy ADS) kiegyensúlyozott, normális kódokat eredményeznek.

$27 \leq K_3(9, 3) \leq 54$. Prompt felső korlát 243. A felső korlát javítása 54-re [60, 65]. Prompt alsó korlát: 24. Az alsó korlát javítása 25-re [57], 27-re [156]. Totókód 54 kódszóval: ismeretlen szerző [Veikkaus-lotto] (1981) és Rankinen [Stora Tipsboken] (1986). Az ismert rekord-tartó konstrukció kiegyensúlyozott, normális kódot eredményez.

$57 \leq K_3(10, 3) \leq 105$. Prompt felső korlát 729. A felső korlát javítása 108-ra [60, 65], 105-re (totókód gyanánt) Bertolo R., Di Pasquale F. és Santisi F. (2005). Prompt alsó korlát: 51. Az alsó korlát javítása 56-ra [66], 57-re [57]. Az ismert rekord-tartó konstrukció kiegyensúlyozatlan, abnormális kód.

$117 \leq K_3(11, 3) \leq 243$. Prompt felső korlát 729. A felső korlát csökkentése 243-ra [60, 65]. Prompt alsó korlát: 114. Az alsó korlát javítása 115-re [57], 117-re [156]. Kétséges alsó korlát a [69]-ban megadott 119 érték. Totókód 243 kódszóval: „ARIC” [Tipslyktan] és „SEPPO” (1974). Az ismert rekord-tartó konstrukció kiegyensúlyozott, normális kódot eredményez.

$282 \leq K_3(12, 3) \leq 657$. Prompt felső korlát 729. A felső korlát javítása 660-ra (totókód gyanánt) Bertolo R., Di Pasquale F. és Santisi F. (2005), 657-re (szintén totókód gyanánt) Rivas Soriano P. P. (2005). Prompt alsó korlát: 260. Az alsó korlát javítása 280-ra [66], 282-re [57]. Az ismert rekord-tartó konstrukció kiegyensúlyozatlan, abnormális kód.

$612 \leq K_3(13, 3) \leq 1215$. Prompt felső korlát 2187. A felső korlát csökkentése 1215-re [60, 70]. Prompt alsó korlát: 607. Az alsó korlát javítása 609-re [57], 611-re [92], 612-re [156]. Totókód 1215 kódszóval: Hämmäläinen H. (1987). Az ismert rekord-tartó konstrukció kiegyensúlyozatlan, abnormális kód.

$1553 \leq K_3(14, 3) \leq 2187$. Prompt felső korlát 6561. A felső korlát csökkentése 2187-re [65]. Prompt alsó korlát: 1448. Az alsó korlát javítása 1553-ra [57]. Totókód 2187 kódszóval: Östergård P. (1991). Az ismert rekord-tartó konstrukció kiegyensúlyozott, abnormális kód.

4.6.4. $R = 4$ elérési sugarú kódokra vonatkozó eredmények

A ternáris esetben – a bináris esettől eltérően – 3-nál nagyobb elérési sugar és $n \leq 14$ esetén sem annyira egyszerűek az optimális és rekord-tartó kód konstrukciók, ezért folytatjuk az adatközlést $R = 7$ elérési sugarig, de itt már csak a 3 szónál hosszabb optimális és rekord-tartó kódokra vonatkozóan. A prompt korlátokat az eddigiekhez hasonló elvek alapján képezzük.

$K_3(8, 4) = 9$. Prompt alsó és felső korlát: 4, ill. 9. Az alsó korlát javítása 6-ra: Honkala (nem publikált, lásd [57]); publikált bizonyítás: [46], javítás 9-re, vagyis a pontos érték igazolása [145]. Az ismert optimális kód konstrukció kiegyensúlyozott, normális kód.

$11 \leq K_3(9, 4) \leq 18$. Prompt felső korlát 27. A felső korlát csökkentése 18-ra [65]. Prompt alsó korlát: 7. Az alsó korlát javítása 8-ra [57], 10-re [129], Theorem 2, 11-re [167]. Az ismert rekord-tartó konstrukció kiegyensúlyozott, normális kód.

$17 \leq K_3(10, 4) \leq 36$. Prompt felső korlát 81. A felső korlát csökkentése 36-ra [65]. Prompt alsó korlát: 14. Az alsó korlát javítása 16-ra [57], 17-re [164]. Az ismert rekord-tartó konstrukció kiegyensúlyozott, normális kód.

$30 \leq K_3(11, 4) \leq 81$. Prompt felső korlát 243. A felső korlát csökkentése 81-re [65]. Prompt alsó korlát: 26. Az alsó korlát javítása 28-ra [57], 30-ra [164]. Az ismert rekord-tartó konstrukció kiegyensúlyozott, normális kód.

$62 \leq K_3(12, 4) \leq 175$. Prompt felső korlát 729. A felső korlát csökkentése 204-re [65], 201-re [171] (2005), 177-re [136] (2005), 175-re [168] (2006). Prompt alsó korlát: 54. Az alsó korlát javítása 62-re [57]. Az ismert rekord-tartó konstrukció kiegyensúlyozatlan, abnormális kód.

$123 \leq K_3(13, 4) \leq 340$. Prompt felső korlát 729. A felső korlát csökkentése 408-ra [65, 70], 366-ra [136] (2005), 348-ra [168] (2006), 340-re [136] (2009). Prompt alsó korlát: 114. Az alsó korlát javítása 123-ra [57]. Az ismert rekord-tartó konstrukció kiegyensúlyozatlan, abnormális kód.

$255 \leq K_3(14, 4) \leq 729$. Prompt felső korlát 2187. A felső korlát csökkentése 729-re [65, 70]. Prompt alsó korlát: 248. Az alsó korlát javítása 251-re [57], 255-re [92]. Az ismert rekord-tartó konstrukció kiegyensúlyozott, abnormális kód.

4.6.5. $R = 5$ elérési sugarú kódokra vonatkozó eredmények

$K_3(9, 5) = 6$. Prompt felső korlát 9. A felső korlát csökkentése 6-ra [65]. Prompt alsó korlát: 3. Az alsó korlát javítása 4-re [57], 6-ra [129]. Az ismert optimális kód kiegyensúlyozott, normális kód.

$9 \leq K_3(10, 5) \leq 12$. Prompt felső korlát 27. A felső korlát csökkentése 12-re [65]. Prompt alsó korlát: 5. Az alsó korlát javítása 6-ra [57], 8-ra [129], 9-re [145]. Az egyszerűen adódó rekord-tartó konstrukciók között kiegyensúlyozott és kiegyensúlyozatlan kódok is találhatók, s ezek között vannak normális kódok.

$11 \leq K_3(11, 5) \leq 27$. Prompt felső korlát 81. A felső korlát csökkentése 27-re [65]. Prompt alsó korlát: 9. Az alsó korlát javítása 10-re [129], Theorem 2, 11-re [164]. Az ismert rekord-tartó konstrukciók kiegyensúlyozott, normális kódokat eredményeznek.

$18 \leq K_3(12, 5) \leq 54$. Prompt felső korlát 243. A felső korlát csökkentése 54-re: Hämäläinen, lásd [65], ill. totókód gyanánt Lahtinen [Veikkaja] (1960), lásd [113]. Prompt alsó korlát: 16. Az alsó korlát javítása 18-ra [57]. Az ismert rekord-tartó kód kiegyensúlyozott, normális kód.

$33 \leq K_3(13, 5) \leq 108$. Prompt felső korlát 729. A felső korlát csökkentése 136-ra [65], 108-ra [113]. Prompt alsó korlát: 29. Az alsó korlát javítása 32-re [57], 33-ra [164]. Az ismert rekord-tartó kód kiegyensúlyozott, normális kód.

$59 \leq K_3(14, 5) \leq 243$. Prompt felső korlát 729. A felső korlát csökkentése 306-ra: Hämäläinen, lásd [65], 243-ra [113]. Prompt alsó korlát: 58. Az alsó korlát javítása 59-re [57]. Az ismert rekord-tartó kód kiegyensúlyozott, normális kód.

4.6.6. $R = 6$ elérési sugarú kódokra vonatkozó eredmények

$K_3(11, 6) = 9$. Prompt alsó és felső korlát: 4, ill. 9. Az alsó korlát javítása 5-re [57], 6-ra [90], 9-re [129]. Az ismert optimális kód kiegyensúlyozott, normális kód.

$10 \leq K_3(12, 6) \leq 18$. Prompt felső korlát 27. A felső korlát csökkentése 18-ra [65]. Prompt alsó korlát: 6. Az alsó korlát javítása 7-re [57], 9-re [145], 10-re [167]. Az ismert rekord-tartó kód kiegyensúlyozott, normális kód.

$13 \leq K_3(13, 6) \leq 36$. Prompt felső korlát 81. A felső korlát csökkentése 48-ra [65], 45-re [90], 36-ra [145]. Prompt alsó korlát: 10. Az alsó korlát javítása 11-re [57], 13-ra [164]. Az ismert rekord-tartó kód kiegyensúlyozott, normális kód.

$21 \leq K_3(14, 6) \leq 81$. Prompt felső korlát 243. A felső korlát csökkentése 102-re [65], 81-re [90]. Prompt alsó korlát: 18. Az alsó korlát javítása 21-re [57]. Az ismert rekord-tartó kód kiegyensúlyozott, normális kód.

4.6.7. $R = 7$ elérési sugarú kódokra vonatkozó eredmények

$K_3(12, 7) = 6$. Prompt felső korlát 9. A felső korlát csökkentése 6-ra [65]. Prompt alsó korlát: 3. Az alsó korlát javítása 4-re [57], 6-ra [90]. Az ismert optimális kód kiegyensúlyozott, normális kód.

$9 \leq K_3(13, 7) \leq 12$. Prompt felső korlát 27. A felső korlát csökkentése 12-re [65]. Prompt alsó korlát: 5. Az alsó korlát javítása 6-ra [90], 9-re [145]. Az egyszerűen adódó rekord-tartó konstrukciók között kiegyensúlyozott és kiegyensúlyozatlan kódok is találhatók, s ezek között vannak normális kódok.

$11 \leq K_3(14, 7) \leq 27$. Prompt felső korlát 81. A felső korlát csökkentése 27-re [65]. Prompt alsó korlát: 7. Az alsó korlát javítása 8-ra [57]. A 11 alsó korlát a $K_3(7, 3) \geq 11$ egyenlőtlenségből [167] következik. Az ismert rekord-tartó kód kiegyensúlyozott, normális kód.

5. fejezet

Nagyobb alapszámú térlefedő kódok

5.1. Csak az 5. fejezetben használt fogalmak

Ebben a fejezetben használjuk legintenzívebben a szűrjektív kódokat, és a tárgyalás során szükségünk lesz néhány további, ezekhez kapcsolódó fogalom értelmezésére. Ezek közül a *lefedő tömb* (angol nyelven *covering array*) lényegében egy alternatív elnevezés a szűrjektív kódra, melyre azért van szükségünk, mert a felhasznált publikációk jó része, sok számunkra érdekes és fontos eredménnyel, ezt a fogalmat és a hozzá kapcsolódó terminológiát használja. A két fogalmat az különbözteti meg egymástól, hogy egy szűrjektív kód a Z_q^n Hamming tér valamely M elemű részhalmaza, egy lefedő tömb viszont egy szűrjektív kód kódszavaiból mint $1 \times n$ méretű tömbökből alkotott $M \times n$ méretű tömb.

Lefedő tömb

Egy $CA(M; s, n, q)$ lefedő tömb az eddig szokásos értelmezés szerint olyan $M \times n$ méretű tömb, melynek minden $M \times s$ méretű résztömbjének sorai között a Z_q^s tér minden pontja legalább egyszer előfordul.

A szokásos jelölésnek megfelelően jelölje $CAN(s, n, q)$ az adott s, n, q paraméterekhez tartozó lefedő tömbök függőleges méretének (M) a minimumát. Ez nyilván minden esetben ugyanazt az értéket eredményezi, mint a szűrjektív kódokra értelmezett $\sigma_q(n, s)$ függvény, tehát fennáll

$$CAN(s, n, q) \equiv \sigma_q(n, s).$$

Kiterjeszthetjük a lefedő tömb fogalmát az alábbi általánosabb értelmezés szerint: Egy $CA_r(M; s, n, q)$ lefedő tömb olyan $M \times n$ méretű tömb, melynek tetszőleges $M \times s$ méretű résztömbje és a Z_q^s tér tetszőleges pontja esetén az előbbinek található olyan sora, amely az utóbbtól legfeljebb r koordináta helyen különbözik. Az így értelmezett lefedő tömbök és az általánosított szűrjektív kódok között ugyanolyan kapcsolat van, mint a hagyományos értelemben vett lefedő tömbök és szűrjektív kódok között, tehát fennáll

$$CAN_r(s, n, q) \equiv \sigma_q(n, s; r),$$

ahol $CAN_r(s, n, q)$ jelöli azt a legkisebb M értéket, melyre létezik $CA_r(M; s, n, q)$ lefedő tömb.

A 2-szűrjektív kódokhoz és így $s = 2$ esetén a lefedő tömbökhöz kapcsolódó fogalom a már Euler által is tanulmányozott latin négyzet fogalma.

Latin négyzet

Latin négyzet alatt olyan $q \times q$ méretű táblázatot értünk, melynek minden cellájában adott q szimbólum valamelyike áll úgy, hogy minden sorban és minden oszlopban a q szimbólum mindegyike pontosan egyszer fordul elő.

Ortogonalis latin négyzetek

Két $q \times q$ méretű $A = (a_{ij})$ és $B = (b_{ij})$ latin négyzet ortogonalis, ha az (a_{ij}, b_{ij}) rendezett párok között nincs két azonos.

Könnyen látható, hogy két ortogonalis latin négyzet $A = (a_{ij})$ és $B = (b_{ij})$ esetén az (i, j, a_{ij}, b_{ij}) négyesekből mint kódszavakból álló kód 2-szűrjektív, az ezekből mint sorokból alkotott tömb tehát $CA(q^2, 2, 4, q)$ lefedő tömb. Ebből viszont következik, hogy $n - 2$ páronként ortogonalis latin négyzet $A = (a_{ij}), B = (b_{ij}), \dots, Z = (z_{ij})$ esetén az $(i, j, a_{ij}, b_{ij}, \dots, z_{ij})$ n -esekből mint kódszavakból álló kód hasonlóan 2-szűrjektív, az ezekből mint sorokból alkotott tömb pedig $CA(q^2, 2, n, q)$ lefedő tömb.

Jelölje $N(q)$ a páronként ortogonalis q -adrendű latin négyzetek maximális számát. Ekkor az előbbiekből az is következik, hogy

$$N(q) = \max\{n : \sigma_q(n, 2) = q^2\} - 2 = \max\{n : \text{CAN}(2, n, q) = q^2\} - 2.$$

Maximális távolságú kód (MDS kód)

A Z_q^n térben értelmezett, k kódszóval generált lineáris kód maximális távolságú kód (a továbbiakban MDS kód, az angol „maximum distance separable” kifejezés kezdőbetűi alapján), ha legkisebb távolságára fennáll, hogy

$$d_{\min} = n - k + 1.$$

Ismeretes, hogy tetszőleges prím vagy prímhatvány q esetén bármely $n \leq q + 1$ -re és $2 \leq k \leq n$ -re létezik az n, k paraméterekhez tartozó MDS kód, és minden ilyen kód k -szűrjektív.

Adjungált kód

Az $R = 1$ elérési sugár esetére Stanton, Horton és Kalbfleisch [21] által bevezetett és alkalmazott *adjungált kód* definíciójához tekintsük a Z_p^n Hamming teret. Most legyenek q_j ($0 \leq j \leq p - 1$) pozitív egészek, és képezzük a

$$T_0 = \{0, 1, \dots, -1 + q_0\}$$

$$T_1 = \{q_0, 1 + q_0, \dots, -1 + q_0 + q_1\}$$

.....

$$T_j = \{\sum_{i=0}^{j-1} q_i, 1 + \sum_{i=0}^{j-1} q_i, \dots, -1 + \sum_{i=0}^j q_i\}$$

.....

$$T_{p-1} = \{\sum_{i=0}^{p-2} q_i, 1 + \sum_{i=0}^{p-2} q_i, \dots, -1 + \sum_{i=0}^{p-1} q_i\}$$

halmazokat. Legyen $C \subseteq Z_p^n$, és a C kód tetszőleges c szava esetén legyen

$$s(c) = \min \{q_{c_i} : 1 \leq i \leq n\}.$$

A fenti jelölésekkel az adjungált kód fogalmát a következőképpen értelmezzük: Egy $C \subseteq Z_p^n$ kódnak a $q_0, q_1, \dots, q_{p-1}$ ($q_i \geq 1$) súlyokhoz tartozó adjungáltja az a $D = \bigcup_{c \in C} D_c \subseteq Z_q^n$ ($q = \sum_{i=0}^{p-1} q_i$) kód, melyre

$$D_c = \left\{ d = (d_1, d_2, \dots, d_n) : d_i \in T_{c_i} (i = 1, 2, \dots, n), \sum_{i=1}^n d_i \equiv 0 \pmod{s(c)} \right\}. \quad (5.1)$$

5.2. Egyszerű konstrukciók

5.2.1. Magasabb rendű ismétléses kódok

Bármely q és n esetén a Z_q^n térben értelmezett

$$\{ (0, 0, \dots, 0), \\ (1, 1, \dots, 1), \\ \dots \\ (q-1, q-1, \dots, q-1) \}$$

ismétléses kód az (1.4)-ben megadott elérési sugárral optimális kód. Következésképpen $K_q(n, \lfloor n(q-1)/q \rfloor = q)$, így pl.

$$K_q(qR + 1, (q - 1)R) = q.$$

5.2.2. Magasabb rendű Hamming kódok

A bináris és ternáris Hamming kódokhoz hasonlóan tetszőleges prím vagy prímhatvány q , bármely $h \geq 2$ egész és $n = \frac{q^h - 1}{q - 1}$ esetére található q alapszámú perfekt kód. A legkisebb ilyen kód ($h = 2$ eset) a ternáris speciális esetre az előző fejezetben felírthoz hasonló egyszerű konstrukcióval adódik, melynek során generáló kódszavaknak a

$$\begin{aligned} h_1 &= (0, 0, \dots 0, 1, 1, 1), \\ h_2 &= (0, 0, \dots 1, 0, 1, 2), \\ &\vdots \\ h_{q-2} &= (0, 1, \dots 0, 0, 1, q-2), \\ h_{q-1} &= (1, 0, \dots 0, 0, 1, q-1) \end{aligned} \tag{5.2}$$

vektorokat választjuk. A Hamming kódok mind a bináris, mind a ternáris, mind a magasabb rendű esetben sok más térlefedő kód-konstrukció alkotó elemét vagy kiindulási alapját képezik.

5.2.3. Egyéb konstrukciók lineáris kóddal

Néhány esetben lineáris kód adja a jelenlegi rekord-tartó kódot. Ilyen lineáris kóddal megadott rekord-tartó kódok a $K_5(6, 2)$, $K_5(6, 3)$, $K_7(6, 2)$, $K_7(7, 4)$, $K_8(6, 2)$ és $K_9(6, 2)$ kifejezések legjobb ismert felső korlátjának a bizonyítására szolgáló kódok. A mellékelt lemezen ezek mindegyikét megadtuk.

5.2.4. Mellékosztályok módszere (mátrix módszer)

A 4.1.4 szakaszban ismertetett módszer tetszőleges prím vagy prímhatvány q -ra alkalmazható, és így újabb magyarázatot már nem igényel.

5.3. Folytatólagos konstrukciók és kapcsolatos egyenlőtlenségek

Az ide tartozó módszerek ismertetése során is szinte szóról szóra ismétellhetjük a ternáris eset megfelelő konstrukciójánál mondottakat.

5.3.1. 1-gyel növelt dimenzió és elérési sugár, változatlan méret

Legyen $C \subset Z_q^n$ egy M kódszóból álló, R elérési sugarú kód. Egészítsük ki C kódszavait egy-egy tetszőleges értékű $(n + 1)$ -edik koordinátával. Az eredményül kapott C' kód R' elérési sugarára fennáll $R \leq R' \leq R + 1$, és következésképpen

$$K_q(n + 1, R + 1) \leq K_q(n, R) \leq K_q(n + 1, R). \quad (5.3)$$

5.3.2. 1-gyel növelt dimenzió, változatlan elérési sugár, q -szoros méret

Legyen $C \subset Z_q^n$ egy M kódszóból álló, R elérési sugarú kód. Egészítsük ki C kódszavait 0 értékű, 1 értékű, $\dots$, $q - 1$ értékű $(n + 1)$ -edik koordinátával. Az eredményül kapott

$$C'' = \bigcup_{i=0}^{q-1} \{|c|i| : c \in C\}$$

kód elérési sugara megegyezik C elérési sugarával, és következésképpen

$$K_q(n + 1, R) \leq qK_q(n, R). \quad (5.4)$$

5.3.3. q -val növelt dimenzió, $(q-1)$ -gyel növelt elérési sugár, változatlan méret

Legyen $C \subset Z_q^n$ egy M kódszóból álló, R elérési sugarú, az utolsó koordinátában normális kód. Bontsuk fel C -t a C_i ($i = 0, 1, \dots, q-1$) kódok egyesítésére úgy, hogy C_i tartalmazza C -nek azokat a kódszavait, melyeknek az utolsó koordinátája i . Egészítsük ki mindegyik C_i minden kódszavát q számú további i értékű koordinátával. A kapott

$$\overline{C} = \bigcup_{i=0}^{q-1} \{|c|ii \dots i| : c \in C_i\}$$

kód elérési sugara legfeljebb $R + q - 1$.

5.3.4. Adjungált kódok módszere

A [21] cikk „Theorem 2” tételében a szerzők – más megfogalmazásban, és $R = 1$ elérési sugárra korlátozódva – lényegében bebizonyították a következő lemma állítását. Az ott közölt bizonyítás lényeges módosítás nélkül átvihető nagyobb elérési sugár esetére is.

5.1. Lemma.

Ha a $C \subseteq Z_p^n$ kód elérési sugara R , akkor az adjungált $D \subseteq Z_q^n$ kód elérési sugara szintén R .

Különösen hasznosnak bizonyult az adjungált kód konstrukciója abban az esetben, amikor C perfekt kód. A q^{q-1} kódszóból álló $q+1$ dimenziós perfekt kódokra a [21] cikk (más megfogalmazásban) az alábbi következményt mondja ki:

5.2. Következmény. (Kalbfleisch és szerzőtársai [25] Theorem 3 következményeként K . és Östergård [135] Corollary 1)

Tetszőleges q prímszám, $r \geq 1$ és $0 < t < q$ esetén

$$K_{qr+t}(q+1, 1) \leq t^q + \sum_{j=1}^q \binom{q+1}{j+1} q^{j-1} t^{q-j} r^j - \sum_{j=1}^{q-1} \binom{q}{j+1} t^{q-j} r^j,$$

$$K_{qr+t}(q+1, 1) \leq t^q + \sum_{j=1}^q \binom{q+1}{j+1} q^{j-1} t^{q-j} r^j - \frac{y_{q,t}}{t} \cdot \left[q(t-1) + t \cdot \sum_{j=1}^{q-1} \binom{q}{j+1} r^j \right],$$

ahol $y_{q,t}$ valamely $(q+1, q^{q-1})_q$ 1 perfekt kód azon $c = (c_1, c_2, \dots, c_{q+1})$ kódszavainak a száma, melyekre teljesül $0 \leq c_i < t$ minden $i = 1, 2, \dots, q+1$ esetén.

Az $y_{q,t}$ mennyiségekre kapható – lehetőleg minél nagyobb – értékek egy részét a [21, 25] publikációk már megadták. További ilyen értékeket számítógépes kereséssel kaptunk. A [135] cikkből átvett 5.1. táblázatban a korábban nem ismert új értékeket *-gal jelöltük. A

t	$q = 3$	$q = 4$	$q = 5$	$q = 7$	$q = 8$	$q = 9$	$q = 11$
2	2	4	4	10*	32*	44*	84*
3	-	18	33	171*	621*	2187*	6999*
4	-	-	164	1380*	8192*	13564*	163872*
5	-	-	-	7985	31040*	121355*	2052255*
6	-	-	-	34278	157536*	747954	18085734*
7	-	-	-	-	630532	3487393	114352742*
8	-	-	-	-	-	13256072	567934056*

5.1. táblázat. $y_{q,t}$ legjobb ismert értékei

továbbiakban az 5.2. következményt a $q = 3, 4, 5$ és 7 esetekre konkrétizáljuk a $K_p(n, 1)$ értékekre megadott egyenlőtlenségek formájában.

A $q = 3$ és $q = 4$ esetekre már a [21] cikk megadta az alábbi egyenlőtlenségeket:

$$\begin{aligned} K_{3r+1}(4, 1) &\leq 9r^3 + 11r^2 + 3r + 1, \\ K_{3r+2}(4, 1) &\leq 9r^3 + 22r^2 + 12r + 8; \end{aligned} \tag{5.5}$$

$$\begin{aligned} K_{4r+1}(5, 1) &\leq 64r^4 + 79r^3 + 36r^2 + 4r + 1, \\ K_{4r+2}(5, 1) &\leq \begin{cases} 64r^4 + 158r^3 + 144r^2 + 32r + 16, \\ 64r^4 + 156r^3 + 144r^2 + 56r + 8, \end{cases} \\ K_{4r+3}(5, 1) &\leq 64r^4 + 222r^3 + 288r^2 + 162r + 33. \end{aligned} \tag{5.6}$$

A [25] cikk tovább lépett a $q = 5$ esetre, és (2 együttható téves értékétől eltekintve) megadta az alábbi egyenlőtlenségeket.

$$\begin{aligned} K_{5r+1}(6, 1) &\leq 625r^5 + 749r^4 + 370r^3 + 90r^2 + 5r + 1, \\ K_{5r+2}(6, 1) &\leq \begin{cases} 625r^5 + 1498r^4 + 1480r^3 + 720r^2 + 80r + 32, \\ 625r^5 + 1496r^4 + 1480r^3 + 760r^2 + 200r + 22, \end{cases} \\ K_{5r+3}(6, 1) &\leq \begin{cases} 625r^5 + 2247r^4 + 3330r^3 + 2430r^2 + 405r + 243, \\ 625r^5 + 2217r^4 + 3210r^3 + 2370r^2 + 885r + 133, \end{cases} \\ K_{5r+4}(6, 1) &\leq 625r^5 + 2836r^4 + 5180r^3 + 4760r^2 + 2200r + 409. \end{aligned} \tag{5.7}$$

Az 5.2. következmény és az $y_{q,t}$ értékekre megadott táblázat együttes használatával kapjuk az alábbi, eddig még nem publikált (de részben a [135] cikkben már bemutatott)

általános egyenlőtlenségeket a $q = 7, 8$ és 9 esetekre:

$$\begin{aligned}
K_{7r+1}(8, 1) &\leq 117649r^7 + 134455r^6 + 67221r^5 + 19187r^4 + 3395r^3 + \\
&\quad + 357r^2 + 7r + 1, \\
K_{7r+2}(8, 1) &\leq \begin{cases} 117649r^7 + 268910r^6 + 268884r^5 + 153496r^4 + 54320r^3 + \\ \quad + 11424r^2 + 448r + 128, \\ 117649r^7 + 268902r^6 + 268842r^5 + 153454r^4 + 54530r^3 + \\ \quad + 12194r^2 + 1582r + 93, \end{cases} \\
K_{7r+3}(8, 1) &\leq \begin{cases} 117649r^7 + 403365r^6 + 604989r^5 + 518049r^4 + 274995r^3 + \\ \quad + 86751r^2 + 5103r + 2187, \\ 117649r^7 + 403197r^6 + 603855r^5 + 515025r^4 + 271845r^3 + \\ \quad + 89271r^2 + 16821r + 1389, \end{cases} \quad (5.8) \\
K_{7r+4}(8, 1) &\leq 117649r^7 + 536444r^6 + 1065988r^5 + 1200332r^4 + 829780r^3 + \\
&\quad + 353108r^2 + 85708r + 9139, \\
K_{7r+5}(8, 1) &\leq 117649r^7 + 664295r^6 + 1624805r^5 + 2233315r^4 + 1864275r^3 + \\
&\quad + 945525r^2 + 269815r + 33409, \\
K_{7r+6}(8, 1) &\leq 117649r^7 + 772458r^6 + 2180262r^5 + 3429090r^4 + 3245550r^3 + \\
&\quad + 1848462r^2 + 586530r + 79981;
\end{aligned}$$

$$\begin{aligned}
K_{8r+1}(9, 1) &\leq 2097152r^8 + 2359295r^7 + 1179640r^6 + 344036r^5 + \\
&\quad + 64456r^4 + 7994r^3 + 616r^2 + 8r + 1, \\
K_{8r+2}(9, 1) &\leq \begin{cases} 2097152r^8 + 4718590r^7 + 4718560r^6 + 2752288r^5 + \\ \quad + 1031296r^4 + 255808r^3 + 39424r^2 + 1024r + 256, \\ 2097152r^8 + 4718560r^7 + 4718336r^6 + 2751616r^5 + \\ \quad + 1030400r^4 + 255808r^3 + 41216r^2 + 3712r + 128; \end{cases} \quad (5.9)
\end{aligned}$$

$$\begin{aligned}
K_{9r+1}(10, 1) &\leq 43046721r^9 + 47829689r^8 + 23914836r^7 + 7085844r^6 + \\
&\quad + 1377726r^5 + 183582r^4 + 16884r^3 + 996r^2 + 9r + 1. \quad (5.10)
\end{aligned}$$

Azokban az esetekben, amelyekre két egyenlőtlenséget adtunk meg, mindig az első ad jobb felső korlátot, ha $r = 1$, más r esetén viszont egyéb körülményektől is függ, hogy melyik egyenlőtlenség jobb a kettő közül. Nagy vonalakban annyit el lehet mondani, hogy általában jobb az első egyenlőtlenség kisebb r -ek esetén, a második egyenlőtlenség pedig nagyobb r -ek esetén, de vannak ez alól kivételek.

5.4. Összetételes konstrukciók és kapcsolatos egyenlőtlenségek

Könnyen verifikálható, hogy 3-nál nagyobb alapszám esetére is átvihetők a DS, ADS és BDS konstrukciókra a bináris esetben mondottakkal analóg állítások, tulajdonságok és bizonyítások.

5.4.1. Szürjektív kódok egyesítése

Kalbfleisch és Stanton [17] észrevették, hogy ha $C_1 \subset Z_{q_1}^3$ és $C_2 \subset Z_{q_2}^3$ 2-szürjektív kódok, ahol $Z_{q_1} = \{0, 1, \dots, q_1 - 1\}$ és $Z_{q_2} = \{q_1, q_1 + 1, \dots, q_1 + q_2 - 1\}$, akkor a $C_1 \cup C_2$ kód elérési sugara 1, és következésképpen

$$K_{q_1+q_2}(3, 1) \leq \sigma_{q_1}(3, 2) + \sigma_{q_2}(3, 2) = q_1^2 + q_2^2. \quad (5.11)$$

Hasonlóan mutatható meg három 2-szürjektív kód egyesítésével, hogy

$$K_{q_1+q_2+q_3}(4, 2) \leq \sigma_{q_1}(4, 2) + \sigma_{q_2}(4, 2) + \sigma_{q_3}(4, 2). \quad (5.12)$$

Az (5.11) és (5.12) egyenlőtlenség bizonyítása helyett az ezeknél sokkal általánosabban, az általánosított szürjektív kódok méretével kapcsolatos $\sigma_q(n, s; r)$ függvényre megfogalmazott alábbi egyenlőtlenséget bizonyítottuk a [135] cikkben.

5.3. Tétel. (*K. és Östergård [135], Theorem 2*)

$$\sigma_{q_1+\dots+q_k}(n, 1-k + \sum_{i=1}^k s_i; 1-k-r + \sum_{i=1}^k s_i) \leq \sum_{i=1}^k \sigma_{q_i}(n, s_i; s_i-r). \quad (5.13)$$

Bizonyítás. Legyen $C = \bigcup_{i=1}^k C_i$, ahol a C_i kód s_i -szürjektív s_i-r sugárral a szimbólumok

$$Z(i) = \left\{ \sum_{j=1}^{i-1} q_j, 1 + \sum_{j=1}^{i-1} q_j, \dots, (q_i - 1) + \sum_{j=1}^{i-1} q_j \right\}$$

halmazán. Ekkor a $Z_{q_1+\dots+q_k}^n$ tér tetszőleges pontjának bármely $1-k + \sum_{i=1}^k s_i = 1 + \sum_{i=1}^k (s_i - 1)$ koordinátájára legalább egy i index esetén teljesül, hogy legalább s_i koordináta értéke $Z(i)$ -ből van (skatulya elv). Következésképpen az ezen i indexhez tartozó C_i -ben van olyan kódszó, amely $(1-k + \sum_{i=1}^k s_i)$ -szürjektív $1-k-r + \sum_{i=1}^k s_i$ sugárral. $\square$

Mivel az eddigi tapasztalatok azt mutatják, hogy gyakorlati szempontból hasznosabb az általános megfogalmazású 5.3. tétel helyett ismételten, $k-1$ lépésben alkalmazni az (5.13) formula két tagra vonatkozó alakját, ezért az utóbbit külön is megadjuk:

$$\sigma_{q_1+q_2}(n, s_1 + s_2 - 1; s_1 + s_2 - 1 - r) \leq \sigma_{q_1}(n, s_1; s_1 - r) + \sigma_{q_2}(n, s_2; s_2 - r). \quad (5.14)$$

Abban a speciális esetben, amikor az (5.13) képlet esetén $n = 1 - k + \sum_{i=1}^k s_i$, ill. az (5.14) képlet esetén $n = s_1 + s_2 - 1$, a szóban forgó mindkét képlet $K(n, n-R)$ értékére fejez ki felső korlátot. Az általánosabb esetre ily módon a következő formulát kapjuk:

5.4. Következmény. (*K. és Östergård [135], Corollary 3*)

$$K_{q_1+\dots+q_k}(kr - k + 1, kr - k + 1 - r) \leq \sum_{i=1}^k \sigma_{q_i}(kr - k + 1, r). \quad (5.15)$$

Ezzel a képlettel a már korábban ismert és alkalmazott (5.11) és (5.12) egyenlőtlenségek általánosítását fogalmaztuk meg.

Végül fontosnak tartom megjegyezni, hogy az e szakaszban tárgyalt összefüggések akkor is érvényesek, ha megengedjük az 1 érték előfordulását a q_i értékek között. Ilyenkor $\sigma_1(n, s) = 1$ és $\sigma_1(n, s; r) = 1$ a paraméterek értékétől függetlenül.

5.5. Nagyobb alapszámhoz tartozó térlefedő kódok mérete

A bináris és ternáris kódok tárgyalásához hasonlóan először felsoroljuk, hogy általános q alapszám esetén az n dimenziós, R elérési sugarú optimális térlefedő kódok méretét kifejező $K_q(n, R)$ mennyiségek pontos értékét milyen esetekben ismerjük. Általános q alapszám esetén is nyilvánvalóan fennáll $K_q(n, 0) = q^n$ és $K_q(n, n) = 1$. E két triviális eseten kívül $K_q(n, R)$ pontos értékét még az alábbi esetekben ismerjük:

- (a) $K_q(n, R) = q$ akkor és csak akkor, ha $R < n < \frac{qR+q}{q-1}$ (azaz $\frac{(q-1)(n-1)}{q} \leq R < n$);
- (b) $K_q(\frac{q^h-1}{q-1}, 1) = q^{\frac{q^h-1}{q-1}-h}$, ahol $h \geq 2$, egész, q pedig prím vagy prímhatvány;
- (c) $K_{tq}(q+1, 1) = t^q q^{q-1}$, ahol $t \geq 2$, egész, q pedig prím vagy prímhatvány;
- (d) $K_q(q, q-2) = q-2 + \sigma_2(q, 2)$, ha $4 \leq q \leq 10$.
- (e) $K_q(3, 1) = \left\lceil \frac{q^2}{2} \right\rceil$;
- (f) $K_q(4, 2) = \left\lceil \frac{q^2}{3} \right\rceil$, ha $9 \leq q \leq 15$ vagy $q \geq 21$;
- (g) $K_q(n, n-2) = \frac{q^2}{n-1}$, ha q osztható $n-1$ -gyel, és a $q/(n-1)$ rendű latin négyzetek között található legalább $n-2$ páronként ortogonális latin négyzet;
- (h) $K_4(4, 1) = 24$, $K_4(4, 2) = 7$, $K_4(8, 5) = 8$, $K_5(4, 2) = 11$, $K_5(10, 7) = 9$, $K_6(5, 3) = 12$, $K_{17}(5, 3) = 73$, $K_{18}(5, 3) = 82$ és $K_{19}(5, 3) = 91$.

Az előző két fejezethez hasonlóan ismét sematikus táblákkal (5.2-5.5. táblázatok) szemléltetjük a megoldott (● jellel jelölt), értelmezhetetlen (○ jellel jelölt), ill. megoldatlan (üresen hagyott mezők) esetek tartományát. Mivel q értékének növelésével $K_q(n, R)$ pontos értékének a meghatározása egyre nehezebbé válik, a táblázatokban a ● jellel ki-fejezett megoldott esetek tartománya láthatóan egyre szűkebb. Az 5.2-5.5. táblázatok teljes jelmagyarázatát lásd a 3.1. táblázatnál.

Az (a) állítást a 4.9. állításban bizonyítottuk. A q alapszámú Hamming kódok segítségével bizonyítható (b) egyenlőséget általánosan Zaremba [9] bizonyította, a (b) alapján levezethető (c) egyenlőséget pedig Blokhuis és Lam [42] bizonyították. A (d) állítást Haas és szerzőtársai [158] bizonyították. Az (e) pont alatt megadott egyenlőséget Kalbfleisch és Stanton [17] fedezték fel és bizonyították.

$q = 4$									
$n \setminus R$	1	2	3	4	5	6	7	8	9
2	•	•	○	○	○	○	○	○	○
3	•	•	•	○	○	○	○	○	○
4	•	•	•	•	○	○	○	○	○
5	•		•	•	•	○	○	○	○
6				•	•	•	○	○	○
7					•	•	•	○	○
8					•	•	•	•	○
9						•	•	•	•
10							•	•	•
11								•	•

$q = 5$									
$n \setminus R$	1	2	3	4	5	6	7	8	9
2	•	•	○	○	○	○	○	○	○
3	•	•	•	○	○	○	○	○	○
4		•	•	•	○	○	○	○	○
5			•	•	•	○	○	○	○
6	•			•	•	•	○	○	○
7					•	•	•	○	○
8						•	•	•	○
9							•	•	•
10								•	•
11									•

5.2. táblázat. Optimális térlefedő kódok megoldott esetei $q = 4$ -re és $q = 5$ -re

$q = 6$									
$n \setminus R$	1	2	3	4	5	6	7	8	9
2	•	•	○	○	○	○	○	○	○
3	•	•	•	○	○	○	○	○	○
4	•		•	•	○	○	○	○	○
5			•	•	•	○	○	○	○
6				•	•	•	○	○	○
7					•	•	•	○	○
8						•	•	•	○
9							•	•	•
10								•	•

$q = 7$									
$n \setminus R$	1	2	3	4	5	6	7	8	9
2	•	•	○	○	○	○	○	○	○
3	•	•	•	○	○	○	○	○	○
4			•	•	○	○	○	○	○
5				•	•	○	○	○	○
6					•	•	○	○	○
7					•	•	•	○	○
8	•					•	•	•	○
9							•	•	•
10								•	•

5.3. táblázat. Optimális térlefedő kódok megoldott esetei $q = 6$ -ra és $q = 7$ -re

$q = 8$									
$n \setminus R$	1	2	3	4	5	6	7	8	9
2	•	•	○	○	○	○	○	○	○
3	•	•	•	○	○	○	○	○	○
4			•	•	○	○	○	○	○
5	•			•	•	○	○	○	○
6					•	•	○	○	○
7						•	•	○	○
8						•	•	•	○
9	•						•	•	•
10								•	•

$q = 9$									
$n \setminus R$	1	2	3	4	5	6	7	8	9
2	•	•	○	○	○	○	○	○	○
3	•	•	•	○	○	○	○	○	○
4	•	•	•	•	○	○	○	○	○
5				•	•	○	○	○	○
6					•	•	○	○	○
7						•	•	○	○
8							•	•	○
9							•	•	•
10	•							•	•

5.4. táblázat. Optimális térlefedő kódok megoldott esetei $q = 8$ -ra és $q = 9$ -re

$q = 10$									
$n \setminus R$	1	2	3	4	5	6	7	8	9
2	•	•	○	○	○	○	○	○	○
3	•	•	•	○	○	○	○	○	○
4		•	•	•	○	○	○	○	○
5				•	•	○	○	○	○
6	•				•	•	○	○	○
7						•	•	○	○
8							•	•	○
9								•	•
10								•	•

5.5. táblázat. Optimális térlefedő kódok megoldott esetei $q = 10$ -re

Az (f) és (g) állítások közül az utóbbit vesszük most előre, mivel az jóval korábban ismert volt. A Rodemichtől [24] származó (g) állítást a páronként ortogonális latin négyzetek maximális számára bevezetett $N(q)$ függvény, a szűrjektív kódok méretére vonatkozó $\sigma_q(n, s)$ függvény, ill. a lefedő tömbök méretére vonatkozó $\text{CAN}(s, n, q)$ függvény használatával a következő (i), (ii), ill. (iii) változatban is kimondhatjuk:

$$K_q(n, n-2) = \frac{q^2}{n-1}, \text{ ha } q \text{ osztható } n-1\text{-gyel, és } \begin{cases} \text{(i)} & N(q/(n-1)) \geq n-2, \\ \text{(ii)} & \sigma_{q/(n-1)}(n, 2) = \frac{q^2}{(n-1)^2}, \\ \text{(iii)} & \text{CAN}(2, n, \frac{q}{n-1}) = \frac{q^2}{(n-1)^2}. \end{cases}$$

Az (f) állítás új eredményt fejez ki, ezért külön tételben is megfogalmazzuk.

5.5. Tétel.

$$K_q(4, 2) = \left\lceil \frac{q^2}{3} \right\rceil, \text{ ha } 9 \leq q \leq 15 \text{ vagy } q \geq 21.$$

Bizonyítás. Rodemich [24] bebizonyította, hogy a $K_q(n, n-2) \geq \frac{q^2}{n-1}$ egyenlőtlenség általánosan, minden további kikötés nélkül is érvényes. Ebből nyilvánvalóan következik, hogy

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

A fordított irányú egyenlőtlenség bizonyításához tekintsük az (5.12) egyenlőtlenséget, minden egyes q esetén annak olyan partícióját választva, ahol q_1, q_2, q_3 közül bármelyik kettő azonos vagy szomszédos, vagyis $q \equiv 0 \pmod{3}$ esetén legyen $q_1 = q_2 = q_3 = q/3$, $q \equiv 1 \pmod{3}$ esetén legyen $q_1 = q_2 = (q-1)/3$ és $q_3 = (q+2)/3$, $q \equiv 2 \pmod{3}$ esetén pedig legyen $q_1 = q_2 = (q+1)/3$ és $q_3 = (q-2)/3$. Ekkor az (f) esetre megadott tartományban mindhárom q_i lehetséges értékeire teljesül $3 \leq q_i \leq 5$ vagy $q_i \geq 7$. Bose és szerzőtársai [13]-ben bizonyították, hogy $N(q) \geq 2$, ha $q \geq 3$ és $q \neq 6$, ennél fogva $\sigma_{q_i}(4, 2) = q_i^2$ fennáll az előbb megadott q_i értékekre. Ebből a $\sigma_{q_1}(4, 2) + \sigma_{q_2}(4, 2) +$

$\sigma_{q_3}(4, 2)$ összegre egyszerű számolással kapjuk a $q^2/3$ kifejezést az első esetben, ill. a $(q^2 + 2)/3$ kifejezést a másik két esetben. Így mindhárom esetben

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

□

A (h) alatt felsorolt szórványos esetekre a pontos érték elérésének folyamatát (az utolsó három eset kivételével) az 5.7-5.9. szakaszokban adjuk meg. Az utolsó három esetre az egyenlőség igazolása a [135] cikkben található.

5.6. Klasszifikációs eredmények nagyobb alapszám eseteire

A térlefedő kódok ezen kategóriájára az alábbi esetekben ismerünk klasszifikációs eredményeket:

(a) Tetszőleges q -ra $n = 2$ és $R = 1$ esetén az inekvivalens optimális térlefedő kódok száma megegyezik q pozitív egész tagokból álló partícióinak a számával.

(b) $q = 4$ vagy 5 , $n = 3$, $R = 1$ esetén az inekvivalens optimális térlefedő kódok száma 1.

(c) $q = 4$, $n = 4$, $R = 2$ esetén az inekvivalens optimális térlefedő kódok száma 8.

A fenti klasszifikációs eredmények részletesebb kifejtésével folytatjuk.

(a) A $K_q(2, 1) = q$ egyenlőséget teljesítő inekvivalens kódok száma Kaski és Östergård [138] munkájában található (Theorem 7.32).

A (b) $K_4(3, 1) = 8$ és $K_5(3, 1) = 13$, ill. (c) $K_4(4, 2) = 7$ esetekre az optimális kódok számát számítógép segítségével határoztuk meg [167]-ban, ill. [129]-ben. Az első két esetre az derült ki, hogy az optimális kód ekvivalenciától eltekintve egyértelmű. A ternáris esethez tartozó megfelelő kód unicitását Östergård [94] bizonyította, a bináris esetre vonatkozó hasonló állítás pedig triviális. Ennélfogva kimondhatjuk a következő tételt.

5.6. Tétel.

A $K_q(3, 1) = \left\lceil \frac{q^2}{2} \right\rceil$ egyenlőséghez tartozó optimális kód $2 \leq q \leq 5$ esetén egyértelmű.

Az egyetlen optimális kód tehát az a kód, amelyet az 5.4.1 szakaszban ismertetett konstrukció eredményez $q_1 = \lfloor \frac{q}{2} \rfloor$ és $q_2 = \lceil \frac{q}{2} \rceil$ választással. Jelenleg nyitott probléma, hogy a tétel állítása kiterjeszthető-e az 5-nél nagyobb q értékekre.

5.7. Az optimális és rekord-tartó térlefedő kódok áttekintése $q = 4$ esetén

Csak az $n \leq 11$ esetekkel foglalkozunk, a mellékelt lemezen is nagyjából ugyanezeket listázzuk. $R = 1$ elérési sugár esetén azonban 9 dimenziónál, $R = 2$ esetén 10 dimenziónál megállunk a kódok listázásával ezek növekvő mérete miatt. A prompt korlátokat itt már nem tüntetjük fel, viszont bizonyos mértékig itt is nyomon követjük a korlátok fokozatos javításának a menetét és megadjuk az ismert optimális, ill. rekord-tartó kódok kiegyensúlyozottságára és normalitására vonatkozó adatokat.

5.7.1. $R = 1$ elérési sugarú kódokra vonatkozó eredmények

$K_4(2, 1) = 4$ és 5 optimális kód létezik. Az optimális kódok alakja

$$\begin{array}{l} * \ 0 \\ * \ 1 \\ * \ 2 \text{ ' } \\ * \ 3 \end{array}$$

ahol a *-gal jelölt helyeken tetszőleges szimbólum állhat.

$K_4(3, 1) = 8$ és egyetlen optimális kód létezik. Konstrukció és egyenlőség bizonyítása: [17, 19]. Klasszifikáció (ami itt az unicitás bizonyítását jelenti): 5.6. tétel. Az egyetlen optimális kód kiegyensúlyozott, abnormális kód.

$K_4(4, 1) = 24$. A 24 alsó korlát és a 32 felső korlát bizonyítása: [17] (1969). (Az alsó korlát bizonyítása az első közleményben kis hibát tartalmazott, ezt a szerzők a folyóirat következő számában korrigálták.) A 24 felső korlát bizonyítása: [21]. Az ismert optimális kód kiegyensúlyozott, abnormális kód.

$K_4(5, 1) = 64$. Pontos érték igazolása: [9]. Az ismert optimális kód perfekt, kiegyensúlyozott, abnormális kód.

$228 \leq K_4(6, 1) \leq 256$. A felső korlát $K_4(5, 1) = 64$ ismeretében az (5.4) egyenlőtlenségből következik. Az alsó korlát bizonyítása: [57]. Az ismert rekord-tartó konstrukció kiegyensúlyozott, normális kód.

$762 \leq K_4(7, 1) \leq 992$. Konstrukció 1008, majd 992 kódszóval: [168] (2005, 2006). A 748 alsó korlát bizonyítása: [57]. Az alsó korlát javítása 752-re [117], 762-re [134]. Az ismert rekord-tartó konstrukció kiegyensúlyozatlan, abnormális kód.

$2731 \leq K_4(8, 1) \leq 3456$. Konstrukció 3456 kódszóval: [113]. A 2731 alsó korlát bizonyítása: [57]. Az ismert rekord-tartó konstrukció kiegyensúlyozatlan, abnormális kód.

$9368 \leq K_4(9, 1) \leq 12288$. Konstrukció 15360 kódszóval: [65], 12288 kódszóval: [113]. A 9364 alsó korlát bizonyítása: [57]. Az alsó korlát javítása 9365-re [82], 9368-ra [156]. Az ismert rekord-tartó konstrukció kiegyensúlyozott, abnormális kód.

$34953 \leq K_4(10, 1) \leq 49152$. A felső korlát $K_4(9, 1) \leq 12288$ ismeretében az (5.4) egyenlőtlenségből következik. A megadott alsó korlát bizonyítása: [57].

$123846 \leq K_4(11, 1) \leq 131072$. Konstrukció 131072 kódszóval: Välinen (2002), és tőle függetlenül [168]. A megadott alsó korlát bizonyítása: [134].

5.7.2. $R = 2$ elérési sugarú kódokra vonatkozó eredmények

$K_4(3, 2) = 4$ és 21 optimális kód létezik. Az optimális kódok alakja

$$\begin{array}{ccc} * & * & 0 \\ * & * & 1 \\ * & * & 2 \\ * & * & 3 \end{array} ,$$

ahol a *-gal jelölt helyeken tetszőleges szimbólum állhat.

$K_4(4, 2) = 7$ és 8 optimális kód létezik. Konstrukció 7 kódszóval: [86]. $K_4(4, 2) \geq 6$ bizonyítása: [24]. A pontos érték igazolása: [97]. Klasszifikáció: [129]. Az optimális kódok részben kiegyensúlyozottak, részben kiegyensúlyozatlanok. Valamennyi optimális kód abnormális.

$15 \leq K_4(5, 2) \leq 16$. Konstrukció 16 kódszóval: [65]. A 12 alsó korlát bizonyítása: [57]. Az alsó korlát javítása 14-re [162], 15-re [167]. Az ismert rekord-tartó konstrukció kiegyensúlyozott, normális kód.

$32 \leq K_4(6, 2) \leq 52$. Konstrukció 64 kódszóval: [65], 52 kódszóval: [113]. A 28 alsó korlát bizonyítása: [57]. Az alsó korlát 32-re javítása: [162]. Az ismert rekord-tartó konstrukció kiegyensúlyozott, abnormális kód.

$84 \leq K_4(7, 2) \leq 128$. Konstrukció 192, ill. 128 kódszóval: [65, 113]. A megadott alsó korlát bizonyítása: [164]. Az ismert rekord-tartó konstrukció kiegyensúlyozott, abnormális kód.

$240 \leq K_4(8, 2) \leq 352$. Konstrukció 512, ill. 384 kódszóval: [65, 113], 352 kódszóval: [168] (2005). A megadott alsó korlát bizonyítása: [57].

$751 \leq K_4(9, 2) \leq 1024$. Konstrukció 1536, ill. 1024 kódszóval: [65, 113]. A 747 alsó korlát bizonyítása: [57]. Az alsó korlát 751-re javítása: [156]. Az ismert rekord-tartó konstrukció kiegyensúlyozott, abnormális kód.

$2412 \leq K_4(10, 2) \leq 4096$. A felső korlát direkt összeg konstrukcióval adódik. A 2408 alsó korlát bizonyítása: [57]. Az alsó korlát 2412-re javítása: [134]. Az ismert rekord-tartó konstrukció kiegyensúlyozott, abnormális kód.

$7974 \leq K_4(11, 2) \leq 15872$. Rekord-tartó konstrukció: [168] (2006). Az alsó korlát bizonyítása: [57].

5.7.3. $R = 3$ elérési sugarú kódokra vonatkozó eredmények

$K_4(4, 3) = 4$ és 79 optimális kód létezik. Az optimális kódok alakja

$$\begin{array}{cccc} * & * & * & 0 \\ * & * & * & 1 \\ * & * & * & 2 \\ * & * & * & 3 \end{array},$$

ahol a *-gal jelölt helyeken tetszőleges szimbólum állhat.

$K_4(5, 3) = 4$ és egyetlen optimális kód létezik, mégpedig egy ismétléses kód, amely kiegyensúlyozott és normális.

$10 \leq K_4(6, 3) \leq 14$. Rekord-tartó konstrukció: [168] (2005). A 8 alsó korlát bizonyítása: [57], az alsó korlát 10-re javítása: [167]. Az ismert rekord-tartó konstrukció kiegyensúlyozatlan, abnormális kód.

$19 \leq K_4(7, 3) \leq 32$, $44 \leq K_4(8, 3) \leq 96$, $110 \leq K_4(9, 3) \leq 256$. Rekord-tartó konstrukció: [65]. Alsó korlát: [164]. Az ismert rekord-tartó konstrukció mindhárom esetben kiegyensúlyozott, normális kód.

$313 \leq K_4(10, 3) \leq 832$. Rekord-tartó konstrukció: [168] (2005). Alsó korlát: [57]. Az ismert rekord-tartó konstrukció kiegyensúlyozott, abnormális kód.

Megjegyzés. Az [57] cikk a $K_4(10, 3) \geq 315$ alsó korlátot adja meg (Table II) és közli, hogy e korlátot Theorem 1 vagy 2 bizonyítja, melyek közül 1-nél nagyobb elérési sugar esetén csak az utóbbi jöhet szóba. Kiderül azonban, hogy a „Theorem 2” tétel alkalmazásával csak a 313 alsó korlát bizonyítható.

$849 \leq K_4(11, 3) \leq 2048$. Rekord-tartó konstrukció: [168] (2005). Alsó korlát: [57]. Az ismert rekord-tartó konstrukció kiegyensúlyozott, abnormális kód.

5.7.4. $R = 4$ elérési sugarú kódokra vonatkozó eredmények

$8 \leq K_4(7, 4) \leq 10$. Konstrukció 12 kódszóval: [65], 10 kódszóval: [136] (2006). Az alsó korlát bizonyítása: [129]. Az ismert rekord-tartó konstrukció kiegyensúlyozatlan, abnormális kód.

$13 \leq K_4(8, 4) \leq 28$. Rekord-tartó konstrukció: [65]. Alsó korlát: [167]. Az ismert rekord-tartó konstrukció kiegyensúlyozatlan, normális kód.

$26 \leq K_4(9, 4) \leq 64$. Rekord-tartó konstrukció: [65]. Alsó korlát: [164]. Az ismert rekord-tartó konstrukció kiegyensúlyozott, normális kód.

$59 \leq K_4(10, 4) \leq 208$. Konstrukció 256 kódszóval: [65], 208 kódszóval: [113]. Alsó korlát: [164]. Az ismert rekord-tartó konstrukció kiegyensúlyozott, normális kód.

$148 \leq K_4(11, 4) \leq 512$. Rekord-tartó kód: [167], ADS konstrukcióval. Az alsó korlát bizonyítása: [57]. Az ismert rekord-tartó konstrukció kiegyensúlyozott, normális kód.

5.7.5. $R = 5$ elérési sugarú kódokra vonatkozó eredmények

$K_4(8, 5) = 8$. Konstrukció 8 kódszóval: [65]. Az 5 alsó korlát bizonyítása: [57]. Az alsó korlát javítása 7-re: [90], 8-ra [129]. Az ismert optimális kód kiegyensúlyozott, normális kód.

$10 \leq K_4(9, 5) \leq 16$. Rekord-tartó konstrukció: [65]. Alsó korlát: [164]. Az ismert rekord-tartó kód kiegyensúlyozott, normális kód.

$18 \leq K_4(10, 5) \leq 54$. Rekord-tartó konstrukció: [136] (2006). Alsó korlát: [164]. Az ismert rekord-tartó kód kiegyensúlyozatlan, abnormális kód.

$36 \leq K_4(11, 5) \leq 128$. Rekord-tartó kód: [167], ADS konstrukcióval. Alsó korlát: [164]. Az ismert rekord-tartó kód kiegyensúlyozott, normális kód.

5.7.6. $R = 6$ elérési sugarú kódokra vonatkozó eredmények

$8 \leq K_4(10, 6) \leq 16$. Rekord-tartó kód: [65] (1991). A 7 alsó korlát bizonyítása: [90], az alsó korlát 8-ra javítása: [129]. Az ismert rekord-tartó kód kiegyensúlyozott, normális kód.

$14 \leq K_4(11, 6) \leq 32$. Rekord-tartó kód: az 5.3.3 szakasz példái között szerepel. Az alsó korlát bizonyítása: [164]. Az ismert rekord-tartó kód kiegyensúlyozott, normális kód.

5.7.7. $R = 7$ elérési sugarú kódokra vonatkozó eredmény

$8 \leq K_4(11, 7) \leq 11$. Rekord-tartó kód: [136]. Az alsó korlát bizonyítása: [129]. Az ismert rekord-tartó kód kiegyensúlyozatlan, normális kód.

5.8. Az optimális és rekord-tartó térlefedő kódok áttekintése $q = 5$ esetén

Ismét csak az $n \leq 11$ esetekkel foglalkozunk, de $R = 1$ és 2 elérési sugar esetén 7 dimenziónál, $R = 3$ esetén 9 dimenziónál megállunk.

5.8.1. $R = 1$ elérési sugarú kódokra vonatkozó eredmények

$K_5(3, 1) = 13$ és egyetlen optimális kód létezik. Konstrukció és egyenlőség bizonyítása: [17]. Klasszifikáció (ami itt az unicitás bizonyítását jelenti): 5.6. tétel. Az egyetlen optimális kód két 2-szűrjektív kód egyesítése; kiegyensúlyozott, abnormális kód.

$46 \leq K_5(4, 1) \leq 51$. Rekord-tartó kód: [21]. A 45 alsó korlát bizonyítása: [19]. Az alsó korlát 46-ra javítása: [23]. Az ismert rekord-tartó kód kiegyensúlyozatlan, abnormális kód.

$160 \leq K_5(5, 1) \leq 184$. Rekord-tartó kód: [21]. A 157 alsó korlát bizonyítása: [19]. Az alsó korlát 160-ra javítása: [122]. Az ismert rekord-tartó kód kiegyensúlyozatlan, abnormális kód.

$K_5(6, 1) = 625$. Pontos érték igazolása: [6, 7, 8]. Az ismert optimális kód perfekt, kiegyensúlyozott, abnormális kód.

$2722 \leq K_5(7, 1) \leq 3125$. A felső korlát az (5.4) egyenlőtlenség alapján adódik. A 2695 alsó korlát bizonyítása: [57]. Az alsó korlát javítása 2702-re [82], 2722-re [134]. Az ismert rekord-tartó kód kiegyensúlyozott, normális kód.

$11945 \leq K_5(8, 1) \leq 15625$. A felső korlát az előző esethez hasonlóan adódik. A 11887 alsó korlát bizonyítása: [57]. Az alsó korlát javítása 11945-re [134].

$53138 \leq K_5(9, 1) \leq 78125$. A felső korlát az előző két esethez hasonlóan adódik. Az 52790 alsó korlát bizonyítása: [57]. Az alsó korlát javítása 52796-ra [82], 52800-ra [117], 53138-ra [134].

$238993 \leq K_5(10, 1) \leq 390625$. A felső korlát az előző 3 esethez hasonlóan adódik. A 238190 alsó korlát bizonyítása: [57]. Az alsó korlát javítása 238193-ra [82], 238200-ra [117], 238993-ra [134].

$1087416 \leq K_5(11, 1) \leq 1525877$. A felső korlát [135], „Proposition 9” állításnál alkalmazott módszerrel bizonyítható. A feltüntetett alsó korlát [57] egyik formulája alapján adódik.

5.8.2. $R = 2$ elérési sugarú kódokra vonatkozó eredmények

$K_5(4, 2) = 11$. Konstrukció 11 kódszóval: [65]. A 9 alsó korlát bizonyítása: [24]. Az alsó korlát 11-re javítása és ezáltal a pontos érték igazolása: [158]. Az ismert optimális kódok között kiegyensúlyozott és kiegyensúlyozatlan kódok is előfordulnak, s ezek valamennyien abnormális kódok.

$22 \leq K_5(5, 2) \leq 35$. Rekord-tartó kód: [65]. Alsó korlát: [164] (2008). Az ismert rekord-tartó kód kiegyensúlyozatlan, abnormális kód.

$71 \leq K_5(6, 2) \leq 125$. Rekord-tartó kód: [65]. Alsó korlát: [164]. Az ismert rekord-tartó kódok kiegyensúlyozottak, s előfordulnak közöttük normális és abnormális kódok is.

$225 \leq K_5(7, 2) \leq 525$. Rekord-tartó kód: [113]. Alsó korlát: [164]. Az ismert rekord-tartó kód kiegyensúlyozatlan, abnormális kód.

$821 \leq K_5(8, 2) \leq 1625$. Konstrukció 2392, ill. 1875 kódszóval: [65, 113], 1625 kódszóval: [136] (2006). A 815 alsó korlát bizonyítása: [57]. Az alsó korlát 821-re javítása: [156].

$3367 \leq K_5(9, 2) \leq 6375$. Konstrukció 8125, ill. 7500 kódszóval: [65, 113], 6375 kódszóval: [136] (2006). Alsó korlát: [57].

$13161 \leq K_5(10, 2) \leq 23000$. Konstrukció 31875 kódszóval: direkt összeg, 23000 kódszóval: [136] (2006). Alsó korlát: [57].

$52842 \leq K_5(11, 2) \leq 78125$. Konstrukció 78125 kódszóval: [136] (2006). Alsó korlát: [134].

5.8.3. $R = 3$ elérési sugarú kódokra vonatkozó eredmények

$K_5(5, 3) = 9$. Konstrukció 10, ill. 9 kódszóval: [65, 86]. A 7 alsó korlát bizonyítása: [24]. Az alsó korlát 9-re javítása és ezáltal a pontos érték igazolása: [158]. Az ismert optimális kódok kiegyensúlyozatlan, abnormális kódok.

Megjegyzés. Optimális kódok konstrukciójához az 5.4.1 szakaszban ismertetett módszert alkalmazzuk $q_1 = 2$, $q_2 = q_3 = q_4 = 1$ értékekkel. Több konstrukciót is bemutatunk a lemez mellékletén, melyek között a különbséget a felhasznált bináris 2-szűrjektív kód eredményezi. A [145], „Table 1” táblázat szerint $n = 5$, $M = 6$ esetén 7 ilyen inekvivalens szűrjektív kód létezik.

$16 \leq K_5(6, 3) \leq 25$. Rekord-tartó kód: [65]. Alsó korlát: [164]. Az ismert rekord-tartó kódok lineáris, kiegyensúlyozott kódok, s közöttük normális és abnormális kód is található.

$38 \leq K_5(7, 3) \leq 100$. Rekord-tartó kód: [128]. Alsó korlát: [164]. Az ismert rekord-tartó kód kiegyensúlyozott, abnormális kód.

$109 \leq K_5(8, 3) \leq 325$. Konstrukció 455 kódszóval: [65], 325 kódszóval: [90]. Alsó korlát: [164]. Az ismert rekord-tartó kód kiegyensúlyozatlan, normális kód.

$330 \leq K_5(9, 3) \leq 1275$. Konstrukció 1625 kódszóval: [65], 1275 kódszóval: [90]. A 329 alsó korlát bizonyítása: [57]. Javítás 330-ra: [116]. Az ismert rekord-tartó kód kiegyensúlyozatlan, normális kód.

$1163 \leq K_5(10, 3) \leq 4375$. Rekord-tartó kód: [136] (2006). Alsó korlát: [156].

$4255 \leq K_5(11, 3) \leq 15625$. Rekord-tartó kód: [136] (2006). Alsó korlát: [57].

5.8.4. $R = 4$ elérési sugarú kódokra vonatkozó eredmények

$12 \leq K_5(7, 4) \leq 21$. Rekord-tartó kód: [136] (2006). Alsó korlát: [164]. Az ismert rekord-tartó kód kiegyensúlyozott, abnormális kód.

$25 \leq K_5(8, 4) \leq 65$. Konstrukció 121 kódszóval: [65], 65 kódszóval: [90]. Alsó korlát: [164]. Az ismert rekord-tartó kód kiegyensúlyozatlan, normális kód.

$64 \leq K_5(9, 4) \leq 255$. Konstrukció 325 kódszóval: [65], 255 kódszóval: [90]. Alsó korlát: [164]. Az ismert rekord-tartó kód kiegyensúlyozatlan, normális kód.

$162 \leq K_5(10, 4) \leq 875$. Konstrukció 875 kódszóval: [90]. Alsó korlát: [57]. Az ismert rekord-tartó kód kiegyensúlyozott, normális kód.

Megjegyzés. A [90] cikkben a 720 felső korlát van megadva (Corollary 8), azonban a cikk anyaga alapján csak a 875 felső korlát bizonyítható. Nemrég megkérdeztem a cikk egyik szerzőjét, hogy mi erről a véleménye, aki e kérdésre adott válaszában megerősítette azt a feltételezésemet, hogy a publikált 720 felső korlát téves volt.

$535 \leq K_5(11, 4) \leq 3125$. Rekord-tartó kód: [90]. Alsó korlát: [57]. Az ismert rekord-tartó kód kiegyensúlyozott, normális kód.

5.8.5. $R = 5$ elérési sugarú kódokra vonatkozó eredmények

$11 \leq K_5(8, 5) \leq 15$. Konstrukció 20 kódszóval: [65], 19, ill. 15 kódszóval: [136] (2006, 2008). A 6 alsó korlát bizonyítása: [57]. Az alsó korlát javítása 9-re: [90], 11-re: [158]. Az ismert rekord-tartó kód kiegyensúlyozott, abnormális kód.

$19 \leq K_5(9, 5) \leq 55$. Konstrukció 65 kódszóval: [65], 55 kódszóval: [90]. Alsó korlát: [164]. Az ismert rekord-tartó kód kiegyensúlyozatlan, normális kód.

$41 \leq K_5(10, 5) \leq 175$. Rekord-tartó kód: [90]. Alsó korlát: [164]. Az ismert rekord-tartó kód kiegyensúlyozott, normális kód.

$103 \leq K_5(11, 5) \leq 625$. Rekord-tartó kód: [90]. Alsó korlát: [164]. Az ismert rekord-tartó kód kiegyensúlyozott, normális kód.

5.8.6. $R = 6$ elérési sugarú kódokra vonatkozó eredmények

$9 \leq K_5(9, 6) \leq 12$. Konstrukció 15 kódszóval: [65], 12 kódszóval: [136] (2008). A 6 alsó korlát bizonyítása: [57]. Az alsó korlát javítása 8-ra [90], 9-re [158]. Az ismert rekord-tartó kód kiegyensúlyozatlan, abnormális kód.

$16 \leq K_5(10, 6) \leq 45$. Rekord-tartó kód: [90]. Alsó korlát: [164]. Az ismert rekord-tartó kód kiegyensúlyozatlan, normális kód.

$29 \leq K_5(11, 6) \leq 125$. Rekord-tartó kód: [90]. Alsó korlát: [164]. Az ismert rekord-tartó kód kiegyensúlyozott, normális kód.

5.8.7. $R = 7$ elérési sugarú kódokra vonatkozó eredmények

$K_5(10, 7) = 9$. Konstrukció 10 kódszóval: [65], 9 kódszóval: [165]. A 6 alsó korlát bizonyítása: [57]. Az alsó korlát 9-re javítása: [158]. Az ismert optimális kód kiegyensúlyozott, abnormális kód.

$12 \leq K_5(11, 7) \leq 25$. Rekord-tartó kód: [90]. Alsó korlát: [164]. Az ismert rekord-tartó kód kiegyensúlyozott, normális kód.

5.9. Az optimális és rekord-tartó térlefedő kódok áttekintése $6 \leq q \leq 10$ esetén

A $6 \leq q \leq 10$ intervallumra vonatkozóan már csak olyan esetekkel foglalkozunk (a teljesség igénye nélkül), melyekre $3 \leq n \leq 7$. Itt sem adunk meg prompt korlátokat, s az egyéb közlendőkből is általában csak a leglényegesebbekre szorítkozunk.

5.9.1. $R = 1$ elérési sugarú kódokra vonatkozó eredmények

$K_6(3, 1) = 18$, $K_7(3, 1) = 25$, $K_8(3, 1) = 32$, $K_9(3, 1) = 41$. Konstrukció és egyenlőség bizonyítása: [17]. A felsorolt esetekre vonatkozóan az ismert optimális kódok mindegyike két 2-szűrjektív kód egyesítése; s valamennyien kiegyensúlyozott, abnormális kódok.

$K_{10}(3, 1) = 50$. Az előbbi esetekre mondottak itt is változatlanul érvényesek.

$K_6(4, 1) = 72$. Konstrukció és egyenlőség bizonyítása: [19]. Az ismert optimális kód kiegyensúlyozott, abnormális kód.

$115 \leq K_7(4, 1) \leq 123$, $171 \leq K_8(4, 1) \leq 192$. Konstrukció 123, ill. 192 kódszóval: [21]. A 115, ill. 171 alsó korlát bizonyítása: [24], általános formulával. Az ismert rekord-tartó kód mindkét esetben kiegyensúlyozott, abnormális kód.

$K_9(4, 1) = 243$. Konstrukció 243 kódszóval: [19]. A 243 alsó korlát (és egyúttal pontos érték) igazolása: [24], általános formulával. Az ismert optimális kód ezúttal is kiegyensúlyozott, abnormális kód.

$334 \leq K_{10}(4, 1) \leq 352$. Rekord-tartó kód: [21]. Az alsó korlát bizonyítása: [24], általános formulával. Az ismert rekord-tartó kód kiegyensúlyozatlan, abnormális kód.

$330 \leq K_6(5, 1) \leq 414$, $606 \leq K_7(5, 1) \leq 769$. Rekord-tartó kódok: [21]. Alsó korlátok: [122]. Az ismert rekord-tartó kód mindkét esetben kiegyensúlyozatlan, abnormális kód.

$K_8(5, 1) = 1024$. Konstrukció és egyenlőség bizonyítása: [19]. Az ismert optimális kód kiegyensúlyozott, abnormális kód.

$1641 \leq K_9(5, 1) \leq 1809$, $2501 \leq K_{10}(5, 1) \leq 2944$. Konstrukció 1809, ill. 2944 kódszóval: [21]. Az alsó korlátok bizonyítása: [24], általános formulával. Az ismert rekord-tartó kód mindkét esetben kiegyensúlyozatlan, abnormális kód.

$1578 \leq K_6(6, 1) \leq 1840$, $3412 \leq K_7(6, 1) \leq 4435$. Rekord-tartó kódok: [25]. Az alsó korlátok bizonyítása: [122]. Az ismert rekord-tartó kód mindkét esetben kiegyensúlyozatlan, abnormális kód.

$6626 \leq K_8(6, 1) \leq 8192$. Rekord-tartó kód: [19]. Alsó korlát: [122]. Az ismert rekord-tartó kód kiegyensúlyozott, normális kód.

$11877 \leq K_9(6, 1) \leq 16010$. Rekord-tartó kód: [25] (1971). Alsó korlát: [122]. Az ismert rekord-tartó kód kiegyensúlyozatlan, abnormális kód.

$K_{10}(6, 1) = 20000$. Konstrukció és egyenlőség bizonyítása: [19]. Az ismert optimális kód kiegyensúlyozott, abnormális kód.

5.9.2. $R = 2$ elérési sugarú kódokra vonatkozó eredmények

$13 \leq K_6(4, 2) \leq 15$, $17 \leq K_7(4, 2) \leq 19$. Rekord-tartó kódok: [86]. Alsó korlátok: [24], általános formulával. Az ismert rekord-tartó kódok között mindkét esetben van kiegyensúlyozott és kiegyensúlyozatlan kód, viszont ezek mind abnormális kódok.

$22 \leq K_8(4, 2) \leq 23$. Rekord-tartó kód: [86]. Alsó korlát: [24], általános formulával. Az ismert rekord-tartó kód kiegyensúlyozott, abnormális kód.

$K_9(4, 2) = 27$. Konstrukció és egyenlőség bizonyítása: [24]. Az ismert optimális kód kiegyensúlyozott, abnormális kód.

$K_{10}(4, 2) = 34$. Konstrukció 34 kódszóval: [135]. Az alsó korlát bizonyítása: [24], általános formulával. Az ismert optimális kód kiegyensúlyozott, abnormális kód.

$36 \leq K_6(5, 2) \leq 66$. Rekord-tartó kód: két szűrjektív kód egyesítése. Alsó korlát: [164]. Az ismert rekord-tartó kód kiegyensúlyozott, abnormális kód.

$55 \leq K_7(5, 2) \leq 97$, $113 \leq K_9(5, 2) \leq 189$. Rekord-tartó kód: két szűrjektív kód egyesítése, lásd 5.4.1 szakasz. Alsó korlát: [164]. Az ismert rekord-tartó kód mindkét esetben kiegyensúlyozatlan, abnormális kód.

$83 \leq K_8(5, 2) \leq 128$, $149 \leq K_{10}(5, 2) \leq 250$. Rekord-tartó kód: [135]. Az alsó korlát bizonyítása: [164]. Az ismert rekord-tartó kód mindkét esetben kiegyensúlyozott, abnormális kód.

$133 \leq K_6(6, 2) \leq 274$. Rekord-tartó kód: [136] (2006). Az alsó korlát bizonyítása: [164]. Az ismert rekord-tartó kód kiegyensúlyozatlan, abnormális kód.

$233 \leq K_7(6, 2) \leq 343$, $585 \leq K_9(6, 2) \leq 729$. Rekord-tartó kód: [135]. Alsó korlát: [164]. Az ismert rekord-tartó kód mindkét esetben lineáris, kiegyensúlyozott, abnormális kód.

$382 \leq K_8(6, 2) \leq 512$. Rekord-tartó kód: [135]. Alsó korlát: [164]. Az ismert rekord-tartó kód lineáris, kiegyensúlyozott, abnormális kód.

$890 \leq K_{10}(6, 2) \leq 1350$. Rekord-tartó kód: [136] (2006). Alsó korlát: [164]. Az ismert rekord-tartó kód kiegyensúlyozatlan, abnormális kód.

5.9.3. $R = 3$ elérési sugarú kódokra vonatkozó eredmények

$K_6(5, 3) = 12$. Konstrukció 12 kódszóval: [136] (2006). A 12 alsó korlát és egyúttal a pontos érték bizonyítása: [158]. Az ismert optimális kód kiegyensúlyozott, abnormális kód.

$14 \leq K_7(5, 3) \leq 17$. Rekord-tartó kód: [136] (2006). Alsó korlát: [158]. Az ismert rekord-tartó kód kiegyensúlyozott, abnormális kód.

$17 \leq K_8(5, 3) \leq 22$. Rekord-tartó kód: [136] (2006). Alsó korlát: [24], általános formulával. Az ismert rekord-tartó kód kiegyensúlyozatlan, abnormális kód.

$21 \leq K_9(5, 3) \leq 27$. Mindkét korlát a [24] cikkben közölt eredményekből adódik. Az ismert rekord-tartó kód kiegyensúlyozott, abnormális kód.

$26 \leq K_{10}(5, 3) \leq 32$. Rekord-tartó kód: [136] (2006). Alsó korlát: [24]. Az ismert rekord-tartó kód kiegyensúlyozatlan, abnormális kód.

$24 \leq K_6(6, 3) \leq 41$, $36 \leq K_7(6, 3) \leq 77$. Rekord-tartó kód: [136] (2006). Alsó korlát: [164]. Az ismert rekord-tartó kód mindkét esetben kiegyensúlyozatlan, abnormális kód.

$52 \leq K_8(6, 3) \leq 107$, $71 \leq K_9(6, 3) \leq 147$, $92 \leq K_{10}(6, 3) \leq 209$. Rekord-tartó kód: [136] (2006). Alsó korlát: [164]. Az ismert rekord-tartó kód mindhárom esetben kiegyensúlyozatlan, abnormális kód.

$70 \leq K_6(7, 3) \leq 246$. Rekord-tartó kód: [136] (2006). Alsó korlát: [164]. Az ismert rekord-tartó kód kiegyensúlyozatlan, normális kód.

$127 \leq K_7(7, 3) \leq 343$, $196 \leq K_8(7, 3) \leq 512$. Rekord-tartó kód: [135]. Alsó korlát: [164]. Az ismert rekord-tartó kód mindkét esetben kiegyensúlyozott, normális kód.

$308 \leq K_9(7, 3) \leq 729$. Rekord-tartó kód: [135]. Alsó korlát: [164]. Az ismert rekord-tartó kód kiegyensúlyozott, abnormális kód.

$451 \leq K_{10}(7, 3) \leq 1350$. Rekord-tartó kód: [136] (2006). Alsó korlát: [164]. Az ismert rekord-tartó kód kiegyensúlyozatlan, abnormális kód.

5.9.4. $R = 4$ elérési sugarú kódokra vonatkozó eredmények

A soron következő első három esetben az 5.15 egyenlőtlenség speciális eseteként adódó $K_{q_1+q_2+q_3+q_4+q_5}(6, 4) \leq \sum_{i=1}^5 \sigma_{q_i}(6, 2)$ egyenlőtlenség alapján öt 2-szűrjektív kód egyesítéseként kapjuk a rekord-tartó kód-konstrukciót.

$K_6(6, 4) = 10$, $13 \leq K_7(6, 4) \leq 15$, $15 \leq K_8(6, 4) \leq 20$. Konstrukció: [135]. Alsó korlát: [158]. Az ismert optimális, ill. rekord-tartó kód mindhárom esetben kiegyensúlyozatlan, abnormális kód.

$18 \leq K_9(6, 4) \leq 24$. Rekord-tartó kód: [136] (2006). Alsó korlát: [158]. Az ismert rekord-tartó kód kiegyensúlyozatlan, abnormális kód.

$21 \leq K_{10}(6, 4) \leq 28$. Rekord-tartó kód: [136] (2006). Alsó korlát: [24]. Az ismert rekord-tartó kód kiegyensúlyozott, abnormális kód.

A következő 4 esetben a felső korlát [169] táblázataiban a lefedő tömbökre megadott felső korlátok segítségével bizonyítható. A rekord-tartó kód-konstrukciót ezekben az esetekben a $K_{q_1+q_2+q_3}(7, 4) \leq \sigma_{q_1}(7, 3) + \sigma_{q_2}(7, 3) + \sigma_{q_3}(7, 3)$ egyenlőtlenség alapján három 3-szűrjektív kód egyesítéseként kapjuk.

$18 \leq K_6(7, 4) \leq 36$. Alsó korlát: [164]. A fenti konstrukció alapján adódó rekord-tartó kód kiegyensúlyozott, abnormális kód.

$37 \leq K_8(7, 4) \leq 92$. Az alsó korlát bizonyítása: [164]. Az ismert rekord-tartó kód kiegyensúlyozatlan, abnormális kód.

$51 \leq K_9(7, 4) \leq 120$, $66 \leq K_{10}(7, 4) \leq 168$. Az alsó korlát bizonyítása: [164]. Az ismert rekord-tartó kód mindkét esetben ismét kiegyensúlyozatlan, abnormális kód.

$25 \leq K_7(7, 4) \leq 49$. Rekord-tartó kód: [135] (2005). Az alsó korlát bizonyítása: [164]. Az ismert rekord-tartó kód lineáris, kiegyensúlyozott, normális kód.

$46 \leq K_6(8, 4) \leq 216$, $76 \leq K_7(8, 4) \leq 343$, $118 \leq K_8(8, 4) \leq 512$. Rekord-tartó kód: [135]. Az alsó korlát bizonyítása: [164].

$181 \leq K_9(8, 4) \leq 729$. Rekord-tartó kód: [135]. Az alsó korlát bizonyítása: [164].

$265 \leq K_{10}(8, 4) \leq 1156$. Felső korlát: direkt összeg konstrukció. Alsó korlát: [164].

$136 \leq K_6(9, 4) \leq 738$, $264 \leq K_7(9, 4) \leq 1843$. Felső korlát: direkt összeg konstrukció. Alsó korlát: [164].

$409 \leq K_8(9, 4) \leq 2944$, $703 \leq K_9(9, 4) \leq 5103$, $1130 \leq K_{10}(9, 4) \leq 8500$. Felső korlát: direkt összeg konstrukció. Alsó korlát: [149].

6. fejezet

Vegyes ternáris/bináris térlefedő kódok

Az 1. fejezetben a fogalmak magyarázata során már említettük a $Z_{q_1}^{n_1} Z_{q_2}^{n_2} \dots Z_{q_m}^{n_m}$ térben értelmezett általános vegyes kódokat és az optimális vegyes térlefedő kódok méretéként értelmezett $K_{q_1, q_2, \dots, q_m}(n_1, n_2, \dots, n_m; R)$ kifejezést. Ebben a fejezetben két különböző (mégpedig a lehető legkisebb két különböző) alapszámhoz, a $q_1 = 3$, $q_2 = 2$ értékpárhoz tartozó vegyes kódokkal foglalkozunk. A bináris kódokhoz hasonlóan a vegyes kódok e legegyszerűbb esetének a tárgyalására vonatkozóan is kialakult az a konvenció, hogy K -nak az alapszámokra utaló indexeit elhagyjuk, tehát $K_{3,2}(t, b; R)$ helyett az index nélküli $K(t, b; R)$ kifejezést használjuk a t ternáris és b bináris koordinátát tartalmazó R elérési sugarú térlefedő kódok minimális méretének a jelölésére.

A vegyes ternáris/bináris kódok tárgyalása során nem zárjuk ki sem $t = 0$, sem $b = 0$ lehetőségét, mivel ezek kizárása nélkül kényelmesebb a tárgyalás.

6.1. Egyszerű konstrukciók

6.1.1. Konstrukciók 3-7 kódszóval

Három kódszóval az ismétléses kódhoz hasonló konstrukción alapul a 6.4 szakaszban megfogalmazásra kerülő 6.10. lemma. Ebben az esetben a megadott kód ternáris része ismétléses kód, bináris része pedig az ismétléses kódból az egyik kódszó duplázásával keletkezik. A 6.13., 6.16., 6.19., 6.20. és 6.21. lemmák 4-7 szavas konstrukciókat ismeretnek. A felsorolt konstrukciók, mint látni fogjuk, minden esetben optimális térlefedő kódot eredményeznek.

6.1.2. Mátrix módszerrel készített konstrukciók

A ternáris kódok esetére már említett mátrix módszer kiterjeszthető vegyes kódokra is. (Ebben az esetben a mellékosztályok módszere elnevezést nem használhatjuk.) A mátrix módszer vegyes kódokra való megfogalmazását és alkalmazását illetően lásd [102].

6.2. Folytatólagos konstrukciók és ezekből adódó egyenlőtlenségek

Mind a bináris, mind a ternáris kódok esetére alkalmazott folytatólagos konstrukciók alkalmazhatók vegyes ternáris/bináris kódokra is. Bináris koordináta vonatkozásában a bináris, ternáris koordináta vonatkozásában a ternáris esetre mondottak érvényesek.

6.2.1. 1-gyel növelt dimenzió és elérési sugár, változatlan méret

Tetszőleges vegyes ternáris/bináris kódot akár újabb bináris, akár újabb ternáris koordinátával kibővíthetjük, az elérési sugár legfeljebb 1-gyel nő (és nyilván soha nem csökken). Ezért fennáll

$$K(t, b + 1; R + 1) \leq K(t, b; R) \leq K(t, b + 1; R). \quad (6.1)$$

és

$$K(t + 1, b; R + 1) \leq K(t, b; R) \leq K(t + 1, b; R). \quad (6.2)$$

6.2.2. Megnövelt dimenzió, változatlan elérési sugár, dupla (tripla) méret

Ha egy vegyes ternáris/bináris kódot úgy növelünk meg újabb bináris koordinátával, hogy minden kódszót 0-val is, 1-essel is folytatva megduplázzunk, vagy ha úgy növeljük meg újabb ternáris koordinátával, hogy minden kódszót 0-val, 1-essel és 2-essel is folytatva megtriplázzunk, az elérési sugár változatlan marad. Következésképpen fennállnak a

$$K(t, b + 1; R) \leq 2K(t, b; R) \quad (6.3)$$

és

$$K(t + 1, b; R) \leq 3K(t, b; R) \quad (6.4)$$

egyenlőtlenségek.

6.2.3. 2-vel (3-mal) növelt dimenzió, 1-gyel (2-vel) növelt elérési sugár, változatlan méret

A 3.3.3 szakaszban bináris kódokra megadott konstrukció vegyes kódra is alkalmazható, ha az normális legalább egy bináris koordinátában. Hasonlóan, a 4.2.3 szakaszban ternáris kódokra megadott konstrukció vegyes kódra is alkalmazható, ha az normális legalább egy ternáris koordinátában. Ebből következik, hogy ha létezik $Z_3^t Z_2^b$ -ben M kódszóból álló, R elérési sugarú kód, amely egy bináris, ill. ternáris koordinátában normális akkor $K(t, b + 2; R + 1) \leq M$, ill. $K(t + 3, b; R + 2) \leq M$.

6.2.4. Ternáris koordináta helyett bináris koordináta

Legyen $C \subseteq Z_3^t Z_2^b$, ahol $t \geq 1$. Képezzük le C kódszavait a $Z_3^{t-1} Z_2^{b+1}$ térbe úgy, hogy C utolsó ternáris koordinátája kivételével a többi koordináta értékét minden kódszóban változatlanul hagyjuk, az utolsó ternáris koordináta értékét pedig, amennyiben ez az érték 2, akkor 0 vagy 1 bármelyikére változtatjuk, egyébként pedig az utolsó ternáris koordináta értékét is változatlanul hagyjuk. Az eredményül kapott kód elérési sugara nyilvánvalóan nem lehet nagyobb C elérési sugaránál, ezért fennáll, hogy

$$K(t-1, b+1; R) \leq K(t, b; R). \quad (6.5)$$

6.2.5. Bináris koordináta helyett ternáris koordináta

Legyen $C = |C_1|C_2|C_3| \subseteq Z_3^t Z_2^b$ egy M kódszóból álló, R elérési sugarú kód, ahol $C_1 \subseteq Z_3^t$, $C_2 \subseteq Z_2$ és $C_3 \subseteq Z_2^{b-1}$ (ezért feltesszük, hogy $b \geq 1$). Az összefüszött C_1, C_2, C_3 kódok szavai között lehetnek ($M > 2$ esetén az 1 dimenziós C_2 kód szavai között nyilván mindig vannak is) ismétlődők. Legyen

$$D_0 = \{|c_1|2|c_3| : c_1 \in C_1, c_2 = 0, c_3 \in C_3\}$$

és

$$D_1 = \{|c_1|2|c_3| : c_1 \in C_1, c_2 = 1, c_3 \in C_3\}.$$

Megmutatjuk, hogy a $C \cup D_0, C \cup D_1 \subseteq Z_3^{t+1} Z_2^{b-1}$ kódok elérési sugara is R . Elég ennek bizonyítását az egyik kódra, pl. $C \cup D_1$ -re megmutatni, melynek elérési sugarát jelöljük R_1 -gyel.

Legyen $x = |x_1|x_2|x_3| \in Z_3^{t+1} Z_2^{b-1}$. Ha $x_2 = 0$ vagy 1, akkor $x \in Z_3^t Z_2^b$, és így C -ben, tehát a nála bővebb $C \cup D_1$ -ben is van olyan kódszó, amely x -től legfeljebb R távolságra van. Ha viszont $x_2 = 2$, akkor $x \in Z_3^t Z_2^b$, és így C -ben van olyan $c = |c_1|c_2|c_3|$ ($c_2 = 0$ vagy 1) kódszó, amely $|x_1|1|x_3|$ -től legfeljebb R távolságra van. $c_2 = 0$ esetén ugyanennyi a $d(x, c)$ távolság is, $c_2 = 1$ esetén pedig ugyanennyi a $d(x, |c_1|2|c_3|)$ távolság is, ahol $|c_1|2|c_3| \in D_1$. Ezzel beláttuk, hogy $R_1 \leq R$.

A fordított egyenlőtlenség bizonyításához legyen $x = |x_1|x_2|x_3| \in Z_3^t Z_2^b$, tetszőlegesen választva. Ekkor van olyan $c = |c_1|c_2|c_3| \in C \cup D_1$, melyre fennáll $d(x, c) \leq R_1$. Most vagy $c \in C$ vagy pedig $c_2 = 2$. Az első esetben azonnal adódik, hogy $d(x, C) \leq R_1$, a második esetben ez abból következik, hogy ilyenkor $|c_1|1|c_3| \in C$ és $d(x_2, c_2) = 1$ folytán $d(x, |c_1|1|c_3|) \leq d(x, c)$. Eszerint mindenképpen fennáll $R \leq R_1$.

Mivel D_0 és D_1 együttes elemszáma megegyezik C elemszámával, ezért $C \cup D_0$ és $C \cup D_1$ közül valamelyiknek az elemszáma nem haladja meg C elemszámának a $3/2$ -szeresét, és következésképpen fennáll

$$K(t+1, b-1; R) \leq \frac{3}{2} \cdot K(t, b; R). \quad (6.6)$$

$c_2 \setminus y_2$	001	110	010	101	100	011	000	111	000	111	000	111
							$j=0$	$j=0$	$j=1$	$j=1$	$j=2$	$j=2$
0	D_0	D'_0	D'_0	D_0	D'_0	D_0	D_3	D'_3	D_0	D'_0	D_0	D'_0
1	D'_1	D_1	D_1	D'_1	D'_1	D_1	D_1	D'_1	D_3	D'_3	D_1	D'_1
2	D'_2	D_2	D_2	D'_2	D'_2	D_2	D_2	D'_2	D_2	D'_2	D_3	D'_3

6.1. táblázat. Választás a D_i , D'_i kódok közül

6.2.6. Ternáris koordináta helyett 3 bináris koordináta

Legyen $C = |C_1|C_2|C_3| \subseteq Z_3^t Z_2^b$ egy M kódszóból álló, R elérési sugarú kód, ahol most $C_1 \subseteq Z_3^{t-1}$, $C_2 \subseteq Z_3$ és $C_3 \subseteq Z_2^b$ (ezért feltesszük, hogy $t \geq 1$). Az összefüzdött C_1, C_2, C_3 kódok szavai között természetesen most is lehetnek ismétlődők. Az 1 dimenziós ternáris C_2 kód helyére egy 3 dimenziós bináris D_2 kódot helyezünk el – egyúttal a kód méretét is növeljük a következő módon:

Jelöljük $i = 0, 1, 2$ -re C_{2i} -vel C_2 -nek azt a részét, ahol az i értékek helyezkednek el. C_2 e felbontásával konzisztens módon bontsuk C_1 -et és C_3 -at (és így a teljes C kódot is) három részre, és ennek megfelelően legyen

$$C_i = |C_{1i}|C_{2i}|C_{3i}| \quad (i = 0, 1, 2),$$

ahol C_i kódszavainak a számát jelöljük M_i -vel ($M_0 + M_1 + M_2 = M$), és legyen $j \in \{0, 1, 2\}$ olyan index, melyre $M_j \leq M_i$ fennáll $i \in \{0, 1, 2\}$ esetén.

Tekintsük most azt a $D \subseteq Z_3^{t-1} Z_2^{b+3}$ kódot mely az alábbi D_i és D'_i kódok egyesítése:

$$D_0 = |C_{10}|001|C_{30}|, \quad D'_0 = |C_{10}|110|C_{30}|,$$

$$D_1 = |C_{11}|010|C_{31}|, \quad D'_1 = |C_{11}|101|C_{31}|,$$

$$D_2 = |C_{12}|100|C_{32}|, \quad D'_2 = |C_{12}|011|C_{32}|,$$

$$D_3 = |C_{1j}|000|C_{3j}|, \quad D'_3 = |C_{1j}|111|C_{3j}|.$$

A D kód mérete $2(M_0 + M_1 + M_2 + M_j) = 2(M + M_j) \leq \frac{8M}{3}$.

A D kód elérési sugara megegyezik C elérési sugarával, vagy annál kisebb. Legyen ugyanis $y = |y_1|y_2|y_3| \in Z_3^{t-1} Z_2^{b+3}$ tetszőleges pont a D kód Hamming terében, és tekintsük a C kód Hamming terében azt az $x = |x_1|x_2|x_3|$ pontot, melyre $x_1 = y_1, x_3 = y_3$, továbbá

$$x_2 = \begin{cases} 0 & \text{ha } y_2 = (001) \text{ vagy } y_2 = (110), \\ 1 & \text{ha } y_2 = (010) \text{ vagy } y_2 = (101), \\ 2 & \text{ha } y_2 = (100) \text{ vagy } y_2 = (011), \\ j & \text{ha } y_2 = (000) \text{ vagy } y_2 = (111). \end{cases}$$

Legyen $c = |c_1|c_2|c_3| \in C$ olyan kódszó, melyre $d(x, c) \leq R$. A D kód értelmezése szerint a $c \in C$ kódszó több lehetséges D -beli megfelelője közül a 6.1. táblázat szerint meghatározott $d \in D$ kódot kiválasztva könnyen látható, hogy d és y távolsága azonos c és x távolságával, tehát legfeljebb R lehet. Következésképpen fennáll az alábbi reláció:

$$K(t-1, b+3; R) \leq \frac{8}{3} \cdot K(t, b; R). \quad (6.7)$$

$t = 1$		$t = 2$		$t = 3$	
$b \setminus R$	1 2 3	$b \setminus R$	1 2 3	$b \setminus R$	1 2 3
1	• • ○	1	• • •	1	• • •
2	• • •	2	• • •	2	• • •
3	• • •	3	• • •	3	• • •
4	• • •	4	• • •	4	• • •
5	• • •	5	• • •	5	• • •
6	• • •	6	• • •	6	• • •
7	• • •	7	• • •	7	• • •
8	• • •	8	• • •	8	• • •
9	• • •	9	• • •	9	• • •

6.2. táblázat. Optimális vegyes térlefedő kódok megoldott esetei $t = 1$, $t = 2$ és $t = 3$ ternáris koordinátával

6.3. Összetételes konstrukciók és kapcsolatos egyenlőtlenségek

Itt már egész röviden csak annyit jegyzünk meg, hogy a DS, ADS és BDS konstrukciók vegyes ternáris/bináris kódok esetére is alkalmazhatók.

6.4. Vegyes ternáris/bináris térlefedő kódok mérete

Az előző fejezetekben tárgyalt kód kategóriákkal összehasonlítva, vegyes ternáris/bináris optimális térlefedő kódoknak lényegesen több családjára vonatkozóan, valamint ugyan-csak sokkal több szórványos esetére ismerjük, ill. tudjuk bizonyítani a pontos méretet, azaz $K(t, b; R)$ pontos értékét. Azért most nem ezeknek az eseteknek az összefoglalásával kezdjük, hanem a méretet (a kódszavak számát) fokozatosan növelve ismertetjük az adott mérethez tartozó, bizonyítottan optimális térlefedő kódok eseteit.

A 6.2-6.3. táblázatokban a korábban tárgyalt kód kategóriákra végzetekhez hasonló módon szemléltetjük a megoldott, értelmezhetetlen, ill. megoldatlan esetek tartományát $t + b \leq 10$ és $R \leq 3$ esetére.

Egy, ill. két kódszóból álló optimális kódokra nyilvánvaló a következő állítás.

6.1. Állítás.

$K(t, b; R) = 1$ akkor és csak akkor áll fenn, ha $R = t + b$;

$K(t, b; R) = 2$ akkor és csak akkor áll fenn, ha $t + \lfloor \frac{b}{2} \rfloor \leq R < t + b$.

$t = 4$		$t = 5$		$t = 6$	
$b \setminus R$	1 2 3	$b \setminus R$	1 2 3	$b \setminus R$	1 2 3
1	• • •	1	• •	1	•
2	• • •	2	•	2	
3	•	3		3	
4	•	4		4	

6.3. táblázat. Optimális vegyes térlefedő kódok megoldott esetei $t = 4$, $t = 5$ és $t = 6$ ternáris koordinátával

Ennél nagyobb méretek esetére vonatkozó hasonló állítások megfogalmazásához és bizonyításához már különböző ötletekre, hat, ill. hét kódszó esetére pedig számítógép segítségével is szükségünk volt. Még nagyobb méretre jelenleg nem tudunk szükséges és elégséges feltételt megadni.

A folytatáshoz több előkészítő jellegű állítást és lemmát fogalmazunk meg. Először tetszőleges vegyes kódra bizonyítunk egy állítást.

6.2. Állítás.

Ha egy M szóból álló $C \subset Z_{q_1}^{n_1} Z_{q_2}^{n_2} \dots Z_{q_m}^{n_m}$ kódban valamely, a Z_{q_i} részhez tartozó j index esetén a kódszavak j -edik koordináta helyén $\min\{q_i, M\}$ -nél kevesebb különböző szimbólum fordul elő, akkor megadható olyan C^ kód, melynek elérési sugara kisebb vagy egyenlő C elérési sugaránál, és melyben már $\min\{q_i, M\}$ különböző szimbólum található a kódszavak j -edik koordináta helyén tetszőleges $i = 1, 2, \dots, m$, $\sum_{k=1}^{i-1} q_k < j \leq \sum_{k=1}^i q_k$ esetén.*

Bizonyítás. Ha a feltételnek megfelelő j -edik koordináta helyen $\min\{q_i, M\}$ -nél kevesebb különböző szimbólum fordul elő, akkor van köztük olyan szimbólum, amely legalább kétszer előfordul ezen a koordináta helyen. Ezek egyikének alkalmas módosításával az e helyen különböző szimbólumok száma 1-gyel növelhető. Könnyen belátható, hogy ilyen módosítás során az elérési sugár nem növekedhet. Ilyen elemi lépések ismételt alkalmazásával véges számú lépésben eljutunk a kívánt tulajdonságú C^* kódhoz. $\square$

Mielőtt tovább mennénk, gondoljuk át, mit mond a 6.2. állítás vegyes ternáris/bináris kódok esetére specifikálva. Ha $M = 2$, akkor a C^* kódra fennáll, hogy a bináris koordináta-helyeken a 0, 1 szimbólumok mindegyike, a ternáris koordináta-helyeken pedig a 0, 1, 2 szimbólumok közül legalább kettő előfordul. Ha viszont $M \geq 3$, akkor azt tudjuk, hogy a bináris koordináta-helyeken a 0, 1 szimbólumok mindegyike, a ternáris koordináta-helyeken pedig a 0, 1, 2 szimbólumok mindegyike előfordul C^* kódszavaiban.

6.3. Állítás.

Ha egy vegyes ternáris/bináris C kód 2 szóból, a kódszavak pedig t ternáris és b bináris koordinátából állnak, akkor a kód elérési sugara legalább $t + \lfloor b/2 \rfloor$.

Bizonyítás. Elég a 6.2. állítás alkalmazásával adódó C^* kódra igazolni az állítást. Ez a C^* kód ekvivalens azzal a kóddal, melyben az első kódszó csupa 0, a második pedig csupa 1 értékű koordinátából áll. Ekkor a ternáris koordináta helyeken csupa 2-est, a bináris koordináta helyeken pedig $\lfloor b/2 \rfloor$ számú 0-t és $\lceil b/2 \rceil$ számú 1-est tartalmazó vektorra igaz, hogy $d(x, c_0) = t + \lceil b/2 \rceil$ és $d(x, c_1) = t + \lfloor b/2 \rfloor$, tehát a C^* kód elérési sugara legalább $t + \lfloor b/2 \rfloor$. $\square$

6.4. Állítás.

Ha egy bináris C kód 3 szóból, a kódszavak pedig b koordinátából állnak, akkor a kód elérési sugara legalább $\lfloor b/2 \rfloor$.

Bizonyítás. Megint elég a 6.2. állítás alkalmazásával adódó C^* kódra igazolni az állítást. Egy ilyen kód ekvivalens átrendezéssel

$$\begin{aligned} \{ & c_0 = (0, \dots, 0, 0, \dots, 0), \\ & c_1 = (1, \dots, 1, 1, \dots, 1), \\ & c_2 = (0, \dots, 0, 1, \dots, 1) \} \end{aligned}$$

alakra hozható, ahol c_2 -ben a 0-k száma kisebb az 1-esek számánál, vagy legfeljebb azzal egyenlő. A $\lfloor b/2 \rfloor$ számú 1-est és $\lceil b/2 \rceil$ számú 0-t tartalmazó $x = (1, \dots, 1, 0, \dots, 0)$ vektorra $d(x, c_0) = \lfloor b/2 \rfloor$, $d(x, c_1) = \lceil b/2 \rceil$ és $d(x, c_2) \geq \lfloor b/2 \rfloor$, tehát a C^* kód elérési sugara legalább $\lfloor b/2 \rfloor$. $\square$

6.5. Állítás.

Ha egy vegyes ternáris/bináris C kód 3 szóból, a kódszavak pedig 1 ternáris és b bináris koordinátából állnak, akkor a kód elérési sugara legalább $\lfloor (b+1)/2 \rfloor$.

Bizonyítás. Ismét a 6.2. állítás alkalmazásával adódó C^* kóddal foglalkozzunk. Egy ilyen kód ekvivalens átrendezéssel

$$\begin{aligned} \{ & c_0 = (0, 0, \dots, 0, 0, \dots, 0), \\ & c_1 = (1, 1, \dots, 1, 1, \dots, 1), \\ & c_2 = (2, 0, \dots, 0, 1, \dots, 1) \} \end{aligned}$$

alakra hozható, ahol c_2 -ben a 0-k száma kisebb az 1-esek számánál, vagy legfeljebb azzal egyenlő. Most a $\lfloor (b-1)/2 \rfloor$ számú 1-est és $\lceil (b+1)/2 \rceil$ számú 0-t tartalmazó $x = (2, 1, \dots, 1, 0, \dots, 0)$ vektorra $d(x, c_0) = \lfloor (b+1)/2 \rfloor$, $d(x, c_1) = \lceil (b+3)/2 \rceil$ és $d(x, c_2) \geq \lfloor (b+1)/2 \rfloor$, tehát a C^* kód elérési sugara legalább $\lfloor (b+1)/2 \rfloor$. $\square$

Az előkészítést a csak bináris, ill. csak ternáris koordinátákat tartalmazó kódok tárgyalása során használt 3.5. és 4.5. következményeknek a vegyes ternáris/bináris kódokra használható változatával folytatjuk, amely két állításból áll. Az alábbi lemma első állítása a ternáris koordináták számának, a második állítása pedig a bináris koordináták számának a változtatásával kapcsolatos.

6.6. Lemma. (vö. K. és Östergård [129], Theorem 3 és 4)

Ha $K(t, b - 2; R - 1) > M$ és $\sigma_2(b, 2) > M$, akkor $K(t, b; R) > M$.

Ha $K(t - 3, b; R - 2) > M$ és $\sigma_3(t, 3; 1) > M$, akkor $K(t, b; R) > M$.

Ennél valamivel többet mond az alábbi, két külön lemmában kimondott két állítás, ezért inkább az utóbbiakat bizonyítjuk.

6.7. Lemma.

Ha C vegyes ternáris/bináris kód legalább 2 bináris koordinátával, melynek elérési sugara R , és C kódszavainak bináris koordinátáiból álló kód nem 2-szűrjektív, akkor a 00, 01, 10, 11 értékpárok mindegyikét nem tartalmazó bármely két bináris koordináta törlésével olyan kódhoz jutunk, melynek elérési sugara legfeljebb $R - 1$.

Bizonyítás. Feltehetjük, hogy a két törölt koordináta az utolsó kettő. Ekkor $C = |C_1|C_2|$, ahol C_1 a két koordináta törlésével keletkező kód, C_2 pedig C -nek a két törölt koordinátához tartozó része. Jelöljük R_i -vel a C_i kód elérési sugarát. Mivel C_2 a 00, 01, 10, 11 párok mindegyikét nem tartalmazza, ezért $R_2 \leq 1$. Mivel a kódszavak összefűzésével származó kód elérési sugara nem lehet kisebb, mint a két összefűzött kód elérési sugarának összege, ezért $R_1 \leq R - R_2 \leq R - 1$. $\square$

6.8. Lemma.

Ha C vegyes ternáris/bináris kód legalább 3 ternáris koordinátával, melynek elérési sugara R , és C kódszavainak ternáris koordinátáiból álló kód nem általánosított 3-szűrjektív kód 1 sugárral, akkor C (a koordináták sorrendjének esetleges megváltoztatásával) felírható $C = |C_1|C_2|$ alakba, ahol C_1 három ternáris koordinátából áll, C_2 elérési sugara pedig legfeljebb $R - 2$.

Bizonyítás. Az általánosított szűrjektív kód definíciójából adódóan C -ben található 3 olyan koordináta, hogy C e három koordinátához tartozó C_1 részének az elérési sugara legalább 2. Az általánosság korlátozása nélkül feltehetjük, hogy C_1 a C kód első három koordinátájára épül, és legyen C_2 a többi koordinátára épülő rész. Ekkor $C = |C_1|C_2|$, és megint R_i -vel jelölve a C_i kód elérési sugarát, az előző bizonyításhoz hasonló érveléssel kapjuk, hogy $R_2 \leq R - R_1 \leq R - 2$. $\square$

Végül a következő állításban összefoglaljuk a $\sigma_q(n, s)$ és a $\sigma_q(n, s; r)$ függvénynek azokat az értékeit, melyekre néhány későbbi bizonyítás gondolatmenete során szükségünk lesz.

6.9. Állítás.

$\sigma_2(4, 2) = 5$, következésképpen $\sigma_2(b, 2) > 4$ ha $b \geq 4$;

$\sigma_2(5, 2) = 6$, következésképpen $\sigma_2(b, 2) > 5$ ha $b \geq 5$;

$\sigma_2(11, 2) = 7$, következésképpen $\sigma_2(b, 2) > 6$ ha $b \geq 11$;

$\sigma_2(16, 2) = 8$, következésképpen $\sigma_2(b, 2) > 7$ ha $b \geq 16$.

$\sigma_3(3, 3; 1) = 5$, következésképpen $\sigma_3(t, 3; 1) > 4$ ha $t \geq 3$;

$\sigma_3(4, 3; 1) = 6$, következésképpen $\sigma_3(t, 3; 1) > 5$ ha $t \geq 4$;

$\sigma_3(5, 3; 1) = 7$, következésképpen $\sigma_3(t, 3; 1) > 6$ ha $t \geq 5$;

$\sigma_3(11, 3; 1) = 8$, következésképpen $\sigma_3(t, 3; 1) > 7$ ha $t \geq 11$;

$\sigma_3(16, 3; 1) = 9$, következésképpen $\sigma_3(t, 3; 1) > 8$ ha $t \geq 16$.

A $\sigma_2(n, 2)$ kifejezés fenti értékeit a [27, 30, 31, 32] cikkek szerzői bizonyították, $\sigma_3(n, 3; 1)$ – a [145] cikkben közölt – fenti értékeit pedig java részt számítógépes vizsgálatokkal határoztuk meg.

A soron következő két lemma alapján a három kódszóból álló optimális térlefedő kódok teljes leírásához jutunk.

6.10. Lemma. (*K. és Östergård [129], Lemma 1*)

A

$$C = \{ c_0 = (0, \dots, 0, 0, \dots, 0), \\ c_1 = (1, \dots, 1, 1, \dots, 1), \\ c_2 = (2, \dots, 2, 1, \dots, 1) \} \subset Z_3^t Z_2^b$$

kód elérési sugara

$$\begin{cases} \lfloor \frac{2t+2b}{3} \rfloor & \text{ha } 2b \leq t, \\ \lfloor \frac{3t+2b}{4} \rfloor & \text{ha } 2b > t. \end{cases}$$

Bizonyítás. Legyen x a $Z_3^t Z_2^b$ tér tetszőleges pontja, és jelölje t_i (b_i) az i -vel egyenlő ternáris (bináris) koordináták számát. Ekkor $t_0 + t_1 + t_2 = t$, $b_0 + b_1 = b$, $d(x, c_0) = t_1 + t_2 + b_1$, $d(x, c_1) = t_0 + t_2 + b_0$, $d(x, c_2) = t_0 + t_1 + b_0$, és következésképpen

$$d(x, C) \leq \frac{d(x, c_0) + d(x, c_1) + d(x, c_2)}{3} = \frac{2t + 2b - b_1}{3} \leq \left\lfloor \frac{2t + 2b}{3} \right\rfloor.$$

Kaptunk tehát egy felső korlátot az elérési sugárra. Megmutatjuk, hogy $t \geq 2b$ esetén e kifejezés pontosan megadja az elérési sugarat. Ennek igazolásához legyen $b_0 = b$, $b_1 = 0$, $t_0 = \lceil (t - 2b)/3 \rceil$, $t_1 = t_2 = \lfloor (t + b)/3 \rfloor$, ha $t + b \equiv 0$ vagy $1 \pmod{3}$, ill. $b_0 = b$, $b_1 = 0$, $t_0 = \lfloor (t - 2b)/3 \rfloor$, $t_1 = t_2 = \lceil (t + b)/3 \rceil$, ha $t + b \equiv 2 \pmod{3}$.

Egy másik (súlyozott összeggel képezett) felső korlát

$$d(x, C) \leq \frac{2d(x, c_0) + d(x, c_1) + d(x, c_2)}{4} = \frac{3t + 2b - t_0}{4} \leq \left\lfloor \frac{3t + 2b}{4} \right\rfloor.$$

Ez viszont $t \leq 2b$ esetén egyenlőséggel teljesül, ha $b_0 = \lceil (2b + t)/4 \rceil$, $b_1 = \lfloor (2b - t)/4 \rfloor$, $t_0 = 0$, $t_1 = \lfloor t/2 \rfloor$ és $t_2 = \lceil t/2 \rceil$. $\square$

6.11. Lemma. (*K. és Östergård [129], Lemma 3*)

Megadott t és b esetén az ezen értékeknek megfelelő bármely 3 szóból álló kód elérési sugara legalább akkora, mint amekkora a 6.10. lemmában definiált kód elérési sugara.

Bizonyítás. A 6.2. állítás szerint feltételezhetjük, hogy a ternáris koordináta helyeken mindenütt 3, a bináris koordináta helyeken 2 különböző érték található a három kódszóban. Osszuk el a koordinátákat két ternáris és egy bináris koordinátát tartalmazó hármas csoportokba. Az egyes csoportoknak megfelelő vetület kódok nyilvánvalóan mind ekvivalensek a $\{000, 111, 221\}$ kóddal, melynek elérési sugara 2.

Képezzünk minél több ilyen csoportot, jelölje ezek számát g , a maradék ternáris, ill. bináris koordináták számát pedig t' , ill. b' . Ekkor a következő három eset lehetséges:

1. *eset.* $2b \leq t$. Ekkor $t' = t - 2g = t - 2b$ és $b' = 0$. Mivel egy 3 szóból álló és t' koordinátát tartalmazó ternáris kód elérési sugara legalább $\lfloor 2t'/3 \rfloor$, a $Z_3^t Z_2^b$ tér vizsgált kódjának elérési sugara legalább

$$2g + \left\lfloor \frac{2t'}{3} \right\rfloor = 2b + \left\lfloor \frac{2(t-2b)}{3} \right\rfloor = \left\lfloor \frac{2t+2b}{3} \right\rfloor.$$

Megjegyezzük, hogy ebben az esetben a vizsgált kód ekvivalens a 6.10. lemmában szereplő kóddal. A további két esetben azonban ez nem feltétlenül lesz így.

2. *eset.* $2b > t$ és t páros. Ekkor $t' = 0$ és $b' = b - g = b - t/2$. A 6.4. állítás alkalmazásával kapjuk, hogy a $Z_3^t Z_2^b$ tér vizsgált kódjának elérési sugara legalább

$$2g + \left\lfloor \frac{b'}{2} \right\rfloor = \left\lfloor t + \frac{b-t/2}{2} \right\rfloor = \left\lfloor \frac{3t+2b}{4} \right\rfloor.$$

3. *eset.* $2b > t$ és t páratlan. Ekkor $t' = 1$ és $b' = b - g = b - (t-1)/2$. A 6.5. állítás alkalmazásával kapjuk, hogy a $Z_3^t Z_2^b$ tér vizsgált kódjának elérési sugara legalább

$$\begin{aligned} 2g + \left\lfloor \frac{b'+1}{2} \right\rfloor &= 2(t-1)/2 + \left\lfloor \frac{b-(t-1)/2+1}{2} \right\rfloor = \\ &= \left\lfloor \frac{b+3(t-1)/2+1}{2} \right\rfloor = \left\lfloor \frac{b+(3t-1)/2}{2} \right\rfloor = \left\lfloor \frac{3t+2b}{4} \right\rfloor. \end{aligned}$$

(Emlékezzünk, hogy t most páratlan, tehát $3t+2b$ szintén páratlan.) □

A 6.1. állítás, valamint a 6.10. és 6.11. lemmák együttesen a következő tétel állítására vezetnek.

6.12. Tétel. (*K. és Östergård [129], Theorem 1 (c)*)

$K(t, b; R) = 3$ akkor és csak akkor áll fenn, ha

$$\min \left\{ \left\lfloor \frac{2t+2b}{3} \right\rfloor, \left\lfloor \frac{3t+2b}{4} \right\rfloor \right\} \leq R < t + \left\lfloor \frac{b}{2} \right\rfloor;$$

Négy kódszó esetére hasonlóan járunk el, először két lemmát bizonyítunk, majd az ehhez az esethez tartozó szükséges és elégséges feltételt tartalmazó tételre következtetünk.

6.13. Lemma. (*K. és Östergård [129], Lemma 2*)

A

$$C = \{ c_0 = (0, \dots, 0, 0, \dots, 0), \\ c_1 = (1, \dots, 1, 1, \dots, 1), \\ c_2 = (2, \dots, 2, 1, \dots, 1), \\ c_3 = (2, \dots, 2, 0, \dots, 0) \} \subset Z_3^t Z_2^b$$

kód elérési sugara

$$\left\lfloor \frac{2t}{3} + \frac{b}{2} \right\rfloor.$$

Bizonyítás. A t_i, b_i jelöléseket a 6.10. lemma bizonyításához hasonló módon értelmezve, tetszőleges $x \in Z_3^t Z_2^b$ pont esetén $d(x, c_0) = t_1 + t_2 + b_1$, $d(x, c_1) = t_0 + t_2 + b_0$, $d(x, c_2) = t_0 + t_1 + b_0$, $d(x, c_3) = t_0 + t_1 + b_1$, tehát

$$d(x, C) \leq \left\lfloor \frac{2d(x, c_0) + 2d(x, c_1) + d(x, c_2) + d(x, c_3)}{6} \right\rfloor = \left\lfloor \frac{4t + 3b}{6} \right\rfloor.$$

Annak igazolásához, hogy a kapott kifejezés pontosan megadja az elérési sugarat, válasszuk most a $b_0 = \lfloor b/2 \rfloor$, $b_1 = \lceil b/2 \rceil$, $t_0 = \lfloor (t+2)/3 \rfloor$, $t_1 = \lfloor t/3 \rfloor$, $t_2 = \lfloor (t+1)/3 \rfloor$ értékeket, helyettesítsük be ezeket a $d(x, c_i)$ kifejezésekbe, majd a paritások lehetséges kombinációira egyenként vizsgáljuk a kifejezések értékét. $\square$

A következő lemmával kissé eltérünk a [129] cikk gondolatmenetétől, hogy ezáltal a bizonyítás inkább az 5, 6 és 7 kódszóra vonatkozó eredmények bizonyításához hasonlítson, tehát az utóbbiakat készítjük ezzel elő.

6.14. Lemma.

$K(t, b; R) > 4$ fennáll, ha $R < \lfloor \frac{2t}{3} + \frac{b}{2} \rfloor$, kivéve azt az esetet, amikor $t = 0$, b pedig páros pozitív egész. Az utóbbi esetben a lehetséges legkisebb elérési sugár $R = b/2 - 1$.

Bizonyítás. Bontsuk fel a lemma állítását t és b paritása szerint. $K(t, b; R)$ monotonitása miatt elég az $R = \lfloor \frac{2t}{3} + \frac{b}{2} \rfloor - 1$ esettel foglalkozni. Ily módon a lemma bizonyításához a következő egyenlőtlenségeket kell bebizonyítani:

$$K(3u, 2v; 2u + v - 1) > 4, \text{ ha } u \geq 1 \text{ és } v \geq 0,$$

$$K(3u, 2v; 2u + v - 2) > 4, \text{ ha } u = 0 \text{ és } v \geq 2,$$

$$K(3u, 2v + 1; 2u + v - 1) > 4, \text{ ha } u \geq 0, v \geq 0 \text{ és } 2u + v - 1 \geq 0,$$

$$K(3u + 1, 2v; 2u + v - 1) > 4, \text{ ha } u \geq 0, v \geq 0 \text{ és } 2u + v - 1 \geq 0,$$

$$K(3u + 1, 2v + 1; 2u + v) > 4, \text{ ha } u \geq 0 \text{ és } v \geq 0,$$

$$K(3u + 2, 2v; 2u + v) > 4, \text{ ha } u \geq 0 \text{ és } v \geq 0,$$

$$K(3u + 2, 2v + 1; 2u + v) > 4, \text{ ha } u \geq 0 \text{ és } v \geq 0.$$

Az első paritási esetre a lemmában megadott kivétel miatt két egyenlőtlenséget kellett felírni.

Most a 6.6. lemma alkalmazásával (valamint a 6.9. állításban megadott adatok figyelembe vételével) a fenti egyenlőtlenségek mindegyikéről elmondhatjuk, hogy ha az teljesül az (u, v) értékpárra, akkor öröklődik az $(u + 1, v)$ értékpárra, és $v \geq 1$ esetén öröklődik az $(u, v + 1)$ értékpárra is. Ennélfogva elég a hét egyenlőtlenség közül az elsőt az $u = 1, v = 0$ és $u = 1, v = 1$ értékpárra, a másodikat az $u = 0, v = 2$ értékpárra, a harmadikat és a negyediket az $u = 0, v = 1$ és $u = 1, v = 0$ értékpárra, a hátralévőket pedig az $u = 0, v = 0$ és $u = 0, v = 1$ értékpárra bizonyítani, vagyis megmutatni, hogy a $K(3, 0; 1)$, $K(3, 2; 2)$, $K(0, 4; 0)$, $K(0, 3; 0)$, $K(3, 1; 1)$, $K(1, 2; 0)$, $K(4, 0; 1)$, $K(1, 1; 0)$, $K(1, 3; 1)$, $K(2, 0; 0)$, $K(2, 2; 1)$, $K(2, 1; 0)$, $K(2, 3; 1)$ értékek mind 4-nél nagyobbak, és ez valóban fennáll valamennyi esetben, lásd pl. [130] vagy [171] táblázataiban, ill. $R = 0$ elérési sugár esetén közvetlenül következik az (a) alatt megadott formula szerint.

A kivételes ($t = 0$, b páros pozitív egész) esetre vonatkozó állítást a bináris térlefedő kódok tárgyalása során már megindokoltuk. $\square$

A 6.1. állítás, valamint a 6.12. tétel, a 6.13. és 6.14. lemmák állításából a következő tétel állítására következtethetünk.

6.15. Tétel. (*K. és Östergård [129], Theorem 1 (d)*)

$K(t, b; R) = 4$ akkor és csak akkor áll fenn, ha

$$\left\lfloor \frac{2t}{3} + \frac{b}{2} \right\rfloor \leq R < \min \left\{ \left\lfloor \frac{2t + 2b}{3} \right\rfloor, \left\lfloor \frac{3t + 2b}{4} \right\rfloor \right\},$$

vagy pedig $t = 0$, b páros pozitív egész és $R = \frac{b}{2} - 1$.

Rátérünk öt kódszó esetére.

6.16. Lemma. (*vö. K. és Östergård [129], Lemma 5*)

Legyenek t , b pozitív egészek esetén, melyekre t osztható 3-mal, b pedig páros. Ekkor

$$K(t, b; \frac{2t}{3} + \frac{b}{2} - 1) = 5.$$

Bizonyítás. Megmutatjuk, hogy a

$$\begin{aligned} C = \{ & c_0 = (0, \dots, 0, 0, \dots, 0, 0), \\ & c_1 = (1, \dots, 1, 1, \dots, 1, 1), \\ & c_2 = (1, \dots, 1, 1, \dots, 1, 0), \\ & c_3 = (2, \dots, 2, 1, \dots, 1, 1), \\ & c_4 = (2, \dots, 2, 0, \dots, 0, 1) \} \subset Z_3^t Z_2^b \end{aligned}$$

kód elérési sugara

$$\left\lfloor \frac{2t}{3} + \frac{b}{2} \right\rfloor - 1.$$

Legyen megint x a $Z_3^t Z_2^b$ tér tetszőleges pontja, és a korábbiakhoz hasonlóan jelölje t_i (b_i) az i -vel egyenlő ternáris (bináris) koordináták számát, azzal a módosítással, hogy b_i értékében az utolsó koordinátát nem vesszük figyelembe. Ezért jelölje külön b'_i az utolsó koordinátára vonatkozó hasonló mennyiséget. (Tehát $b'_i = i$, ha x utolsó koordinátája 1, és $b'_i = 1 - i$, ha x utolsó koordinátája 0.)

E jelölésekkel fennáll $d(x, c_0) = t_1 + t_2 + b_1 + b'_1$, $d(x, c_1) = t_0 + t_2 + b_0 + b'_0$, $d(x, c_2) = t_0 + t_2 + b_0 + b'_1$, $d(x, c_3) = t_0 + t_1 + b_0 + b'_0$, $d(x, c_4) = t_0 + t_1 + b_1 + b'_0$, és következésképpen

$$d(x, C) \leq \left\lfloor \frac{2d(x, c_0) + d(x, c_1) + d(x, c_2) + d(x, c_3) + d(x, c_4)}{6} \right\rfloor = \left\lfloor \frac{2t}{3} + \frac{b}{2} \right\rfloor.$$

Mivel $2t$ osztható 3-mal, b pedig páros, a kapott egyenlőtlenség akkor és csak akkor teljesülhet egyenlőséggel, ha $d(x, c_0) = \dots = d(x, c_4)$. Viszont $d(x, c_1) = d(x, c_2)$ esetén $b'_0 = b'_1$ adódik, ami $b'_0 + b'_1 = 1$ miatt lehetetlen. Ezért

$$d(x, C) \leq \frac{2t}{3} + \frac{b}{2} - 1,$$

amiből pedig következik, hogy

$$K(t, b; \frac{2t}{3} + \frac{b}{2} - 1) \leq 5.$$

A fordított irányú egyenlőtlenség a 6.14. lemmából következik, ami egyúttal azt is bizonyítja, hogy a C kód elérési sugara a megadott kifejezésnél kisebb nem lehet. $\square$

Megjegyzés. A 6.16. lemma előzménye, hogy a $t = 3$ speciális esetre vonatkozó állítást Kolev és Landgev [84] már korábban bizonyították.

6.17. Lemma.

A 4.6. tételben ($K(3, 0; 1) = 5$) és a 6.16. lemmában megadott két eseten kívül nincs más olyan eset, amelyre $K(t, b; R) = 5$.

Bizonyítás. A 6.14. lemma bizonyításának a menetét követjük, és a $K(t, b; R) > 5$ egyenlőtlenséget bizonyítjuk az alábbi esetekre bontva:

$$K(3u, 2v; 2u + v - 1) > 5, \text{ ha } u \geq 2 \text{ és } v = 0,$$

$$K(3u, 2v; 2u + v - 2) > 5, \text{ ha } u \geq 0, v \geq 0 \text{ és } 2u + v - 2 \geq 0,$$

$$K(3u, 2v + 1; 2u + v - 1) > 5, \text{ ha } u \geq 0, v \geq 0 \text{ és } 2u + v - 1 \geq 0,$$

$$K(3u + 1, 2v; 2u + v - 1) > 5, \text{ ha } u \geq 0, v \geq 0 \text{ és } 2u + v - 1 \geq 0,$$

$$K(3u + 1, 2v + 1; 2u + v) > 5, \text{ ha } u \geq 0 \text{ és } v \geq 0,$$

$$K(3u + 2, 2v; 2u + v) > 5, \text{ ha } u \geq 0 \text{ és } v \geq 0,$$

$$K(3u + 2, 2v + 1; 2u + v) > 5, \text{ ha } u \geq 0 \text{ és } v \geq 0.$$

Az első egyenlőtlenség itt úgy adódott, hogy a 6.14. lemma bizonyításában szereplő hasonló egyenlőtlenségből elhagytuk azokat az eseteket, amelyekre már azt tudjuk, hogy $K(t, b; R) = 5$. Ezek elhagyása miatt bizonyítani kell az 1-gyel csökkentett elérési sugárra vonatkozó hasonló egyenlőtlenséget, amit viszont összevonhatunk a korábbi második (de 4 helyett 5 jobb oldallal felírt) hasonló egyenlőtlenséggel.

Ismét a 6.6. lemma alkalmazásával és a 6.9. állításban megadott adatok figyelembe vételével vizsgáljuk a felsorolt egyenlőtlenségek öröklődését. Ennek alapján megállapítható, hogy az első egyenlőtlenséget elég az $u = 2, v = 0$ értékpárra, a másodikat az $u = 0, v = 2$; $u = 1, v = 0$; $u = 1, v = 1$ és $u = 1, v = 2$ értékpárookra, a harmadikat az $u = 0, v = 1$; $u = 1, v = 0$ és $u = 1, v = 1$ értékpárookra, a negyediket az $u = 0, v = 1$ és $u = 0, v = 2$ értékpárookra, az ötödiket és a hetediket az $u = 0, v = 0$ és $u = 0, v = 1$ értékpárookra, a hatodikat pedig az $u = 0, v = 0$; $u = 0, v = 1$ és $u = 0, v = 2$ értékpárookra bizonyítani, vagyis megmutatni, hogy a $K(6, 0; 3)$, $K(0, 4; 0)$, $K(3, 0; 0)$, $K(3, 2; 1)$, $K(3, 4; 2)$, $K(0, 3; 0)$, $K(3, 1; 1)$, $K(3, 3; 2)$, $K(1, 2; 0)$, $K(1, 4; 1)$, $K(1, 1; 0)$, $K(1, 3; 1)$, $K(2, 0; 0)$, $K(2, 2; 1)$, $K(2, 4; 2)$, $K(2, 1; 0)$, $K(2, 3; 1)$ értékek mind 5-nél nagyobbak, ami ismét a [130] vagy [171] táblázataiban található értékek, ill. $R = 0$ elérési sugár esetén közvetlenül, az (a) alatt megadott formula alapján verifikálható.

A bizonyításhoz figyelembe vehetjük a (6.1), (6.2) és (6.5) alatt megadott egyenlőtlenségeket, mivel ezek alkalmazása lehetővé teszi az ellenőrzendő egyedi esetek számának csökkentését. $\square$

Az eddigiekből következik az alábbi tétel állítása.

6.18. Tétel. *(K. és Östergård [129], Theorem 11)*

$K(t, b; R) = 5$ akkor és csak akkor áll fenn, ha t hárommal osztható pozitív egész, b páros pozitív egész és $R = \frac{2t}{3} + \frac{b}{2} - 1$, vagy pedig $t = 3$, $b = 0$ és $R = 1$.

Hat és hét kódszó esetére is először néhány kód család kódjainak optimalitását bizonyítjuk.

6.19. Lemma. *(K. és Östergård [129], Theorem 13)*

Legyen $t = 3u + 1$ alakú, $b = 2v + 1$ alakú pozitív egész. Ekkor

$$K(t, b; \frac{2t-2}{3} + \frac{b-1}{2}) = K(3u+1, 2v+1; 2u+v) = 6.$$

Bizonyítás. Megmutatjuk, hogy a

$$\begin{aligned} C = \{ & c_0 = (0, \dots, 0, 0, \dots, 0), \\ & c_1 = (0, \dots, 0, 1, \dots, 1), \\ & c_2 = (1, \dots, 1, 0, \dots, 0), \\ & c_3 = (1, \dots, 1, 1, \dots, 1), \\ & c_4 = (2, \dots, 2, 0, \dots, 0), \\ & c_5 = (2, \dots, 2, 1, \dots, 1) \} \subset Z_3^t Z_2^b \end{aligned}$$

kód elérési sugara

$$\left\lfloor \frac{2t}{3} \right\rfloor + \left\lfloor \frac{b}{2} \right\rfloor.$$

A t_i és b_i mennyiségeket a korábbi esetekhez hasonló módon értelmezve azt kapjuk, hogy tetszőleges $x \in Z_3^t Z_2^b$ esetén $d(x, c_0) = t_1 + t_2 + b_1$, $d(x, c_1) = t_1 + t_2 + b_0$, $d(x, c_2) = t_0 + t_2 + b_1$, $d(x, c_3) = t_0 + t_2 + b_0$, $d(x, c_4) = t_0 + t_1 + b_1$, $d(x, c_5) = t_0 + t_1 + b_0$.

A felírt egyenlőségekből következik, hogy

$$\begin{aligned} d(x, C) &\leq \\ &\leq \min \left\{ \left\lfloor \frac{d(x, c_0) + d(x, c_2) + d(x, c_4)}{3} \right\rfloor, \left\lfloor \frac{d(x, c_1) + d(x, c_3) + d(x, c_5)}{3} \right\rfloor \right\} = \\ &= \min \left\{ \left\lfloor \frac{2t}{3} + b_1 \right\rfloor, \left\lfloor \frac{2t}{3} + b_0 \right\rfloor \right\} = \left\lfloor \frac{2t}{3} \right\rfloor + \min\{b_1, b_0\} \leq \left\lfloor \frac{2t}{3} \right\rfloor + \left\lfloor \frac{b}{2} \right\rfloor = 2u + v, \end{aligned}$$

és ennél fogva

$$K(3u + 1, 2v + 1; 2u + v) \leq 6.$$

A fordított irányú egyenlőtlenség a 6.18. tételből következik. Ezzel bizonyítást nyert az is, hogy a C kód elérési sugara a megadott kifejezéssel egyenlő. $\square$

6.20. Lemma. (*Kolev és Landgev [84], Proposition 3.3*)

$K(2, 2v; v) = 6$ fennáll tetszőleges pozitív egész v esetén.

6.21. Lemma. (*K. és Östergård [145], Theorem 6*)

$K(3u + 2, 2v; 2u + v) = 7$, ha $u \geq 1$ és $v \geq 1$.

Bizonyítás. Megmutatjuk, hogy a

$$\begin{aligned} C = \{ &c_0 = (0, 0, \dots, 0, 0, \dots, 0, 0), \\ &c_1 = (0, 2, \dots, 2, 0, \dots, 0, 1), \\ &c_2 = (0, 2, \dots, 2, 1, \dots, 1, 0), \\ &c_3 = (1, 0, \dots, 0, 0, \dots, 0, 0), \\ &c_4 = (1, 1, \dots, 1, 1, \dots, 1, 1), \\ &c_5 = (2, 0, \dots, 0, 1, \dots, 1, 1), \\ &c_6 = (2, 1, \dots, 1, 0, \dots, 0, 0) \} \subset Z_3 Z_3^{3u+1} Z_2^{2v-1} Z_2 \end{aligned}$$

kód elérési sugara $2u + v$.

A C kód szavaiban itt az első (ternáris) és az utolsó (bináris) koordinátát elkülönítettük. Tetszőleges $x \in Z_3^{3u+2} Z_2^{2v}$ pont esetén az első és az utolsó koordinátát hasonló módon elkülönítve, jelölje t_i (b_i) a közbeeső helyeken lévő i -vel egyenlő ternáris (bináris) koordináták számát, melyekre a jelenlegi esetben $t_0 + t_1 + t_2 = 3u + 1$ és $b_0 + b_1 = 2v - 1$. Most x első és utolsó koordinátájának lehetséges értékeire egyenként vizsgáljuk x -nek a C kódtól való távolságát.

Ha x első és utolsó koordinátája is 0, akkor

$$d(x, C) \leq \frac{d(x, c_1) + d(x, c_3) + d(x, c_6)}{3} = \frac{2(t_0 + t_1 + t_2) + 3b_1 + 3}{3} = 2u + b_1 + \frac{5}{3}$$

és

$$d(x, C) \leq \frac{d(x, c_2) + d(x, c_4) + d(x, c_5)}{3} = \frac{2(t_0 + t_1 + t_2) + 3b_0 + 4}{3} = 2u + b_0 + 2.$$

E két egyenlőtlenségből következik, hogy

$$d(x, C) \leq 2u + \min\{b_0, b_1\} + 2 \leq 2u + (v - 1) + 2 = 2u + v + 1.$$

Tegyük fel, hogy $d(x, C) = 2u + v + 1$. Ez csak úgy lehetséges, ha $b_0 = v - 1$ és $b_1 = v$. Ekkor viszont $d(x, c_2) = d(x, c_4) = d(x, c_5)$, és következésképpen $t_0 = t_1 = u + 1$ és $t_2 = u - 1$. A t_i -k és b_i -k ezen értékrendszere esetén azonban $d(x, c_0) = 2u + v$.

Ha x első koordinátája 0, utolsó koordinátája pedig 1, akkor hasonló gondolatmenetet alkalmazhatunk, azonban a gondolatmenet végén $b_0 = v$ -re és $b_1 = v - 1$ -re, utána viszont megint $t_0 = t_1 = u + 1$ -re és $t_2 = u - 1$ -re következtethetünk. Erre az értékrendszerre megint $d(x, c_0) = 2u + v$ teljesül.

Ha x első koordinátája 1, utolsó koordinátája pedig 0, akkor megint hasonló gondolatmenettel $b_0 = v - 1$ -re és $b_1 = v$ -re jutunk, viszont most a $d(x, c_2) = d(x, c_4) = d(x, c_5)$ egyenlőségekből $t_1 = t_2 = u$ és $t_0 = u + 1$ adódik. Erre az értékrendszerre pedig $d(x, c_3) = 2u + v$ teljesül. Ugyanígy történhet a bizonyítás a még hátralévő esetekre is, vagy figyelembe véve, hogy a c_0 kódszót most nem használtuk a bizonyításhoz, a c_0 elhagyásával adódó kód szimmetriájára is hivatkozhatunk.

Ezzel beláttuk, hogy a C kód elérési sugara legfeljebb $2u + v$ lehet. A bizonyítás eddigi részében felírt bármelyik t_i , b_i értékrendszerre kiszámítva egy ilyen értékrendszerhez tartozó x pontnak minden egyes kódszótól való távolságát, azt kapjuk, hogy $d(x, C) = 2u + v$, tehát C elérési sugara is pontosan ennyi. Ebből még csak az következik ugyan, hogy $K(3u + 2, 2v; 2u + v) \leq 7$ minden pozitív egész u és v esetén, a fordított egyenlőtlenség azonban következik a 6.14. és a 6.17. lemmából. $\square$

Most megfogalmazzuk az ismert feltételek összességének szükségességét hat és hét kódszó esetére.

6.22. Lemma. (*K. és Östergård [145], Theorem 5 és 7*)

A 4.6. tételben $(K(\frac{3R+3}{2}, 0; R) = 6$ ha $R \geq 3$, páratlan), valamint a 6.19 és 6.20. lemmákban megadott két eseten kívül nincs más olyan eset, amelyre $K(t, b; R) = 6$.

A 3.9. tételben $(K(0, 2R + 3; R) = 7$ ha $R \geq 1$, páratlan), valamint a 6.21. lemmában megadott két eseten kívül nincs más olyan eset, amelyre $K(t, b; R) = 7$.

A 6.22. lemma mindkét állítása bizonyításának menete lényegében azonos a 6.14. és 6.17. lemmák bizonyításával analóg, csak azoknál bonyolultabb és már számítógép intenzív használatát is igényli, különösen a 7 szavas kódokra vonatkozó állítás, melynek

számítógépes bizonyításához kb. 150 millió kód elérési sugarának az ellenőrzésére volt szükség. Ezért a bizonyítást területi ok miatt elhagyjuk. A bizonyítás részleteit angol nyelven a [145] cikk, magyar nyelven a [167] monográfia tartalmazza.

A 6.22. lemma állítását áttekinthetőbb formában mutatja az alábbi tétel.

6.23. Tétel.

$K(t, b; R) = 6$ akkor és csak akkor áll fenn, ha t ötnél nagyobb, hárommal osztható egész, $b = 0$ és $R = \frac{2t}{3} - 1$, vagy $t - 1$ hárommal osztható nemnegatív egész, b páratlan pozitív egész és $R = \frac{2t-2}{3} + \frac{b-1}{2}$, vagy pedig $t = 2$, b páros pozitív egész és $R = \frac{b}{2}$;

$K(t, b; R) = 7$ akkor és csak akkor áll fenn, ha $t = 0$, b háromnál nagyobb páratlan egész és $R = \frac{b-3}{2}$, vagy pedig $t - 2$ hárommal osztható pozitív egész, b páros pozitív egész és $R = \frac{2t-4}{3} + \frac{b}{2}$.

Nyolc, kilenc vagy annál is több kódszó esetére már csak optimális kódok néhány esetét tudjuk megadni, de nem tudunk válaszolni arra a kérdésre, hogy ezeken az eseteken kívül további nyolc szavas (kilenc szavas stb.) vegyes ternáris/bináris optimális térlefedő kódok léteznek-e.

6.24. Tétel. (*K. és Östergård [145], Theorem 10, 11 és 12*)

$$K(1, 2v; v - 1) = 8 \text{ ha } v \geq 2,$$

$$K(3u, 2v + 1; 2u + v - 1) = 8 \text{ ha } u \geq 1 \text{ és } v \geq 1,$$

$$K(5, 0; 2) = 8.$$

Bizonyítás. Az eddigiekből következik, hogy az első két eset mindegyikében az egyenlőség jelét a nagyobb vagy egyenlő jellel helyettesítve fennállnak az így kapott egyenlőtlenségek. Az első esetben a fordított egyenlőtlenség az ismert $K(1, 4, 1) = 8$ egyenlőségből, s az ehhez tartozó optimális kódok bináris koordinátában való normalitásából következik. (Alkalmazzuk valamelyik optimális kódra az ADS konstrukciónak azt a speciális esetét, ahol a konstrukció másik elemét képező kód páratlan dimenziós ismétléses kód.)

A második esetben tekintsük először a hat kódszóból álló

$$C = \bigcup_{i \in Z_3, j \in Z_2} |c_{i,j}|d_{i,j}|,$$

kódot, ahol $c_{i,j} = (i, \dots, i, j, \dots, j) \in Z_3^{3u} Z_2^{2v-1}$, $d_{0,0} = d_{1,1} = 00$, $d_{0,1} = d_{1,0} = 11$, $d_{2,0} = 01$, és $d_{2,1} = 10$ ($d_{i,j} \in Z_2^2$). Tetszőleges $x \in Z_3^{3u} Z_2^{2v+1}$ esetén jelölje t_i az i -vel egyenlő ternáris koordináták számát, b_i pedig a két utolsó koordinátán kívüli i -vel egyenlő bináris koordináták számát.

Ha most $t_i > u + 1$ valamely i -re, akkor van olyan j , melyre $d(x, |c_{i,j}|d_{i,j}|) \leq (2u - 2) + (v - 1) + 2 = 2u + v - 1$.

Ha $t_i = u + 1$ és $b_j > v$ valamely i, j párra, akkor $d(x, |c_{i,j}|d_{i,j}|) \leq (2u - 1) + (v - 2) + 2 = 2u + v - 1$.

Ha $t_i = u + 1$ és $b_j = v$ valamely i, j párra, akkor $d(x, |c_{i,j}|d_{i,j}|) \leq (2u - 1) + (v - 1) + 1 = 2u + v - 1$, kivéve azt az esetet, ha x két utolsó koordinátájának mindegyike $d_{i,j}$ -től eltér, vagyis $d_{i,1-j}$ -vel egyezik. Az utóbbi esetben $d(x, |c_{i,1-j}|d_{i,1-j}|) \leq (2u - 1) + v + 0$.

Ha $t_0 = t_1 = t_2 = u$ és $b_j > v$ valamely j -re, akkor van olyan i , melyre fennáll $d(x, |c_{i,j}|d_{i,j}|) \leq 2u + (v - 2) + 1$.

Végül ha $t_0 = t_1 = t_2 = t$ és $b_j = b + 1$, akkor $d(x, |c_{i,j}|d_{i,j}|) \leq 2u + (v - 1) + 0$ fennáll valamely i -re, feltéve, hogy i választható úgy, hogy x két utolsó koordinátája $d_{i,j}$ legyen. Ilyen i csak akkor nem választható, ha $j = 0$ és x két utolsó koordinátája 10, vagy $j = 1$ és x két utolsó koordinátája 01. A további két kódszóval kibővített $C \cup \{2 \dots 20 \dots 010, 2 \dots 21 \dots 101\}$ kód már megoldja ezt a problémát, e 8-szavas kód elérési sugara tehát $2u + v - 1$.

A harmadik esettel a ternáris térlefedő kódok fejezetében már foglalkoztunk. □

Megjegyzés. Ha zéró elérési sugarat is figyelembe veszünk, akkor még egy esetet említhetünk, a $K(0, 3; 0) = 8$ esetet.

A továbbiakban a kilenc vagy annál több kódszó esetére ismert vagy (többnyire számítógéppel bizonyított) új eredményeket bizonyítás nélkül felsoroljuk.

6.25. Tétel. (*K. és Östergård [145], Theorem 9, 13 és 14, ill. Hamming kód*)

$$K(3u + 2, 0; 2u) = 9 \quad \text{ha } u \geq 2,$$

$$K(3u, 1; 2u - 1) = 9 \quad \text{ha } 1 \leq u \leq 3,$$

$$K(4, 0; 1) = 9.$$

Megjegyzés. Ha zéró elérési sugarat is figyelembe veszünk, akkor itt is még egy esetet említhetünk, a $K(2, 0; 0) = 9$ esetet.

Az eddig tárgyaltakon kívül $K(t, b; R)$ pontos értékét még egy kód családra és több szórványos esetre ismerjük. A ternáris Hamming kódoknak 1 bináris koordinátával történő kiegészítéseire vonatkozik a következő eset:

6.26. Tétel. (*Bertolo és szerzőtársai [130], Corollary 2.1*)

$$K\left(\frac{3^h - 1}{2}, 1; 1\right) = 2 \cdot 3^{\frac{3^h - 1}{2} - h} \quad \text{minden } h \geq 2 \text{ esetén.}$$

Szórványos esetek, melyekre $K(t, b; R)$ értékét korábban is ismertük:

6.27. Állítás.

$$\begin{array}{lll} K(4, 2; 2) = 10, & K(4, 4; 3) = 10, & K(2, 5; 2) = 11, \\ K(2, 7; 3) = 11, & K(1, 7; 2) = 12, & K(1, 9; 3) = 12, \\ K(2, 3; 1) = 12, & K(5, 1; 2) = 12, & K(3, 4; 2) = 13, \\ K(1, 5; 1) = 16, & K(2, 6; 2) = 16, & K(3, 2; 1) = 16, \\ K(2, 4; 1) = 20, & K(1, 6; 1) = 24, & K(3, 3; 1) = 24, \\ K(4, 2; 1) = 36. & & \end{array}$$

Két új, számítógéppel bizonyított, eddig még nem publikált esetet adunk meg a következő tételben.

6.28. Tétel.

$$K(3, 6; 3) = 12 \text{ és } K(1, 8; 2) = 20.$$

6.5. Klasszifikációs eredmények vegyes térlefedő kódokra

Két triviális esettel kezdjük.

$R = 0$ esetén csak a $Z_3^t Z_2^b$ tér összes pontjából álló kód optimális, tehát az inekvivalens optimális kódok száma bármely t és b esetén 1.

$R = t + b$ esetén az optimális kódok 1 kódszóból állnak, az egyszavas kódok pedig nyilván valamennyien ekvivalensek egymással, tehát az inekvivalens optimális kódok száma ilyenkor is 1.

A következő állítás elemi úton bizonyítható.

6.29. Tétel.

Ha $t > 0$, b páratlan pozitív egész és $R = t + \frac{b-1}{2}$, akkor $t + 1$ inekvivalens optimális kód létezik:

$$\left\{ \begin{array}{l} (0, \dots, 0, 0, \dots, 0), \\ (0, \dots, 0, 1, \dots, 1) \end{array} \right\} \quad \left\{ \begin{array}{l} (0, \dots, 0, 0, \dots, 0), \\ (0, \dots, 1, 1, \dots, 1) \end{array} \right\} \quad \cdots \quad \left\{ \begin{array}{l} (0, \dots, 0, 0, \dots, 0), \\ (1, \dots, 1, 1, \dots, 1) \end{array} \right\}$$

A felsorolt kódokban a ternáris koordináták állnak elől. Az első kódszóban minden ternáris és minden bináris koordináta értéke 0. A második kódszavakat viszont úgy adtuk meg, hogy az i -edik kódban ott $t + 1 - i$ számú 0 és $i - 1$ számú 1 értékű ternáris koordináta helyezkedik el, a bináris koordináták értéke pedig végig 1. *Bizonyítás.* Könnyű belátni, hogy a megadott t , b , R paraméterek esetén egy kétszavas $C \in Z_3 Z_2^b$ kód akkor és csak akkor optimális, ha az összes bináris koordináta értéke a két kódszóban különböző, tehát a bináris koordinátákból álló rész ekvivalens a csupa 0 és csupa 1

értékű koordinátából álló kóddal. Ezért csak a ternáris koordináták értékétől függően kapunk különböző (inekvivalens) kódokat. $\square$

A következő esetre vonatkozó állítást teljes indukcióval bizonyítjuk.

6.30. Tétel.

Ha $t = 1$, b páros pozitív egész és $R = \frac{b}{2}$, akkor ekvivalenciától eltekintve az alábbi egyetlen optimális kód létezik:

$$\{ (0, 0, \dots, 0), \\ (1, 1, \dots, 1), \\ (2, 1, \dots, 1) \}.$$

Bizonyítás. A 6.10. és a 6.11. lemmából következik, hogy a megadott kód optimális. Bebizonyítjuk először $b = 2$ -re, hogy nincs más optimális kód.

Egy optimális kód szavaiban a ternáris koordináta-helyen három különböző értéknek kell állnia, mert ellenkező esetben a két bináris koordináta-helyen a 00, 01, 10, 11 variációk mindegyikének elő kellene fordulnia, ami 3 kódszó esetén lehetetlen. Ezért tetszőleges optimális kód ekvivalens egy

$$\{ (0, 0, 0), \\ (1, *, *), \\ (2, *, *) \}$$

alakú kóddal, ahol a csillagok helyén egyelőre még 0 vagy 1 is állhat. Most az $x = (0, 1, 1) \in Z_3 Z_2^2$ pont $R = 1$ sugárral történő fedéséhez szükség van egy $(*, 1, 1)$ alakú kódszóra, feltehetjük, hogy ez a harmadik kódszó, amely így $(2, 1, 1)$ -re véglegesíthető. Ekkor az $(1, 0, 1)$ és $(1, 1, 0)$ pontok mindegyikének $R = 1$ sugárral történő fedéséhez a középső kódszóban a kicsillagozott két helyen két azonos értéknek kell állnia. Akár két 0-t, akár két 1-et teszünk a csillagok helyére, a kapott kód 0-k esetén ekvivalens, 1-esek esetén azonos a tételben megadott kóddal.

Rátérünk az indukciós lépésre, melynek kiindulásaként feltesszük, hogy igaz az állítás $b = 2v$ esetén, és megmutatjuk, hogy az optimális kód unicitására vonatkozó állítás $b = 2v$ -ról öröklődik $b = 2v + 2$ -re.

Legyen C egy, a $b = 2v + 2$, $R = v + 1$ paraméterekhez tartozó optimális kód. A 6.7. lemma szerint C -ből két bináris koordináta elhagyásával keletkező kód $t = 1$ ternáris és $b = 2v$ bináris koordinátát tartalmazó kód, melynek elérési sugara legfeljebb v . Esetünkben az elérési sugár pontosan v , ennél kisebb ugyanis a 6.11. lemma szerint nem lehet. Ugyanezen lemma szerint a kapott kód optimális, így az indukciós feltevés miatt ekvivalens a bizonyítandó tételben megadott kóddal. Ebből következik, hogy a $b = 2v + 2$ dimenzióhoz tartozó optimális kód ekvivalenciától eltekintve

$$\{ (0, 0, \dots, 0, *, *), \\ (1, 1, \dots, 1, *, *), \\ (2, 1, \dots, 1, *, *) \}.$$

alakban felírható. Az első kódszóban lévő csillagok helyére az általánosság csorbítása nélkül 0-kat írhatunk, ezt követően a további 4 csillag karakter 0-val vagy 1-gyel való

helyettesítésére 16 lehetséges variáció marad, de ezek csak 7 inekvivalens esetet eredményeznek. (Semmi, egy, három vagy négy 1-essel egy-egy esetet, két 1-essel pedig három különböző esetet kapunk.)

Megmutatjuk, hogy 7 közül 6 esetben a kapott kód elérési sugara $(v + 1)$ -nél nagyobb. Az egyes esetekhez tartozó kódokat a $v = 3$ esetre, vagyis $b = 8$ -ra és $R = 4$ -re írjuk fel, de az indoklást az általános esetre is megadjuk.

Tekintsük először az alábbi 4 kódot:

$$\begin{array}{ll} \{ (0, 0, 0, 0, 0, 0, 0, 0, 0), & \{ (0, 0, 0, 0, 0, 0, 0, 0, 0), \\ (1, 1, 1, 1, 1, 1, 1, 0, 0), & (1, 1, 1, 1, 1, 1, 1, 0, 0), \\ (2, 1, 1, 1, 1, 1, 1, 0, 0) \} & (2, 1, 1, 1, 1, 1, 1, 0, 1) \} \\ \\ \{ (0, 0, 0, 0, 0, 0, 0, 0, 0), & \{ (0, 0, 0, 0, 0, 0, 0, 0, 0), \\ (1, 1, 1, 1, 1, 1, 1, 0, 1), & (1, 1, 1, 1, 1, 1, 1, 0, 1), \\ (2, 1, 1, 1, 1, 1, 1, 0, 1) \} & (2, 1, 1, 1, 1, 1, 1, 1, 0) \} \end{array}$$

A fenti négy kód esetén a tér $(0, 0, 0, 0, 1, 1, 1, 1, 1)$ pontja ezektől 4-nél nagyobb távolságra van. Az általános esetben tekintsük azt az $x \in Z_3 Z_2^{2v+2}$ pontot, amelyben $v + 1$ számú 0 értékű koordinátát $v + 2$ számú 1 értékű koordináta követ. E pontnak a fenti típusú kódoktól való távolsága $v + 1$ -nél nagyobb, tehát a felsorolt kódok nem lehetnek optimálisak. Hasonlóan mutatható meg a

$$\{ (0, 0, 0, 0, 0, 0, 0, 0, 0), \\ (1, 1, 1, 1, 1, 1, 1, 0, 0), \\ (2, 1, 1, 1, 1, 1, 1, 1, 1) \}$$

kód esetén az $(1, 0, 0, 0, 0, 1, 1, 1, 1)$ pont, általános esetben az 1-gyel kezdődő, majd először $v + 1$ számú 0-val, utána pedig $v + 1$ számú 1-essel folytatódó pont használatával, a

$$\{ (0, 0, 0, 0, 0, 0, 0, 0, 0), \\ (1, 1, 1, 1, 1, 1, 1, 0, 1), \\ (2, 1, 1, 1, 1, 1, 1, 1, 1) \}$$

kód esetén pedig az $(1, 0, 0, 0, 1, 1, 1, 1, 0)$ pont, általános esetben az 1-gyel kezdődő, majd először v számú 0-val, utána pedig $v + 1$ számú 1-essel folytatódó, és 0-val befejeződő pont használatával, hogy ezek a kódok sem optimálisak. Egyetlen optimális kódnak marad a 7 lehetőség közül eddig konkrétan még nem említett

$$\{ (0, 0, 0, 0, 0, 0, 0, 0, 0), \\ (1, 1, 1, 1, 1, 1, 1, 1, 1), \\ (2, 1, 1, 1, 1, 1, 1, 1, 1) \}$$

kód.

□

Ugyancsak teljes indukcióval bizonyítható a most következő állítás is.

6.31. Tétel.

Ha $t = 3$, b páratlan pozitív egész és $R = \frac{b+3}{2}$, akkor ekvivalenciától eltekintve az alábbi egyetlen optimális kód létezik:

$$\{ (0, 0, 0, 0, \dots, 0), \\ (1, 1, 1, 0, \dots, 0), \\ (2, 2, 2, 1, \dots, 1) \}$$

Bizonyítás. Az előző tétel bizonyításához hasonló módon mutatható meg, hogy a megadott kód optimális. Könnyű belátni, hogy $b = 1$ esetén – ekvivalenciától eltekintve – nincs más optimális kód.

Rátérve az indukciós lépésre, feltesszük hogy igaz az állítás $b = 2v + 1$ esetén, és megmutatjuk, hogy az optimális kód unicitására vonatkozó állítás $b = 2v + 1$ -ről öröklődik $b = 2v + 3$ -ra, ha $v \geq 1$.

Legyen C egy, a $b = 2v + 3$, $R = v + 3$ paraméterekhez tartozó optimális kód. A 6.7. lemma szerint C -ből két bináris koordináta elhagyásával keletkező kód olyan $t = 3$ ternáris és $b = 2v + 1$ bináris koordinátát tartalmazó kód, melynek elérési sugara legfeljebb $v + 2$. Az előző bizonyításhoz hasonlóan kapjuk, hogy az elérési sugár pontosan $v + 2$. Az indukciós feltevés miatt a kapott kód ekvivalens a bizonyítandó tételben megadott kóddal. Ebből az is következik, hogy C kódszavaiban a bináris koordináták legfeljebb 2 koordináta kivételével azonosak. (Mindhárom kódszóban vagy csupa 0, vagy csupa 1.) Mivel ez bármely két bináris koordináta elhagyásával adódó kódra fennáll, ezért $v \geq 2$ esetén (amikor a redukció után még legalább 3 bináris koordináta marad) ebből következik, hogy a kiindulásul vett C kód szavaiban is a bináris koordináták azonosak, tehát C a tétel állításában megadott alakú kód. A $v = 1$ esetre egyszerű számítógépes programmal verifikálható, hogy ha a bináris koordináták nem azonosak minden kódszóban, akkor C elérési sugara nagyobb mint 3. $\square$

A következő két – klasszifikációs eredményt adó – tétel bizonyítását elhagyjuk, mivel az akár kézzel, akár számítógép segítségével végezve nagyon egyszerű.

Háromszavas optimális kódok egy további egyedi esetére fennáll a következő állítás:

6.32. Tétel.

Ha $t = 2$, $b = 2$ és $R = 2$, akkor 5 inekvivalens optimális kód létezik, melyek közül az alábbi két kód kiegyensúlyozott és valamennyi koordinátában normális.

$$\{ (0, 0, 0, 0), \\ (1, 1, 0, 0), \\ (2, 2, 1, 1) \} \quad , \quad \{ (0, 0, 0, 0), \\ (1, 1, 0, 1), \\ (2, 2, 1, 0) \}.$$

Még mindig 3 szóból álló optimális kódokra vonatkozik a következő állítás. Az ezen esethez tartozó inekvivalens optimális kódokat a mellékelt lemezen megtalálhatjuk.

6.33. Tétel.

$t = 4$, $b = 1$, $R = 3$ esetén 5 inekvivalens optimális kód létezik.

Négyszavas optimális kódok tekintetében mindössze egy egyedi esetre tudunk klasszifikációs eredményt kimondani:

6.34. Tétel.

Ha $t = 2$, $b = 1$ és $R = 1$, akkor az alábbi két inekvivalens optimális kód létezik:

$$\begin{array}{ccc} \{ (0, 0, 0), & & \{ (0, 1, 0), \\ (0, 0, 1), & & (0, 2, 0), \\ (1, 1, 0), & \text{és} & (1, 0, 1), \\ (2, 2, 1) \} & & (2, 0, 1) \}. \end{array}$$

Bizonyítás. A két ternáris koordináta-helyen a 0, 1, 2 értékek mindegyikének elő kell fordulnia, mivel ellenkező esetben egy ternáris koordináta elhagyása után maradó kódnak zéró sugárral fednie kellene a teret, ami nyilván lehetetlen. Feltehetjük, hogy mindkét ternáris koordinátában a 0 két kódszóban, az 1-es és 2-es pedig egy-egy kódszóban fordul elő, továbbá a bináris koordinátát is az egyik kódszóban 0 értéken rögzíthetjük. Eszerint az alábbi lehetőségeket kell vizsgálnunk:

$$\begin{array}{ccc} \{ (0, 0, 0), & \{ (0, 1, 0), & \{ (0, 0, 0), \\ (0, 0, *), & (0, 2, *), & (0, 1, *), \\ (1, 1, *), & (1, 0, *), & (1, 0, *), \\ (2, 2, *) \} & (2, 0, *) \} & (2, 2, *) \}. \end{array} \quad \text{és}$$

A csillag karakterek helyén a 0, 1 értékeket minden lehetséges módon variálva, és a kapott kódok elérési sugarát ellenőrizve azt állapíthatjuk meg, hogy az első esetben két egymással ekvivalens optimális kódot, a második esetben egyetlen optimális kódot kapunk, a harmadik eset viszont nem folytatható úgy, hogy optimális kódhoz jussunk. $\square$

Számos további egyedi esetre számítógépes program segítségével határoztuk meg az inekvivalens optimális kódok számát. Az ilyen esetekre vonatkozó klasszifikációs eredményeket a 6.6. szakasz részletei, valamint a CD melléklet megfelelő táblázata mutatja. Itt csak egyet emelünk ki az ilyen esetek közül, a $K(1, 6; 1) = 24$ esetet, melyre két inekvivalens optimális kódot találtunk. Ezeket egyébként úgy kaphatjuk meg, hogy a H_7 bináris Hamming kód kódszavai közül kiválasztjuk a 0-val kezdődő, ill. a páros súlyú kódszavakat, majd a kiválasztott kódszavak mindegyikében az első koordinátát 2-re módosítva, a H_7 kódot kibővítjük a 8 módosított kódszóval.

6.6. A vegyes ternáris/bináris térlefedő kódok áttekintése

A vegyes ternáris/bináris térlefedő kódoknak a paraméterek $t + b \leq 10$, $R \leq 3$ tartományához tartozó eseteit összegezzük. Mivel itt meglehetősen sok eset kerül egyenkénti felsorolásra, a korlátok javításának nyomon követését többnyire csak az aktuálisan ismert legjobb és az ezt megelőzően ismert legjobb alsó és/vagy felső korlátra vonatkozó eredmény forrásának megadására korlátozzuk. A tárgyalt kódok jellegzetességeit 3-nál több szóból álló kódok esetén adjuk meg.

Nem adunk meg itt prompt korlátokat, bár a szférikus alsó korlátot minden tárgyalt esetre kiszámítottuk, és ennek alapján kiderült, hogy a szférikus alsó korlát csak 2 esetben maradt a legjobb ismert alsó korlát. Ezek egyike a $K(1, 9; 2)$ -re megadott alsó korlát. Kissé más a helyzet $K(2, 2; 1)$ esetén, mivel ennek pontos értéket is ismerjük, amely véletlenül egyenlő a szférikus alsó korláttal.

A szférikus alsó korlát értelmezéséhez előbb a $Z_3^t Z_2^b$ vegyes Hamming térre értelmeznünk kell az x középpontú R sugarú gömb fogalmát, amit az 1. fejezetben tárgyalt esethez hasonló

$$B_R(x) = \{y \in Z_3^t Z_2^b : d(x, y) \leq R\}$$

formula fejez ki, és meg kell határoznunk a benne lévő pontok számát. Elemi úton adódik, hogy az R sugarú gömb a középpont választásától függetlenül

$$V(t, b; R) = \sum_{i=0}^R \sum_{j=0}^i 2^j \binom{t}{j} \binom{b}{i-j} \quad (6.8)$$

számú pontból áll. Ennek alapján a szférikus alsó korlátot a

$$K(t, b; R) \geq \left\lceil \frac{3^t 2^b}{V(t, b; R)} \right\rceil = \left\lceil \frac{3^t 2^b}{\sum_{i=0}^R \sum_{j=0}^i 2^j \binom{t}{j} \binom{b}{i-j}} \right\rceil.$$

képlet adja.

Célszerűségi szempont indokolja, hogy a „normális kód” kifejezést ebben a szakaszban a bevezetés 1.2 szakaszában adott definíciótól eltérően használjuk. Mivel a konkrétan tárgyalt vegyes ternáris/bináris kódok valamennyien normálisak legalább egy bináris koordinátában, a bináris koordináták szerinti normalitás közlésétől eltekintünk. Ezzel összefüggésben, az egyszerűbb megfogalmazás érdekében, a „normális kód” kifejezés itt mindig azt fogja jelenteni, hogy „legalább egy ternáris koordinátában normális kód”. Az ezzel ellenkező tulajdonságú kódok esetén viszont szeretném elkerülni az „abnormális kód” kifejezés használatát, ehelyett a „nem normális kód” kifejezés fogja azt jelenteni, hogy az illető kód egyetlen ternáris koordinátára nézve sem normális, függetlenül attól, hogy bináris koordinátákban normális-e vagy sem.

6.6.1. $R = 1$ elérési sugarú kódokra vonatkozó eredmények

$K(1, 1; 1) = 2$ és 2 optimális kód létezik. Magyarázat, klasszifikáció: 6.29. tétel.

$K(1, 2; 1) = 3$ és egyetlen optimális kód létezik. Magyarázat, klasszifikáció: 6.30. tétel.

$K(1, 3; 1) = 6$ és 24 optimális kód létezik. Magyarázat: a 6.2.2 szakaszban vázolt eljárás vagy a 6.19. tétel egyaránt alkalmazható. Konstrukció 6 kódszóval: [60]. Alsó korlát és egyúttal a pontos érték bizonyítása: [78, 84, 102]. Klasszifikáció: [167]. Az optimális kódok között kiegyensúlyozott és kiegyensúlyozatlan, normális és nem normális kódok is találhatók.

$K(1, 4; 1) = 8$ és 2 optimális kód létezik. Konstrukció 8 kódszóval: [60]. Alsó korlát és egyúttal a pontos érték bizonyítása: [63]. Klasszifikáció: [76]. Totó kód 8 kódszóval: Di Nasso R. (1950). Az egyik optimális kód kiegyensúlyozatlan, a másik kiegyensúlyozott, és egyik sem normális.

$K(1, 5; 1) = 16$ és 120 optimális kód létezik. Konstrukció 16 kódszóval: [60]. Alsó korlát és egyúttal a pontos érték bizonyítása: [78, 102]. Klasszifikáció: [167]. Totó kód 16 kódszóval: Di Nasso R. (1950). Az optimális kódok között kiegyensúlyozott és kiegyensúlyozatlan, normális és nem normális kódok is találhatók. Az optimális kódok némelyikében található egy koordináta-helyen eltérő hármas kódszó-csoport, ezek egyikeben két ilyen kódszó-csoport van.

$K(1, 6; 1) = 24$ és 2 optimális kód létezik. Konstrukció 24 kódszóval: [60]. Alsó korlát és egyúttal a pontos érték bizonyítása: [63]. Klasszifikáció: [167]. Totó kód 24 kódszóval: Ericson A. „ARIC” (1936). A bináris Hamming kódból származtatható mindkét optimális kód kiegyensúlyozott és egyikük sem normális.

$42 \leq K(1, 7; 1) \leq 48$. Konstrukció 48 kódszóval: [60]. Alsó korlát: [149]. Totó kód 48 kódszóval: Ericson A. „ARIC” (1936). Az ismert rekord-tartó kód kiegyensúlyozott és nem normális, találhatók benne két koordináta-helyen eltérő négyes kódszó-csoportok.

$76 \leq K(1, 8; 1) \leq 84$. Konstrukció 84 kódszóval: [60]. Alsó korlát: [63]. Totó kód 84 kódszóval: Pico A. (1975). Az ismert rekord-tartó kód kiegyensúlyozott és nem normális.

$134 \leq K(1, 9; 1) \leq 160$. Konstrukció 160 kódszóval: [78, 102]. A 131 alsó korlát bizonyítása: [130]. Az alsó korlát javítása 134-re: [149]. Totó kód 160 kódszóval: Fagioli C. (1976). Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális, találhatók benne két koordináta-helyen eltérő négyes kódszó-csoportok.

$K(2, 1; 1) = 4$ és 2 optimális kód létezik. Konstrukció 4 kódszóval: [60]. Alsó korlát és egyúttal a pontos érték bizonyítása: [63]. Klasszifikáció: [167], 6.34. tétel. Totó kód 4 kódszóval: Di Nasso R. (1950). Mindkét optimális kód kiegyensúlyozott, s egyikük normális.

$K(2, 2; 1) = 6$ és egyetlen optimális kód létezik. Magyarázat: 6.20. tétel. Konstrukció 6 kódszóval: [60]. Szférikus alsó korlát eredményezi a felső korláttal egyező 6 értéket. Klasszifikáció (ami itt az unicitás bizonyítását jelenti): [167]. Totó kód 6 kódszóval: Di Nasso R. (1950). Az optimális kód kiegyensúlyozott és nem normális.

$K(2, 3; 1) = 12$ és 23 optimális kód létezik. Konstrukció 12 kódszóval: [60]. Alsó korlát és egyúttal a pontos érték bizonyítása: [78, 84, 102]. Klasszifikáció: [167]. Totókód 12 kódszóval: „BIG” (1941). Az optimális kódok között kiegyensúlyozott és kiegyensúlyozatlan, normális és nem normális kódok is találhatók.

$K(2, 4; 1) = 20$ és egyetlen optimális kód létezik. Konstrukció 20 kódszóval: [60]. Alsó korlát és egyúttal a pontos érték bizonyítása: [78, 84, 102]. Klasszifikáció (ami itt az unicitás bizonyítását jelenti): [167]. Totókód 20 kódszóval: „BIG” (1941). Az egyetlen optimális kód kiegyensúlyozatlan és nem normális.

$32 \leq K(2, 5; 1) \leq 36$. Konstrukció 36 kódszóval: [60]. A 31 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 32-re: [149]. Totókód 36 kódszóval: Ericson A. „ARIC” (1936). Az ismert rekord-tartó kód kiegyensúlyozott és nem normális, találhatóak benne két koordináta-helyen eltérő négyes kódszó-csoportok.

$57 \leq K(2, 6; 1) \leq 64$. Konstrukció 64 kódszóval: [60]. Az 56 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 57-re: [149]. Totókód 64 kódszóval: Stene O. (1947). Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális, találhatóak benne két koordináta-helyen eltérő négyes kódszó-csoportok.

$101 \leq K(2, 7; 1) \leq 122$. Konstrukció 124 kódszóval [102], 122 kódszóval: [130]. A 100 alsó korlát bizonyítása: [130]. Az alsó korlát javítása 101-re: [149]. Totókód 122 kódszóval: Bertolo R. és Santisi F. (1998). Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális, találhatóak benne két koordináta-helyen eltérő négyes kódszó-csoportok.

$187 \leq K(2, 8; 1) \leq 232$. Konstrukció 232 kódszóval [102]. Alsó korlát: [63]. Totókód 232 kódszóval: Rosatella M. és Fagioli C. (1981). Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális, találhatóak benne két koordináta-helyen eltérő négyes kódszó-csoportok.

$K(3, 1; 1) = 9$ és 4 optimális kód létezik. Konstrukció 9 kódszóval: [60]. A 8 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 9-re, és ezáltal a pontos érték bizonyítása: [102]. Klasszifikáció: [145]. Totókód 9 kódszóval: ismeretlen szerző (1946). Az optimális kódok között kiegyensúlyozott és kiegyensúlyozatlan kódok is találhatók, s a négy optimális kód egyike sem normális.

$K(3, 2; 1) = 16$ és 3 optimális kód létezik. Konstrukció 16 kódszóval: [60]. Az alsó korlát, és egyúttal a pontos érték bizonyítása: [78, 84, 102]. Klasszifikáció: [167]. Totókód 16 kódszóval: „BIG” (1941). Mindhárom optimális kód kiegyensúlyozatlan, egy közülük normális.

$K(3, 3; 1) = 24$ és 2 optimális kód létezik. Konstrukció 24 kódszóval: [60]. Az alsó korlát, és egyúttal a pontos érték bizonyítása: [63]. Klasszifikáció: [167]. Totókód 24 kódszóval: ismeretlen szerző (1946). Mindkét optimális kód kiegyensúlyozott és nem normális.

$44 \leq K(3, 4; 1) \leq 48$. Konstrukció 48 kódszóval: [60]. A 41 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 44-re: [149]. Totókód 48 kódszóval: ismeretlen szerző (1946). Az ismert rekord-tartó kód kiegyensúlyozott és nem normális, találhatóak benne két koordináta-helyen eltérő négyes kódszó-csoportok.

$78 \leq K(3, 5; 1) \leq 92$. Konstrukció 92 kódszóval: [60, 102]. A 76 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 78-ra: [149]. Totókód 92 kódszóval: Pico A. (1979). Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális.

$140 \leq K(3, 6; 1) \leq 171$. Konstrukció 171 kódszóval: [102]. A 139 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 140-re: [149]. Totókód 171 kódszóval: Hämäläinen H. (1994). Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális, találhatóak benne két koordináta-helyen eltérő négyes kódszó-csoportok.

$256 \leq K(3, 7; 1) \leq 312$. Konstrukció 312 kódszóval [102]. Alsó korlát: [63]. Totókód 312 kódszóval: Pico A. (1979). Az ismert rekord-tartó kód kiegyensúlyozott és nem normális, találhatóak benne két koordináta-helyen eltérő négyes kódszó-csoportok.

$K(4, 1; 1) = 18$ és 5 optimális kód létezik. Konstrukció 18 kódszóval: [60]. Az alsó korlát, és egyúttal a pontos érték bizonyítása: [63, 76]. Klasszifikáció: [167]. Totókód 18 kódszóval: ismeretlen szerző (1946). Mind az öt optimális kód kiegyensúlyozott, egy közülük normális.

$K(4, 2; 1) = 36$. Konstrukció 36 kódszóval: [60]. Az alsó korlát, és egyúttal a pontos érték bizonyítása: [88]. Totókód 36 kódszóval: ismeretlen szerző (1946). Az ismert optimális kódok kiegyensúlyozottak, s előfordul közöttük normális és nem normális kód is. Az utóbbiak egyikében találhatóak két koordináta-helyen eltérő négyes kódszó-csoportok.

$60 \leq K(4, 3; 1) \leq 72$. Konstrukció 72 kódszóval: [60]. Az 58 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 60-ra: [149]. Totókód 72 kódszóval: ismeretlen szerző (1946). Az ismert rekord-tartó kódok kiegyensúlyozottak, egyikük normális, és találhatóak bennük két koordináta-helyen eltérő négyes kódszó-csoportok.

$107 \leq K(4, 4; 1) \leq 128$. Konstrukció 128 kódszóval: [99]. A 103 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 107-re: [149]. Totókód 128 kódszóval: Hämäläinen H., Madsen E. (1994). Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális, találhatóak benne két koordináta-helyen eltérő négyes kódszó-csoportok.

$195 \leq K(4, 5; 1) \leq 238$. Konstrukció 238 kódszóval: [99]. A 194 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 195-re: [130]. Totókód 238 kódszóval: Hämäläinen H., Madsen E. (1994). Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális.

$356 \leq K(4, 6; 1) \leq 432$. Konstrukció 432 kódszóval: Johansson, lásd [60]. Alsó korlát: [63]. Totókód 432 kódszóval: Cercone De Lucia F. (1962). Az ismert rekord-tartó kód kiegyensúlyozott és normális.

$45 \leq K(5, 1; 1) \leq 54$. Konstrukció 54 kódszóval: [60]. A 44 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 45-re: [130]. Totókód 54 kódszóval: ismeretlen szerző (1946). Az ismert rekord-tartó kód kiegyensúlyozott és normális, találhatóak benne egy koordináta-helyen eltérő hármas, valamint két koordináta-helyen eltérő négyes kódszó-csoportok.

$80 \leq K(5, 2; 1) \leq 96$. Konstrukció 96 kódszóval: [60]. A 76 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 80-ra: [149]. Totókód 96 kódszóval: D'Amato G. (1953). Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális.

$148 \leq K(5, 3; 1) \leq 168$. Konstrukció 168 kódszóval: [60]. A 147 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 148-ra: [130]. Totókód 168 kódszóval: D'Amato G. (1953). Az ismert rekord-tartó kód kiegyensúlyozott és nem normális.

$268 \leq K(5, 4; 1) \leq 324$. Konstrukció 324 kódszóval: [102]. A 265 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 268-ra: [149]. Totókód 324 kódszóval: Conti N. (1976). Az ismert rekord-tartó kód kiegyensúlyozott és nem normális.

$509 \leq K(5, 5; 1) \leq 624$. Konstrukció 639 kódszóval: [102], 624 kódszóval: [130]. Az 508 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 509-re: [130]. Totókód 624 kódszóval: Bertolo R., Di Pasquale F. és Santisi F. (1999). Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális.

$113 \leq K(6, 1; 1) \leq 132$. Konstrukció 132 kódszóval: [60]. A 112 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 113-ra: [130]. Totókód 132 kódszóval: D'Amato G. (1953). Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális, találhatóak benne két koordináta-helyen eltérő négyes kódszó-csoportok.

$204 \leq K(6, 2; 1) \leq 252$. Konstrukció 252 kódszóval: [60]. A 197 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 204-re: [149]. Totókód 252 kódszóval: D'Amato G. (1953). Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális, találhatóak benne egy koordináta-helyen eltérő hármas, valamint két koordináta-helyen eltérő négyes kódszó-csoportok.

$386 \leq K(6, 3; 1) \leq 468$. Konstrukció 468 kódszóval: [78, 102]. A 384 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 386-ra: [130]. Totókód 468 kódszóval: Leonardi P. (1992). Az ismert rekord-tartó kód kiegyensúlyozott és nem normális.

$700 \leq K(6, 4; 1) \leq 864$. Konstrukció 864 kódszóval: Johansson (1988), lásd [60]. A 697 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 700-ra: [149]. Totókód 864 kódszóval: Cavallaro G. (1963). Az ismert rekord-tartó kód kiegyensúlyozott és nem normális.

$292 \leq K(7, 1; 1) \leq 333$. Konstrukció 333 kódszóval: [78, 102]. A 291 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 292-re: [130]. Totókód 333 kódszóval: Östergård P. (1990). Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális, találhatóak benne két koordináta-helyen eltérő négyes kódszó-csoportok.

$525 \leq K(7, 2; 1) \leq 648$. Konstrukció 648 kódszóval: [78, 102]. Az 519 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 525-re: [149]. Totókód 648 kódszóval: Cavallaro G. (1963). Az ismert rekord-tartó kód kiegyensúlyozott és nem normális, találhatóak benne két koordináta-helyen eltérő négyes kódszó-csoportok.

$1022 \leq K(7, 3; 1) \leq 1296$. Konstrukció 1296 kódszóval: [60]. Az 1019 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 1022-re: [130]. Totókód 1296 kódszóval: Cavallaro G. (1963). Az ismert rekord-tartó kód kiegyensúlyozott és normális, találhatóak benne két koordináta-helyen eltérő négyes kódszó-csoportok.

$772 \leq K(8, 1; 1) \leq 948$. Konstrukció 948 kódszóval: [130]. A 770 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 772-re: [130]. Totókód 948 kódszóval: Di Pasquale F. (2001). Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális, találhatóak benne egy koordináta-helyen eltérő hármas és két koordináta-helyen eltérő négyes kódszó-csoportok.

$1395 \leq K(8, 2; 1) \leq 1728$. Konstrukció 1728 kódszóval: [78, 102]. Az 1390 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 1395-re: [149]. Totókód 1728 kódszóval: Hämäläinen H. (1991). Az ismert rekord-tartó kód kiegyensúlyozott és nem normális, találhatóak benne két koordináta-helyen eltérő négyes kódszó-csoportok.

$2072 \leq K(9, 1; 1) \leq 2520$. Konstrukció 2538 kódszóval: [130], 2529 kódszóval: [168], 2520 kódszóval: Hämäläinen [159]. A 2067 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 2072-re: [130]. Totókód 2520 kódszóval: Hämäläinen H. (2009). Az ismert rekord-tartó kód kiegyensúlyozott és nem normális, találhatóak benne egy koordináta-helyen eltérő hármas kódszó-csoportok.

6.6.2. $R = 2$ elérési sugarú kódokra vonatkozó eredmények

$K(1, 2; 2) = 2$ és 4 optimális kód létezik. Az optimális kódok alakja

$$\begin{array}{ccc} * & * & 0 \\ * & * & 1 \end{array},$$

ahol a *-gal jelölt helyeken tetszőleges szimbólum állhat.

$K(1, 3; 2) = 2$ és 2 optimális kód létezik. Magyarázat és klasszifikáció: 6.29. tétel.

$K(1, 4; 2) = 3$ és egyetlen optimális kód létezik. Magyarázat és klasszifikáció: 6.30. tétel.

$K(1, 5; 2) = 6$ és 155 optimális kód létezik. Konstrukció 6 kódszóval: [60]. Alsó korlát és egyúttal a pontos érték bizonyítása: [78, 84, 102]. Klasszifikáció: [167]. Totókód 6 kódszóval: „ARIC” v. Weikel (1947). Az optimális kódok között kiegyensúlyozott és kiegyensúlyozatlan, normális és nem normális kódok is találhatók.

$K(1, 6; 2) = 8$ és 6 optimális kód létezik. Konstrukció 8 kódszóval: [60]. Alsó korlát és egyúttal a pontos érték bizonyítása: [78, 102]. Klasszifikáció: [167]. Totókód 8 kódszóval: ismeretlen szerző (1940). Az optimális kódok között kiegyensúlyozott és kiegyensúlyozatlan kódok is találhatók, s ezek egyike sem normális.

$K(1, 7; 2) = 12$ és egyetlen optimális kód létezik. Konstrukció 12 kódszóval: [60]. A 10 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 12-re: [130]. Klasszifikáció (ami itt az unicitás bizonyítását jelenti): [167]. Totókód 12 kódszóval: „ARIC” (1943). Az ismert optimális kód kiegyensúlyozott és nem normális.

$K(1, 8; 2) = 20$. Konstrukció 20 kódszóval: [60]. A 17 alsó korlát bizonyítása: [130]. Az alsó korlát javítása 20-ra, és ezáltal a pontos érték bizonyítása: 6.28. tétel. Totókód 20 kódszóval: Hämäläinen H. (1982). Az ismert optimális kód kiegyensúlyozatlan és nem normális.

$24 \leq K(1, 9; 2) \leq 35$. Konstrukció 35 kódszóval: [78, 102]. Szférikus alsó korlát eredményezi a megadott 24 értéket. Totókód 35 kódszóval: Östergård P. (1988). Az ismert rekord-tartó kód kiegyensúlyozott és nem normális.

$K(2, 1; 2) = 2$ és 3 optimális kód létezik. Magyarázat és klasszifikáció: 6.29. tétel.

$K(2, 2; 2) = 3$ és 5 optimális kód létezik. Magyarázat és klasszifikáció: 6.32. tétel.

$K(2, 3; 2) = 4$ és 6 optimális kód létezik. Konstrukció 4 kódszóval: [60]. Alsó korlát és egyúttal a pontos érték bizonyítása: [63]. Klasszifikáció: [167]. Totókód 4 kódszóval: „ARIC” v. Weikel (1947). Valamennyi optimális kód kiegyensúlyozott, s közülük 2 kód normális.

$K(2, 4; 2) = 6$ és egyetlen optimális kód létezik. Konstrukció 6 kódszóval: [60]. Alsó korlát és egyúttal a pontos érték bizonyítása: [78, 84, 102]. Klasszifikáció (ami itt az unicitás bizonyítását jelenti): [167]. Totókód 6 kódszóval: ismeretlen szerző (1941). Az egyetlen optimális kód kiegyensúlyozott és nem normális.

$K(2, 5; 2) = 11$ és 91 optimális kód létezik. Konstrukció 11 kódszóval: [60]. Alsó korlát és egyúttal a pontos érték bizonyítása: [130]. Klasszifikáció: [167]. Totókód 11 kódszóval: Hämäläinen H. (1989). Az optimális kódok között kiegyensúlyozott és kiegyensúlyozatlan kódok is találhatók, s ezek egyike sem normális.

$K(2, 6; 2) = 16$. Konstrukció 16 kódszóval: [60]. A 12 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 16-ra és ezáltal a pontos érték bizonyítása: [130]. Totókód 16 kódszóval: ismeretlen szerző (1940). Az ismert optimális kód kiegyensúlyozatlan és nem normális.

$22 \leq K(2, 7; 2) \leq 28$. Konstrukció 28 kódszóval: [60]. A 19 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 22-re: [130]. Totókód 28 kódszóval: Ciaburri V. & I. (1983). Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális.

$33 \leq K(2, 8; 2) \leq 48$. Konstrukció 48 kódszóval: [60]. A 32 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 33-ra: [149]. Totókód 48 kódszóval: „ARIC” v. Weikel (1947). Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális.

$K(3, 1; 2) = 3$ és egyetlen optimális kód létezik. Magyarázat és klasszifikáció: 6.31. tétel.

$K(3, 2; 2) = 5$ és egyetlen optimális kód létezik. Konstrukció 5 kódszóval: [60]. Alsó korlát és egyúttal a pontos érték bizonyítása: [78, 84, 102]. Klasszifikáció (ami itt az unicitás bizonyítását jelenti): [167]. Totókód 5 kódszóval: ismeretlen szerző (1950). Az egyetlen optimális kód kiegyensúlyozott és normális.

$K(3, 3; 2) = 8$ és 15 optimális kód létezik. Konstrukció 8 kódszóval: [60]. Alsó korlát és egyúttal a pontos érték bizonyítása: [78, 102]. Klasszifikáció: [167]. Totókód 8 kódszóval: ismeretlen szerző (1951). Az optimális kódok között kiegyensúlyozott és kiegyensúlyozatlan, normális és nem normális kódok is találhatók.

$K(3, 4; 2) = 13$ és egyetlen optimális kód létezik. Konstrukció 13 kódszóval: [60]. Alsó korlát és egyúttal a pontos érték bizonyítása: [130]. Klasszifikáció (ami itt az unicitás bizonyítását jelenti): [167]. Totókód 13 kódszóval: „ARIC” (1943). Az egyetlen optimális kód kiegyensúlyozott és nem normális.

$17 \leq K(3, 5; 2) \leq 23$. Konstrukció 23 kódszóval: [60]. A 15 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 17-re: [130]. Totókód 23 kódszóval: Weikel (1950). Az ismert rekord-tartó kód kiegyensúlyozott és nem normális.

$25 \leq K(3, 6; 2) \leq 36$. Konstrukció 36 kódszóval: [60]. A 24 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 25-re: [149]. Totókód 36 kódszóval: „ARIC” v. Weikel (1946). Az ismert rekord-tartó kód kiegyensúlyozott és nem normális.

$43 \leq K(3, 7; 2) \leq 56$. Konstrukció 56 kódszóval: [78, 102]. Alsó korlát: [63]. Totókód 56 kódszóval: D’Agostino F (1989). Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális.

$K(4, 1; 2) = 6$ és 11 optimális kód létezik. Konstrukció 6 kódszóval: [60]. Az 5 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 6-ra és ezáltal a pontos érték bizonyítása: [78, 84, 102]. Klasszifikáció: [167]. Totókód 6 kódszóval: „ARIC” (1947). Valamennyi optimális kód kiegyensúlyozott, s köztük normális és nem normális kód is található.

$K(4, 2; 2) = 10$ és 4 optimális kód létezik. Konstrukció 10 kódszóval: [60]. Alsó korlát és egyúttal a pontos érték bizonyítása: [130]. Klasszifikáció: [167]. Totókód 10 kódszóval: ismeretlen szerző (1941). Az optimális kódok között kiegyensúlyozott és kiegyensúlyozatlan kód is található, s ezek egyike sem normális.

$15 \leq K(4, 3; 2) \leq 18$. Konstrukció 18 kódszóval: [60]. A 14 alsó korlát bizonyítása: [130]. Az alsó korlát javítása 15-re: [167]. Totókód 18 kódszóval: „ARIC” (1940). Az ismert rekord-tartó kód kiegyensúlyozatlan és normális.

$20 \leq K(4, 4; 2) \leq 24$. Konstrukció 24 kódszóval: [60]. A 19 alsó korlát bizonyítása: [130]. Az alsó korlát javítása 20-ra: [149]. Totókód 24 kódszóval: „ARIC” v. Weikel (1934). Az ismert rekord-tartó kód kiegyensúlyozott és normális.

$32 \leq K(4, 5; 2) \leq 48$. Konstrukció 48 kódszóval: [60]. Alsó korlát: [63]. Totókód 48 kódszóval: „ARIC” v. Weikel (1934). Az ismert rekord-tartó kód kiegyensúlyozott és normális.

$55 \leq K(4, 6; 2) \leq 72$. Konstrukció 72 kódszóval: [60]. Alsó korlát: [63]. Totókód 48 kódszóval: Weikel (1946). Az ismert rekord-tartó kód kiegyensúlyozott és nem normális.

$K(5, 1; 2) = 12$ és egyetlen optimális kód létezik. Konstrukció 12 kódszóval: [60]. A 9 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 12-re és ezáltal a pontos érték bizonyítása: [130]. Klasszifikáció (ami itt az unicitás bizonyítását jelenti): [167]. Totókód 12 kódszóval: Hämmäläinen H. (1984). Az optimális kód kiegyensúlyozott és nem normális.

$16 \leq K(5, 2; 2) \leq 21$. Konstrukció 21 kódszóval: [78, 102]. Alsó korlát: [130]. Totókód 21 kódszóval: D’Agostino F (1989). Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális.

$24 \leq K(5, 3; 2) \leq 36$. Konstrukció 36 kódszóval: [60]. Alsó korlát: [63]. Totókód 36 kódszóval: „ARIC” v. Weikel (1934). Az ismert rekord-tartó kódok kiegyensúlyozottak és normálisak.

$42 \leq K(5, 4; 2) \leq 64$. Konstrukció 64 kódszóval: [60]. Alsó korlát: [63]. Totókód 64 kódszóval: Härmäläinen H. (1987). Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális.

$71 \leq K(5, 5; 2) \leq 108$. Konstrukció 108 kódszóval: [60]. A 70 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 71-re: [149]. Totókód 108 kódszóval: Weikel (1946). Az ismert rekord-tartó kód kiegyensúlyozott és nem normális.

$19 \leq K(6, 1; 2) \leq 27$. Konstrukció 27 kódszóval: [60]. A 18 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 19-re: [130]. Totókód 27 kódszóval: ismeretlen szerző (1941). Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális.

$33 \leq K(6, 2; 2) \leq 48$. Konstrukció 48 kódszóval: [60]. Alsó korlát: [63]. Totókód 48 kódszóval: Weikel (1958). Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális.

$54 \leq K(6, 3; 2) \leq 72$. Konstrukció 72 kódszóval: [60]. Az 53 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 54-re: [149]. Totókód 72 kódszóval: „ARIC” (1939). Az ismert rekord-tartó kód kiegyensúlyozott és nem normális.

$94 \leq K(6, 4; 2) \leq 144$. Konstrukció 144 kódszóval: [60]. Alsó korlát: [63]. Totókód 144 kódszóval: „ARIC” (1939). Az ismert rekord-tartó kód kiegyensúlyozott és normális.

$42 \leq K(7, 1; 2) \leq 54$. Konstrukció 54 kódszóval: [60]. A 41 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 42-re: [149]. Totókód 54 kódszóval: „ARIC” (1941). Az ismert rekord-tartó kód kiegyensúlyozott és normális.

$72 \leq K(7, 2; 2) \leq 108$. Konstrukció 108 kódszóval: [60]. A 70 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 72-re: [149]. Totókód 108 kódszóval: „ARIC” (1941). Az ismert rekord-tartó kód kiegyensúlyozott és normális.

$130 \leq K(7, 3; 2) \leq 216$. Konstrukció 216 kódszóval: [60]. Alsó korlát: [63]. Totókód 216 kódszóval: „ARIC” (1941). Az ismert rekord-tartó kódok kiegyensúlyozottak és normálisak. Egyikben található két koordináta-helyen eltérő négyes kódszó-csoportok, egy másikban pedig egy koordináta-helyen eltérő hármas kódszó-csoportok.

$99 \leq K(8, 1; 2) \leq 162$. Konstrukció 162 kódszóval: [60]. Alsó korlát: [63]. Totókód 162 kódszóval: „ARIC” (1936). Az ismert rekord-tartó kód kiegyensúlyozott és normális, találhatóak benne egy koordináta-helyen eltérő hármas kódszó-csoportok.

$167 \leq K(8, 2; 2) \leq 288$. Konstrukció 288 kódszóval: [60]. Alsó korlát: [63]. Totókód 288 kódszóval: Härmäläinen H. (1985). Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális.

$219 \leq K(9, 1; 2) \leq 396$. Konstrukció 396 kódszóval: [60]. Alsó korlát: [63]. Totókód 396 kódszóval: Härmäläinen H. (1985). Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális.

6.6.3. $R = 3$ elérési sugarú kódokra vonatkozó eredmények

$K(1, 3; 3) = 2$ és 6 optimális kód létezik. Az optimális kódok alakja

$$\begin{array}{cccc} * & * & * & 0 \\ * & * & * & 1 \end{array},$$

ahol a *-gal jelölt helyeken tetszőleges szimbólum állhat.

$K(1, 4; 3) = 2$ és 4 optimális kód létezik. Az optimális kódok alakja

$$\begin{array}{ccccc} * & * & 0 & 0 & 0 \\ * & * & 1 & 1 & 1 \end{array},$$

ahol a *-gal jelölt helyeken tetszőleges szimbólum állhat.

$K(1, 5; 3) = 2$ és 2 optimális kód létezik. Magyarázat és klasszifikáció: 6.29. tétel.

$K(1, 6; 3) = 3$ és egyetlen optimális kód létezik. Magyarázat és klasszifikáció: 6.30. tétel.

$K(1, 7; 3) = 6$ és 573 optimális kód létezik. Konstrukció 6 kódszóval: [60]. Alsó korlát és egyúttal a pontos érték bizonyítása: [78, 84, 102]. Klasszifikáció: [167]. Totókód 6 kódszóval: ismeretlen szerző (1963). Az optimális kódok között kiegyensúlyozott és kiegyensúlyozatlan, normális és nem normális kódok is találhatók.

$K(1, 8; 3) = 8$ és 21 optimális kód létezik. Konstrukció 8 kódszóval: [60]. A 6 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 8-ra, és ezáltal a pontos érték bizonyítása: [130]. Klasszifikáció: [167]. Totókód 8 kódszóval: ismeretlen szerző (1975). Az optimális kódok között kiegyensúlyozott és kiegyensúlyozatlan kódok is találhatók, s ezek egyike sem normális.

$K(1, 9; 3) = 12$ és 5 optimális kód létezik. Konstrukció 12 kódszóval: [60]. A 8 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 12-re, és ezáltal a pontos érték bizonyítása: [130]. Klasszifikáció: [167]. Totókód 12 kódszóval: ismeretlen szerző (kb. 1975). Valamennyi optimális kód kiegyensúlyozott, és egyikük sem normális.

$K(2, 2; 3) = 2$ és 6 optimális kód létezik. Az optimális kódok alakja

$$\begin{array}{cccc} * & * & * & 0 \\ * & * & * & 1 \end{array},$$

ahol a *-gal jelölt helyeken tetszőleges szimbólum állhat.

$K(2, 3; 3) = 2$ és 3 optimális kód létezik. Magyarázat és klasszifikáció: 6.29. tétel.

$K(2, 4; 3) = 3$ és 5 optimális kód létezik. Pontos érték bizonyítása: 6.10–6.11. tétel. Klasszifikáció: [167].

$K(2, 5; 3) = 4$ és 12 optimális kód létezik. Konstrukció 4 kódszóval: [60]. Alsó korlát és egyúttal a pontos érték bizonyítása: [78, 84, 102]. Klasszifikáció: [167]. Totókód 4 kódszóval: ismeretlen szerző [Valiosysteemit] (1963). Valamennyi optimális kód kiegyensúlyozott, s közülük 3 kód normális.

$K(2, 6; 3) = 6$ és 2 optimális kód létezik. Konstrukció 6 kódszóval: [60]. Alsó korlát és egyúttal a pontos érték bizonyítása: [78, 84, 102]. Klasszifikáció: [167]. Totókód 6 kódszóval: „SEPPO” (1975). Mindkét optimális kód kiegyensúlyozott, s egyik sem normális.

$K(2, 7; 3) = 11$. Konstrukció 11 kódszóval: [60]. A 7 alsó korlát bizonyítása: [129]. Az alsó korlát javítása 11-re, és ezáltal a pontos érték bizonyítása: [130]. Totókód 11 kódszóval: Hämäläinen H. (1986). Az ismert optimális kód kiegyensúlyozott, és nem normális.

$14 \leq K(2, 8; 3) \leq 16$. Konstrukció 16 kódszóval: [60]. Alsó korlát: [130]. Totókód 16 kódszóval: „SEPPO” (1975). Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális.

$K(3, 1; 3) = 2$ és 4 optimális kód létezik. Magyarázat és klasszifikáció: 6.29. tétel.

$K(3, 2; 3) = 3$ és 16 optimális kód létezik. Pontos érték bizonyítása: 6.10–6.11. tétel. Klasszifikáció: [167].

$K(3, 3; 3) = 3$ és egyetlen optimális kód létezik. Magyarázat és klasszifikáció: 6.31. tétel.

$K(3, 4; 3) = 5$ és 2 optimális kód létezik. Konstrukció 5 kódszóval: [60]. A 4 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 5-re, és ezáltal a pontos érték bizonyítása: [78, 84, 102]. Klasszifikáció: [167]. Totókód 5 kódszóval: „BEJON” (1975). Mindkét optimális kód kiegyensúlyozott és normális.

$K(3, 5; 3) = 8$ és 131 optimális kód létezik. Konstrukció 8 kódszóval: [60]. A 6 alsó korlát bizonyítása: [129]. Az alsó korlát javítása 8-ra, és ezáltal a pontos érték bizonyítása: [130]. Klasszifikáció: [167]. Totókód 8 kódszóval: Weikel (1974). Az optimális kódok között kiegyensúlyozott és kiegyensúlyozatlan, normális és nem normális kódok is találhatók.

$K(3, 6; 3) = 12$. Konstrukció 12 kódszóval: [60]. A 11 alsó korlát bizonyítása: [130]. Az alsó korlát javítása 12-re, és ezáltal a pontos érték bizonyítása: 6.28. tétel. Totókód 12 kódszóval: „ARIC” v. Weikel (1975). Az ismert optimális kód kiegyensúlyozott és nem normális.

$15 \leq K(3, 7; 3) \leq 20$. Konstrukció 20 kódszóval: [60]. A 12 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 15-re: [130]. Totókód 20 kódszóval: Hämäläinen H. (1986). Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális.

$K(4, 1; 3) = 3$ és 5 optimális kód létezik. Magyarázat és klasszifikáció: 6.10–6.11. és 6.33. tétel.

$K(4, 2; 3) = 4$ és 11 optimális kód létezik. Konstrukció 4 kódszóval: [60]. Alsó korlát és egyúttal a pontos érték bizonyítása: [78, 102]. Klasszifikáció: [167]. Totókód 4 kódszóval: ismeretlen szerző (kb. 1975). Az optimális kódok között kiegyensúlyozott és kiegyensúlyozatlan, normális és nem normális kódok is találhatók.

$K(4, 3; 3) = 6$ és 45 optimális kód létezik. Konstrukció 6 kódszóval: [60]. Alsó korlát és egyúttal a pontos érték bizonyítása: [78, 102]. Klasszifikáció: [167]. Totókód 6 kódszóval: „ARIC” (1974). Az optimális kódok között kiegyensúlyozott és kiegyensúlyozatlan, normális és nem normális kódok is találhatók.

$K(4, 4; 3) = 10$. Konstrukció 10 kódszóval: [60]. Alsó korlát és egyúttal a pontos érték bizonyítása: [130]. Totókód 10 kódszóval: Weikel (1972). Az ismert optimális kódok közül az egyik kiegyensúlyozott és nem normális, egy másik kiegyensúlyozatlan és normális.

$12 \leq K(4, 5; 3) \leq 16$. Konstrukció 16 kódszóval: Johansson, lásd [60]. A 9 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 12-re: [130]. Totókód 16 kódszóval: „BEJON” (1988). Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális.

$16 \leq K(4, 6; 3) \leq 24$. Konstrukció 24 kódszóval: [60]. A 14 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 16-ra: [130]. Totókód 24 kódszóval: „SEPPO” (1975). Az ismert rekord-tartó kód kiegyensúlyozott és normális.

$K(5, 1; 3) = 4$ és egyetlen optimális kód létezik. Konstrukció 4 kódszóval: [60]. Alsó korlát és egyúttal a pontos érték bizonyítása: [63]. Klasszifikáció (ami itt az unicitás bizonyítását jelenti): [167]. Totókód 4 kódszóval: Weikel (1974). Az egyetlen optimális kód kiegyensúlyozott és normális.

$K(5, 2; 3) = 7$ és egyetlen optimális kód létezik. Konstrukció 7 kódszóval: Johansson, lásd [60]. A 6 alsó korlát bizonyítása: [129]. Az alsó korlát javítása 7-re, és ezáltal a pontos érték bizonyítása: [130]. Klasszifikáció (ami itt az unicitás bizonyítását jelenti): [167]. Totókód 7 kódszóval: „BEJON” (1984). Az egyetlen optimális kód kiegyensúlyozott és normális.

$11 \leq K(5, 3; 3) \leq 12$. Konstrukció 12 kódszóval: [60]. A 8 alsó korlát bizonyítása: [129]. Az alsó korlát javítása 11-re: [130]. Totókód 12 kódszóval: „ARIC” v. Weikel (1975). Az ismert rekord-tartó kód kiegyensúlyozott és nem normális.

$13 \leq K(5, 4; 3) \leq 21$. Konstrukció 21 kódszóval: [78, 102]. A 11 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 13-ra: [130]. Totókód 21 kódszóval: Hämäläinen H. (1992). Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális.

$18 \leq K(5, 5; 3) \leq 32$. Konstrukció 32 kódszóval: [60]. A 17 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 18-ra: [149]. Totókód 32 kódszóval: Hämäläinen H. (1987). Az ismert rekord-tartó kód kiegyensúlyozatlan és normális.

$K(6, 1; 3) = 9$ és 4 optimális kód létezik. Konstrukció 9 kódszóval: [78, 102]. A 6 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 9-re, és ezáltal a pontos érték bizonyítása: [130]. Klasszifikáció: [145]. Totókód 9 kódszóval: Östergård P. (1988). Valamennyi optimális kód kiegyensúlyozott, és egyikük sem normális.

$11 \leq K(6, 2; 3) \leq 16$. Konstrukció 16 kódszóval: Johansson, lásd [60]. A 9 alsó korlát bizonyítása: [129]. Az alsó korlát javítása 11-re: [130]. Totókód 16 kódszóval: „BEJON” (1987). Az ismert rekord-tartó kód kiegyensúlyozott és nem normális. Található benne két koordináta-helyen eltérő négyes kódszó-csoport.

$15 \leq K(6, 3; 3) \leq 24$. Konstrukció 16 kódszóval: [60]. A 14 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 15-re: [130]. Totókód 24 kódszóval: Madsen E. (1986). Az ismert rekord-tartó kód kiegyensúlyozatlan és normális.

$22 \leq K(6, 4; 3) \leq 42$. Konstrukció 44 kódszóval: [60], 42 kódszóval (totókód gyanánt): [168] (2005). A 21 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 22-re: [149]. Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális.

$12 \leq K(7, 1; 3) \leq 18$. Konstrukció 18 kódszóval: [60]. A 11 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 12-re: [149]. Totókód 18 kódszóval: Weikel (1975). Az ismert rekord-tartó kód kiegyensúlyozott és normális.

$18 \leq K(7, 2; 3) \leq 33$. Konstrukció 33 kódszóval: [78, 102]. A 17 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 18-ra: [149]. Totókód 33 kódszóval: Hämmäläinen H. (1992). Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális.

$27 \leq K(7, 3; 3) \leq 54$. Konstrukció 54 kódszóval: [60]. A 26 alsó korlát bizonyítása: [140]. Az alsó korlát javítása 27-re: [149]. Totókód 54 kódszóval: „BEJON” (1987). Az ismert rekord-tartó kód kiegyensúlyozott és normális.

$21 \leq K(8, 1; 3) \leq 42$. Konstrukció 42 kódszóval: [78, 102]. A 20 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 21-re: [149]. Totókód 42 kódszóval: „BEJON” (1987). Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális.

$34 \leq K(8, 2; 3) \leq 70$. Konstrukció 72 kódszóval: [60], 70 kódszóval (totókód gyanánt): [168] (2005). A 33 alsó korlát bizonyítása: [63]. Az alsó korlát javítása 34-re: [149]. Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális.

$45 \leq K(9, 1; 3) \leq 91$. Konstrukció 93 kódszóval: [78, 102], 91 kódszóval: [136] (2009). Alsó korlát: [63]. Az ismert rekord-tartó kód kiegyensúlyozatlan és nem normális.

7. fejezet

Különösen vegyes térlefedő kódok

7.1. Méretre vonatkozó eredmények

Ebben a fejezetben a $Z_4^q Z_3^t Z_2^b$ térben értelmezett, tehát a 4, 3 és 2 alapszámokra épülő vegyes kódokra vonatkozó tételeket és konstrukciókat ismertetünk. Az ebbe a kategóriába tartozó, megadott számú kódszóból álló optimális térlefedő kódokra 4 kódszóig szükséges és elégséges feltételt, 5 kódszó esetére elégséges feltételt tudunk megadni.

Egy, kettő, ill. három kódszóból álló optimális kódokra nyilvánvaló vagy egyszerű módon következtethető a ternáris/bináris kódokra bizonyított analóg állításból a következő állítás egy-egy sora.

7.1. Állítás.

$K_{4,3,2}(q, t, b; R) = 1$ akkor és csak akkor áll fenn, ha $R = q + t + b$;

$K_{4,3,2}(q, t, b; R) = 2$ akkor és csak akkor áll fenn, ha $q + t + \lfloor \frac{b}{2} \rfloor \leq R < q + t + b$;

$K_{4,3,2}(q, t, b; R) = 3$ akkor és csak akkor áll fenn, ha $q + \min \left\{ \left\lfloor \frac{2t+2b}{3} \right\rfloor, \left\lfloor \frac{3t+2b}{4} \right\rfloor \right\} \leq R < q + t + \lfloor \frac{b}{2} \rfloor$.

A négyszavas esetre vonatkozó tételt néhány lemmával készítjük elő.

7.2. Lemma. (K. [143], Lemma 1)

Ha $q, t, b, R \geq 0$, $q + t + b \geq 1$ és

$$R \geq \min \left(\left\lfloor \frac{3q + 3t + 2b}{4} \right\rfloor, \left\lfloor \frac{5q + 4t + 3b}{6} \right\rfloor \right),$$

akkor $K_{4,3,2}(q, t, b; R) \leq 4$.

Bizonyítás. A lemma állításának helyességét bizonyítja, ha megmutatjuk, hogy a

$$C = \{ c_0 = (0, \dots, 0, 0, \dots, 0, 0, \dots, 0), \\ c_1 = (1, \dots, 1, 0, \dots, 0, 1, \dots, 1), \\ c_2 = (2, \dots, 2, 1, \dots, 1, 0, \dots, 0), \\ c_3 = (3, \dots, 3, 2, \dots, 2, 1, \dots, 1) \} \subset Z_4^q Z_3^t Z_2^b$$

kód elérési sugara

$$\begin{cases} \lfloor \frac{3q+3t+2b}{4} \rfloor & \text{ha } q \geq t, \\ \lfloor \frac{5q+4t+3b}{6} \rfloor & \text{ha } q < t. \end{cases}$$

Tetszőleges $x \in Z_4^q Z_3^t Z_2^b$ pont esetén jelölje $q_i(t_i, b_i)$ az egyes blokkokban az i -vel egyenlő koordináták számát, legyen továbbá $\bar{d}(x, c_j) = (q + t + b) - d(x, c_j)$ és $\bar{d}(x, C) = (q + t + b) - d(x, C)$. Ekkor $q_0 + q_1 + q_2 + q_3 = q$, $t_0 + t_1 + t_2 = t$, $b_0 + b_1 = b$, $\bar{d}(x, c_0) = q_0 + t_0 + b_0$, $\bar{d}(x, c_1) = q_1 + t_0 + b_1$, $\bar{d}(x, c_2) = q_2 + t_1 + b_0$ és $\bar{d}(x, c_3) = q_3 + t_2 + b_1$.

A felsorolt egyenlőségekből következik, hogy

$$\bar{d}(x, C) \geq \frac{\bar{d}(x, c_0) + \bar{d}(x, c_1) + \bar{d}(x, c_2) + \bar{d}(x, c_3)}{4} = \frac{q + t + 2b + t_0}{4},$$

és

$$\bar{d}(x, C) \geq \frac{\bar{d}(x, c_0) + \bar{d}(x, c_1) + 2\bar{d}(x, c_2) + 2\bar{d}(x, c_3)}{6} = \frac{q + 2t + 3b + q_2 + q_3}{6}.$$

Ezzel a C kód elérési sugarára kapunk két különböző felső korlátot:

$$d(x, C) \leq \left\lfloor \frac{3q + 3t + 2b}{4} \right\rfloor \quad \text{és} \quad d(x, C) \leq \left\lfloor \frac{5q + 4t + 3b}{6} \right\rfloor.$$

Megmutatjuk, hogy alkalmasan megadott q_i, t_i, b_i mennyiségek választásával $q \geq t$ esetén az első, $q \leq t$ esetén pedig a második egyenlőtlenség egyenlőséggel teljesíthető. Ehhez most sajnos elég sok esetet kell egyenként ellenőrizni, azonban ügyes összevonással az esetek száma az alábbi 14-re csökkenthető:

Ha $q \geq t$, q páros, $q + t$ osztható 4-gyel, akkor legyen

$$b_0 = \lfloor b/2 \rfloor, b_1 = \lceil b/2 \rceil, t_0 = 0, t_1 = \lceil t/2 \rceil, t_2 = \lfloor t/2 \rfloor, \\ q_0 = q_1 = (q + t)/4, q_2 = q_3 = (q - t)/4.$$

Ha $q \geq t$, q páros, $q + t + 1$ osztható 4-gyel, akkor legyen

$$b_0 = \lfloor b/2 \rfloor, b_1 = \lceil b/2 \rceil, t_0 = 0, t_1 = \lceil t/2 \rceil, t_2 = \lfloor t/2 \rfloor, \\ q_0 = (q + t + 1)/4, q_1 = (q + t - 3)/4, q_2 = (q - t - 1)/4, q_3 = (q - t + 3)/4.$$

Ha $q \geq t$, q páros, $q + t + 2$ osztható 4-gyel, akkor legyen

$$b_0 = \lfloor b/2 \rfloor, b_1 = \lceil b/2 \rceil, t_0 = 0, t_1 = \lceil t/2 \rceil, t_2 = \lfloor t/2 \rfloor, \\ q_0 = (q + t + 2)/4, q_1 = (q + t - 2)/4, q_2 = (q - t + 2)/4, q_3 = (q - t - 2)/4.$$

Ha $q \geq t$, q páros, $q + t + 3$ osztható 4-gyel , akkor legyen

$$b_0 = \lfloor b/2 \rfloor, b_1 = \lceil b/2 \rceil, t_0 = 0, t_1 = \lceil t/2 \rceil, t_2 = \lfloor t/2 \rfloor, \\ q_0 = (q + t + 3)/4, q_1 = (q + t - 1)/4, q_2 = (q - t - 3)/4, q_3 = (q - t + 1)/4.$$

Ha $q \geq t$, q páratlan, $q + t$ osztható 4-gyel , akkor legyen

$$b_0 = \lfloor b/2 \rfloor, b_1 = \lceil b/2 \rceil, t_0 = 0, t_1 = \lceil t/2 \rceil, t_2 = \lfloor t/2 \rfloor, \\ q_0 = q_1 = (q + t)/4, q_2 = (q - t - 2)/4, q_3 = (q - t + 2)/4.$$

Ha $q \geq t$, q páratlan, $q + t + 1$ osztható 4-gyel , akkor legyen

$$b_0 = \lfloor b/2 \rfloor, b_1 = \lceil b/2 \rceil, t_0 = 0, t_1 = \lceil t/2 \rceil, t_2 = \lfloor t/2 \rfloor, \\ q_0 = q_1 = (q + t + 1)/4, q_2 = (q - t + 1)/4, q_3 = (q - t - 3)/4.$$

Ha $q \geq t$, q páratlan, $q + t + 2$ osztható 4-gyel , akkor legyen

$$b_0 = \lfloor b/2 \rfloor, b_1 = \lceil b/2 \rceil, t_0 = 0, t_1 = \lceil t/2 \rceil, t_2 = \lfloor t/2 \rfloor, \\ q_0 = (q + t + 2)/4, q_1 = (q + t - 2)/4, q_2 = q_3 = (q - t)/4.$$

Ha $q \geq t$, q páratlan, $q + t + 3$ osztható 4-gyel , akkor legyen

$$b_0 = \lfloor b/2 \rfloor, b_1 = \lceil b/2 \rceil, t_0 = 0, t_1 = \lceil t/2 \rceil, t_2 = \lfloor t/2 \rfloor, \\ q_0 = q_1 = (q + t - 1)/4, q_2 = (q - t + 3)/4, q_3 = (q - t - 1)/4.$$

Ha $q < t$, q páros, $q + 2t$ osztható 3-mal , akkor legyen

$$b_0 = \lfloor b/2 \rfloor, b_1 = \lceil b/2 \rceil, q_0 = \lceil q/2 \rceil, q_1 = \lfloor q/2 \rfloor, q_2 = q_3 = 0, \\ t_0 = (t - q)/3, t_1 = t_2 = (q + 2t)/6.$$

Ha $q < t$, q páros, $q + 2t + 1$ osztható 3-mal , akkor legyen

$$b_0 = \lfloor b/2 \rfloor, b_1 = \lceil b/2 \rceil, q_0 = \lceil q/2 \rceil, q_1 = \lfloor q/2 \rfloor, q_2 = q_3 = 0, \\ t_0 = (t - q - 1)/3, t_1 = (q + 2t + 4)/6, t_2 = (q + 2t - 2)/6.$$

Ha $q < t$, q páros, $q + 2t + 2$ osztható 3-mal , akkor legyen

$$b_0 = \lfloor b/2 \rfloor, b_1 = \lceil b/2 \rceil, q_0 = \lceil q/2 \rceil, q_1 = \lfloor q/2 \rfloor, q_2 = q_3 = 0, \\ t_0 = (t - q + 1)/3, t_1 = (q + 2t + 2)/6, t_2 = (q + 2t - 4)/6.$$

Ha $q < t$, q páratlan, $q + 2t$ osztható 3-mal , akkor legyen

$$b_0 = \lfloor b/2 \rfloor, b_1 = \lceil b/2 \rceil, q_0 = \lceil q/2 \rceil, q_1 = \lfloor q/2 \rfloor, q_2 = q_3 = 0, \\ t_0 = (t - q)/3, t_1 = (q + 2t + 3)/6, t_2 = (q + 2t - 3)/6.$$

Ha $q < t$, q páratlan, $q + 2t + 1$ osztható 3-mal , akkor legyen

$$b_0 = \lfloor b/2 \rfloor, b_1 = \lceil b/2 \rceil, q_0 = \lceil q/2 \rceil, q_1 = \lfloor q/2 \rfloor, q_2 = q_3 = 0, \\ t_0 = (t - q - 1)/3, t_1 = t_2 = (q + 2t + 1)/6.$$

Végül, ha $q < t$, q páratlan, $q + 2t + 2$ osztható 3-mal, akkor legyen

$$b_0 = \lfloor b/2 \rfloor, b_1 = \lceil b/2 \rceil, q_0 = \lceil q/2 \rceil, q_1 = \lfloor q/2 \rfloor, q_2 = q_3 = 0, \\ t_0 = (t - q - 2)/3, t_1 = (q + 2t + 5)/6, t_2 = (q + 2t - 1)/6.$$

A felsorolt esetekre a megadott q_i, t_i, b_i mennyiségekhez tartozó $x \in Z_4^q Z_3^t Z_2^b$ pontnak a kódszavaktól való távolságát kiszámítva azt kapjuk, hogy C elérési sugara $\lfloor \frac{3q+3t+2b}{4} \rfloor$ minden olyan esetben, amikor $q \geq t$ és $\lfloor \frac{5q+4t+3b}{6} \rfloor$ minden olyan esetben, amikor $q < t$. $\square$

7.3. Lemma. (*K. [143], Theorem 1 egyik esete*)

$$K_{4,3,2}(2, 2, 0; 2) = 5.$$

Bizonyítás. Tekintsük a

$$C = \{ (0, 0, 0, 0), \\ (1, 1, 0, 0), \\ (1, 1, 1, 1), \\ (2, 2, 1, 1), \\ (3, 3, 2, 2) \} \subset Z_4^2 Z_3^2$$

kódot. Könnyű belátni, hogy C elérési sugara 2, következésképpen $K_{4,3,2}(2, 2, 0; 2) \leq 5$. Az ellentétes irányú egyenlőtlenség bizonyításához tegyük fel indirekten, hogy létezik $Z_4^2 Z_3^2$ -ben olyan négyszavas kód, melynek elérési sugara legfeljebb 2. Egy ilyen kód esetén a kódszavak első két koordinátájában a 0, 1, 2, 3, a két ternáris koordinátában pedig a 0, 1, 2 szimbólumok mindegyikének elő kell fordulnia, mivel ellenkező esetben $K_{4,3,2}(1, 2, 0; 1) \leq 4$ -re, ill. $K_{4,3,2}(2, 1, 0; 1) \leq 4$ -re, ezekből pedig $K_{3,2}(3, 0; 1) \leq 4$ -re következtethetnénk, amiről viszont tudjuk, hogy nem igaz. Ekkor feltehetjük, hogy az első két koordináta-helyen 0123 áll, a harmadik és negyedik koordinátában pedig 0012 tetszőleges permutációja. Ilyen kódokra az alábbi három inekvivalens lehetőség van:

$$\begin{array}{ccc} \{ (0, 0, 0, 0), & \{ (0, 0, 0, 0), & \{ (0, 0, 0, 1), \\ (1, 1, 0, 0), & (1, 1, 0, 1), & (1, 1, 0, 2), \\ (2, 2, 1, 1), & (2, 2, 1, 0), & (2, 2, 1, 0), \\ (3, 3, 2, 2) \} & (3, 3, 2, 2) \} & (3, 3, 2, 0) \}. \end{array} \quad \text{és}$$

Ezek elérési sugara azonban 2-nél nagyobb, mivel az első két kód esetén a $(0, 1, 1, 2)$ pont ezektől való távolsága 3, a harmadik kód esetén pedig a $(0, 2, 2, 2)$ pont van attól 3 távolságra. $\square$

Szükségünk lesz a 6.6. lemma kiterjesztésére a $Z_4^q Z_3^t Z_2^b$ térben értelmezett kódokra, valamint e kód kategória esetében még egy harmadik hasonló állításra is. Azonban a 6.6. lemma megfelelőjét most csak az $M = 4$ speciális esetre mondjuk ki és bizonyítjuk. Főleges is lenne ennél általánosabban fogalmazni, mivel a kiegészítő harmadik állítás nem általánosítható tetszőleges M -re. A szövegezésben figyelembe vesszük és a bizonyításban felhasználjuk, hogy $\sigma_2(4, 2) > 4$ és $\sigma_3(3, 3; 1) = K_3(3, 1) > 4$.

7.4. Lemma.

Ha $K_{4,3,2}(q, t-3, b; R-2) > 4$, $t \geq 3$ és $R \geq 2$, akkor $K_{4,3,2}(q, t, b; R) > 4$.

Ha $K_{4,3,2}(q, t, b-2; R-1) > 4$, $b \geq 4$ és $R \geq 1$, akkor $K_{4,3,2}(q, t, b; R) > 4$.

Ha $K_{4,3,2}(q-2, t-2, b; R-3) > 4$, $q \geq 2$, $t \geq 2$ és $R \geq 3$, akkor $K_{4,3,2}(q, t, b; R) > 4$.

Bizonyítás. Mindhárom állítást indirekten bizonyítjuk, tehát a bizonyítás első mondata mindhárom esetben így szól: Tegyük fel, hogy az adott feltételek mellett $K_{4,3,2}(q, t, b; R) \leq 4$.

Legyen $C \subset Z_4^q Z_3^t Z_2^b$ olyan négy szóból álló kód melynek elérési sugara legfeljebb R . Bontsuk fel C -t a C_1 és C_2 kódok konkatenációjára, ahol az első esetben $C_1 \subset Z_4^q Z_3^{t-3} Z_2^b$ és $C_2 \subset Z_3^3$, a második esetben $C_1 \subset Z_4^q Z_3^t Z_2^{b-2}$, $C_2 \subset Z_2^2$, és C_2 nem 2-szűrjektív – $\sigma_2(4, 2) > 4$ miatt van ilyen felbontás –, a harmadik esetben pedig $C_1 \subset Z_4^{q-2} Z_3^{t-2} Z_2^b$ és $C_2 \subset Z_4^2 Z_3^2$. Jelölje C_i elérési sugarát R_i .

A megfelelő esetre vonatkozó feltételből az első esetben $R_1 \geq R-1$, a második esetben $R_1 \geq R$, a harmadik esetben pedig $R_1 \geq R-2$ következik. Ugyanakkor az első esetben $R_2 \geq 2$ (mivel $K_3(3, 1) > 4$), a második esetben $R_2 \geq 1$ (C_2 választása folytán), a harmadik esetben pedig $R_2 \geq 3$ (a 7.3. lemma következtében). Mindhárom esetben azt kapjuk, hogy $R_1 + R_2 \geq R+1$, ami lehetetlen, mert az összefűzéssel nyert kód elérési sugara nem lehet az összefűzött kódok elérési sugarának az összegénél kisebb. Az így kapott ellentmondás bizonyítja az állítás mindhárom részének a helyességét. $\square$

7.5. Lemma. (K. [143], Lemma 2)

Adott $q, t, b \geq 0$ esetén, melyekre fennáll $b+t+q \geq 1$ és $q \leq t$, bármely 4 szóból álló $C \subset Z_4^q Z_3^t Z_2^b$ kód elérési sugara legalább

$$\left\lfloor \frac{5q+4t+3b}{6} \right\rfloor,$$

kivéve a $q=t=0$, b páros esetet, melyre a lehető legkisebb elérési sugár $b/2-1$.

Bizonyítás. A lemma állításának a következő indirekt átfogalmazását bizonyítjuk: Ha $t \geq q \geq 0$, $b \geq 0$, és

$$R = \left\lfloor \frac{5q+4t+3b}{6} \right\rfloor - 1,$$

akkor $K_{4,3,2}(q, t, b; R) > 4$ – a kivételként megfogalmazott esetet kivéve. Az indirekt átfogalmazás során a $K_{4,3,2}(q, t, b; R)$ függvény monotonitását is felhasználtuk. (Nyilvánvaló, hogy R értékének csökkentése esetén $K_{4,3,2}(q, t, b; R)$ értéke növekszik vagy esetleg változatlan marad.)

Először a q, t, b paraméterek néhány kisebb értékére vizsgáljuk, számítógép segítségével is igénybe véve, a lemma állításának a helyességét, ami ezekben az esetekben a következő egyenlőtlenségek bizonyítását jelenti.

$$K_{4,3,2}(0, 1, b; R) > 4 \text{ ha } 1 \leq b \leq 3 \text{ és } R = \lfloor (3b - 2)/6 \rfloor,$$

$$K_{4,3,2}(0, 2, b; R) > 4 \text{ ha } 0 \leq b \leq 3 \text{ és } R = \lfloor (3b + 2)/6 \rfloor,$$

$$K_{4,3,2}(0, 3, b; R) > 4 \text{ ha } 0 \leq b \leq 3 \text{ és } R = \lfloor (3b + 6)/6 \rfloor,$$

$$K_{4,3,2}(1, 1, b; R) > 4 \text{ ha } 0 \leq b \leq 3 \text{ és } R = \lfloor (3b + 3)/6 \rfloor,$$

$$K_{4,3,2}(1, 2, b; R) > 4 \text{ ha } 0 \leq b \leq 3 \text{ és } R = \lfloor (3b + 7)/6 \rfloor,$$

$$K_{4,3,2}(1, 3, b; R) > 4 \text{ ha } 0 \leq b \leq 3 \text{ és } R = \lfloor (3b + 11)/6 \rfloor,$$

$$K_{4,3,2}(2, 2, b; R) > 4 \text{ ha } 0 \leq b \leq 3 \text{ és } R = \lfloor (3b + 12)/6 \rfloor.$$

A $q = 0$ speciális esetre vonatkozóan a 6.14. lemmában bebizonyítottuk az állítást, egyúttal a kivételt is tisztáztuk. A fenti egyenlőtlenségek között azért kellett mégis felírni $q = 0$ -ra vonatkozó egyenlőtlenségeket, mivel a 7.4. lemma három állítására épülő rekurzióhoz ezekre is szükség van.

Ha a felsorolt egyenlőtlenségeket a b paraméter lehetséges értékeire külön-külön felírjuk, akkor a $q = 0$ esethez tartozó, a 6. fejezetben már megtárgyalt eseteken kívül ez összesen 16 egyenlőtlenséget jelent. Ezek között vannak nyilvánvalóan fennálló, vannak könnyen bizonyítható és vannak számítógép segítségével bizonyított, gépi program nélkül nehezen bizonyítható egyenlőtlenségek. A 9. fejezetben tárgyalásra kerülő algoritmusnak a vegyes $4/3/2$ kódokra kiterjesztett változatával az érintett $K(q, t, b; R)$ mennyiségek pontos értékét is meg tudtuk határozni, sőt legtöbb esetben az inekvivalens megoldások számát is. Valamennyi esetben $K(q, t, b; R)$ értékére legalább 5-öt kaptunk, nevezetesen

$$K_{4,3,2}(1, 1, 0; 0) = 12, \quad K_{4,3,2}(1, 1, 1; 1) = K_{4,3,2}(1, 1, 3; 2) = 5, \quad K_{4,3,2}(1, 1, 2; 1) = 8,$$

$$K_{4,3,2}(1, 2, 0; 1) = K_{4,3,2}(1, 2, 2; 2) = 6, \quad K_{4,3,2}(1, 2, 1; 1) = 12, \quad K_{4,3,2}(1, 2, 3; 2) = 8,$$

$$K_{4,3,2}(1, 3, 0; 1) = K_{4,3,2}(1, 3, 2; 2) = 12, \quad K_{4,3,2}(1, 3, 1; 2) = 8, \quad K_{4,3,2}(1, 3, 3; 3) = 7,$$

$$K_{4,3,2}(2, 2, 0; 2) = K_{4,3,2}(2, 2, 2; 3) = 5, \quad K_{4,3,2}(2, 2, 1; 2) = K_{4,3,2}(2, 2, 3; 3) = 8.$$

Vegyük észre, hogy b értékét 2-vel növelve, az R -re megadott kifejezés értéke pontosan 1-gyel növekszik. Ennélfogva a 7.4. lemma második állítását alkalmazva arra tudunk következtetni, hogy a felsorolt 7 egyenlőtlenség a b -re vonatkozó korlátozás nélkül is fennáll.

Hasonlóan, t értékét 3-mal növelve, az R -re megadott kifejezés értéke 2-vel növekszik. Most a 7.4. lemma első állítását alkalmazva arra a következtetésre jutunk, hogy $K_{4,3,2}(q, t, b; R) > 4$ fennáll, ha $0 \leq q \leq 1$, $t \geq 1$, b tetszőleges és $R = \lfloor \frac{5q+4t+3b}{6} \rfloor - 1$.

Végül, q értékét és t értékét is 2-vel növelve, az R -re megadott kifejezés értéke 3-mal növekszik. Ekkor a 7.4. lemma harmadik állításának alkalmazása azt eredményezi, hogy $K_{4,3,2}(q, t, b; R) > 4$ fennáll a megadott R kifejezéssel minden olyan esetben, melyre $0 \leq q \leq t$, nem mindkettő 0, b pedig tetszőleges. Ez megegyezik azzal az állítással, amit bizonyítani akartunk. $\square$

7.6. Lemma. (*K. [143], Lemma 3*)

Adott $q, t, b \geq 0$ esetén, melyekre fennáll $b + t + q \geq 1$ és $q \geq t$, bármely 4 szóból álló $C \subset Z_4^q Z_3^t Z_2^b$ kód elérési sugara legalább

$$\left\lfloor \frac{3q + 3t + 2b}{4} \right\rfloor$$

ugyanazzal a kivétellel, mint a 7.5. lemma esetén.

Bizonyítás. Ha $q = t$, akkor az állítás következik a 7.5. lemmából, mivel ilyenkor az elérési sugarra megadott két eltérő kifejezés azonos értéket vesz fel.

Ha $q = t + 1$, akkor legyen $t_1 = q = t + 1$ és $q_1 = t$. Az új paraméter-értékekre már $q_1 < t_1$, ezért a 7.5. lemma alkalmazható.

Ekkor

$$\left\lfloor \frac{5q_1 + 4t_1 + 3b}{6} \right\rfloor = \left\lfloor \frac{5t + 4(t + 1) + 3b}{6} \right\rfloor = \left\lfloor \frac{3t + b + 1}{2} \right\rfloor$$

és

$$\left\lfloor \frac{3q + 3t + 2b}{4} \right\rfloor = \left\lfloor \frac{3(t + 1) + 3t + 2b}{4} \right\rfloor = \left\lfloor \frac{3t + b + 1}{2} \right\rfloor.$$

A 7.5. lemma szerint bármely 4-szavas $C \subset Z_4^t Z_3^{t+1} Z_2^b$ kód elérési sugara legalább annyi, mint a fenti kifejezések értéke. Ekkor a $Z_4^{t+1} Z_3^t Z_2^b$ térben értelmezett 4-szavas kódokra még inkább fennáll, hogy minden ilyen kód elérési sugara legalább $\left\lfloor \frac{3t+b+1}{2} \right\rfloor$.

Végül, ha $q \geq t + 2$, akkor legyen $q_1 = \left\lceil \frac{q+t}{2} \right\rceil$ és $t_1 = \left\lfloor \frac{q+t}{2} \right\rfloor$. Ezekre a módosított paraméter-értékekre $q_1 = t_1$ vagy $q_1 = t_1 + 1$. Ilyen értékekre az állítást már bebizonyítottuk. Mivel most

$$\left\lfloor \frac{3q_1 + 3t_1 + 2b}{4} \right\rfloor = \left\lfloor \frac{3q + 3t + 2b}{4} \right\rfloor,$$

a könnyen belátható $K_{4,3,2}(q, t, b; R) \geq K_{4,3,2}(q_1, t, b; R)$ egyenlőtlenség figyelembe vételével az állítás helyessége $q \geq t + 2$ esetére is következik. $\square$

A 7.2., 7.5. és 7.6. lemmák alapján kimondhatjuk a következő tételt.

7.7. Tétel. (*vö. K. [143], Theorem 2 és 7.1. állítás*)

$K_{4,3,2}(q, t, b; R) = 4$ akkor és csak akkor áll fenn, ha

$$\min \left\{ \left\lfloor \frac{3q + 3t + 2b}{4} \right\rfloor, \left\lfloor \frac{5q + 4t + 3b}{6} \right\rfloor \right\} \leq R < q + \min \left\{ \left\lfloor \frac{2t + 2b}{3} \right\rfloor, \left\lfloor \frac{3t + 2b}{4} \right\rfloor \right\},$$

vagy pedig $q = t = 0$, b páros pozitív egész és $R = \frac{b}{2} - 1$.

Ötszavas kódokra a következő két tételt tudjuk megfogalmazni.

7.8. Tétel. (K. [143], Theorem 4 első része)

Ha $q, t, R \geq 0$, $t + q \geq 1$ és

$$R \geq \min \left(\left\lfloor \frac{3q + 3t}{4} \right\rfloor, \left\lfloor \frac{7q + 6t}{9} \right\rfloor \right),$$

akkor $K_{4,3,2}(q, t, 0; R) \leq 5$.

7.9. Tétel. (K. [143], Theorem 5 speciális esete)

Ha $q, t, b, R \geq 0$, $t \geq q \geq 1$ és

$$\left\lfloor \frac{5q + 4t + 3b - 1}{6} \right\rfloor \leq R < \left\lfloor \frac{5q + 4t + 3b}{6} \right\rfloor,$$

akkor $K_{4,3,2}(q, t, b; R) = 5$.

A két utóbbi tétel bizonyítása az eddigiekhez képest új eszközöket nem igényel, ezért terjedelmi okból ezek bizonyítását elhagyjuk. Mindkét bizonyítást angol nyelven a [143] cikk, magyar nyelven a [167] monográfia tartalmazza.

A 7.8. tétel feltétele teljesül pl. abban a speciális esetben, ha $q = 2u$, $t = 2u + 3v$ és $R = 3u + 2v - 1$, tehát fennáll

$$K_{4,3,2}(2u, 2u + 3v, 0; 3u + 2v - 1) = 5 \text{ ha } u \geq 1 \text{ és } v \geq 0.$$

Ennek egy speciális esete a korábban külön is bizonyított $K_{4,3,2}(2, 2, 0; 2) = 5$ egyenlőség.

A 7.9. tétel feltétele alapján nagyon sok ötszavas kódot tudunk képezni, a következő paraméter-értékekkel:

$$K_{4,3,2}(6u + 2z + 1, 6u + 3v + 2z + 1, 2w + 1; 9u + 2v + w + 3z + 1) = 5,$$

$$K_{4,3,2}(6u + 2z + 2, 6u + 3v + 2z + 2, 2w; 9u + 2v + w + 3z + 2) = 5.$$

Mindkét esetben u, v, w, z tetszőleges nemnegatív egészek lehetnek.

Hatszavas kódokra a következő tételt mondhatjuk ki.

7.10. Tétel.

$$K_{4,3,2}(3u + 3, u + 3v + 1, 0; 3u + 2v + 2) = 6 \text{ tetszőleges } u, v \geq 0 \text{ esetén.}$$

A bizonyítást elhagyjuk, mivel az a már többször alkalmazott technikákon kívül új ötletet nem igényel.

Nyolcszavas kódokra két érdekes paraméteres esetet találtunk.

7.11. Tétel.

$$K_{4,3,2}(1, 0, 2u + 4; u + 1) = 8 \text{ ha } u \geq 0.$$

$$K_{4,3,2}(1, 2, 2u + 3; u + 2) = 8 \text{ ha } u \geq 0.$$

Bizonyítás. Csak az első esetet bizonyítjuk. Tekintsük a

$$\begin{array}{ll} C = \{ (0, 0, 0, 0, 0), & C(u) = \{ (0, 0, 0, 0, 0, \dots, 0), \\ (0, 1, 1, 1, 1), & (0, 1, 1, 1, 1, \dots, 1), \\ (1, 0, 0, 1, 1), & (1, 0, 0, 1, 1, \dots, 1), \\ (1, 1, 1, 0, 0), & (1, 1, 1, 0, 0, \dots, 0), \\ (2, 0, 1, 0, 1), & (2, 0, 1, 0, 1, \dots, 1), \\ (2, 1, 0, 1, 0), & (2, 1, 0, 1, 0, \dots, 0), \\ (3, 0, 1, 1, 0), & (3, 0, 1, 1, 0, \dots, 0), \\ (3, 1, 0, 0, 1) \} \subset Z_4 Z_2^4 & \text{és} & (3, 1, 0, 0, 1, \dots, 1) \} \subset Z_4 Z_2^3 Z_2^{2u+1} \end{array}$$

kódokat. Az utóbbi az előbbiből úgy jön létre, hogy C kódszavaiban az utolsó koordináta értékét $2u + 1$ -szer ismételjük. C a Lindström [37] által talált vegyes perfekt kódok közé tartozik, melynek elérési sugara 1, legkisebb távolsága pedig 3. Ennek ismeretében, valamint tudva, hogy C a bináris koordinátáira nézve normális kód, könnyen belátható, hogy $C(u)$ elérési sugara $u + 1$, tehát fennáll $K_{4,3,2}(1, 0, 2u + 4; u + 1) \leq 8$. Az ellenkező irányú egyenlőtlenség következik abból a vegyes ternáris/bináris kódokra vonatkozó ismeretünkből, hogy $K_{3,2}(1, 2u + 4; u + 1) \geq 8$. $\square$

A szórványos esetek közül itt egyet emelünk ki, a $K_{4,3,2}(1, 0, 12; 1) = 1024$ egyenlőséget, amely szintén a Lindström [37] által talált egyik vegyes perfekt kód segítségével bizonyítható.

7.2. Az optimális kódok méretére és klasszifikációjára vonatkozó eredmények néhány konkrét esetben

Ezúttal csupán azokra az esetekre korlátozódunk, melyeknél az elérési sugár legfeljebb 3 és $K_{4,3,2}(q, t, b; R)$ értékét pontosan meg tudjuk adni. A legtöbb ilyen esetre az inekviválens optimális kódok számát is meghatároztuk.

Mivel itt többnyire kis méretű kódokról lesz szó, nem foglalkozunk a kódok történetével. A legtöbb esetben nem is lehet megállapítani a prioritást az ezekre a viszonylag egyszerű esetekre adott konstrukciókat illetően (és véleményem szerint itt nem is túl érdekes). Két perfekt vegyes kód esetén már megadtuk a [37] irodalmi hivatkozást. Néhány e kategóriába tartozó vegyes kód esetére Östergård [86] közölt korábban eredményeket, egyebek között a $K_{4,3,2}(1, 2, 0; 1) \leq 6$ és $K_{4,3,2}(1, 2, 3; 2) \leq 8$ korlátokat. Más esetekre vonatkozóan egy torinói team – Bertolo és szerzőtársai [168] – adott konstrukciót és ezzel egyúttal felső korlátot $K_{4,3,2}(q, t, b; R)$ értékére. Tőlük kaptam meg pl. a

$K_{4,3,2}(3, 2, 1; 3) \leq 7$ és $K_{4,3,2}(4, 0, 2; 3) \leq 6$ korlátot bizonyító két konstrukciót. Az egyenlőséget minden esetre magam bebizonyítottam, mivel alsó korlátokra (és egyenlőségekre) vonatkozó irodalmi előzményt nem találtam. A legtöbb esetre a bizonyítást számítógépes vizsgálattal végeztem. Néhány esetben segítettek a ternáris/bináris kódokra vonatkozó ismeretek, pl. $K_{3,2}(1, 5; 1) = 16$ -ból levezethető a $K_{4,3,2}(1, 0, 5; 1) = 16$ egyenlőség, vagy $K_{3,2}(2, 3; 1) = 12$ -ből a $K_{4,3,2}(1, 1, 3; 1) = 12$ egyenlőség. Legegyszerűbben (a szférikus alsó korlát segítségével) a $K_{4,3,2}(2, 0, 2; 1) = 8$ esetre bizonyítható az egyenlőség.

A vizsgált esetekre vonatkozó egyenkénti felsorolást most mellőzve, táblázatokba foglalva adjuk meg az optimális kódok számára, normalitási tulajdonságaira és legkisebb távolságára vonatkozó adatokat. E táblázatokban még egy jellegzetességet feltüntetünk, ami nem az esetekhez tartozó optimális kódokat, hanem magukat az egyes eseteket minősíti. Ennek magyarázatához a következő megfigyelésből indulhatunk ki.

A (3.2), (4.1), (5.3), (6.1), (6.2) egyenlőtlenségekkel analóg, azokhoz hasonlóan bizonyítható

$$K_{4,3,2}(q, t, b; R) \leq K_{4,3,2}(q - 1, t, b; R - 1) \quad (7.1)$$

reláció bizonyos esetekben egyenlőséggel teljesül. Ilyenkor a $q - 1, t, b, R - 1$ paraméterekhez tartozó bármely optimális kód szavait tetszőleges módon kiegészítve a $\{0, 1, 2, 3\}$ kódábécéből vett értékekkel, akár pl. csupa 0 értékű koordinátával, az 1-gyel növelt méretű térben 1-gyel nagyobb elérési sugarú optimális kódhoz jutunk. Az ilyen esetekhez tartozó optimális kódok nyilván kevésbé érdekesek, mint az olyanok, ahol (7.1)-ben határozott egyenlőtlenség áll fennáll, azaz a dimenzió és az elérési sugár 1-gyel történő szimultán növelése a kódszavak számának csökkenéséhez vezet az optimális kódokban.

Az előző fejezetekben e kérdéssel azért nem volt értelme foglalkozni, mivel a tapasztalatok szerint eddig csak triviális esetekben, legfeljebb 4 kódszó esetén fordult elő, hogy (3.2), (4.1) vagy (6.2) első egyenlőtlensége egyenlőséggel teljesülne. 4 kódszóval sem könnyű példát találni olyan vegyes ternáris/bináris optimális kódra, melyre

$$K(t, b; R) = K(t - 1, b; R - 1) = 4.$$

Legfeljebb 4 elérési sugárig valószínűleg nincs is ilyen kód, 5 elérési sugárral azonban van, amire legegyszerűbb példák a $K(6, 3; 5) = 4$ egyenlőséghez tartozó optimális kódok. Könnyű ellenőrizni, hogy $t = 5, b = 3, R = 4$, ill. $t = 6, b = 3, R = 5$ esetén egyaránt fennáll a 6.4 szakaszban az (e) esetre felírt egyenlőtlenség-pár.

Visszatérve a $Z_4^q Z_3^t Z_2^b$ térben értelmezett vegyes kódokra, itt már jóval több esetben, és még 6, 7, 8, 9 kódszóval is előfordul, hogy (7.1) egyenlőséggel teljesül, pl. $K_{4,3,2}(1, 2, 2; 2) = K_{4,3,2}(0, 2, 2; 1) = 6$, $K_{4,3,2}(1, 0, 5; 2) = K_{4,3,2}(0, 0, 5; 1) = 7$, $K_{4,3,2}(2, 0, 4; 2) = K_{4,3,2}(1, 0, 4; 1) = 8$, $K_{4,3,2}(1, 4, 0; 2) = K_{4,3,2}(0, 4, 0; 1) = 9$.

A 7.1-7.4 táblázatokban felsoroljuk azokat az eseteket, melyekre összegyűjtöttük az optimális kódok számára és jellegzetességeire vonatkozó adatokat. A táblázatok jobb áttekinthetősége érdekében a $K_{4,3,2}(q, t, b; R)$ kifejezésben elhagytuk a K melletti indexeket ezekben a táblázatokban.

A táblázatok első oszlopa mutatja az adott esetnek megfelelő optimális kódok szavainak a számát, a második oszlop az inekvivalens optimális kódok számát, a következő 3 oszlop a 4-normális, 3-normális, 2-normális koordináták számának létező legnagyobb értékét az

eset	inekv.	4-n.	3-n.	2-n.	dmin	megjegyzés
$K(1, 0, 1; 1) = 2$	2	0	-	1	2	
$K(1, 0, 2; 1) = 4$	9	1	-	2	2	
$K(1, 0, 3; 1) = 7$	17	0	-	3	1	$K(0, 0, 3; 0) = 8$
$K(1, 0, 4; 1) = 8$	1	0	-	4	3	$K(0, 0, 4; 0) = 16$
$K(1, 0, 5; 1) = 16$	8	0	-	5	2	$K(0, 0, 5; 0) = 32$
$K(1, 1, 0; 1) = 3$	3	0	1	-	2	
$K(1, 1, 1; 1) = 5$	2	0	1	1	1	$K(0, 1, 1; 0) = 6$
$K(1, 1, 2; 1) = 8$	5	0	0	2	2	$K(0, 1, 2; 0) = 12$
$K(1, 1, 3; 1) = 12$	1	0	0	3	1	$K(0, 1, 3; 0) = 24$
$K(1, 2, 0; 1) = 6$	1	0	0	-	1	$K(0, 2, 0; 0) = 9$
$K(1, 2, 1; 1) = 12$	770	1	2	1	2	$K(0, 2, 1; 0) = 18$
$K(1, 2, 2; 1) = 18$	5	0	0	2	2	$K(0, 2, 2; 0) = 36$
$K(1, 3, 0; 1) = 12$	1	0	0	-	1	$K(0, 3, 0; 0) = 27$
$K(2, 0, 1; 1) = 6$	4	2	-	1	2	$K(1, 0, 1; 0) = 8$
$K(2, 0, 2; 1) = 8$	1	0	-	2	2	$K(1, 0, 2; 0) = 16$
$K(2, 0, 3; 1) = 16$	20	1	-	3	2	$K(1, 0, 3; 0) = 32$
$K(2, 1, 0; 1) = 8$	7	0	1	-	2	$K(1, 1, 0; 0) = 12$
$K(2, 1, 1; 1) = 12$	1	0	0	1	1	$K(1, 1, 1; 0) = 24$
$K(2, 2, 0; 1) = 16$	1	0	0	-	1	$K(1, 2, 0; 0) = 36$
$K(3, 0, 1; 1) = 16$	34	3	-	1	2	$K(2, 0, 1; 0) = 32$

7.1. táblázat. Az optimális kódok jellegzetességei ($R = 1$)

optimális kódokban, az utolsó előtti oszlop pedig az optimális kódok lehetséges legnagyobb kódtávolságát. Végül az utolsó (megjegyzés) oszlopban csak akkor van bejegyzés, nevezetesen $K(q-1, t, b; R-1)$ értékének megadása, ha $K(q, t, b; R)$ értéke csökken hozzá képest. Az utolsó oszlopot üresen hagytuk azokban a kevésbé érdekes esetekben, amikor $K(q, t, b; R) = K(q-1, t, b; R-1)$.

A 7.5 táblázatban néhány olyan esetet sorolunk fel, melyekre $K_{4,3,2}(q, t, b; R)$ értéke ismert, de az inekvivalens optimális kódok száma nem. E táblázat esetén a normális koordinátákra és a kódtávolságra megadott adatok nem a létező legjobb értéket jelentik, hanem a mellékelt lemezen megadott optimális kód jellegzetességeit fejezik ki.

Az e táblázatokban összefoglalt eredmények tekintélyes részét számítógép segítségével kaptuk. Ehhez a 9. fejezetben ismertetésre kerülő algoritmus módosított változatát használtuk. Az S_1 input fájl generálásához ilyenkor nem 3, hanem 4 tagú partíciókat használunk, tehát az input fájl rekordjainak a száma a korábbi $P(M, 3)$, ill. $Q(M, 3)$ helyett most a tipikus esetekben $P(M, 4)$, ill. $Q(M, 4)$. A további lépések logikája megegyezik a 9. fejezetben elmondottakkal.

eset	inekv.	4-n.	3-n.	2-n.	dmin	megjegyzés
$K(1, 0, 2; 2) = 2$	4	0	-	2	3	
$K(1, 0, 3; 2) = 2$	2	0	-	3	4	
$K(1, 0, 4; 2) = 4$	19	1	-	4	3	
$K(1, 0, 5; 2) = 7$	441	0	-	5	3	
$K(1, 0, 6; 2) = 8$	1	0	-	6	3	$K(0, 0, 6; 1) = 12$
$K(1, 1, 1; 2) = 2$	4	0	0	1	3	
$K(1, 1, 2; 2) = 3$	4	0	0	2	2	
$K(1, 1, 3; 2) = 5$	13	0	1	3	2	$K(0, 1, 3; 1) = 6$
$K(1, 1, 4; 2) = 8$	1089	1	1	4	3	
$K(1, 2, 0; 2) = 3$	10	0	2	-	3	
$K(1, 2, 1; 2) = 4$	23	1	2	1	3	
$K(1, 2, 2; 2) = 6$	61	0	2	2	3	
$K(1, 2, 3; 2) = 8$	1	0	0	3	3	$K(0, 2, 3; 1) = 12$
$K(1, 3, 0; 2) = 4$	1	0	3	-	1	$K(0, 3, 0; 1) = 5$
$K(1, 3, 1; 2) = 8$	938	1	3	1	3	$K(0, 3, 1; 1) = 9$
$K(1, 4, 0; 2) = 9$	68	0	3	-	3	
$K(2, 0, 1; 2) = 2$	3	0	-	1	3	
$K(2, 0, 2; 2) = 4$	52	2	-	2	3	
$K(2, 0, 3; 2) = 6$	110	2	-	3	3	$K(1, 0, 3; 1) = 7$
$K(2, 0, 4; 2) = 8$	74	2	-	4	3	
$K(2, 1, 0; 2) = 3$	7	0	1	-		
$K(2, 1, 1; 2) = 4$	2	2	1	1	3	$K(1, 1, 1; 1) = 5$
$K(2, 1, 2; 2) = 7$	15	0	1	2	3	$K(1, 1, 2; 1) = 8$
$K(2, 1, 3; 2) = 10$	1	0	0	3	1	$K(1, 1, 3; 1) = 12$
$K(2, 2, 0; 2) = 5$	3	0	2	-	2	$K(1, 2, 0; 1) = 6$
$K(2, 2, 1; 2) = 8$	5	0	2	1	2	$K(1, 2, 1; 1) = 12$
$K(2, 3, 0; 2) = 10$	1	0	0	-	2	$K(1, 3, 0; 1) = 12$
$K(3, 0, 1; 2) = 4$	1	3	-	1	3	$K(2, 0, 1; 1) = 6$
$K(3, 0, 2; 2) = 8$	305	3	-	2	3	
$K(3, 1, 0; 2) = 6$	10	3	1	-	2	$K(2, 1, 0; 1) = 8$
$K(3, 1, 1; 2) = 10$	11	0	1	1	2	$K(2, 1, 1; 1) = 12$
$K(4, 0, 1; 2) = 11$	2	0	-	1	2	$K(3, 0, 1; 1) = 16$

7.2. táblázat. Az optimális kódok jellegzetességei ($R = 2$)

eset	inekv.	4-n.	3-n.	2-n.	dmin	megjegyzés
$K(1, 0, 3; 3) = 2$	6	0	-	3	4	
$K(1, 0, 4; 3) = 2$	4	0	-	4	5	
$K(1, 0, 5; 3) = 2$	2	0	-	5	6	
$K(1, 0, 6; 3) = 4$	36	1	-	6	5	
$K(1, 0, 7; 3) = 7$	2445	0	-	7	3	
$K(1, 0, 8; 3) = 8$	2	0	-	8	3	$K(0, 0, 8; 2) = 12$
$K(1, 1, 2; 3) = 2$	8	0	0	2	4	
$K(1, 1, 3; 3) = 2$	4	0	0	3	5	
$K(1, 1, 4; 3) = 3$	4	0	0	4	2	
$K(1, 1, 5; 3) = 5$	38	0	1	5	3	$K(0, 1, 5; 2) = 6$
$K(1, 1, 6; 3) = 8$	10985	1	1	6	4	
$K(1, 2, 1; 3) = 2$	6	0	0	1	4	
$K(1, 2, 2; 3) = 3$	21	0	2	2	4	
$K(1, 2, 3; 3) = 4$	71	1	2	3	4	
$K(1, 2, 4; 3) = 6$	189	0	2	4	3	
$K(1, 2, 5; 3) = 8$	1	0	0	5	3	$K(0, 2, 5; 2) = 11$
$K(1, 3, 0; 3) = 3$	25	0	3	-	4	
$K(1, 3, 1; 3) = 3$	4	0	3	1	4	
$K(1, 3, 2; 3) = 4$	2	0	3	2	3	$K(0, 3, 2; 2) = 5$
$K(1, 3, 3; 3) = 7$	4	0	3	3	2	$K(0, 3, 3; 2) = 8$
$K(1, 4, 0; 3) = 3$	3	0	4	-	5	
$K(1, 4, 1; 3) = 5$	1	0	4	1	1	$K(0, 4, 1; 2) = 6$
$K(1, 4, 2; 3) = 8$	6	0	4	2	4	$K(0, 4, 2; 2) = 10$
$K(1, 5, 0; 3) = 7$	68	0	5	-	4	$K(0, 5, 0; 2) = 8$

7.3. táblázat. Az optimális kódok jellegzetességei ($R = 3$, 1. rész)

eset	inekv.	4-n.	3-n.	2-n.	dmin	megjegyzés
$K(2, 0, 2; 3) = 2$	6	0	-	2	4	
$K(2, 0, 3; 3) = 2$	3	0	-	3	5	
$K(2, 0, 4; 3) = 4$	116	2	-	4	4	
$K(2, 0, 5; 3) = 6$	640	2	-	5	4	$K(1, 0, 5; 2) = 7$
$K(2, 0, 6; 3) = 8$	203	2	-	6	5	
$K(2, 1, 1; 3) = 2$	6	0	0	1	4	
$K(2, 1, 2; 3) = 3$	11	0	0	2	3	
$K(2, 1, 3; 3) = 4$	6	2	1	3	4	$K(1, 1, 3; 2) = 5$
$K(2, 1, 4; 3) = 7$	137	0	1	4	4	$K(1, 1, 4; 2) = 8$
$K(2, 2, 0; 3) = 3$	25	0	2	-	4	
$K(2, 2, 1; 3) = 4$	184	2	2	1	4	
$K(2, 2, 2; 3) = 5$	4	0	2	2	3	$K(1, 2, 2; 2) = 6$
$K(2, 3, 0; 3) = 4$	14	2	3	-	4	
$K(2, 3, 1; 3) = 6$	33	0	3	1	4	$K(1, 3, 1; 2) = 8$
$K(3, 0, 1; 3) = 2$	4	0	-	1	4	
$K(3, 0, 2; 3) = 4$	247	3	-	2	4	
$K(3, 0, 3; 3) = 4$	3	3	-	3	5	$K(2, 0, 3; 2) = 6$
$K(3, 1, 0; 3) = 3$	14	0	1	-	4	
$K(3, 1, 1; 3) = 4$	26	3	1	1	4	
$K(3, 1, 2; 3) = 6$	267	3	1	2	4	$K(2, 1, 2; 2) = 7$
$K(3, 2, 0; 3) = 4$	3	3	2	-	4	$K(2, 2, 0; 2) = 5$
$K(3, 2, 1; 3) = 7$	15	3	2	1	3	$K(2, 2, 1; 2) = 8$
$K(4, 0, 1; 3) = 4$	8	4	-	1	4	
$K(4, 0, 2; 3) = 6$	8	4	-	2	3	$K(3, 0, 2; 2) = 8$
$K(4, 1, 0; 3) = 4$	1	4	0	-	4	$K(3, 1, 0; 2) = 6$

7.4. táblázat. Az optimális kódok jellegzetességei ($R = 3, 2$. rész)

eset	4-n.	3-n.	2-n.	dmin	megjegyzés
$K(1, 0, 12; 1) = 1024$	0	-	12	3	$K(0, 0, 12; 0) = 4096$
$K(1, 1, 5; 2) = 12$	0	0	5	1	$K(0, 1, 5; 1) = 16$
$K(1, 3, 2; 2) = 12$	0	0	2	1	$K(0, 3, 2; 1) = 16$
$K(3, 2, 0; 2) = 12$	1	0	-	2	$K(2, 2, 0; 1) = 16$
$K(1, 3, 4; 3) = 10$	0	0	4	1	$K(0, 3, 4; 2) = 13$
$K(2, 2, 3; 3) = 8$	0	0	3	2	
$K(2, 4, 0; 3) = 8$	0	2	-	2	$K(1, 4, 0; 2) = 9$
$K(3, 0, 4; 3) = 8$	3	-	4	1	
$K(3, 1, 3; 3) = 8$	3	0	3	3	$K(2, 1, 3; 2) = 10$
$K(3, 3, 0; 3) = 9$	3	3	-	3	$K(2, 3, 0; 2) = 10$
$K(4, 0, 3; 3) = 8$	4	-	3	3	$K(3, 0, 3; 2) \geq 10$
$K(4, 1, 1; 3) = 8$	4	0	1	1	$K(3, 1, 1; 2) = 10$
$K(5, 0, 1; 3) = 8$	5	-	1	1	$K(4, 0, 1; 2) = 11$

7.5. táblázat. További egyenlőségek (az optimális kódok számának meghatározása nélkül)

8. fejezet

Optimális térlefedő kódok mérete és normalitás

8.1. ADS konstrukció optimális térlefedő kóddal és ismétléses kóddal

Az eddigiekben tárgyalt egyes kód kategóriákra a 3.3.3, 4.2.3, 5.3.3, ill. 6.2.3 szakaszban ismertetésre került a normális kódokra alkalmazható ADS konstrukciónak az a speciális esete, ahol a konstrukció egyik elemét képező kód $q + 1$ dimenziós ismétléses kód. Tekintve, hogy e konstrukció a másik elem kódszavainak számával azonos számú kódszóból álló kódot hoz létre, ezért a lineáris, ternáris, ill. tetszőleges q alapszámú kódok esetére megállapítható az alábbi állítások érvényessége:

(a) Ha a $K(n, R)$ -hez tartozó optimális kódok között van normális kód, akkor

$$K(n + 2, R + 1) \leq K(n, R); \quad (8.1)$$

(b) ha a $K_3(n, R)$ -hez tartozó optimális kódok között van normális kód, akkor

$$K_3(n + 3, R + 2) \leq K_3(n, R); \quad (8.2)$$

(c) ha a $K_q(n, R)$ -hez tartozó optimális kódok között van normális kód, akkor

$$K_q(n + q, R + q - 1) \leq K_q(n, R). \quad (8.3)$$

A fentiekkel analóg állítások vegyes kódokra is megadhatók. Az alábbiakban csak a vegyes ternáris/bináris kódokra vonatkozó analóg állításokat írjuk fel.

(d) Ha a $K(t, b; R)$ -hez tartozó optimális kódok között van bináris koordinátában normális kód, akkor

$$K(t, b + 2; R + 1) \leq K(t, b; R); \quad (8.4)$$

(e) ha a $K(t, b; R)$ -hez tartozó optimális kódok között van ternáris koordinátában normális kód, akkor

$$K(t + 3, b; R + 2) \leq K(t, b; R). \quad (8.5)$$

Idáig eljutva önkéntelenül is felvetődik az emberben a kérdés, hogy nem teljesülnek-e általános érvénnyel a (8.1)–(8.5) egyenlőtlenségek. Ezek bármelyikének általános érvényűsége elvileg lehetséges vagy úgy, hogy a normális kód létezését feltételező premissza igaz minden paraméter-pár (paraméter-hármas) esetén, vagy pedig az egyenlőtlenség fennáll minden olyan esetben is, amikor a premissza nem igaz. Az elfajuló $n = R$, ill. $t + b = R$ eseteket, melyekre az egyenlőtlenségek jobb oldalának értéke 1, kizárjuk a vizsgálatból. Ezekre az elfajuló esetekre nyilvánvalóan nem állhatnak fenn a felsorolt egyenlőtlenségek.

A kérdésre jelenlegi tudásunk szerint az a válasz, hogy a (8.1) egyenlőtlenség általános érvényűsége még nyitott probléma, a (8.2)–(8.5) egyenlőtlenségek viszont nem állnak fenn általános érvénnyel. A nemleges válasz az alábbi ellenpéldákkal támasztható alá:

$$K_3(6, 3) = 6 > K_3(3, 1) = 5, \quad K_3(8, 4) = 9 > K_3(5, 2) = 8;$$

$$K_4(8, 5) = 8 > K_4(4, 2) = 7;$$

$$K(6, 3; 5) = 4 > K(6, 1; 4) = 3, \quad K(8, 4; 7) = 4 > K(8, 2; 6) = 3;$$

$$K(4, 4; 3) = 10 > K(1, 4; 1) = 8, \quad K(5, 2; 3) = 7 > K(2, 2; 1) = 6.$$

A bináris esetre Cohen és szerzőtársai a [47] cikkben felvetették a (8.1) egyenlőtlenség általános érvényűségére vonatkozó sejtésüket. Ennek helyessége az $R = 1$ esetre már bebizonyosodott, ugyanis a [47]-ben (Proposition 2.2) megfogalmazott állítás szerint $N = 9$ és $N = 16$ esetleges kivételével ebben az esetben a sejtés igaz. Ma már tudjuk, hogy $K(11, 2) \leq 44$ (ez 1988-ban az [51] cikkben publikált eredmény) és $K(18, 2) \leq 2944$ (ez pedig 1998-ban a [107] cikkben publikált eredmény), s mivel e felső korlátok kisebbek, mint a $K(9, 1)$, ill. $K(16, 1)$ szférikus alsó korlátjaként számított 52, ill. 3856 érték, ezzel bebizonyosodott, hogy a [47]-ben esetleges kivételként említett két eset sem kivétel, tehát már kimondhatjuk az alábbi állítást:

8.1. Állítás.

$$K(n + 2, 2) \leq K(n, 1) \quad \text{tetszőleges } n \geq 2 \text{ egész esetén.} \quad (8.6)$$

Ez egyébként következik az 1991-ben megjelent [62] cikknek abból az eredményéből is, mely szerint $n \geq 3$ esetén minden 1 elérési sugarú bináris optimális térlefedő kód normális minden koordinátában. Az viszont mindmáig eldöntetlen régi sejtés, hogy (8.1) fennáll-e tetszőleges $n \geq R + 1$ egész esetén ha $R \geq 2$.

8.2. A kódtávolság korlátja normális kód esetén

Az előző szakaszban tárgyalt egyenlőtlenségek viselkedésének magyarázatát adja a következő tétel, amely egyúttal közelebb visz annak a tapasztalati úton megfigyelhető jelenségnek a magyarázatához is, hogy az ismert optimális térlefedő kódok többsége miért normális a bináris kódok körében és miért abnormális a nem bináris kódok körében.

8.2. Tétel.

Legyen $C \subset Z_q^n$ normális kód R elérési sugárral. Ekkor fennáll a következő egyenlőtlenség:

$$d_{\min}(C) \leq R + 1 + \frac{R}{q-1} \quad (8.7)$$

Bizonyítás. A normális kód definíciója szerint fennáll az (1.5) egyenlőtlenség tetszőleges $x \in Z_q^n$ esetén, tehát a kódszavak esetén is. Mivel tetszőleges $c \in C \setminus C_j$ kódszóra $d(c, C_j) \geq d_{\min}(C)$, ezért kódszó x esetén az (1.5) bal oldalán álló összeg tagjai egy kivétellel a $d_{\min}(C)$ kódtávolságnál nem kisebbek, $c \in C_j$ esetén viszont $d(c, C_j) = 0$, ennél fogva fennáll

$$(q-1)d_{\min}(C) \leq qR + q - 1.$$

Ebből minimális átalakítással kapjuk a (8.7) egyenlőtlenséget. $\square$

Bináris kód esetén a (8.7) korlát semmitmondó, hiszen a bármely kódra érvényes (1.1) egyenlőtlenségre redukálódik, q növelésével viszont egyre szorosabb korlátot fejez ki (változatlan R esetén), mivel (8.7) jobb oldala fokozatosan csökken, egyre távolabb kerül a perfekt kódok kódtávolságát kifejező $2R+1$ értéktől és aszimptotikusan $R+1$ értékéhez közeledik.

Logikus elvárás, ha az optimális (és az optimálishoz elég közeli rekord-tartó) kódokról azt várjuk, hogy az (1.1) egyenlőtlenség két oldalának értéke közel legyen egymáshoz. A normális kódokra fennálló (8.7) egyenlőtlenség viszont éppen ezzel ellentétes követelményt határoz meg, ha $q \geq 3$. Ez az ellentét annál jelentősebb mértékű, minél nagyobb a q alapszám értéke.

Könnyen belátható, hogy a 8.2. tétel kis módosítással érvényes vegyes kódok tetszőleges kategóriája esetén; ilyenkor a (8.7) egyenlőtlenség jobb oldalán a nevezőben álló q helyére azt a legnagyobb q_i -t kell helyettesíteni, amelyhez tartozó valamelyik koordinátára nézve az adott kód normális. Részben ez a tény indokolja a soron következő elemzés elvégzését.

8.3. Normális vegyes és ternáris kódok minimális mérete

Tekintve, hogy az optimális vegyes ternáris/bináris (és hasonlóan a tisztán ternáris) térlefedő kódok között a (8.7) egyenlőtlenség folytán, s egyúttal az eddigi tapasztalatok szerint is csak az esetek kisebb részarányában található ternáris koordinátában normális kód, viszont az évek során, és még a közelmúltban is sok új optimális, ill. rekord-javító térlefedő kódot eredményező ADS konstrukció (lásd 4.2.3. és 6.2.3. szakasz) többnyire csak normális kódokra alkalmazható, ezért megvizsgáltam, hogy azokban az esetekben, amikor ismerjük $K(t, b; R)$ pontos értékét, mekkora a térlefedő kódoknak az a minimális mérete, amelyre létezik t (> 0) ternáris és b bináris koordinátát tartalmazó, R elérési sugarú, ternáris koordinátában normális térlefedő kód. Jelölje $K^*(t, b; R)$ ezt a minimális méretet. E méret meghatározásával foglalkozunk ebben a szakaszban, ahol tudjuk, ott az

inekvivalens megoldások számát is megadva. Mindenütt szögletes zárójelben feltüntetjük $K(t, b; R)$ értékét is, mivel így azonnal látható, hogy $K^*(t, b; R)$ és $K(t, b; R)$ mely esetekben egyezik, és mely esetekben különbözik egymástól, továbbá azt is, hogy eltérés esetén mekkora rés van közöttük. A mellékelt CD lemezen a „ $K^*(t, b; R)$ táblázata és minimális méretű normális kódok listázása” cím alatt konkrétan is megadom a $K^*(t, b; R)$ értékéhez tartozó normális kódokat, ill. klasszifikációs eredmény híján legalább egy ehhez az értékhez tartozó normális kódot. Ez különösen olyan esetekben érdekes, amikor $K(t, b; R)$ és $K^*(t, b; R)$ értéke különbözik egymástól. Az ide vonatkozó valamennyi eredményt számítógép segítségével kaptam.

Az alábbiakban felsoroljuk azokat az eseteket, amelyekre ismerjük $K^*(t, b; R)$ pontos értékét. Ahol tudjuk, az inekvivalens megoldások számát is megadjuk.

$$K^*(1, 1; 1) = 3 \quad [K(1, 1; 1) = 2] \text{ — 2 inekvivalens megoldással.}$$

$$K^*(1, 2; 1) = 4 \quad [K(1, 2; 1) = 3] \text{ — 4 inekvivalens megoldással.}$$

$$K^*(1, 3; 1) = 6 \quad [K(1, 3; 1) = 6] \text{ — 9 inekvivalens megoldással.}$$

$$K^*(1, 4; 1) = 10 \quad [K(1, 4; 1) = 8] \text{ — 14 inekvivalens megoldással.}$$

$$K^*(1, 5; 1) = 16 \quad [K(1, 5; 1) = 16] \text{ — 10 inekvivalens megoldással.}$$

$$K^*(2, 0; 1) = 3 \quad [K(2, 0; 1) = 3] \text{ — 3 inekvivalens megoldással.}$$

$$K^*(2, 1; 1) = 4 \quad [K(2, 1; 1) = 4] \text{ — 1 inekvivalens megoldással.}$$

$$K^*(2, 2; 1) = 7 \quad [K(2, 2; 1) = 6] \text{ — 1 inekvivalens megoldással.}$$

$$K^*(2, 3; 1) = 12 \quad [K(2, 3; 1) = 12] \text{ — 9 inekvivalens megoldással.}$$

$$K^*(3, 0; 1) = 6 \quad [K(3, 0; 1) = 5] \text{ — 5 inekvivalens megoldással.}$$

$$K^*(3, 1; 1) = 10 \quad [K(3, 1; 1) = 9] \text{ — 49 inekvivalens megoldással.}$$

$$K^*(3, 2; 1) = 16 \quad [K(3, 2; 1) = 16] \text{ — 1 inekvivalens megoldással.}$$

$$K^*(4, 0; 1) = 12 \quad [K(4, 0; 1) = 9] \text{ — 2 inekvivalens megoldással.}$$

$$K^*(4, 1; 1) = 18 \quad [K(4, 1; 1) = 18] \text{ — 1 inekvivalens megoldással.}$$

$$K^*(4, 2; 1) = 36 \quad [K(4, 2; 1) = 36].$$

$$K^*(5, 0; 1) = 27 \quad [K(5, 0; 1) = 27] \text{ — 17 inekvivalens megoldással.}$$

$$K^*(1, 2; 2) = 3 \quad [K(1, 2; 2) = 2] \text{ — 3 inekvivalens megoldással.}$$

$$K^*(1, 3; 2) = 3 \quad [K(1, 3; 2) = 2] \text{ — 3 inekvivalens megoldással.}$$

$$K^*(1, 4; 2) = 4 \quad [K(1, 4; 2) = 3] \text{ — 7 inekvivalens megoldással.}$$

$$K^*(1, 5; 2) = 6 \quad [K(1, 5; 2) = 6] \text{ — 40 inekvivalens megoldással.}$$

$$\begin{aligned}
K^*(1, 6; 2) &= 10 \quad [K(1, 6; 2) = 8]. \\
K^*(2, 1; 2) &= 3 \quad [K(2, 1; 2) = 2] \text{ — 7 inekvivalens megoldással.} \\
K^*(2, 2; 2) &= 3 \quad [K(2, 2; 2) = 3] \text{ — 2 inekvivalens megoldással.} \\
K^*(2, 3; 2) &= 4 \quad [K(2, 3; 2) = 4] \text{ — 2 inekvivalens megoldással.} \\
K^*(2, 4; 2) &= 7 \quad [K(2, 4; 2) = 6] \text{ — 4 inekvivalens megoldással.} \\
K^*(2, 5; 2) &= 12 \quad [K(2, 5; 2) = 11]. \\
K^*(3, 0; 2) &= 3 \quad [K(3, 0; 2) = 3] \text{ — 7 inekvivalens megoldással.} \\
K^*(3, 1; 2) &= 3 \quad [K(3, 1; 2) = 3] \text{ — 1 inekvivalens megoldással.} \\
K^*(3, 2; 2) &= 5 \quad [K(3, 2; 2) = 5] \text{ — 1 inekvivalens megoldással.} \\
K^*(3, 3; 2) &= 8 \quad [K(3, 3; 2) = 8] \text{ — 6 inekvivalens megoldással.} \\
K^*(4, 0; 2) &= 3 \quad [K(4, 0; 2) = 3] \text{ — 1 inekvivalens megoldással.} \\
K^*(4, 1; 2) &= 6 \quad [K(4, 1; 2) = 6] \text{ — 10 inekvivalens megoldással.} \\
K^*(4, 2; 2) &= 11 \quad [K(4, 2; 2) = 10] \text{ — 12 inekvivalens megoldással.} \\
K^*(5, 0; 2) &= 9 \quad [K(5, 0; 2) = 8] \text{ — 342 inekvivalens megoldással.} \\
K^*(1, 3; 3) &= 3 \quad [K(1, 3; 3) = 2] \text{ — 6 inekvivalens megoldással.} \\
K^*(1, 4; 3) &= 3 \quad [K(1, 4; 3) = 2] \text{ — 6 inekvivalens megoldással.} \\
K^*(1, 5; 3) &= 4 \quad [K(1, 5; 3) = 2] \text{ — 68 inekvivalens megoldással.} \\
K^*(1, 6; 3) &= 4 \quad [K(1, 6; 3) = 3] \text{ — 10 inekvivalens megoldással.} \\
K^*(1, 7; 3) &= 6 \quad [K(1, 7; 3) = 6] \text{ — 148 inekvivalens megoldással.} \\
K^*(2, 2; 3) &= 3 \quad [K(2, 2; 3) = 2] \text{ — 12 inekvivalens megoldással.} \\
K^*(2, 3; 3) &= 3 \quad [K(2, 3; 3) = 2] \text{ — 14 inekvivalens megoldással.} \\
K^*(2, 4; 3) &= 4 \quad [K(2, 4; 3) = 3] \text{ — 127 inekvivalens megoldással.} \\
K^*(2, 5; 3) &= 4 \quad [K(2, 5; 3) = 4] \text{ — 3 inekvivalens megoldással.} \\
K^*(2, 6; 3) &= 7 \quad [K(2, 6; 3) = 6] \text{ — 14 inekvivalens megoldással.} \\
K^*(3, 1; 3) &= 3 \quad [K(3, 1; 3) = 2] \text{ — 17 inekvivalens megoldással.} \\
K^*(3, 2; 3) &= 3 \quad [K(3, 2; 3) = 3] \text{ — 9 inekvivalens megoldással.} \\
K^*(3, 3; 3) &= 4 \quad [K(3, 3; 3) = 3] \text{ — 56 inekvivalens megoldással.}
\end{aligned}$$

$$K^*(3, 4; 3) = 5 \quad [K(3, 4; 3) = 5] \text{ — 2 inekvivalens megoldással.}$$

$$K^*(3, 5; 3) = 8 \quad [K(3, 5; 3) = 8] \text{ — 61 inekvivalens megoldással.}$$

$$K^*(4, 0; 3) = 3 \quad [K(4, 0; 3) = 3] \text{ — 14 inekvivalens megoldással.}$$

$$K^*(4, 1; 3) = 3 \quad [K(4, 1; 3) = 3] \text{ — 5 inekvivalens megoldással.}$$

$$K^*(4, 2; 3) = 4 \quad [K(4, 2; 3) = 4] \text{ — 9 inekvivalens megoldással.}$$

$$K^*(4, 3; 3) = 6 \quad [K(4, 3; 3) = 6] \text{ — 36 inekvivalens megoldással.}$$

$$K^*(4, 4; 3) = 10 \quad [K(4, 4; 3) = 10].$$

$$K^*(5, 0; 3) = 3 \quad [K(5, 0; 3) = 3] \text{ — 3 inekvivalens megoldással.}$$

$$K^*(5, 1; 3) = 4 \quad [K(5, 1; 3) = 4] \text{ — 1 inekvivalens megoldással.}$$

$$K^*(5, 2; 3) = 7 \quad [K(5, 2; 3) = 7] \text{ — 1 inekvivalens megoldással.}$$

$$K^*(6, 0; 3) = 6 \quad [K(6, 0; 3) = 6] \text{ — 24 inekvivalens megoldással.}$$

A 6.4. szakaszban számos egyenlőséget adtunk meg egy vagy több paramétert tartalmazó esetekben $K(t, b; R)$ pontos értékére legfeljebb 9 kódszó esetén. $K^*(t, b; R)$ -nek a fenti felsorolásban megadott értékei $K(t, b; R)$ értékeinek a következő tételben szereplő felső korlátait eredményezik. Ezek konstruktív bizonyítása olyan eljárásan alapul, melynek során ternáris koordinátában normális kódokon ternáris ismétléses kóddal végzett ADS konstrukciót többszörösen alkalmazunk. Az alábbi tételben néhány 9 kódszónál hosszabb esetre gyűjtöttem össze az ily módon adódó felső korlátokat, pl. a 8.3. tétel első egyenlőtlenségét a $K^*(1, 4; 1) = 10$ egyenlőségből kapjuk.

8.3. Tétel.

Tetszőleges nemnegatív u egészre fennállnak a következő egyenlőtlenségek.

$$\begin{array}{ll} K(3u + 1, 4; 2u + 1) \leq 10, & K(3u + 1, 5; 2u + 1) \leq 16, \\ K(3u + 2, 3; 2u + 1) \leq 12, & K(3u + 3, 1; 2u + 1) \leq 10, \\ K(3u + 3, 2; 2u + 1) \leq 16, & K(3u + 4, 0; 2u + 1) \leq 12, \\ K(3u + 4, 1; 2u + 1) \leq 18, & K(3u + 5, 0; 2u + 1) \leq 27, \\ K(3u + 1, 6; 2u + 2) \leq 10, & K(3u + 2, 5; 2u + 2) \leq 12, \\ K(3u + 4, 2; 2u + 2) \leq 11. & \end{array}$$

Érdemes végigfutni ezeken az egyenlőtlenségeken az $u = 1$ esetben külön is. Ekkor azt találjuk, hogy az első egyenlőtlenség optimális térlefedő kódot, a többi egyenlőtlenség egy kivétellel rekord-tartó térlefedő kódot eredményez, ha $u = 1$.

9. fejezet

Algoritmus és gépi program vegyes térlefedő kódok klasszifikációjára

A vegyes ternáris/bináris térlefedő kódok esetére közölt klasszifikációs eredmények jelentős részét számítógép segítségével nyertük. Az e célra alkalmazott algoritmust ebben a fejezetben ismertetjük. Kisebb vagy nagyobb módosításokkal ez az algoritmus más kód kategóriák esetére is alkalmazható.

A gépi program segítségével végzett klasszifikáció lényege egy olyan, tulajdonképpen már régóta ismert és alkalmazott módszer, melynek során az eredményhalmazba, vagyis az adott esethez tartozó inekvivalens optimális térlefedő kódok halmazába tartozó kódokat koordinátáinként építjük fel. A módszer bináris kódokra megfogalmazott egyszerűbb változatát már a [16] és a [22] cikk szerzői megfogalmazták és kisebb méretek esetére alkalmazták, később a [103], valamint a [121] cikk szerzői továbbfejlesztették, továbbra is még csak a bináris esetre, és még nem klasszifikációs célra, hanem alsó korlátok javítására. A módszer vegyes kódokra vonatkozó változatának alkalmazásáról először a [130] cikk számol be, azonban magát a módszert csak nagyon röviden vázolja. A Z_q^n térre vonatkozó változatot, amely tehát a bináris, ternáris, és magasabb alapszámú kódokra is érvényes, a [138] könyv 7.2. szakaszában fogalmazták meg a szerzők. Kifejezetten klasszifikáció céljából alkalmazták (de nem magyarázták) a módszer vegyes kódokra vonatkozó változatát a [145] cikk szerzői a „Theorem 14” tétel bizonyításába beékelte megjegyzés során. A módszer bináris változatát – továbbfejlesztett formában – a [155] cikk szerzői klasszifikációra (Theorem 6), valamint alsó korlátok javítására (Theorem 7, 8, 10) alkalmazták.

Az általam alkalmazott algoritmus tehát nem saját, hanem már korábban ismert ötleteken alapul, viszont a számításokat nem készen kapott meglévő, hanem saját készítésű gépi programokkal végeztem, az itt ismertetett algoritmust személyi számítógépre implementálva, és különböző kód kategóriákra adaptálva, néhány esetben a gépi programot az adott paraméter értékekre kiélezve.

Visszatérve a vegyes ternáris/bináris kódok esetére, Legyen $t \geq 1$, $b \geq 0$, $n = t + b$, $R \geq 1$ és $M \geq 2$. A t ternáris, b bináris koordinátát, tehát összesen n koordinátát tartalmazó, R elérési sugarú, M kódszóból álló inekvivalens térlefedő kódok halmazának meghatározására szolgáló algoritmus-változatot az alábbiakban ismertetjük.

Amennyiben az eredményül kapott halmaz üres, ezzel azt bizonyítjuk, hogy $K(t, b; R) > M$. Ha viszont az eredményül kapott halmaz nem üres, de az 1-gyel kisebb M -re, egyébként azonos paraméterekkel lefolytatott hasonló eljárás üres halmazt eredményez, akkor $K(t, b; R) = M$ és az inekvivalens optimális kódok számát az eredmény-halmaz elemszáma adja meg. (Ha ismerjük $K(t, b; R)$ értékét, akkor természetesen már nem kell az optimális kódoknál 1-gyel kevesebb kódszót tartalmazó kódokkal foglalkoznunk a klasszifikáció elvégzése során.)

Az algoritmus fájljainak értelmezése

Az algoritmus által használt fájlok olyan halmazok, melyek rekordjait képező kódok kódszavai között lehetnek azonosak. Legyenek $S_1, S_2, \dots, S_n$ az 1-től n -ig növekvő méretű, eleinte ternáris, később (attól kezdve, amint S indexe meghaladja t értékét) vegyes ternáris/bináris Hamming terek meghatározott kódjaiból mint rekordokból álló fájlok. (Kivétel a $b = 0$ eset, amikor végig ternáris Hamming terek kódjairól van szó.) Az így értelmezett fájl-sorozatban S_1 az input fájl, S_n az output fájl (vagyis az eredmény halmaz), $S_2, S_3, \dots, S_{n-1}$ pedig a közbeeső lépések során kapott fájlok.

A vegyes kódok koordinátáit úgy rendezzük el, hogy balról jobbra elől álljanak a ternáris koordináták, és utánuk következzenek a bináris koordináták. Így tehát az S_k fájl k ternáris koordinátát tartalmazó kódokból áll, ha $k \leq t$, viszont t ternáris és $k - t$ bináris koordinátát tartalmazó kódokból áll, ha $k > t$.

Az input fájl elkészítése

Input fájl gyanánt minden esetben vehetjük az 1 dimenziós Z_3 Hamming tér összes inekvivalens M kódszóból álló kódjából mint rekordokból álló fájl. (Ebben az egyszerű esetben minden kódszó egyetlen szimbólum, tehát 0, 1, 2 valamelyike.) Így pl. $M = 2$ esetén az S_1 input fájl rekordjainak választhatjuk a $C_1 = \{0, 0\}$ és $C_2 = \{0, 1\}$ kódokat, $M = 3$ esetén a $C_1 = \{0, 0, 0\}$, $C_2 = \{0, 0, 1\}$, és $C_3 = \{0, 1, 2\}$ kódokat, $M = 4$ esetén a $C_1 = \{0, 0, 0, 0\}$, $C_2 = \{0, 0, 0, 1\}$, $C_3 = \{0, 0, 1, 1\}$, és $C_4 = \{0, 0, 1, 2\}$ kódokat stb. Tetszőleges M érték esetén a megfelelő S_1 fájl egyszerű programmal generálható.

Érdemes észrevenni a kapcsolatot az S_1 fájl rekordjai és az M egész legfeljebb 3 pozitív tagból álló partíciói között, melyek kölcsönösen egyértelmű kapcsolatban állnak egymással. Tetszőleges $M = M_0 + M_1 + M_2$ ($M_0 \geq M_1 \geq M_2$) partícióhoz rendeljük hozzá az M_0 számú 0-ból, M_1 számú 1-esből és M_2 számú 2-esből mint 1 hosszúságú kódszavakból álló kódot. Két pozitív tag esetén az $M = M_0 + M_1$ ($M_0 \geq M_1$) partícióhoz rendeljük hozzá az M_0 számú 0-ból és M_1 számú 1-esből álló kódot, az egy tagú $M = M_0$ partícióhoz pedig rendeljük hozzá a csupa 0-ból álló kódot. A megfeleltetésből az is kiderül, hogy az S_1 fájl rekordjainak a száma $P(M, 3)$. (Emlékeztetésül: $P(N, t)$ jelöli az N egész legfeljebb t pozitív tagból álló partícióinak a számát.)

Sok esetben, főleg nagyobb M értékek esetén, S_1 előbbi specifikációjától eltérően elég S_1 -ben azokat a Z_3 -beli kódokat összegyűjteni, melyekben a 0, 1, 2 szimbólumok mindegyike legalább egyszer előfordul. Erre akkor van lehetőség, ha tudjuk, hogy $K(t, b; R) > K(t - 1, b; R - 1)$. Könnyű belátni, hogy ilyenkor a $K(t, b; R)$ -hez tartozó tetszőleges optimális térlefedő kód esetén minden ternáris koordinátában legalább

egyszer elő kell fordulnia mindhárom szimbólumnak. Ilyen esetekben $M = 3$ és $M = 4$ esetén az S_1 fájl egyetlen rekordból, a $\{0, 1, 2\}$, ill. $\{0, 0, 1, 2\}$ kódot tartalmazó rekordból áll, továbbá tetszőleges M -re S_1 rekordjai az M egész pontosan 3 pozitív tagból álló partícióiból képezhetők. Jelöljük ezek számát $Q(M, 3)$ -mal (és általában az N egész pontosan t pozitív tagból álló partícióinak a számát $Q(N, t)$ -vel). Egyszerű gondolatmenettel adódik, hogy tetszőleges N és t pozitív egész esetén $P(N, t) = Q(N + t, t)$. A $P(M, 3)$ értékek sorozata pedig $M = 60$ -ig megtalálható a *The on-line encyclopedia of integer sequences* [175] összeállításban, mint az A001399 azonosítóval jelölt sorozat tagjai. $P(M, 3)$ és $Q(M, 3)$ értékei ismeretében az algoritmus indításához generált S_1 input fájl teljességét ellenőrizni tudjuk.

A kódhossz (vagyis a koordináták számának) fokozatos növelése

Az algoritmus fő része az S_{k-1} fájl feldolgozása alapján az S_k fájl elkészítése. Ezt a lépést $k = 2, 3, \dots, n$ -re, tehát összesen $n - 1$ -szer ismétljük. Az S_{k-1} fájlban tárolt minden egyes C kód esetén figyelembe vesszük a C kódnak egy további (k -adik) koordinátával minden lehetséges módon történő meghosszabbítását. Mivel minden kódszó ternáris koordináta esetén három különböző szimbólummal, bináris koordináta esetén két különböző szimbólummal egészíthető ki 1 koordinátával hosszabb kódszóvá, így a meghosszabbításra $k \leq t$ esetén 3^M lehetőség, $k > t$ esetén pedig 2^M lehetőség van. Természetesen az S_k fájlban nem tároljuk az összes lehetséges meghosszabbított kódot, hanem csak azokat, amelyek bizonyos feltételeket (egyenlőtlenségeket) kielégítenek. Az utolsó lépésnél ez a feltétel egyszerűen annak vizsgálata, hogy a vizsgált kód elérési sugarának az értéke R vagy annál kisebb legyen. A feltételek teljesülésének vizsgálatán túlmenően arra is ügyelünk, hogy minden egyes lépés során S_k rekordjai közé csak egymástól különböző és csak inekvivalens kódok kerüljenek.

A feltételek megfogalmazása

Minden lépésben annyi egyenlőtlenség teljesülését vizsgáljuk, mint amennyi az elkészítendő és S_k -ban tárolandó kódok méretének megfelelő Hamming tér (Z_3^k ha $k \leq t$, ill. $Z_3^t Z_2^{k-t}$ ha $k > t$) pontjainak a száma. Ez az első esetben 3^k , a második esetben $3^t 2^{k-t}$ egyenlőtlenség.

Legyen most D valamely $C \in S_{k-1}$ kódnak egyelőre még tetszőleges, az algoritmus előző mozzanatában említett meghosszabbítása, és legyen $v = (v_1, v_2, \dots, v_k)$ a Z_3^k vagy $Z_3^t Z_2^{k-t}$ tér tetszőleges pontja. Jelölje $w_0, w_1, \dots, w_R$ a D kód azon kódszavainak a számát, amelyek a v ponttól $0, 1, \dots, R$ távolságra vannak.

Jelöljük $Z(v)$ -vel a $Z_3^t Z_2^b$ Hamming térnek azt az $n - k$ dimenziós alterét, amelyet az első k koordináta értékének $v_1, v_2, \dots, v_k$ értéken való rögzítése határoz meg. Ha most egy $c \in D$ kódszót további $n - k$ koordinátával kiegészítünk, akkor az így kapott n koordinátából álló szó a $Z(v)$ altérben egy $R - d(c, v)$ sugarú gömb pontjaitól, és csak azoktól van R -nél kisebb vagy egyenlő távolságra. Az ilyen pontok száma $V(t - k, b; R - d(c, v))$, ill. $V(0, t + b - k; R - d(c, v))$, attól függően, hogy $k \leq t$ vagy $k > t$, ahol $V(t, b; R)$ a $Z_3^t Z_2^b$ Hamming tér R sugarú gömbjének a (6.8) képlettel megadott elemszáma. Legyen

$$y_i = \begin{cases} V(t - k, b; R - i) \text{ és } Y = 3^{t-k} 2^b & \text{ha } k \leq t, \\ V(0, t + b - k; R - i) \text{ és } Y = 2^{t+b-k} & \text{ha } k > t. \end{cases}$$

Ahhoz, hogy az összes $c \in D$ kódszó további $n - k$ koordinátával bárhogy történő meghosszabbításai együttesen R távolságon belül elérjék a $Z(v)$ altér valamennyi pontját, fenn kell állnia a következő egyenlőtlenségnek:

$$\sum_{i=0}^R w_i y_i \geq Y \quad (9.1)$$

Az utolsó lépés, melynél már $k = n$, külön megfontolást igényel. Ilyenkor a D kód tárolásának a feltételét már közvetlenül az elérési sugárra vonatkozó követelmény szabja meg, ami formálisan a $\sum_{i=0}^R w_i \geq 1$ egyenlőtlenséggel is kifejezhető, tehát ebben az esetben (9.1)-ben minden y_i , valamint Y értéke is 1-nek veendő. Egyébként a (6.8) képlet formális alkalmazása a $t = b = 0$ esetre ugyanezeket az értékeket eredményezi.

A fentiek alapján az eljárás a következő: Az S_k fájl egy lehetséges rekordjaként szóba jövő minden egyes D kód esetén a v vektorral bejárjuk a Z_3^k , ill. $Z_3^t Z_2^{k-t}$ altér pontjait, és minden ilyen v -re ellenőrizzük, hogy a (9.1) egyenlőtlenség fennáll-e. Ha akár csak egy v vektor esetén (9.1) nem teljesül, akkor a D kódot elvetjük, ha viszont (9.1) minden v vektorra fennáll, akkor a D kódot rekordként elhelyezzük az S_k fájlba. (Feltéve, hogy S_k rekordjai között nincs még D -vel ekvivalens kód.)

Annak biztosítása, hogy csak inekvivalens kódokat gyűjtsünk össze

Az inekvivalenciát egyszerű lexikografikus szabállyal tudjuk biztosítani. Ennek első követelménye, hogy minden egyes S_k fájl kódjaiban a kódszókat a koordináták sora szerint lexikografikusan nemcsökkenő sorrendbe helyezzük el. Az ilyen, lexikografikusan elrendezett kódszavakból álló kódok teljes komplexumára viszont – mivel az egyes lépésekben nem a kódszavak számát, hanem a koordináták számát gyarapítjuk – oszlopfolytonos lexikográfiát értelmezzünk, vagyis a kódokat elsődlegesen az első kódszó első koordinátája, utána a második kódszó első koordinátája, ..., az utolsó kódszó első koordinátája, majd az első kódszó második koordinátája, a második kódszó második koordinátája szerint rendezzük, és így tovább, a végén az utolsó előtti kódszó utolsó koordinátája, majd az utolsó kódszó utolsó koordinátája szerint rendezünk. Ezt a rendezést nem kell ténylegesen is elvégezni, hanem mindig csak azt kell vizsgálni, hogy egy, a (9.1) feltételeket kielégítő kód esetén a vele ekvivalens kódok között nincs-e az oszlopfolytonos lexikografikus rendezésben a vizsgált kódot megelőző kód, és az adott kódot csak akkor tároljuk el az S_k fájlba, ha ez a vizsgálat nemleges eredménnyel zárul.

Az algoritmus implementálása, tesztelése és alkalmazása

A fentiekben megfogalmazott algoritmust személyi számítógépen C programnyelven implementálva először olyan kisméretű eseteken teszteltük, amelyekre az inekvivalens kódok számát gép nélkül is egyszerűen meg tudtuk határozni, vagy a 6.29–6.34, ill. 4.10 tételek valamelyike alapján meghatároztuk. Ezt a tényt az alábbi táblázatokban a megjegyzés oszlop bejegyzései mutatják, továbbá ugyanitt jegyeztük meg, ha a klasszifikációs eredmény valamelyik hivatkozott publikáció eredménye. Ahol a megjegyzés oszlop nem tartalmaz bejegyzést, ott eddig még nem publikált klasszifikációs eredményről van szó.

A táblázatokba foglalt valamennyi esetben megadtuk az algoritmus által generált S_i fájlok méretét. A táblázatok minden sorában az utolsó nem kihúzott számadat az adott esethez tartozó inekvivalens optimális kódok száma. (Három hasonló felépítésű táblázatot adunk meg, egyet-egyet az $R = 1$, $R = 2$, ill. $R = 3$ elérési sugár esetére.)

Mint látható, nemcsak vegyes kódokra, hanem néhány ternáris kódra vonatkozó adatokat is megadtunk ezekben a táblázatokban, mivel az algoritmus megfogalmazásában is megengedtük a $b = 0$ egyenlőség fennállását. Az egyetlen eddig még nem publikált (és 3 kódszónál hosszabb) ternáris kódra vonatkozó klasszifikáció menete a $K(6, 0; 3) = 6$ -hoz tartozó sorban található.

Az ismertetett algoritmus és gépi program változtatás nélkül alkalmazható, és alkalmaztuk is a 8.3 szakaszban tárgyalt normális vegyes és ternáris kódok minimális méretével kapcsolatos számításra, valamint 3-nál nagyobb elérési sugár esetére is.

A tér dimenziójának (főleg a ternáris koordináták számának) bizonyos határon túl való növelése a futási időt nagyon meghosszabbította, ezért pl. a $K(1, 8; 2)$ -re és $K(1, 9; 3)$ -ra vonatkozó számításokat megszakítottuk. Azt még sikerült viszonylag könnyebben bizonyítani az algoritmus segítségével, hogy $K(1, 8; 2) > 18$. Végül az az ötlet segített, hogy olyan esetekben, amikor t kicsi, és b nagy, fordítsuk meg a koordináták sorrendjét. Ez az algoritmus több részletének módosítását vonja maga után, pl. az S_1 input halmaz rekordjait az M egész legfeljebb 2 (vagy pontosan 2) pozitív tagból álló partíciói alapján értelmezzük, az algoritmus fájljainak a sorában pedig az elől álló fájlokban nem ternáris, hanem bináris kódokat tárolunk.

Az algoritmusnak ez az utóbbi változata már a $K(1, 5; 1) = 16$ esetre is az eredeti változatánál kisebb méretű fájlakat eredményezett, ugyanis az S_i fájl méretére az alábbi értéksort kaptuk: 11, 35, 115, 72, 120. Viszonylag kevés gépidő felhasználásával sikerült a $K(1, 9; 3) = 12$ eset klasszifikációját is megoldani; erre az esetre a fájl méretek sora: 43, 513, 8502, 154515, 899477, 206227, 4496, 51, 5. Az algoritmus utóbbi változatának alkalmazása megmutatta, hogy $K(1, 8; 2) = 19$ nem állhat fenn, ugyanis 19 kódszóval a fájl méretek sorára 26, 296, 5139, 49804, 2411, 426, 558, 0 adódott. Érdekes itt a méret növekedés 426-ról 558-ra. Emiatt az utolsó, több mint egy hét gépidőt igénylő lépés eredményére várva azt reméltem, hogy talán sikerül rekord-javító optimális kódot találni 19 kódszóval, de végül ehelyett a $K(1, 8; 2) = 20$ egyenlőséget sikerült számítógéppel bizonyítani. Hasonlóan, az algoritmus utóbbi változatának alkalmazásával, számítógép segítségével történt a $K(3, 6; 3) = 12$ egyenlőség bizonyítása.

eset \ szint	S_2	S_3	S_4	S_5	S_6	S_7	megj.
$K(1, 2; 1) = 3$	1	1	-	-	-	-	6.30.t.
$K(2, 1; 1) = 4$	3	2	-	-	-	-	6.34.t.
$K(3, 0; 1) = 5$	2	1	-	-	-	-	[94]
$K(1, 3; 1) = 6$	12	24	24	-	-	-	-
$K(2, 2; 1) = 6$	3	3	1	-	-	-	-
$K(3, 1; 1) = 9$	10	8	4	-	-	-	[145]
$K(4, 0; 1) = 9$	1	1	1	-	-	-	[17]
$K(1, 4; 1) = 8$	2	4	2	2	-	-	[76]
$K(2, 3; 1) = 12$	35	123	138	23	-	-	-
$K(3, 2; 1) = 16$	42	2019	1840	3	-	-	-
$K(4, 1; 1) = 18$	1	4	5	5	-	-	-
$K(1, 5; 1) = 16$	34	342	1731	845	120	-	-
$K(2, 4; 1) = 20$	45	525	1559	73	1	-	-
$K(3, 3; 1) = 24$	3	5	5	7	2	-	-
$K(1, 6; 1) = 24$	4	4	6	6	2	2	-

eset \ szint	S_2	S_3	S_4	S_5	S_6	S_7	S_8	megj.
$K(1, 2; 2) = 2$	4	4	-	-	-	-	-	triv.
$K(2, 1; 2) = 2$	3	3	-	-	-	-	-	6.29.t.
$K(3, 0; 2) = 3$	7	7	-	-	-	-	-	4.10.t.
$K(1, 3; 2) = 2$	2	2	2	-	-	-	-	6.29.t.
$K(2, 2; 2) = 3$	3	5	5	-	-	-	-	6.32.t.
$K(3, 1; 2) = 3$	1	1	1	-	-	-	-	6.31.t.
$K(4, 0; 2) = 3$	1	1	1	-	-	-	-	4.10.t.
$K(1, 4; 2) = 3$	1	1	1	1	-	-	-	6.30.t.
$K(2, 3; 2) = 4$	3	7	13	6	-	-	-	-
$K(3, 2; 2) = 5$	10	17	26	1	-	-	-	-
$K(4, 1; 2) = 6$	11	19	29	11	-	-	-	-
$K(5, 0; 2) = 8$	37	438	499	1	-	-	-	[130]
$K(1, 5; 2) = 6$	19	87	247	342	155	-	-	-
$K(2, 4; 2) = 6$	11	34	45	20	1	-	-	-
$K(3, 3; 2) = 8$	37	500	2026	802	15	-	-	-
$K(4, 2; 2) = 10$	108	2393	14789	822	4	-	-	-
$K(5, 1; 2) = 12$	315	10754	5350	243	1	-	-	-
$K(1, 6; 2) = 8$	37	120	274	304	80	6	-	-
$K(2, 5; 2) = 11$	285	14037	263535	940216	179739	91	-	-
$K(3, 4; 2) = 13$	710	122433	3964002	5878979	46185	1	-	-
$K(1, 7; 2) = 12$	70	474	2756	3293	142	8	1	-

eset \ szint	S_2	S_3	S_4	S_5	S_6	S_7	S_8	S_9	megj.
$K(1, 3; 3) = 2$	4	6	6	-	-	-	-	-	triv.
$K(2, 2; 3) = 2$	3	6	6	-	-	-	-	-	triv.
$K(3, 1; 3) = 2$	3	4	4	-	-	-	-	-	6.29.t.
$K(4, 0; 3) = 3$	7	14	14	-	-	-	-	-	4.10.t.
$K(1, 4; 3) = 2$	4	4	4	4	-	-	-	-	triv.
$K(2, 3; 3) = 2$	3	3	3	3	-	-	-	-	6.29.t.
$K(3, 2; 3) = 3$	7	7	14	16	-	-	-	-	-
$K(4, 1; 3) = 3$	7	7	7	5	-	-	-	-	6.33.t.
$K(5, 0; 3) = 3$	3	3	3	3	-	-	-	-	4.10.t.
$K(1, 5; 3) = 2$	2	2	2	2	2	-	-	-	6.29.t.
$K(2, 4; 3) = 3$	3	5	5	6	5	-	-	-	-
$K(3, 3; 3) = 3$	1	1	1	2	1	-	-	-	6.31.t.
$K(4, 2; 3) = 4$	3	6	11	35	11	-	-	-	-
$K(5, 1; 3) = 4$	3	6	5	6	1	-	-	-	-
$K(6, 0; 3) = 6$	26	204	680	609	28	-	-	-	-
$K(1, 6; 3) = 3$	1	1	1	1	1	1	-	-	6.30.t.
$K(2, 5; 3) = 4$	3	12	13	20	29	12	-	-	-
$K(3, 4; 3) = 5$	10	50	123	163	112	2	-	-	-
$K(4, 3; 3) = 6$	26	204	680	1842	727	45	-	-	-
$K(5, 2; 3) = 7$	60	719	1199	4861	1109	1	-	-	-
$K(6, 1; 3) = 9$	198	12272	409721	202121	4162	4	-	-	[145]
$K(1, 7; 3) = 6$	24	128	572	1621	2624	2154	573	-	-
$K(2, 6; 3) = 6$	26	124	445	762	342	71	2	-	-
$K(3, 5; 3) = 8$	128	5469	86133	666075	645651	33638	131	-	-
$K(1, 8; 3) = 8$	57	641	5629	12626	19479	8714	893	21	-

A. Függelék

Szűrjektív kódok méretére, konstrukciójára és klasszifikációjára vonatkozó eredmények

A térlefedő kódok optimális méretének a problémája a $K_q(n, R)$ kifejezés, valamint a egyes kódokra értelmezett hasonló kifejezés értéke meghatározásának a kérdésére vezetett. A paraméterek bizonyos értékeire

$$K_q(n, R) = \text{érték}$$

egyenlőséget, többnyire azonban csak

$$\text{alsó korlát} \leq K_q(n, R) \leq \text{felső korlát}$$

egyenlőtlenségpárt tudtunk megadni. A $K_q(n, R)$ kifejezés értékének, ill. korlátainak a kutatása során a térlefedő kódok szinte valamennyi vizsgált kategóriája esetén az egyik vagy mindkét korlát meghatározásához több esetben is szűrjektív kódok méret-adataira vonatkozó ismereteket használtunk. Alsó korlátok beállításához vagy javításához hasznos eszköznek bizonyult bináris kódok esetében a 3.1. lemma és annak 3.2–3.6. következményei, ternáris és magasabb rendű kódok esetére az előbbiekhöz hasonló, de általánosabban megfogalmazott 4.2. lemma és annak 4.3–4.5. következményei, egyes kódok esetén pedig a 6.7–6.8. lemmák. Felső korlátok beállításához vagy javításához az 5.4.1 szakaszban tárgyalt módszert – szűrjektív kódok egyesítését – igen sok esetben tudtuk alkalmazni az 5.4 következmény formulája alapján.

Mindezek indokolják, hogy a szűrjektív (és általánosított szűrjektív) kódok méretével, klasszifikációjával, az ismert szűrjektív kódok struktúrájával is az eddigieknél koncentráltabban foglalkozzunk. Mivel azonban a szűrjektív kódok nem tartoznak szorosan a munka fő témájához, hanem segédeszközként használva itt csak alárendelt szerepük van, ezért került ez az anyagrész a függelékbe. Ugyanezen ok miatt a mondanivaló kifejtése itt kevésbé részletes, továbbá a hosszabb bizonyítások ismertetése helyett csak utalást adok azok elérési helyére.

A.1. Ismert pontos értékek

A továbbiakban először az adott q alapszámhoz tartozó n dimenziós s -szürjektív kódok minimális méretét kifejező $\sigma_q(n, s)$ függvény értékeivel, majd az általánosabb $\sigma_q(n, s; r)$ függvény értékeivel foglalkozunk a $q \geq 2$ és $2 \leq s \leq n$ kikötések mellett. Ezek ismert pontos értékeit, ill. legjobb ismert alsó és felső korlátait az [166] cikk szürjektív kódokra vonatkozó táblázataiban adtuk meg $q \leq 8$, $n, s \leq 10$ (bináris kódokra $n, s \leq 14$) esetén. Számos esetben sikerült meghatározni az adott paraméterekhez tartozó inekvivalens szürjektív kódok számát is.

Az alábbiakban néhány egyszerűbb, ill. érdekesebb esetről teszünk említést.

(a) Ha $n = s$ vagy $n = s + 1$, akkor $\sigma_q(n, s)$ értékére nyilvánvalóan fennáll

$$\sigma_q(s, s) = q^s \text{ és } \sigma_q(s + 1, s) = q^s \quad (\text{A.1})$$

tetszőleges 1-nél nagyobb q, s egészekre.

Az MDS kódok elméletéből ismert az alábbi két állítás:

(b₁) Ha q prím vagy prímhatvány és $s < q$, akkor

$$\sigma_q(q + 1, s) = q^s,$$

és következésképpen (továbbra is feltéve, hogy q prím vagy prímhatvány)

$$\sigma_q(n, s) = q^s \text{ minden olyan } n \text{ esetén, melyre } s < n \leq q + 1. \quad (\text{A.2})$$

(b₂) Ha q páros prímhatvány (azaz 2-nek pozitív egész kitevős hatványa), akkor

$$\sigma_q(q + 2, 3) = q^3 \text{ és } \sigma_q(q + 2, q - 1) = q^{q-1}. \quad (\text{A.3})$$

Számos olyan esetben is ismerjük $\sigma_q(n, s)$ értékét, amikor az nagyobb, mint q^n . Ilyen esetek például:

$$(c_1) \sigma_2(4, 2) = 5,$$

$$(c_2) \sigma_2(n, 2) = 6, \text{ ha } 5 \leq n \leq 10,$$

$$(c_3) \sigma_2(n, 2) = 7, \text{ ha } 11 \leq n \leq 15 \text{ stb., a (3.13) formula szerint.}$$

(d) Az alábbi formulát Johnson és Entringer [53], valamint Roux [48] egymástól függetlenül találták. (Lásd még [61], Theorem 6).

$$\sigma_2(n, n - 2) = \lfloor 2^n / 3 \rfloor. \quad (\text{A.4})$$

$$(e_1) \sigma_2(6, 3) = \sigma_2(7, 3) = \dots = \sigma_2(11, 3) = 12, \sigma_2(12, 3) = 15.$$

$$(e_2) \sigma_2(7, 4) = \sigma_2(8, 4) = \dots = \sigma_2(12, 4) = 24.$$

Itt külön érdekesség az (e_2) valamennyi esetéhez tartozó szürjektív kód unicitása. Ezt számítógép segítségével tudtam bizonyítani. (e_1)-nél viszont új eredmény az utolsó esetre

vonatkozó egyenlőség – ugyancsak számítógépes – bizonyítása, mivel eddig csak kisebb vagy egyenlő relációval volt ismert.

Rátérve az általánosított szürjektív kódok vizsgálatára, tekintsük először azokat az eseteket, amikor $K_q(s, r) = q$. A 4.9. állítás szerint az ilyen esetek azok és csak azok, melyekre fennáll $r < s < \frac{qr+q}{q-1}$. Az ilyen esetekhez tartozó egyik optimális térlefedő kód az s dimenziós ismétléses kód, ezért ilyenkor tetszőleges $n \geq s$ esetén az n dimenziós ismétléses kód segítségével adódik, hogy $\sigma_q(n, s; r) = q$. Ilyen esetek pl. az alábbiak: $\sigma_2(n, 3; 1) = 2$, $\sigma_2(n, 5; 2) = 3$, $\sigma_3(n, 4; 2) = 3$, $\sigma_4(n, 5; 3) = 4$ stb. Az is eléggé nyilvánvaló, hogy a $K_q(s, r) = q$ egyenlőséghez tartozó optimális kód unicitása esetén a $\sigma_q(n, s; r) = q$ egyenlőséghez tartozó általánosított szürjektív kódból is csak egy van (az ismétléses kód) tetszőleges $n > s$ esetén.

Egyszerű konstrukcióval adódik a

$$\sigma_2(n, n-1; (n-3)/2) = 4 \quad (\text{A.5})$$

egyenlőség tetszőleges 1-nél nagyobb páratlan n esetére, ami a

$$\{ (0, \dots, 0, 0, 0), \\ (0, \dots, 0, 1, 1), \\ (1, \dots, 1, 0, 1), \\ (1, \dots, 1, 1, 0) \}$$

kód segítségével bizonyítható, de a 3.10. állítás következményeként is kimondható. Hasonló konstrukcióval vagy a 3.12, 3.16, ill. 3.17. tétel következményeként adódik, hogy

$$\sigma_2(n, n-1; (n-4)/2) = 7 \quad (\text{A.6})$$

tetszőleges 4-nél nagyobb páros n esetén,

$$\sigma_2(n, n-1; (n-5)/2) \leq 12 \quad (\text{A.7})$$

tetszőleges 5-nél nagyobb páratlan n esetén,

$$\sigma_2(n, n-1; (n-6)/2) \leq 16 \quad (\text{A.8})$$

tetszőleges 6-nál nagyobb páros n esetén.

A.2. Felső korlátok

A paraméterek kiterjedt tartományára ($2 \leq q \leq 25$, $2 \leq s \leq 6$, $n \leq 10000$ vagy $n \leq 10000$) a Colbourn által készített és időnként frissített [169] táblázat-rendszerben megtalálhatók a $\sigma_q(n, s)$ kifejezés legjobb ismert felső korlátjai. Itt csak néhány esetet említünk, amelyekre valamelyik $K_q(n, R)$ felső korlátjának meghatározásához szükségünk volt:

$$\sigma_3(5, 3) \leq 33, \sigma_3(7, 3) \leq 40, \sigma_4(7, 3) \leq 88.$$

Megjegyezzük, hogy a korlátok esetleges javítása lehetővé tenné $K_q(n, R)$ jelenleg ismert legjobb felső korlátjának a csökkentését néhány esetben. Ha ugyanis feltesszük, hogy a szóban forgó $\sigma_q(n, R)$ értékek valamelyikére (vagy netán ezek mindegyikére) a jelenleg ismert legjobb felső korláthoz képest valaki $\Delta_1, \Delta_2, \Delta_3$ mértékű javítást talál, azaz bizonyítja, hogy

$$\sigma_3(5, 3) \leq 33 - \Delta_1, \quad \sigma_3(7, 3) \leq 40 - \Delta_2, \quad \sigma_4(8, 3) \leq 88 - \Delta_3,$$

akkor az 5.4.1 szakasz végén a példák kapcsán megadott egyenlőtlenségek alapján az adódna, hogy

$$K_6(5, 2) \leq 66 - 2\Delta_1, \quad K_7(5, 2) \leq 97 - \Delta_1,$$

továbbá

$$K_8(7, 4) \leq 92 - 2\Delta_2, \quad K_9(7, 4) \leq 120 - 3\Delta_2, \quad K_{10}(7, 4) \leq 168 - 2\Delta_2 - \Delta_3.$$

A.3. Klasszifikáció és az elérési sugár számítása

Az A.1 szakaszban felsorolt esetek közül az 1.1 szakaszban definiált ekvivalencia értelmében csak az (a), (c), (d) és (e) esetekre ismerünk klasszifikációs eredményt. A vizsgált szűrjektív kódok elérési sugarát a $2 \leq q \leq 10$, $3 \leq n \leq 15$ tartományban számítottuk ki, de általában csak azokra a kódokra, amelyekben a kódszavak száma legfeljebb 10000.

A részletek ismertetését az A.1 szakaszban megadott sorrendben folytatjuk.

(a) Tetszőleges $s \geq 2$ egészre $n = s + 1$ esetén az n dimenziós s -szűrjektív kódok elérési sugara nyilvánvalóan 1, q értékétől függetlenül. A bináris esetben az ilyen s -szűrjektív kódokra minden kódszó súlyának azonos paritásúnak kell lennie, amiből következik az ilyen bináris kódok unicitása. Nagyon egyszerű a klasszifikáció akkor is, ha $n = 3$, $s = 2$ és $q = 3$ vagy $q = 4$. Az utóbbi két esetben az inekvivalens 2-szűrjektív kódok száma 1, ill. 2.

(b) A (b_1) és (b_2) esetre a lineáris kódok körére szűkítetten értelmezett ekvivalenciára nézve ismerünk klasszifikációs eredményeket, lásd [105], [142] és [172]. Néhány speciális esetben ismerjük az MDS kódok elérési sugarának az értékét is. Ilyenek a Reed–Solomon kódok, a szimpla kiterjesztésű Reed–Solomon kódok, lásd [97], Theorem 10.5.7, valamint a dupla kiterjesztésű Reed–Solomon kódok, lásd [81].

(c) $q = 2$, $s = 2$, $3 \leq n \leq 35$ esetére a [145] cikk Table 1 jelű táblázatát átvéve és kissé módosítva, az A.1. és A.2. táblázatokban megadjuk az inekvivalens szűrjektív kódok számát és elérési sugarát. Az A.1. táblázat a $3 \leq n \leq 15$ intervallumra vonatkozóan szám szerint is mutatja a különböző elérési sugarú szűrjektív kódok számát.

(d) Johnson és Entringer [53] bebizonyították a $\sigma_2(n, n - 2)$ -höz tartozó 2-szűrjektív kód unicitását. E kódok elérési sugarára nyilvánvalóan $1 \leq R \leq 2$. A kis n -ekhez tartozó elérési sugarak pontos értékét az A.4. táblázat tartalmazza.

(e) Sloane [79] észrevette, hogy a ± 1 értékű elemekből álló H_{12} Hadamard mátrixból elhagyva azt az egy oszlopot, amelyben csupa azonos érték van, az így adódó 12×11

n	$\sigma_2(n, 2)$	db.	R
3	4	1	1
4	5	1	1
5	6	7	2 mind
6	6	4	2 (3 kód), 3 (1 kód)
7	6	3	3 mind
8	6	1	3
9	6	1	4
10	6	1	5
11	7	26	5 mind
12	7	10	5 (8 kód), 6 (2 kód)
13	7	4	6 mind
14	7	1	6
15	7	1	7

A.1. táblázat. Bináris 2-szűrjektív kódok száma és elérési sugara $3 \leq n \leq 15$ esetén

méretű mátrix sorai 3-szűrjektív kódot alkotnak. Ennek kapcsán felmerült bennem, hogy a változatlanul hagyott Hadamard mátrix soraiból és azok komplementeiből alkotott 24 szóból álló kód hátha 4-szűrjektív. Számítógépes vizsgálat azt mutatta, hogy valóban így van. Ugyanerre a méretre J. Yan [150] és C. J. Colbourn [161] is talált egy-egy konstrukciót, melyek közül az utóbbi ciklikus transláció alapján.

A fentiek szerint $\sigma_2(11, 3) \leq 12$ és $\sigma_2(12, 4) \leq 24$, tehát $\sigma_2(n, 3) \leq 12$, ha $n \leq 11$, ill. $\sigma_2(n, 4) \leq 24$, ha $n \leq 12$. A fordított egyenlőtlenségek $n \geq 6$ ($n \geq 7$) esetén az ismert $\sigma_q(n+1, s+1) \geq q\sigma_q(n, s)$ reláció segítségével bizonyíthatók. Az ezeknek az eseteknek megfelelő egy-egy kód elérési sugarát az A.5. táblázat mutatja.

Néhány további 2-, ill. 3-szűrjektív esetre az elérési sugár a következő értékeket kaptuk: A $\sigma_3(5, 2) = 11$ (lásd Östergård [86]), $\sigma_3(6, 3) = 33$ (lásd Chateauneuf és szerzőtársai [111]), $\sigma_6(4, 2) = 37$ (lásd Stevens [108]) esetekhez tartozó kódok elérési sugara egyaránt 2.

A $\sigma_3(n, 3; 1)$ kifejezéshez tartozó általánosított szűrjektív kódokra a [145] cikk Table 2 jelű táblázatát átvéve és kissé módosítva, az A.6. táblázatban megadjuk az ilyen általánosított szűrjektív kódok számát és elérési sugarát.

Az általánosított szűrjektív kódok bizonyos eseteire a klasszifikáció gép nélkül is könnyűszerrel elvégezhető. Így például könnyen belátható a $\sigma_2(5, 4; 1) = 4$ egyenlőséghez tartozó kód unicitása.

A számítógép használatával kapott eredményeket (számos alsó korlátot és klasszifikációs eredményt) a 9. fejezetben ismertetett algoritmushoz hasonló módszerrel kaptuk. Az egyetlen lényeges eltérés a korábbihoz képest, hogy minden szinten (tehát nemcsak a befejező lépésben) az aktuálisan vizsgált szűrjektív fennállását ellenőrizzük. Az összegyűjtött kódok inekvivalenciájának biztosítása a korábbi esettel teljesen azonos módon történik.

n	$\sigma_2(n, 2)$	db.	R
16	8	700759	7 vagy 8
17	8	579466	7 vagy 8 vagy 9
18	8	440826	8 vagy 9
19	8	309338	9 vagy 10
20	8	200326	9 vagy 10
21	8	119752	10 mind
22	8	65993	10 vagy 11
23	8	33463	11 mind
24	8	15596	11 vagy 12
25	8	6704	12 mind
26	8	2646	12 vagy 13
27	8	977	13 mind
28	8	343	13 vagy 14
29	8	118	14 mind
30	8	39	14 vagy 15
31	8	15	15 mind
32	8	5	15 vagy 16
33	8	2	16 mind
34	8	1	16
35	8	1	17

A.2. táblázat. Bináris 2-szűrjektív kódok száma és elérési sugara $16 \leq n \leq 35$ esetén

n	$\sigma_2(n, 2)$	db.	R
56	9	1	27
126	10	1	63
210	11	1	105
462	12	1	231
792	13	1	396

A.3. táblázat. Extrém bináris 2-szűrjektív kódok száma és elérési sugara

n	$\sigma_2(n, n-2)$	db.	R
5	10	1	1
6	21	1	2
7	42	1	2
8	85	1	2
9	170	1	1
10	341	1	1

A.4. táblázat. Bináris (n-2)-szűrjektív kódok száma és elérési sugara

n	$\sigma_2(n, 3)$	R	$\sigma_2(n + 1, 4)$	R
6	12	2	24	1
7	12	2	24	2
8	12	3	24	3
9	12	3	24	3
10	12	4	24	3
11	12	5	24	4

A.5. táblázat. Néhány bináris 3-szűrjektív és 4-szűrjektív kód elérési sugara

n	$\sigma_3(n, 3; 1)$	db.	R
4	6	7	2 mind
5	7	89	3 mind
6	7	28	3 (6 kód), 4 (22 kód)
7	7	4	4 mind
8	7	1	5
9	7	1	6
10	7	1	6
11	8	239	7 mind
12	8	35	7 (1 kód), 8 (34 kód)
13	8	7	8 mind
14	8	2	9 mind
15	8	1	10

A.6. táblázat. Ternáris, $r = 1$ sugárral 3-szűrjektív kódok száma és elérési sugara

A.4. Térlefedő kódokra vonatkozó korlátok javítása szűrjektív kódok segítségével

A szűrjektív kódok lehető legkisebb méretének ismert pontos értékei és felső korlátai (lásd [166, 169]) segítségével a térlefedő kódokra vonatkozóan is számos, az eddig ismertnél jobb alsó, ill. felső korlátot nyerünk.

Bináris kódra vonatkozóan újonnan nyert alsó korlát a $\sigma_2(9, 7; 2) \geq 10$ -ből és $K(14, 5) \geq 10$ -ből következő, a (4.3) formula alapján bizonyítható alábbi egyenlőtlenség:

$$K(21, 8) \geq \min\{\sigma_2(9, 7; 2), K(14, 5)\} \geq 10.$$

Ezután $\sigma_2(11, 5; 1) \geq 13$ -ból ugyancsak a (4.3) formula alapján kapjuk, hogy

$$K(13, 4) \geq \min\{\sigma_2(11, 5; 1), K(8, 2)\} \geq 12;$$

$$K(15, 5) \geq \min\{\sigma_2(11, 5; 1), K(10, 3)\} \geq 12;$$

$$K(20, 7) \geq \min\{\sigma_2(11, 5; 1), K(15, 5)\} \geq 12;$$

$$K(17, 6) \geq \min\{\sigma_2(11, 5; 1), K(12, 4)\} \geq 11;$$

$$K(22, 8) \geq \min\{\sigma_2(11, 5; 1), K(17, 6)\} \geq 11;$$

$$K(19, 7) \geq \min\{\sigma_2(11, 5; 1), K(14, 5)\} \geq 10;$$

$$K(24, 9) \geq \min\{\sigma_2(11, 5; 1), K(19, 7)\} \geq 10;$$

$$K(26, 10) \geq \min\{\sigma_2(11, 5; 1), K(21, 8)\} \geq 10.$$

Hasonlóan adódik két új ternáris alsó korlát $\sigma_3(5, 2; 0) = 11$, ill. $\sigma_3(9, 5; 2) \geq 10$ ismeretében:

$$K_3(9, 4) \geq \min\{\sigma_3(5, 2; 0), K_3(7, 3)\} \geq 11;$$

$$K_3(12, 6) \geq \min\{\sigma_3(9, 5; 2), K_3(7, 3)\} \geq 10.$$

Hasonló módon kapjuk vegyes ternáris/bináris kódokra az eddig ismerteknél jobb $K(1, 12; 4) \geq 12$, $K(2, 11; 4) \geq 13$, $K(3, 9; 4) \geq 12$, $K(4, 7; 4) \geq 10$, $K(4, 8; 4) \geq 12$, $K(5, 6; 4) \geq 11$, $K(6, 4; 4) \geq 10$, $K(6, 5; 4) \geq 12$, $K(7, 3; 4) \geq 11$, $K(7, 4; 4) \geq 13$, $K(8, 2; 4) \geq 11$, $K(9, 1; 4) \geq 12$ alsó korlátokat.

Néhány felső korlát javítása az (5.13) formula alapján a következő módon adódik:

$n = 8, r = 3, k = 3, s_1 = s_2 = 3, s_3 = 4$ paraméter értékekkel kapjuk, hogy

$$K_6(8, 5) = \sigma_6(8, 8; 5) \leq \sigma_2(8, 3; 0) + \sigma_2(8, 3; 0) + \sigma_2(8, 4; 1) = 2 \cdot 12 + 6 = 30;$$

$$K_8(8, 5) = \sigma_8(8, 8; 5) \leq \sigma_3(8, 3; 0) + \sigma_3(8, 3; 0) + \sigma_2(8, 4; 1) \leq 2 \cdot 42 + 6 = 90;$$

$n = 10, r = 3, k = 4, s_1 = s_2 = s_3 = 3, s_4 = 4$ paraméter értékekkel pedig, hogy

$$K_7(10, 7) \leq \sigma_1(10, 3; 0) + 2 \cdot \sigma_2(10, 3; 0) + \sigma_2(10, 4; 1) = 1 + 2 \cdot 12 + 8 = 33;$$

$$K_8(10, 7) \leq 3 \cdot \sigma_2(10, 3; 0) + \sigma_2(10, 4; 1) = 3 \cdot 12 + 8 = 44.$$

A függelékben tárgyalt szűrjektív kódokra vonatkozóan az alábbi tömörített fájlokban elhelyezett interneten tárolt kód listázások állnak rendelkezésre: A [166] cikk melléklete céljából készült

http://www.sztaki.hu/~keri/arrays/CA_listings.zip
http://www.sztaki.hu/~keri/arrays/CAR_listings.zip
http://www.sztaki.hu/~keri/arrays/CCA_listings.zip
http://www.sztaki.hu/~keri/arrays/CCA1_listings.zip
http://www.sztaki.hu/~keri/arrays/CCA2_listings.zip
http://www.sztaki.hu/~keri/arrays/CCA3_listings.zip

anyagok (melyek közül az első kettőt P. P. Rivas Sorianótól kaptam) továbbá ezek kiegészítéseként a már korábban ismert néhány fontosabb szűrjektív kód listáját tartalmazó

http://www.sztaki.hu/~keri/codes-hu/CA_listings.zip
http://www.sztaki.hu/~keri/codes-hu/CAR_listings.zip
http://www.sztaki.hu/~keri/codes-hu/CCA_listings.zip

anyagok. Mindkét felsorolásból a CC kezdetű zip fájlok a (zömében e munka szerzője által kapott) klasszifikációs eredményeket tartalmazzák.

Irodalomjegyzék

- [1] G. Tarry, Le problème de 36 officiers, *Compte Rendu de l'Assoc. Français Avanc. Sci. Naturel.*, 1 (1900), 122–123 and 2 (1901), 170–203.
- [2] E. Sperner, Ein Satz über Untermengen einer endlichen Menge, *Math. Z.*, 27 (1928), 544–548.
- [3] O. Taussky and J. Todd, Covering theorems for groups, *Ann. Soc. Polon. Math.*, 21 (1948), 303–305.
- [4] M. J. E. Golay, Notes on digital coding, *Proc. I.R.E. (IEEE)*, 37 (1949), 657.
- [5] R. W. Hamming, Error detecting and error correcting codes, *Bell System Tech. J.*, 29 (1950), 147–160.
- [6] E. Mattioli, Sopra una particolare proprietà dei gruppi Abelian finiti, *Ann. Scuola Norm. Sup. Pisa* (3), 3 (1950), 59–65.
- [7] J. G. Mauldon, Covering theorems for groups, *Quart. J. of Math. (Oxford)*, (2) 1 (1950), 284–287.
- [8] S. K. Zaremba, A covering theorem for Abelian groups, *J. London Math. Soc.*, 26 (1951), 71–72.
- [9] S. K. Zaremba, Covering problems concerning Abelian groups, *J. London Math. Soc.*, 27 (1952), 242–246.
- [10] K. A. Bush, Orthogonal arrays of index unity, *Ann. Math. Statistics*, 23 (1952), 426–434.
- [11] A. Fontaine and W. Peterson, Group code equivalence and optimum codes, *IRE Trans. Circuit Theory*, 6 (1959), 60–70.
- [12] E. T. Parker, Orthogonal Latin squares, *Proc. Natl. Acad. Sci. USA*, 45 (1959), 859–862.
- [13] R. C. Bose, S. S. Shrikhande and E. T. Parker, Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture, *Canad. J. Math.*, 12 (1960), 189–203.
- [14] P. Erdős, C. Ko and R. Rado, Intersection theorems for systems of finite sets, *Quart. J. Math. Oxford*, 12 (1961), 313–318.

- [15] S. W. Golomb and E. C. Posner, Rook domains, Latin squares, affine planes, and error-distributing codes, *IEEE Trans. Inform. Theory*, 10 (1964), 196–208.
- [16] H. J. L. Kamps and J. H. van Lint, The football pool problem for 5 matches, *J. Combin. Theory*, 3 (1967), 315–325.
- [17] J. G. Kalbfleisch and R. G. Stanton, A combinatorial theorem of matching, *J. London Math. Soc. (1)*, 44 (1969), 60–64; and (2), 1 (1969), 398.
- [18] R. G. Stanton and J. G. Kalbfleisch, Covering problems for dichotomized matchings, *Aequationes Math.*, 1 (1968), 94–103.
- [19] J. G. Kalbfleisch and P. H. Weiland, Some new results for the covering problem, *Recent Progress in Combinatorics (Proc. 3rd Waterloo Conf. Combinatorics, 1968)* (W. T. Tutte, ed.) Academic, New York (1969), 37–45.
- [20] R. G. Stanton, Covering theorems in groups (or: How to win at football pools), *Recent Progress in Combinatorics (Proc. 3rd Waterloo Conf. Combinatorics, 1968)* (W. T. Tutte, ed.) Academic, New York (1969), 21–36.
- [21] R. G. Stanton, J. D. Horton and J. G. Kalbfleisch, Covering theorems for vectors with special reference to the case of four and five components, *J. London Math. Soc.*, 1 (1969), 493–499.
- [22] R. G. Stanton and J. G. Kalbfleisch, Intersection inequalities for the covering problem, *SIAM J. Appl. Math.*, 17 (1969), 1311–1316.
- [23] H. J. L. Kamps and J. H. van Lint, A covering problem, *Combinatorial theory and its applications, Colloq. Math. Soc. János Bolyai*, Balatonfüred, Hungary (1969), North-Holland, Amsterdam (1970), 679–685.
- [24] E. R. Rodemich, Coverings by rook domains, *J. Combin. Theory*, 9 (1970), 117–128.
- [25] J. G. Kalbfleisch, R. G. Stanton and J. D. Horton, On covering sets and error-correcting codes, *J. Combin. Theory Ser. A*, 11 (1971), 233–250.
- [26] A. Rényi, *Foundations of probability*, Wiley, New York (1971).
- [27] A. Brace and D. E. Daykin, Sperner type theorems for finite sets, *Combinatorics (Proc. Conf. Combinatorial Math., Math. Inst., Oxford)* (D. J. A. Welsh and D. R. Woodall, Eds.), Inst. Math. Appl., Southend-on-Sea (1972), 18–37.
- [28] H. J. Helgert, Noncyclic generalizations of BCH and Srivastava codes, *Information and Control*, 21 (1972), 280–290.
- [29] S. M. Johnson, A new lower bound for coverings by rook domains, *Utilitas Math.*, 1 (1972), 121–140.
- [30] B. Bollobás, Sperner systems consisting of pairs of complementary subsets, *J. Combin. Theory Ser. A*, 15 (1973), 363–366.
- [31] G. O. H. Katona, Two applications (for search theory and truth functions) of Sperner type theorems, *Period. Math. Hungar.*, 3 (1973), 19–26.

- [32] D. J. Kleitman and J. Spencer, Families of k -independent sets, *Discrete Math.*, 6 (1973), 255–262.
- [33] S. L. Snover, The uniqueness of the Nordstrom–Robinson and the Golay binary codes, PhD thesis, *Michigan State University*, 1973.
- [34] J. Dénes and A. D. Keedwell, *Latin squares and their applications*, Academic Press, New York and London (1974).
- [35] Zs. Baranyai, On the factorization of the complete uniform hypergraph, *Infinite and finite sets (Colloq., Keszthely, 1973; dedicated to P. Erdős on his 60th birthday)*, Vol. I, *Colloq. Math. Soc. János Bolyai*, Vol. 10, North-Holland, Amsterdam, (1975), 91–108.
- [36] P. Delsarte and J.-M. Goethals, Unrestricted codes with the Golay parameters are unique, *Discrete Math.*, 12 (1975), 211–224.
- [37] B. Lindström, Group partitions and mixed perfect codes, *Canad. Math. Bull.*, 18 (1975), 57–60.
- [38] G. E. Andrews, *The Theory of Partitions*, Addison-Wesley, Reading (1976).
- [39] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam (1977).
- [40] E. W. Weber, On the football pool problem for 6 matches: A new upper bound, *J. Combin. Theory Ser. A* 35 (1983), 106–108.
- [41] H. Fernandes and E. Rechtschaffen, The football pool problem for 7 and 8 matches, *J. Combin. Theory Ser. A*, 35 (1983), 109–114.
- [42] A. Blokhuis and C. W. H. Lam, More coverings by rook domains, *J. Combin. Theory Ser. A*, 36 (1984), 240–244.
- [43] R. L. Graham and N. J. A. Sloane, On the covering radius of codes, *IEEE Trans. Inform. Theory*, 31 (1985), 385–401.
- [44] D. R. Hughes and F. C. Piper, *Design Theory*, Cambridge University Press, Cambridge (1985).
- [45] D. Billington, Lattices and degree sequences of uniform hypergraphs, *Ars Combin.*, 21A (1986), 9–19.
- [46] G. D. Cohen, A. C. Lobstein, and N. J. A. Sloane, Further results on the covering radius of codes, *IEEE Trans. Inform. Theory*, 32 (1986), 680–694.
- [47] G. D. Cohen, A. C. Lobstein, and N. J. A. Sloane, On a conjecture concerning coverings of Hamming space, *Applied algebra, algorithmics and error-correcting codes (Toulouse, 1984)*, Lecture Notes in Computer Science, Vol. 228, Springer-Verlag, Berlin (1986), 79–89.
- [48] G. Roux, k -propriétés dans des tableaux de n colonnes: cas particulier de la k -surjectivité et de la k -permutivité, Thèse, *Université Paris*, France, (1987), 133 pp.

- [49] L. T. Wille, The football pool problem for 6 matches: a new upper bound obtained by simulated annealing, *J. Combin. Theory Ser. A*, 45 (1987), 171–177.
- [50] I. S. Honkala, Lower bounds for binary covering codes, *IEEE Trans. Inform. Theory*, 34 (1988), 326–329.
- [51] I. S. Honkala and H. O. Hämmäläinen, A new construction for covering codes, *IEEE Trans. Inform. Theory*, 34 (1988), 1343–1344.
- [52] G. J. M. van Wee, Improved sphere bounds on the covering radius of codes, *IEEE Trans. Inform. Theory*, 34 (1988), 237–245.
- [53] K. A. Johnson and R. Entringer, Largest induced subgraphs of the n -cube that contain no 4-cycles, *J. Combin. Theory Ser. B*, 46 (1989), 346–355.
- [54] P. J. M. van Laarhoven, E. H. L. Aarts, J. H. van Lint, and L. T. Wille, New upper bounds for the football pool problem for 6, 7, and 8 matches, *J. Combin. Theory Ser. A*, 52 (1989), 304–312.
- [55] A. C. Lobstein and G. J. M. van Wee, On normal and subnormal q -ary codes, *IEEE Trans. Inform. Theory*, 35 (1989), 1291–1295; and 36 (1990), 1498.
- [56] P. Baldi, On a generalized family of colorings, *Graphs Combin.*, 6 (1990), 95–110.
- [57] W. Chen and I. S. Honkala, Lower bounds for q -ary covering codes, *IEEE Trans. Inform. Theory*, 36 (1990), 664–671.
- [58] L. T. Wille, Improved binary code coverings by simulated annealing, *Congr. Numer.*, 73 (1990), 53–58.
- [59] B. D. McKay, *nauty* user’s guide (version 1.5), Technical Report TR-CS-90-02, Computer Science Department, Australian National University, Canberra, (1990).
- [60] H. Hämmäläinen and S. Rankinen, Upper bounds for football pool problems and mixed covering codes, *J. Combin. Theory Ser. A*, 56 (1991), 84–95.
- [61] I. S. Honkala, Modified bounds for covering codes, *IEEE Trans. Inform. Theory*, 37 (1991), 351–365.
- [62] I. S. Honkala and H. O. Hämmäläinen, Bounds for abnormal binary codes, *IEEE Trans. Inform. Theory*, 37 (1991), 372–375.
- [63] J. H. van Lint and G. J. M. van Wee, Generalized bounds on binary/ternary mixed packing and covering codes, *J. Combin. Theory Ser. A*, 57 (1991), 130–143.
- [64] P. R. J. Östergård, A new binary code of length 10 and covering radius 1, *IEEE Trans. Inform. Theory*, 37 (1991), 179–180.
- [65] P. R. J. Östergård, Upper bounds for q -ary covering codes, *IEEE Trans. Inform. Theory*, 37 (1991), 660–664; and 37 (1991), 1738.
- [66] G. J. M. van Wee, Bounds on packings and coverings by spheres in q -ary and mixed Hamming spaces, *J. Combin. Theory Ser. A*, 57 (1991), 117–129.

- [67] Z. Zhang, Linear inequalities for covering codes: Part I – Pair covering inequalities, *IEEE Trans. Inform. Theory*, 37 (1991), 573–582.
- [68] I. S. Honkala, A Graham-Sloane type construction for s -surjective matrices, *J. Algebraic Combin.*, 1 (1992), 347–351.
- [69] C. Lo and Z. Zhang, New lower bounds for $K_3(n, R)$ from linear inequalities, *Communication Sciences Institute, Electrical Engineering Systems, University of Southern California*, (1992), 15 pp.
- [70] P. R. J. Östergård, Further results on (k, t) -subnormal covering codes, *IEEE Trans. Inform. Theory*, 38 (1992), 206–210.
- [71] Z. Zhang and C. Lo, Linear inequalities for covering codes: Part II – Triple covering inequalities, *IEEE Trans. Inform. Theory*, 38 (1992), 1648–1662.
- [72] A. Barg, At the dawn of the theory of codes, *Mathematical Intelligencer*, 15 (1993), 20–26.
- [73] T. Etzion, G. Greenberg and I. S. Honkala, Normal and abnormal codes, *IEEE Trans. Inform. Theory*, 39 (1993), 1453–1456.
- [74] H. O. Härmäläinen, I. S. Honkala, M. K. Kaikkonen and S. N. Litsyn, Bounds for binary multiple covering codes, *Des. Codes Cryptogr.*, 3 (1993), 251–275.
- [75] E. Kolev, Codes over $\text{GF}(3)$ of length 5, 27 codewords and covering radius 1, *J. Combin. Designs*, 1 (1993), 265–275.
- [76] E. Kolev, Lower bounds for mixed covering codes of length 5, *C. R. Acad. Bulgare Sci.*, (8) 46 (1993), 9–11.
- [77] K. U. Koschnick, A new upper bound for the football pool problem for nine matches *J. Combin. Theory Ser. A*, 62 (1993), 162–167.
- [78] P. R. J. Östergård and H. O. Härmäläinen, New upper bounds for binary/ternary mixed covering codes, *Helsinki University of Technology, Digital Systems Laboratory*, Research Reports, No. 22, (1993), 33 pp.
- [79] N. J. A. Sloane, Covering arrays and intersecting codes, *J. Combin. Designs*, 1 (1993), 51–63.
- [80] G. J. M. van Wee, Some new lower bounds for binary and ternary covering codes, *IEEE Trans. Inform. Theory*, 39 (1993), 1422–1424.
- [81] A. Dür, On the covering radius of Reed–Solomon codes, *Discrete Math.*, 126 (1994), 99–105.
- [82] L. Habsieger, Lower bounds for q -ary coverings by spheres of radius one, *J. Combin. Theory Ser. A*, 67 (1994), 199–222.
- [83] I. S. Honkala, A new lower bound on codes with covering radius one, *Proc. Int. Symp. Information Theory and its Applications*, Sydney, Australia (1994), Vol. 1., 39–41.

- [84] E. Kolev and I. Landgev, On some mixed covering codes of small length, *Algebraic Coding* (G. Cohen, S. Litsyn, A. Lobstein, and G. Zémor, eds.), Lecture Notes in Computer Science, Vol. 781, Springer-Verlag, Berlin (1994), 38–50.
- [85] D. Li and W. Chen, New lower bounds for binary covering codes, *IEEE Trans. Inform. Theory*, 40 (1994), 1122–1129.
- [86] P. R. J. Östergård, Construction methods for mixed covering codes, *Analysis, Algebra, and Computers in Mathematical Research: Proc. 21st Nordic Congress of Mathematicians* (M. Gyllenberg and L. E. Persson, eds.), Marcel Dekker, New York (1994), 387–407.
- [87] P. R. J. Östergård, New upper bounds for the football pool problem for 11 and 12 matches, *J. Combin. Theory Ser. A*, 67 (1994), 161–168.
- [88] E. Kolev, Mixed covering codes with two binary and four ternary coordinates, *Applied algebra, algebraic algorithms and error-correcting codes* Lecture Notes in Computer Science, Vol. 948, Springer-Verlag, Berlin (1995), 312–322.
- [89] J. Bierbrauer, Bounds on orthogonal arrays and resilient functions, *J. Combin. Des.*, 3 (1995), 179–183.
- [90] M. C. Bhandari and C. Durairajan, A note on bounds for q -ary covering codes, *IEEE Trans. Inform. Theory*, 42 (1996), 1640–1642.
- [91] L. Habsieger, A new lower bound for the football pool problem for 7 matches, *J. Thèor. Nombres Bordeaux*, 8 (1996), 481–484.
- [92] L. Habsieger, Some new lower bounds for ternary covering codes, *Electron. J. Combin.*, 3(2) (1996), #R23, 14 pp.
- [93] P. R. J. Östergård, A combinatorial proof for the football pool problem for six matches, *J. Combin. Theory Ser. A*, 76 (1996), 160–163.
- [94] P. R. J. Östergård, The football pool problem, *Congr. Numer.*, 114 (1996), 33–43.
- [95] L. T. Wille, New binary covering codes obtained by simulated annealing, *IEEE Trans. Inform. Theory*, 42 (1996), 300–302.
- [96] J. C. Cock and P. R. J. Östergård, Ternary covering codes derived from BCH codes, *J. Combin. Theory Ser. A*, 80 (1997), 283–289.
- [97] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*, North-Holland, Amsterdam (1997).
- [98] G. D. Cohen, S. N. Litsyn, A. C. Lobstein and H. F. Mattson, Covering radius 1985–1994, *Appl. Algebra Engrg. Comm. Comput.*, 8 (1997), 173–239.
- [99] R. Davies and G. F. Royle, Graph domination, tabu search and the football pool problem, *Discrete Appl. Math.*, 74 (1997), 217–228.
- [100] L. Habsieger, Binary codes with covering radius one: some new lower bounds, *Discrete Math.*, 176 (1997), 115–130.

- [101] P. R. J. Östergård, Constructing covering codes by tabu search, *J. Combin. Designs*, 5 (1997), 71–80.
- [102] P. R. J. Östergård and H. O. Härmäläinen, A new table of binary/ternary mixed covering codes, *Des. Codes Cryptogr.*, 1 (1997), 151–178.
- [103] U. Blass and S. Litsyn, Several new lower bounds on the size of codes with covering radius one, *IEEE Trans. Inform. Theory*, 44 (1998), 1998–2002.
- [104] U. Blass and S. Litsyn, Several new lower bounds for football pool systems, *Ars Combinatoria*, 50 (1998), 297–302.
- [105] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, 2nd ed., Clarendon, Oxford (1998).
- [106] E. Kolev, A $(9, 56)_1$ binary code does not exist, *C. R. Acad. Bulgare Sci.* (11–12), 51 (1998), 25–28.
- [107] P. R. J. Östergård and M. K. Kaikkonen, New upper bounds for binary covering codes, *Discrete Math.*, 178 (1998), 165–179.
- [108] B. Stevens, Transversal covers and packings, PhD thesis, *University of Toronto*, (1998), 148 pp.
- [109] B. Stevens, L. Moura and E. Mendelsohn, Lower Bounds for transversal covers, *Des. Codes Cryptogr.*, 15 (1998), 279–299.
- [110] U. Blass and S. Litsyn, The smallest covering code of length 8 and radius 2 has 12 words, *Ars Combin.*, 52 (1999), 309–318.
- [111] M. A. Chateauneuf, C. J. Colbourn and D. L. Kreher, Covering arrays of strength three, *Des. Codes Cryptogr.*, 16 (1999), 235–242.
- [112] E. Kolev and R. Hill, An improved lower bound on the covering number $K_2(9, 1)$, *Discrete Math.*, 197–198 (1999), 483–489.
- [113] P. R. J. Östergård, New constructions for q -ary covering codes, *Ars Combin.*, 52 (1999), 51–63.
- [114] P. R. J. Östergård and W. D. Weakley, Constructing covering codes with given automorphism, *Designs, Codes and Cryptography*, 16 (1999), 65–73.
- [115] E. Dantsin, A. Goerdt, E. A. Hirsch and U. Schöning, Deterministic algorithms for k -SAT based on covering codes and local search, *Automata, languages and programming (Geneva, 2000)*, Lecture Notes in Computer Science, Vol. 1853, Springer-Verlag, Berlin (2000), 236–247.
- [116] L. Habsieger and A. Plagne, New lower bounds for covering codes, *Discrete Math.*, 222 (2000), 125–149.
- [117] W. Haas, Lower bounds for q -ary codes of covering radius one, *Discrete Math.*, 219 (2000), 97–106.
- [118] P. R. J. Östergård and W. D. Weakley, Classification of binary covering codes, *J. Combin. Des.*, 8 (2000), 391–401.

- [119] C. J. Colbourn and J. H. Dinitz, Mutually orthogonal Latin squares: a brief survey of constructions, *J. Statist. Plann. Inference*, 95 (2001), 9–48.
- [120] I. J. Dejter and K. T. Phelps, Ternary Hamming and binary perfect covering codes. *Codes and association schemes* (A. Barg and S. Litsyn eds.), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., Amer. Math. Soc., Providence, RI, 56 (2001), 111–113.
- [121] P. R. J. Östergård and U. Blass, On the size of optimal binary codes of length 9 and covering radius 1, *IEEE Trans. Inform. Theory*, 47 (2001), 2556–2557.
- [122] J. Quistorff, On codes with given minimum distance and covering radius, *Beiträge Algebra Geom.*, 42 (2001), 601–611.
- [123] M. Chateaneuf and D. L. Kreher, On the state of strength-three covering arrays, *J. Combin. Des.*, 10 (2002), 217–238.
- [124] W. Haas, Binary and ternary codes of covering radius one: some new lower bounds, *Discrete Math.*, 256 (2002), 161–178.
- [125] P. R. J. Östergård and A. Wassermann, A new lower bound for the football pool problem for six matches, *J. Combin. Theory Ser. A*, 99 (2002), 175–179.
- [126] P. R. J. Östergård and W. D. Weakley, Classifying optimal ternary codes of length 5 and covering radius 1, *Beiträge Algebra Geom.*, 43 (2002), 445–449.
- [127] F. Di Pasquale and P. R. J. Östergård, An improved upper bound for the football pool problem for nine matches, *J. Combin. Theory Ser. A*, 102 (2003), 204–206.
- [128] R. L. G. Gommard and A. Plagne, $K_5(7, 3) \leq 100$, *J. Combin. Theory Ser. A*, 104 (2003), 365–370.
- [129] G. Kéri and P. R. J. Östergård, On the covering radius of small codes, *Studia Sci. Math. Hungar.*, 40 (2003), 243–256.
- [130] R. Bertolo, P. R. J. Östergård and W. D. Weakley, An updated table of binary/ternary mixed covering codes, *J. Combin. Des.*, 12 (2004), 157–176.
- [131] J. Carlson and D. Stolarski, The correct solution to Berlekamp’s switching game, *Discrete Math.*, 287 (2004), 145–150.
- [132] G. Kéri and Á. Kisvölcsy, On computing the Hamming distance, *Acta Cybernetica*, 16 (2004), 443–449.
- [133] K. J. Nurmela, Upper bounds for covering arrays by tabu search, *Discrete Appl. Math.*, 138 (2004), 143–152.
- [134] D. Gijswijt, Matrix Algebras and Semidefinite Programming Techniques for Codes, PhD thesis, *University of Amsterdam*, (2005), 93 pp.
- [135] G. Kéri and P. R. J. Östergård, Bounds for covering codes over large alphabets, *Des. Codes Cryptogr.*, 137 (2005), 45–60.
- [136] P. P. Rivas Soriano, private communication by e-mail (2005–2009).

- [137] B. Hnich, S. D. Prestwich, E. Selensky and B. M. Smith, Constraint models for the covering test problem, *Constraints*, 11 (2006), 199–219.
- [138] P. Kaski and P. R. J. Östergård, *Classification Algorithms for Codes and Designs*, Springer, Berlin (2006).
- [139] G. Kéri and P. R. J. Östergård, The number of inequivalent $(2R + 3, 7)R$ optimal covering codes, *J. Integer Seq.*, 9 (2006), Article 06.4.7 (electronic).
- [140] J. Quistorff, Improved sphere bounds in finite metric spaces, *Bull. Inst. Combin. Appl.*, 46 (2006), 69–80.
- [141] W. D. Weakley, Optimal binary covering codes of length 2^j , *J. Combin. Des.*, 14 (2006), 1–13.
- [142] G. Kéri, Types of superregular matrices and the number of n -arcs and complete n -arcs in $PG(r, q)$, *Journal of Combinatorial Designs*, 14 (2006), 363–390 és 16 (2008), 262.
- [143] G. Kéri, On small covering codes in arbitrary mixed Hamming spaces, *Studia Sci. Math. Hungar.*, 44 (2007), 517–534.
- [144] W. Haas, Lower bounds for the football pool problem for 7 and 8 matches, *Electron. J. Combin.*, 14 (2007), #R27, 12 pp.
- [145] G. Kéri and P. R. J. Östergård, Further results on the covering radius of small codes, *Discrete Math.*, 307 (2007), 69–77.
- [146] G. Kéri and Zs. Tuza, Balanced degree sequences of uniform hypergraphs, Note, *manuscript* (2007).
- [147] J. Linderöth, F. Margot and G. Thain, A natural turf for high-throughput computing, <http://www.lehigh.edu/~jtl3/papers/tg-football.pdf> (2007).
- [148] J. Linderöth, F. Margot and G. Thain, Improving bounds on the football pool problem by integer programming and high-throughput computing, *INFORMS Journal on Computing*, 21 (2009), 445–457.
- [149] W. Lang, J. Quistorff and E. Schneider, New results on integer programming for codes, *Congr. Numer.*, 188 (2007), 97–107.
- [150] J. Yan, A backtracking search tool for constructing combinatorial test suites, Technical Report ISCAS-LCS-07-04, Institute of Software, Chinese Academy of Sciences, Beijing, China (2007).
- [151] W. Zhang, S. Wang and X. Zhang, Improving embedding efficiency of covering codes for applications in steganography, *Communications Letters, IEEE*, 11 (2007), 680–682.
- [152] J. Bierbrauer and J. Fridrich: Constructing good covering codes for applications in steganography, *Transactions on Data Hiding and Multimedia Security III*, Lecture Notes in Computer Science, Vol. 4920, Springer-Verlag, Berlin (2008), 1–22.

- [153] C. J. Colbourn, Strength two covering arrays: existence tables and projection, *Discrete Math.*, 308 (2008), 772–786.
- [154] G. Kéri, The covering radius of extreme binary 2-surjective codes, *Des. Codes Cryptogr.*, 46 (2008), 191–198.
- [155] G. Kéri and P. R. J. Östergård, On the minimum size of binary codes with length $2R + 4$ and covering radius R , *Des. Codes Cryptogr.*, 48 (2008), 165–169.
- [156] W. Lang, J. Quistorff and E. Schneider, Integer programming for covering codes, *J. Combin. Math. Combin. Comput.*, 66 (2008), 279–288.
- [157] P. R. J. Östergård and O. Pottonen, The perfect binary one-error-correcting codes of length 15: Part I. Classification, *IEEE Trans. Inform. Theory*, 55 (2009), 4657–4660.
- [158] W. Haas, J.-C. Schlage-Puchta and J. Quistorff, Lower bounds on covering codes via partition matrices, *Journal of Combinatorial Theory (Ser. A)*, 116 (2009), 478–484.
- [159] E. Madsen, private communication by e-mail (2009).
- [160] A. Plagne, A remark on Haas’ method, *Discrete Math.*, 309 (2009), 3318–3322.
- [161] C. J. Colbourn and G. Kéri, Binary covering arrays and existentially closed graphs, *Coding and Cryptography*, Lecture Notes in Computer Science, Vol. 5557, Springer-Verlag, Berlin (2009), 22–33.
- [162] W. Haas, Lower bounds for quaternary covering codes, *Ars Combin.*, to appear.
- [163] J. Quistorff and J.-C. Schlage-Puchta, On generalized surjective codes, *Studia Sci. Math. Hungar.*, to appear.
- [164] W. Haas, I. Halupczok and J.-C. Schlage-Puchta, Lower bounds for q -ary codes with large covering radius, *Electron. J. Combin.*, 16(1) (2009), #R133, 21 pp.
- [165] C. Mendes, E. L. Monte Carmelo and M. Poggi, Bounds for short covering codes and reactive tabu search, *Discrete Appl. Math.*, to appear.
- [166] C. J. Colbourn, G. Kéri, P. P. Rivas Soriano and J.-C. Schlage-Puchta, Covering and radius-covering arrays: constructions and classification, *Discrete Appl. Math.*, to appear.
- [167] Kéri G., A térfedő kódok (covering codes) története, módszertana, rendszerezése, kézirat.
- [168] R. Bertolo, F. Di Pasquale, F. Santisi and others, Sistemi per totocalcio, totip, superenalotto, totogol, <http://www.totolx2.it>.
- [169] C. J. Colbourn, Covering array tables, <http://www.public.asu.edu/~ccolbou/src/tabby/catable.html>.
- [170] D. M. Gordon, La Jolla covering repository, <http://www.ccrwest.org/cover.html>.
- [171] G. Kéri, Tables for covering codes, <http://www.sztaki.hu/~keri/codes>.

- [172] G. Kéri, Tables for n -arcs and lists for complete n -arcs in $PG(r, q)$,
<http://www.sztaki.hu/~keri/n-arcs>.
- [173] A. C. Lobstein, Rayon de recouvrement: une bibliographie? Non, la bibliographie!,
<http://www.infres.enst.fr/~lobstein/biblio.html>.
- [174] P. P. Rivas Soriano, QuiniWin
<http://personal.telefonica.terra.es/web/quiniweb2>.
- [175] N. J. A. Sloane, The on-line encyclopedia of integer sequences,
<http://www.research.att.com/~njas/sequences>.