

Optimális térlefedő kódok kutatása

Kéri Gerzson

Akadémiai doktori értekezés tézisei

Budapest, 2009

Bevezetés

A térlefedő kódok (covering codes) lényegében többdimenziós diszkrét terek (Hamming terek) adott sugárral történő lefedését biztosító halmazok, melyek a számítástechnika számos területén alkalmazhatók. (Adattömörítés, adathiba és adatvesztés dekódolása, műsorszórás tervezése összekapcsolt hálózatokban, egyszer írható memória jobb kihasználása, az emberi beszéd kódolása, sejt elvén alapuló távközlés, logikai formulák kielégíthetőségének vizsgálata, szteganográfiai eljárások.)

A térlefedő kódok alapproblémája: Hamming terekben, vagyis adott hosszúságú bináris, ternáris stb. jelek sorozatai által alkotott terekben előírt elérési sugarú és lehetőleg minél kisebb számosságú kódok keresése. Ugyanez a probléma vegyes Hamming terekben is vizsgálható. Ezek a problémák általában nagyon nehéz optimalizálási problémák, kezelésükre általános módszer nem ismeretes, szinte minden eset külön megfontolást igényel. Az alkalmazott módszertan kombinatorika, kombinatorikus optimalizálás, lineáris algebra, egészértékű programozás 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 megvizsgálására is szükség lehet. Általában komoly eredménynek számít az optimum értékére jó alsó, illetve felső korlát megadása, ami ma már általában az ismert alsó vagy felső korlát javítását jelenti. Az optimális kód(ok) méretének pontos értéke csak kevés esetben ismeretes.

I. A kitűzött kutatási feladat rövid összefoglalása

Kódelméleti kutatásaim elsődleges motivációja hézagpótlás célzatú. Östergårddal közösen (az én kezdeményezésemre) lefolytatott vizsgálatokkal, elemzésekkel feltérképeztük a legfeljebb 8 kódszóval megadható bináris, ternáris, ill. vegyes ternáris/bináris optimális térlefedő kódok valamennyi lehetséges esetét. Korábban ilyen eredmény a bináris kódok esetén csak 7 kódszónál rövidebb, a ternáris kódok esetén csak 5 kódszónál rövidebb, a vegyes ternáris/bináris kódok esetén pedig csak 3 kódszónál rövidebb kódok esetére volt ismert. Az értekezésben tárgyalt további eredmények egy része is társszerzős, de többségük egyedül elért eredmény. A célul kitűzött kutatási eredményeket illetően elsősorban olyan eredmények elérésére törekedtem, amelyek valamilyen – egy vagy több paramétert tartalmazó – általánosabb megfogalmazásban fejezik ki optimális térlefedő kódok méretét, illetve annak egyik vagy mindkét irányból vett korlátját. Mivel a bináris és ternáris térlefedő kódokra vonatkozó ismeretek viszonylag jóval kiterjedtebbek a sportfogadásokra történő közismert alkalmazási lehetőségük miatt, azért elsősorban az ilyen kódok körében egyedi (vagyis nem paraméterrel megadott) esetekkel külön is érdemes foglalkozni.

II. Az elvégzett vizsgálatok, a feldolgozott módszerek, a források

Az elvégzett vizsgálatok és módszerek

1. Mindegyik tárgyalt kód kategória esetén először azt a kérdést vizsgáljuk, hogy milyen feltételek fennállása biztosítja az optimális térlefedő kódok különböző, előre megadott méreteit. Ehhez általában valamilyen paraméteres egészértékű lineáris programozási probléma megoldására van szükség. Kézenfekvő módszernek látszik a relaxált LP probléma megoldása primál simplex módszerrel, majd a paraméterek különböző arányaihoz tartozó optimális megoldásokra való áttéréseknek duál simplex módszerrel történő megvalósítása. A tételek kimondásához több esetben ilyen indulással jutottam el, prezentálásuk és bizonyításuk viszont szebben valósítható meg lineáris programozási módszerek nélkül, elemi egyenlőtlenségekkel, továbbá kombinatorikai és logikai megfontolásokkal, ezért ez utóbbi utat választottam.
2. Amennyiben a pontos méret értékét nem tudjuk meghatározni, egyenlőtlenségeket, lehetőleg általános, paraméteres egyenlőtlenségeket keresünk az optimális kódok méretének alsó vagy felső korlátja kifejezésére. Ehhez jó módszertani segédeszköznek bizonyult a szűrjektív és általánosított szűrjektív kódok alkalmazása.
3. A szűrjektív, általánosított szűrjektív kódok nemcsak módszertani segédeszközök, hanem maguk is vizsgálatok tárgyai, melyeknek megvan a saját módszertani eszköztára. Ilyenek a lefedő tömbök (covering arrays) kutatási területén alkalmazott *ortogonális tömbök*, *kompozíció*, *simulated annealing*, *tabu search*, esetleg valamilyen *mohó algoritmus* módszere, továbbá olyan speciális szűrjektív kódokra vonatkozó sajátos módszertani eszközök, mint amilyenek az MDS kódok és a latin négyzetek.
4. Szűrjektív kódok elérési sugara lehetséges tartományának a meghatározása is egyrészt vizsgálat tárgya, de ugyanakkor eszköz az optimális térlefedő kódok méretének behatárolására. Az ide tartozó számításokhoz kombinatorikai és számítógépes módszereket egyaránt alkalmaztam, de főleg az utóbbiakat.
5. Az extrém szűrjektív kódok elérési sugarának meghatározásához hipergráfok segítségét vettem igénybe.
6. Az elvégzett klasszifikációs vizsgálatok eszközei is részben kombinatorikai, részben számítógépes módszerek. Az utóbbiak a vizsgált kódok valamilyen fajta lexikografikus rendezésén alapulnak.

A legfontosabb fogalmak ismertetése

Hamming távolság, Hamming metrika, Hamming tér

Az $x, y \in Z_q^n$ pontok 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 részhalmaza a 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.

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

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

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

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

Optimális térlefedő kód

Adott q alapszám, n dimenziószám 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 $K_q(n, R)$ kifejezés értelmezése

A q, n, R paraméterekhez tartozó optimális térlefedő kódok méretét fejezzük ki vele.

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 részhalmaza értjük, ahol $m \geq 1$, $n_i \geq 0$, $\sum_{i=1}^m n_i \geq 1$ és $q_i \geq 2$. A $K_q(n, R)$ kifejezés megfelelője vegyes kódok esetén a $K_{q_1, q_2, \dots, q_m}(n_1, n_2, \dots, n_m; R)$ kifejezés.

Források

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

A fentiek részletesebb kifejtését és a folytatódó történetet az értekezés 2. fejezete („A térlefedő kódok rövid története”) tartalmazza.

Az irodalmi forrásokat az értekezés irodalomjegyzéke sorolja fel. A témakör irodalmának egy bővebb gyűjteménye található az A. Lobstein által összeállított és karbantartott <http://www.infres.enst.fr/~lobstein/biblio.html> weblapon.

III. A tudományos eredmények rövid összefoglalása

Az értekezésben bizonyított tételek közül 32 szerepel ebben az összefoglalásban, mégpedig 14 társszerzővel kapott és 18 egyedül elért eredményre vonatkozó tétel. A tételeknek az összefoglalóban található sorszámai az értekezésben képzett sorszámaikkal azonos, ezért itt a számozás hézagos. A felhasználásra kerülő könnyebben bizonyítható vagy ismert eredmények az értekezésben nem tételként, hanem *állításokként* kerülnek megfogalmazásra. Kivétel ez alól az 5.3. és a 8.2. Tétel, melyeknek a bizonyítása viszonylag egyszerű, a második esetben kifejezetten könnyű, ezeket azonban elvi jelentőségük miatt soroltam mégis a tételek közé. Az új klasszifikációs eredményeket is tételként fogalmaztam meg, beleértve a nagyon egyszerűen bizonyítható 6.29. Tételt is. Több esetben *állításokként* fogalmaztam meg az olyan korábbi eredményeket, amelyek a tételekben kimondott eredmények előzményeinek tekinthetők. Ezeket az állításokat ugyancsak az eredeti számozással – de kisebb betűmérettel szedve – adom meg ebben az összefoglalásban. Néhány esetben számozás nélküli *állításokként* utalok az előzményre vagy előzményekre. A *lemmákat* segédtétel értelemben használok, ezek eszközül szolgálnak különböző tételek bizonyításához. A *következmények* többnyire lemmákból, de néhány esetben tételekből vagy más következményekből levezethető állítások.

A tárgyalt kód kategóriák mindegyike esetén az optimális térlefedő kódok méretére vonatkozó eredményekkel kezdem. (Méreten a kódszavak számát értve.) Az ilyen eredmények általában a $K_q(n, R)$, ill. vegyes kódok esetén pl. a $K_{3,2}(t, b; R)$ vagy $K_{4,3,2}(q, t, b; R)$ kifejezés értékére vagy valamelyik (esetleg mindkét) korlátjára vonatkozó relációként kerülnek megfogalmazásra. A méretekre vonatkozó eredmények után következnek a klasszifikációs, majd a térlefedő kódokkal összefüggésben kapott egyéb eredmények.

Az optimális térlefedő kódok méretének a problémája a következőképpen is megfogalmazható. Adott kód kategória és adott méret esetén mely paraméter-értékek esetére teljesül, hogy az optimális térlefedő kódok mérete a megadott mérettel egyenlő?

Ha ez a megadott méret 1, akkor a válasz triviális, hiszen egyetlen kódszóból álló kód elérési sugara a teljes dimenziószámmal, az általános esetben $\sum_{i=1}^m n_i$ -vel egyenlő. Ezen a triviális eseten kívül az előbbi formában feltett kérdésre csak kevés esetben ismerjük a választ. Egy ilyen eset a következő, amelynek az ismerete több kód kategória esetén is fontos kiindulópont és egyúttal előzmény az újabb eredményekhez. Először W. Chen és I. S. Honkala a „Lower bounds for q -ary covering codes”, *IEEE Trans. Inform. Theory*, Vol. 36, 1990, 664–671. cikkben fogalmazták meg az alábbi állítást (amely a skatulya elv alapján könnyen bizonyítható).

Állítás.

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

Az általános q alapszám esetére a fent megfogalmazott állításnál lényegesen többet ma sem tudunk mondani. Azt az egyet könnyen be lehet látni, ezért már régóta ismert tény, hogy tetszőleges adott q esetén 1-nél több és q -nál kevesebb kódszóból álló optimális térlefedő kód nem létezik. Ugyancsak evidens a vegyes kódokra vonatkozó hasonló állítás, mely szerint 1-nél több és a pozitív n_i értékekhez tartozó q_i alapszámok minimumánál kevesebb kódszóból álló optimális térlefedő kód szintén nem létezik.

A továbbiakban az értekezés fejezetei szerint haladva sorra vesszük az egyes tárgyalt kód kategóriákat.

Bináris térlefedő kódokra az alábbiakban foglaljuk össze a régi és új eredményeket.

G. D. Cohen, A. C. Lobstein és N. J. A. Sloane „Further results on the covering radius of codes”, *IEEE Trans. Inform. Theory* Vol. 32, 1986, 680–694. cikke tartalmazza az alábbi eredményeket:

Állítás.

$$K_2(n, R) = 4 \text{ akkor és csak akkor áll fenn, ha } n = 2R + 2.$$

$$K_2(n, R) = 7 \text{ ha } n = 2R + 3 \text{ és } R \text{ pozitív egész.}$$

$$7 \leq K_2(n, R) \leq 12 \text{ ha } n = 2R + 4 \text{ és } R \text{ pozitív egész.}$$

Cohen és szerzőtársai idézett cikkéből az is kiderül, hogy 3, 5 vagy 6 kódszóból álló bináris optimális térlefedő kód nem létezik. Nyitva maradt akkor még az a kérdés, hogy az általuk leírt eseteken kívül van-e más olyan eset, amelyre $K_2(n, R) = 7$.

Bináris 2-szűrjektív kódokra vonatkozó klasszifikációs eredmények alapján a fenti állítás harmadik sorában megadott általános alsó korlátot az alábbi tétel szerint 7-ről 9-re tudtuk javítani. (K. és Östergård, a IV. részben 8. sorszámmal megadott cikk, Theorem 8.)

3.7. Tétel.

$$9 \leq K_2(2R + 4, R) \leq 12 \text{ fennáll tetszőleges pozitív egész } R \text{ esetén.}$$

A fentebb tárgyalt korábbi ismeretek alapján a legfeljebb 6 kódszóból álló optimális térlefedő kódok méretére vonatkozó ismert eredményeket a következőképpen foglalhatjuk össze:

3.8. Állítás.

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

$$K_2(n, R) = 3 \text{ nem lehetséges;}$$

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

$$K_2(n, R) = 5 \text{ nem lehetséges;}$$

$$K_2(n, R) = 6 \text{ nem lehetséges.}$$

A jórészt a 3.7. Tételen alapuló új eredmény a következő. (K. és Östergård, 8. sorszámu cikk.)

3.9. Tétel.

$K_2(n, R) = 7$ 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 $n = 3$.

A fenti tétel első állításához kapcsolódó új klasszifikációs eredmény a következő. (K. és Östergård, 7. sorszámú cikk, Theorem 3.3.)

3.13. Tétel.

Minden olyan esetben, amikor $K_2(n, R) = 7$, a nem ekvivalens 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.

Az értekezés 3.12. Tétele az összes lehetséges optimális kód leírását tartalmazza.

A 3.7. Tétel néhány speciális esetére egyenlőséget és klasszifikációs eredményt tudunk megfogalmazni. ($R = 1$ és $R = 2$ esetén korábban ismert, $R = 3$ esetén új eredmény.)

3.14. Állítás.

A $K_2(6, 1) = 12$ 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 $K_2(8, 2) = 12$ 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, ill. Blass és Litsyn bizonyították, az inekvivalens optimális kódok számának meghatározása mindkét esetre Östergård és Weakley eredménye. Az optimális kódok kiegyensúlyozottság és szűrjektivitás szerinti megoszlását már én tettem hozzá.

A következő tételben megfogalmazott esetre az egyenlőség bizonyítása és a klasszifikáció egyaránt K. és Östergård eredménye (11. sorszámú cikk).

3.15. Tétel.

$K_2(10, 3) = 12$ 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-szűrjektív 1490 kód, az 5938 kiegyensúlyozatlan optimális kód közül pedig 2-szűrjektív 1589 kód.

Bináris térlefedő kódok méretének alsó korlátjának kérdéséhez kapcsolódóan merült fel a 2-szűrjektív kódok lehetséges elérési sugarainak a vizsgálata. Erre vonatkozóan *extrém* bináris 2-szűrjektív kódok elérési sugarára egy önmagában is érdekes eredményt kaptam.

Előzményként említhető Bollobás, Brace és Daykin, Katona, illetve Kleitman és Spencer egymástól függetlenül elért egyik eredménye, amely egy binomiális együtthatós formulával megadja

az adott számú kódszóból álló 2-szűrjektív bináris kódok dimenziószámának a maximális lehetséges értékét (más megfogalmazásban). Ez az érték M kódszó esetén nem lehet nagyobb, mint

$$\binom{M-1}{\lfloor (M-2)/2 \rfloor}.$$

A felsorolt szerzők idevágó publikációiból az is kiderül, hogy $n = \binom{M-1}{\lfloor (M-2)/2 \rfloor}$ esetén a Z_q^n térben (izomorfiától eltekintve) egyetlen M kódszóból álló 2-szűrjektív kód létezik, melynek a struktúráját is megadták. Ehhez kapcsolódik a következő tétel állítása, amely hipergráfok segítségével bizonyítható. Ez egyedül elért eredmény, melyre két különböző bizonyítást is találtam. Az egyikhez Baranyai faktorizációs tételére, a másik bizonyításhoz pedig egy k -uniform hipergráfokra vonatkozó egzisztenciátételre volt szükség. Az első bizonyítást az értekezés, a másodikat a 10. sorszámú cikk tartalmazza.

3.21. Tétel.

Ha $n = \binom{M-1}{\lfloor (M-2)/2 \rfloor}$, akkor a Z_q^n térben megadható egyetlen M kódszóból álló 2-szűrjektív kód elérési sugara $\frac{n}{2} - 1$, ha $M = 2^p + 1$ alakú, valamely 1-nél nagyobb p egészre; $\lfloor \frac{n}{2} \rfloor$ egyébként.

Ternáris térlefedő kódokra kapott eredmények összefoglalása.

A régi és új eredmények alapján kiderül, hogy $K_3(n, R)$ értéke 1, 3, 5, 6, 8 vagy az utóbbi fölötti érték lehet. Ezek közül a legkisebb méretek esetére nyilvánvaló módon, ill. a q alapszámra már általánosan felírt állítás speciális eseteként adódik a következő.

4.1. Állítás.

$$\begin{aligned} K_3(n, R) &= 1 \text{ akkor és csak akkor, ha } n = R; \\ K_3(n, R) &= 2 \text{ nem lehetséges;} \\ K_3(n, R) &= 3 \text{ akkor és csak akkor, ha } R < n < \frac{3R+3}{2}. \end{aligned}$$

Ternáris szűrjektív kódok segítségével bizonyítható az alábbi három tétel állítása. (Eredetileg K. és Östergård, 1. sorszámú cikk, Theorem 11, ill. 8. sorszámú cikk, Theorem 3, 5, 9 és 10.)

4.6. Tétel.

$$\begin{aligned} K_3(n, R) &= 4 \text{ nem lehetséges;} \\ K_3(n, R) &= 5 \text{ akkor és csak akkor, ha } n = 3 \text{ és } R = 1; \\ K_3(n, R) &= 6 \text{ akkor és csak akkor, ha } R \geq 3, \text{ páratlan és } n = \frac{3R+3}{2}; \\ K_3(n, R) &= 7 \text{ nem lehetséges.} \end{aligned}$$

4.7. Tétel.

$$K_3(n, R) = 8 \text{ akkor és csak akkor áll fenn, ha } n = 5 \text{ és } R = 2.$$

4.8. Tétel.

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

A 9 kódszóra megadott feltétel szükségessége egyelőre még nyitott kérdés.

A ternáris esetre bizonyított, egyedül elért új klasszifikációs eredmény a következő.

4.10. Tétel.

Minden olyan esetben, amikor $K_3(n, R) = 3$, a nem ekvivalens 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.

Speciális esetre vonatkozó egyedül elért új eredmény a következő. (Speciális volta ellenére ennek az eredménynek a jelentőségét az adja, hogy ternáris optimális térlefedő kódok körében eddig ez volt a legegyszerűbb olyan eset, melyre korábban nem volt még megoldva a klasszifikáció, továbbá hogy ennek segítségével szűrjektív kódokra is sikerült új eredményeket kapni.)

4.11. Tétel.

Az $n = 6, R = 3$ paraméter értékekhez tartozó inekvivalens ternáris optimális térlefedő kódok száma 28.

Szűrjektív kódokra és nagyobb alapszámú térlefedő kódokra vonatkozó eredmények.

A szűrjektív kódok (amennyiben a kódszavak ismétlődését is megengedjük) és a lefedő tömbök (covering arrays) egymással ekvivalens fogalmak. Az ezek közül általam elsősorban vizsgált extrémális tulajdonságú objektumokban szűrjektív kód esetén ugyanaz a kódszó, lefedő tömb esetén ugyanaz a sor egynél többször nyilvánvalóan nem fordul elő.

Definíciók:

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.

Egy $CA(M; s, n, q)$ lefedő tömb 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.

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 utóbbitól legfeljebb r koordináta helyen tér el.

Az r sugárral s -szűrjektív kód általam bevezetett fogalma egyszerre általánosítása a hagyományos értelemben vett szűrjektív kódnak ($r = 0$ esetén) és a térlefedő kódnak ($s = n$ esetén). Hasonlóan a lefedő tömb (covering array) fogalmának az általánosítása (melyre Charles J. Colbourn javaslatára angol nyelven a *radius-covering array* elnevezést fogadtam el) nemcsak a hagyományos értelemben vett lefedő tömbnek, hanem a térlefedő kódnak is általánosítása.

Mindkét fajta szűrjektív kód (lefedő tömb) fogalma igen hasznosnak bizonyult térlefedő kódok méretének vizsgálatához.

Jelölje $\sigma_q(n, s; r)$ a q alapszámhoz és n dimenziószámhoz tartozó, legfeljebb r sugárral s -szűrjektív kódok méretének a minimumát. Ennek megfelelője a lefedő tömbök terminológiájában a $CAN_r(s, n, q)$ függvény, amely azt a legkisebb M értéket jelenti, melyre létezik $CA_r(M; s, n, q)$ lefedő tömb.

Szürjektív kódokkal kifejezett összefüggéseket már az értekezés előző fejezeteiben felhasználtunk alsó korlátok bizonyításához. Nem vegyes (tehát bináris, ternáris vagy magasabb alapszámú) kódok esetén az 1. számú cikkben (K. és Östergård) Theorem 2, az értekezésben 4.3. Következmény keretében tárgyalt alábbi egyenlőtlenséget tudjuk alkalmazni.

4.3. Következmény.

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

Ennek alapján adódnak az eddig említett eredményeken kívül bináris kódokra konkrétan a $K_2(13, 4) \geq 12$, $K_2(15, 5) \geq 12$, $K_2(16, 6) \geq 9$, $K_2(17, 6) \geq 11$, $K_2(18, 7) \geq 9$ stb. egyenlőtlenségek, ternáris kódokra a $K_3(9, 4) \geq 11$, $K_3(9, 5) \geq 6$, $K_3(10, 5) \geq 9$, $K_3(11, 5) \geq 11$, $K_3(12, 6) \geq 10$, $K_3(13, 7) \geq 9$, $K_3(14, 8) \geq 9$ korlátok, $q = 4$ esetére pedig a $K_4(7, 4) \geq 8$, $K_4(8, 5) \geq 8$, $K_4(10, 6) \geq 8$ és $K_4(11, 7) \geq 8$ korlátok.

Szürjektív kódokra vonatkozó ismereteket a $K_q(n, R)$ kifejezésnek nemcsak alsó, hanem felső korlátjának vizsgálatára is fel tudunk használni. Az 5. számú cikkben (K. és Östergård) bebizonyítjuk a következő egyenlőtlenséget.

5.3. Tétel.

$$\sigma_{q_1+\dots+q_k}(n, 1 - k + \sum_{i=1}^k s_i; 1 - k - r + \sum_{i=1}^k s_i) \leq \sum_{i=1}^k \sigma_{q_i}(n, s_i; s_i - r).$$

A fenti tétel jelentőségét a nagyobb alapszámú térlefedő kódokra való alkalmazhatósága mutatja. E tétel segítségével $K_q(n, R)$ felső korlátjára az értekezés mellékletében táblázatba foglalt esetek közül 108 esetben a jelenleg ismert legkisebb korlátot kapjuk, amely 18 esetben élesnek bizonyult. Néhány példa egyenlőséggel:

$$\begin{aligned} K_{17}(5, 3) = 73, \quad K_{18}(5, 3) = 82, \quad K_{19}(5, 3) = 91, \quad K_6(6, 4) = 10, \\ K_7(7, 5) = 11, \quad K_8(8, 6) = 12, \quad K_9(9, 7) = 13, \quad K_{10}(10, 8) = 14, \end{aligned}$$

ill. egyenlőtlenséggel:

$$\begin{aligned} K_6(8, 5) = \sigma_6(8, 8; 5) &\leq \sigma_2(8, 3; 0) + \sigma_2(8, 3; 0) + \sigma_2(8, 4; 1) = 2 \cdot 12 + 6 = 30, \\ K_8(8, 5) = \sigma_8(8, 8; 5) &\leq \sigma_3(8, 3; 0) + \sigma_3(8, 3; 0) + \sigma_2(8, 4; 1) \leq 2 \cdot 42 + 6 = 90, \end{aligned}$$

$$\begin{aligned} K_7(10, 7) &\leq \sigma_1(10, 3; 0) + 2 \cdot \sigma_2(10, 3; 0) + \sigma_2(10, 4; 1) = 1 + 2 \cdot 12 + 8 = 33, \\ K_8(10, 7) &\leq 3 \cdot \sigma_2(10, 3; 0) + \sigma_2(10, 4; 1) = 3 \cdot 12 + 8 = 44. \end{aligned}$$

J. G. Kalbfleisch és R. G. Stanton az „A combinatorial theorem of matching” J. London Math. Soc. (1), Vol. 44 (1969), 60–64. cikkben lényegében szürjektív kódok segítségével (de a későbbi keletű *szürjektív kód* elnevezést nem használva) bizonyították a következőt.

Állítás.

$$K_q(3, 1) = \left\lceil \frac{q^2}{2} \right\rceil.$$

Kalbfleisch és Stanton eredményének bizonyos értelemben és bizonyos mértékig általánosításai a következő, E. R. Rodemich (Coverings by rook domains, „J. Combin. Theory” Vol. 9 (1970), 117–128.) által bizonyított egyenlőtlenségek.

Állítás.

$$K_q(4, 2) \geq \left\lceil \frac{q^2}{3} \right\rceil, K_q(5, 3) \geq \left\lceil \frac{q^2}{4} \right\rceil, \dots, K_q(n, n-2) \geq \left\lceil \frac{q^2}{n-1} \right\rceil.$$

Rodemich megadta az egyenlőség fennállásának alábbi szükséges és elégséges feltételét is.

Állítás.

$K_q(n, n-2) = \frac{q^2}{n-1}$ akkor és csak akkor, ha q osztható $(n-1)$ -gyel, és a $q/(n-1)$ rendű latin négyzetek között található legalább $n-2$ páronként ortogonális.

Felmerült bennem a kérdés: Vannak-e olyan esetek, amikor $K_q(n, n-2)$ értéke a $\frac{q^2}{n-1}$ tört pontos értékével nem, de annak felső egész részével már egyenlő? Könnyen belátható, hogy sok ilyen eset van, azonban az ilyen esetek általánosan történő megadása nagyon nehéz problémának tűnik. Az alábbi tételben felírt speciális esetre vonatkozó állítást azonban szürjektív kódok segítségével nem nehéz bebizonyítani.

5.5. Tétel.

$$K_q(4, 2) = \left\lceil \frac{q^2}{3} \right\rceil, \text{ ha } 9 \leq q \leq 15 \text{ vagy } q \geq 21.$$

A következő tétel állítása $q = 2$ és $q = 3$ esetre régóta ismert, a $q = 4$ -re és $q = 5$ -re történő bizonyítása viszont új klasszifikációs eredmény.

5.6. Tétel.

$$A K_q(3, 1) = \left\lceil \frac{q^2}{2} \right\rceil \text{ egyenlőséghez tartozó optimális kód } 2 \leq q \leq 5 \text{ esetén egyértelmű.}$$

Vegyes térlefedő kódokra kapott eredmények összefoglalása.

Vegyes ternáris/bináris kódok esetén a két legkisebb méretre (1, ill. 2 kódszó) vonatkozó alábbi állítás bizonyítása könnyű.

6.1. Állítás.

$$\begin{aligned} K_{3,2}(t, b; R) &= 1 \text{ akkor és csak akkor áll fenn, ha } R = t + b; \\ K_{3,2}(t, b; R) &= 2 \text{ akkor és csak akkor áll fenn, ha } t + \left\lfloor \frac{b}{2} \right\rfloor \leq R < t + b. \end{aligned}$$

A 3, ill. 4 kódszó esetre vonatkozó hasonló eredmények feltárásához és bizonyításához már komolyabb ötletekre volt szükség. Az alábbi két tétel első bizonyítását paraméteres egészértékű lineáris programozási probléma vizsgálatával adtam meg, a K. és Östergård, 1. sorszámú cikkben (Theorem 1) publikált és az értekezésbe is átültetett bizonyítás rövidebb, de a lineáris programozási háttér ezáltal rejtve maradt.

6.12. Tétel.

$K_{3,2}(t, b; R) = 3$ akkor és csak akkor áll fenn, ha

$$\min \left\{ \left\lceil \frac{2t+2b}{3} \right\rceil, \left\lceil \frac{3t+2b}{4} \right\rceil \right\} \leq R < t + \left\lfloor \frac{b}{2} \right\rfloor.$$

6.15. Tétel.

$K_{3,2}(t, b; R) = 4$ 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 $R = \frac{b}{2} - 1$.

Részben az eddigiekhez hasonló, részben azoktól eltérő gondolatmenetekre épül az értekezésből kiragadott következő négy tétel bizonyítása.

E tételek felírását megelőzően itt szeretném közbevetőleg megjegyezni, hogy a 6.15., 6.18. és 6.23. Tételek előzményeinek tekinthető egyes eredmények megtalálhatók E. Kolev és I. Landgev, On some mixed covering codes of small length, Algebraic Coding, Lecture Notes in Computer Science, Vol. 781, Springer-Verlag, Berlin (1994), 38–50. oldalon közölt publikációban; ezek az eredmények a következők: négy kódszó esetére $K_{3,2}(2, 2R - 1; R) = 4$; öt kódszó esetére $K_{3,2}(3, 2R - 2; R) = 5$; hat kódszó esetére $K_{3,2}(1, 2R + 1; R) = 6$, $K_{3,2}(2, 2R; R) = 6$ és $K_{3,2}(4, 1; 2) = 6$. Az előző és az alább felsorolt általunk adott tételekben megfogalmazott eredmények ezeknél általánosabbak, teljesebbek, s ennél is lényegesebb különbség, hogy szükséges és elégséges feltételek, míg az előzménybeliek csak elégségesek.

6.18. Tétel. (K. és Östergård, 1. sorszámú cikk, Theorem 11.)

$K_{3,2}(t, b; R) = 5$ 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 $R = 1$.

6.23. Tétel. (K. és Östergård, 8. sorszámú cikk, Theorem 5. és 7.)

$K_{3,2}(t, b; R) = 6$ 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 $R = \frac{b}{2}$;

$K_{3,2}(t, b; R) = 7$ 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 $R = \frac{2t-4}{3} + \frac{b}{2}$.

6.24. Tétel. (K. és Östergård, 8. sorszámú cikk, Theorem 11. és 12.)

$K_{3,2}(t, b; R) = 8$ fennáll, ha $t = 1$, b kettőnél nagyobb páros egész és $R = \frac{b}{2} - 1$, vagy pedig t hárommal osztható pozitív egész, b egynél nagyobb páratlan egész és $R = \frac{2t}{3} + \frac{b-3}{2}$.

6.25. Tétel. (K. és Östergård, 8. sorszámú cikk, Theorem 13. és 14.)

$K_{3,2}(3u, 1; 2u - 1) = 9$ ha $1 \leq u \leq 3$.

Vegyes ternáris/bináris kódokra vonatkozó új (egyedül elért) klasszifikációs eredményeket tárgyal az értekezés 6.5 szakasza. Az itt szereplő tételek közül az első könnyen bizonyítható, a többihez már ötletekre van szükség.

6.29. Tétel.

Ha $t > 0$, b páratlan pozitív egész és $R = t + \frac{b-1}{2}$, akkor $t + 1$ inekvivalens optimális kód létezik:

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

6.30. Tétel.

Ha $t = 1$, b páros pozitív egész és $R = \frac{b}{2}$, akkor ekvivalenciától eltekintve az alábbi egyetlen optimális kód létezik:

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

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:

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

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.

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

6.33. Tétel.

$t = 4$, $b = 1$, $R = 3$ esetén 5 inekvivalens optimális kód létezik.

6.34. Tétel.

Ha $t = 2$, $b = 1$ és $R = 1$, akkor az alábbi két inekvivalens optimális kód létezik:

$$\begin{array}{ccc} \{ (0, 0, 0), & & \{ (0, 1, 0), \\ (0, 0, 1), & & (0, 2, 0), \\ (1, 1, 0), & \text{és} & (1, 0, 1), \\ (2, 2, 1) \} & & (2, 0, 1) \}. \end{array}$$

Megjegyzem, hogy erre a kód kategóriára vonatkozó klasszifikációs kérdésekkel tudomásom szerint eddig még senki más nem foglalkozott rajtam kívül.

Az itt említett tételek folytán megoldott eseteken kívül számos további esetre az értekezés 9. fejezetében ismertetett algoritmus és program használatával kaptam klasszifikációs eredményekre.

A vegyes ternáris/bináris kódokra az értekezés mellékletét képező anyag

táblázata a paraméterek véges tartományára vonatkozóan mutatja, hogy eddig milyen esetekre sikerült meghatározni az inekvivalens optimális kódokat. (Ezek számát a felső indexek tartalmazták a táblázatban.)

Különösen vegyes térlefedő kódokra kapott eredmények összefoglalása.

Az ebben a részben tárgyalt eredmények mind egyedül elért eredmények, amelyek a IV. részben 9. sorszámmal megadott cikkben kerültek publikálásra.

A *különösen vegyes* szóhasználattal eredetileg a vegyes ternáris/bináris kódok körébe nem tartozó minden más vegyes kódra kívántam utalni. Később azonban a cikkből az értekezésbe is átvett eredményeket néhány olyan tétel és konstrukció ismertetésére szűkítettem, amelyek a 4, 3, 2 alapszámokra épülő vegyes kódokra vonatkoznak, vagyis a $K_{4,3,2}(q, t, b; R)$ kifejezés értékeivel és korlátaival kapcsolatosak.

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.

$$\begin{aligned} K_{4,3,2}(q, t, b; R) &= 1 \text{ akkor és csak akkor áll fenn, ha } R = q + t + b; \\ K_{4,3,2}(q, t, b; R) &= 2 \text{ akkor és csak akkor áll fenn, ha } q + t + \left\lfloor \frac{b}{2} \right\rfloor \leq R < q + t + b; \\ K_{4,3,2}(q, t, b; R) &= 3 \text{ akkor és csak akkor áll fenn, ha} \end{aligned}$$

$$q + \min \left\{ \left\lfloor \frac{2t + 2b}{3} \right\rfloor, \left\lfloor \frac{3t + 2b}{4} \right\rfloor \right\} \leq R < q + t + \left\lfloor \frac{b}{2} \right\rfloor.$$

Négy kódszó esetére a következő eredményt kaptam.

7.7. Tétel.

$K_{4,3,2}(q, t, b; R) = 4$ 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 $R = \frac{b}{2} - 1$.

A 7.7. Tétel bizonyítása az eddig tárgyalt kód kategóriák négy szavas eseteinél sokkal nehezebb. Az általam adott bizonyításban külön tárgyalom a $q \leq t$, ill. $q > t$ esetet, s e két eset bizonyítása egymástól eltérő ötleteken alapul.

Négyenél több kódszó esetére is sikerült néhány részeredményt (lényegében elégséges feltételeket) elérni. Ilyenek a következő tételek állításai.

7.8. Tétel.

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.

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 $K_{4,3,2}(q, t, b; R) = 5$.

7.10. Tétel.

$K_{4,3,2}(3u + 3, u + 3v + 1, 0; 3u + 2v + 2) = 6$ tetszőleges $u, v \geq 0$ esetén.

7.11. Tétel.

$K_{4,3,2}(1, 0, 2u + 4; u + 1) = 8$ ha $u \geq 0$;

$K_{4,3,2}(1, 2, 2u + 3; u + 2) = 8$ ha $u \geq 0$.

Számos ide vonatkozó klasszifikációs eredményt is megadtam az értekezésben, a 7.1-7.4 táblázatokban. Ezek nagyon új, és így cikkben még nem publikált (többnyire számítógépes) eredmények.

Normális kódokra vonatkozó néhány eredmény.

Normális kód (definíció)

Valamely R elérési sugarú $C \subseteq Z_q^n$ kód esetén legyen i 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

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

A normális kód definíciója alapján egyszerűen bizonyítható alábbi tétel magyarázatot ad arra a tapasztalati tényre, hogy az ismert optimális térlefedő kódok többsége miért normális a bináris esetben és miért abnormális a nem bináris esetben.

8.2. Tétel.

Ha $C \subset Z_q^n$ normális kód, akkor fennáll a

$$d_{\min}(C) \leq R + 1 + \frac{R}{q - 1}$$

egyenlőtlenség. Hasonló egyenlőtlenség érvényes bármely olyan vegyes kódra, amely valamely q -adrendű koordinátában normális.

Az értekezés 8.3. szakaszában ternáris koordinátában normális kódok minimális méretének a kiszámításával foglalkozunk. Ezek segítségével különböző – egy paraméterrel megadott – kódcsaládokra vonatkozóan a következő tételben szereplő felső korlátokat tudjuk levezetni.

8.3. Tétel.

Tetszőleges nemnegatív u egészre fennállnak a következő egyenlőtlenségek.

$$\begin{array}{ll} K(3u+1, 4; 2u+1) \leq 10, & K(3u+1, 5; 2u+1) \leq 16, \\ K(3u+2, 3; 2u+1) \leq 12, & K(3u+3, 1; 2u+1) \leq 10, \\ K(3u+3, 2; 2u+1) \leq 16, & K(3u+4, 0; 2u+1) \leq 12, \\ K(3u+4, 1; 2u+1) \leq 18, & K(3u+5, 0; 2u+1) \leq 27, \\ K(3u+1, 6; 2u+2) \leq 10, & K(3u+2, 5; 2u+2) \leq 12, \\ K(3u+4, 2; 2u+2) \leq 11. \end{array}$$

IV. Az értekezés témaköréből készült publikációk

1. On the covering radius of small codes, *Studia Scientiarum Mathematicarum Hungarica* 40(2003)243-256. (Társszerző: P. R. J. Östergård.)
2. On computing the Hamming distance, *Acta Cybernetica* 16(2004)443-449. (Társszerző: Kisvölcsy Ákos.)
3. Classification of MDS codes by exhaustive computer search, 6th International Conference on Applied Informatics (Eger, Hungary, January 27 - 31, 2004) (ed. L. Csőke, P. Olajos, P. Szigetváry and T. Tómacs), Vol. II, 179-185.
4. Egy minimax probléma halmazrendszerekre, *Matematikai Lapok* 12(2004-2005)20-30. (Társszerző: Tuza Zsolt.)
5. Bounds for covering codes over large alphabets, *Designs, Codes and Cryptography* 37(2005)45-60. (Társszerző: P. R. J. Östergård.)
6. 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.
7. The Number of Inequivalent $(2R+3, 7)R$ Optimal Covering Codes, *Journal of Integer Sequences*, 9(2006) Article 06.4.7 (electronical), 8 pp. (Társszerző: P. R. J. Östergård.)
8. Further results on the covering radius of small codes, *Discrete Mathematics* 307(2007)69-77. (Társszerző: P. R. J. Östergård.)
9. On small covering codes in arbitrary mixed Hamming spaces, *Studia Scientiarum Mathematicarum Hungarica*, 44(2007)517-534.
10. The covering radius of extreme binary 2-surjective codes, *Designs, Codes and Cryptography*, 46(2008)191-198.
11. On the minimum size of binary codes with length $2R+4$ and covering radius R , *Designs, Codes and Cryptography*, 48(2008)165-169. (Társszerző: P. R. J. Östergård.)