Válasz Szőnyi Tamásnak
az „Optimális térlefedő kódok kutatása” című
doktori értekezés opponensi bírálatára

Mindenekelőtt szeretném megköszönni Szőnyi Tamásnak, az MTA doktorának a támogató véleményét. Kérdést ez a bírálat nem tartalmaz, a bíráló észrevételeire és megjegyzéseire a következőket szeretném válaszolni.

A 2. oldal első bekezdésében az opponens megjegyzi, hogy „a Hamming-kód leírása $q > 3$-ra csak akkor érthető, ha valaki ismeri a konstrukciót”. Továbbá azt is megjegyzi, hogy „talán a bináris Golay-kódok, valamint az 1-hibajavító perfekt nem-lineáris kódok konstrukcióját is érdemes lett volna a teljesség kedvéért tárgyalni (nem is annyira a jelen disszertáció, mint az anyagból tervezett monográfia miatt)”. Ezt megszívlelve, az időközben gyakorlatilag teljesen elkészült monográfiát több helyen kibővítettem az előző állapotához képest. A Hamming-kód felépítésének a magyarázatát a $q = 4$ esetre vonatkozó példával is illusztráltam. A bináris Golay-kódra vonatkozóan, valamint az 1-hibajavító perfekt nem-lineáris kódok konstrukciójára egy-egy külön alfejezetet illesztettem be a monográfiába. Végül a különösen vegyes térlefedő kódok fejezetéhez is írtam egy vegyes perfekt kódokat tárgyaló alfejezetet. Az értekezésbe azért nem tartottam fontosnak, hogy ezeket bevegyem, mivel itt nincsenek saját eredmények.

Válaszom bizonyítékaként a monográfia említett, pótlólagos részleteit (3.2.3, 5.2.2, 5.3.5, 7.1 szakaszait) a válaszhoz tartozó függelékként mellékelem a következő lapokon.

Budapest, 2011. 11. 16.

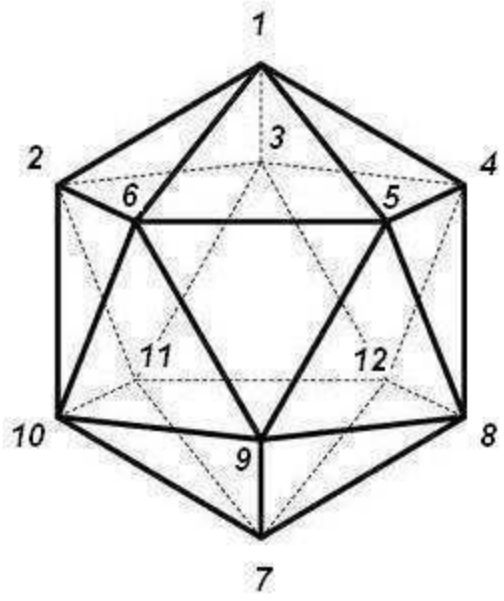
Kéri Gerzson

3.2.3. A bináris Golay-kód

Az 1-nél nagyobb elérési sugarú perfekt kódok kutatása során arra az eredményre jutottak a kutatók, hogy egyetlen ilyen perfekt bináris kód létezik, nevezetesen a $\mathcal{G}_{23}$ Golay-kód, amely $2^{12} = 4096$ kódszóból álló $R = 3$ elérési sugarú optimális térlefedő (covering) kód. A $\mathcal{G}_{23}$ kód egyúttal optimális 3-hibajavító kód is, ebben a minőségében egy szép alkalmazása volt a Voyager 1 és Voyager 2 űrhajók által a Jupiterről és a Szaturnuszról 1979-ben és 1980-ban készített színes képek közvetítése. (Egész pontosan: a kiterjesztett $\mathcal{G}_{24}$ Golay-kódot alkalmazták, amely a kódszavaknak egy paritás bittel történő meghosszabbításával adódik a $\mathcal{G}_{23}$ kódból.)

A bináris Golay kódok struktúrájának az ismertetéséhez éppen fordított logikát célszerű követni. Szemléletesebben lehet elmagyarázni a $\mathcal{G}_{24}$ Golay-kódot, s miután annak szerkezetét már ismerjük, mindössze arra az egyszerű megjegyzésre van szükség, hogy a $\mathcal{G}_{24}$ kód szavaiból egy tetszőleges (például az utolsó) koordináta elhagyásával megkapjuk a perfekt bináris $\mathcal{G}_{23}$ Golay-kódot.

Mindkét bináris Golay-kód lineáris kód, tehát generátormátrixszal megadható kódok. A $\mathcal{G}_{24}$ kód egy generátor mátrixának összeállításához számozzuk meg a szabályos ikozaéder csúcsait (lásd 3.1. ábra), ezután pedig írjuk fel az ikozaéder élhálózati gráfjának az $A = (a_{ij})_{i,j=1,2,\ldots,12}$ szomszédossági mátrixát, amit most úgy értelmezünk, hogy legyen $a_{ij} = 0$, ha az i és j csúcsok szomszédosak (vagyis él köti össze őket) és legyen $a_{ij} = 1$, ha az i és j csúcsok nem szomszédosak (beleértve az $i = j$ esetet is, tehát az A mátrix főátlójába csupa 1-es értéket helyezünk). Az ikozaéder csúcsainak számozása tetszőleges, az ábrán alkalmazott számozástól eltérő bármely más számozás is helyes eredményre vezet.



3.1. ábra. Ikozaéder

Ha az A mátrixot elkészítettük, akkor elé helyezve egy 12×12 méretű egységmátrixot, megkapjuk a $\mathcal{G}_{24}$ Golay-kód egy generátormátrixát. Jobb áttekinthetőség kedvéért itt csak az 1-eseket írtuk be, az üresen hagyott helyekre mindenütt 0 értendő.

Az $(I \mid A)$ mátrix sorvektorai a $\mathcal{G}_{24}$ kód generáló kódszavai. A mátrixból az utolsó oszlopot, annak sorvektoraiból az utolsó koordinátát elhagyva megkapjuk a perfekt $\mathcal{G}_{23}$ kód generátormátrixát, ill. generáló kódszavait. A bináris perfekt Golay-kódra a változatosság kedvéért az utóbbiakat írjuk fel.

$$(I \mid A) = \begin{pmatrix}
1 & & & & & & & & & & & 1 & & & & & 1 & 1 & 1 & 1 & 1 & 1 \\
 & 1 & & & & & & & & & & & 1 & & 1 & 1 & & 1 & 1 & 1 & & & 1 \\
 & & 1 & & & & & & & & & & & 1 & & 1 & 1 & 1 & 1 & 1 & 1 & & \\
 & & & 1 & & & & & & & & & 1 & & 1 & & 1 & 1 & & 1 & 1 & 1 & \\
 & & & & 1 & & & & & & & & 1 & 1 & & 1 & & 1 & & & 1 & 1 & 1 \\
 & & & & & 1 & & & & & & & & 1 & 1 & & 1 & 1 & 1 & & & 1 & 1 \\
 & & & & & & 1 & & & & & 1 & 1 & 1 & 1 & 1 & 1 & 1 & & & & & \\
 & & & & & & & 1 & & & & 1 & 1 & 1 & & & 1 & & 1 & & 1 & 1 & \\
 & & & & & & & & 1 & & & 1 & 1 & 1 & 1 & & & & & 1 & & 1 & 1 \\
 & & & & & & & & & 1 & & 1 & & 1 & 1 & 1 & & & 1 & & 1 & & 1 \\
 & & & & & & & & & & 1 & 1 & & & 1 & 1 & 1 & & & 1 & 1 & & \\
 & & & & & & & & & & & 1 & 1 & 1 & & & 1 & 1 & & & 1 & 1 & & 1
\end{pmatrix}.$$

$$\begin{aligned}
g_1 &= (1,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,1,1,1,1,1),\\
g_2 &= (0,1,0,0,0,0,0,0,0,0,0,0,0,1,0,1,1,0,1,1,1,0,0),\\
g_3 &= (0,0,1,0,0,0,0,0,0,0,0,0,0,0,1,0,1,1,1,1,1,1,0),\\
g_4 &= (0,0,0,1,0,0,0,0,0,0,0,0,0,1,0,1,0,1,1,0,1,1,1),\\
g_5 &= (0,0,0,0,1,0,0,0,0,0,0,0,0,1,1,0,1,0,1,0,0,1,1),\\
g_6 &= (0,0,0,0,0,1,0,0,0,0,0,0,0,0,1,1,0,1,1,1,0,0,1),\\
g_7 &= (0,0,0,0,0,0,1,0,0,0,0,0,1,1,1,1,1,1,1,0,0,0,0),\\
g_8 &= (0,0,0,0,0,0,0,1,0,0,0,0,1,1,1,0,0,1,0,1,0,1,1),\\
g_9 &= (0,0,0,0,0,0,0,0,1,0,0,0,1,1,1,1,0,0,0,0,1,0,1),\\
g_{10} &= (0,0,0,0,0,0,0,0,0,1,0,0,1,0,1,1,1,0,0,1,0,1,0),\\
g_{11} &= (0,0,0,0,0,0,0,0,0,0,1,0,1,0,0,1,1,1,0,1,1,0,1),\\
g_{12} &= (0,0,0,0,0,0,0,0,0,0,0,1,1,1,0,0,1,1,0,0,1,1,0).
\end{aligned}$$

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

$$\begin{array}{lcl} h_1 & = & (0,0,\ldots 0,1,1,1), \\ h_2 & = & (0,0,\ldots 1,0,1,2), \\ . & . & \ldots\ldots\ldots\ldots\ldots\ldots \\ h_{q-2} & = & (0,1,\ldots 0,0,1,q-2), \\ h_{q-1} & = & (1,0,\ldots 0,0,1,q-1) \end{array} \tag{5.2}$$

vektorokat választjuk. A Hamming-kódok mind a bináris, mind a ternáris, mind a magasabb rendű esetben sok más térlefedő (covering) kód-konstrukció alkotó elemét vagy kiindulási alapját képezik.

A mellékelt lemezen $q = 4$-re és $q = 5$-re megadtuk az $(5, 4^3)_4 1$ és a $(6, 5^4)_5 1$ Hamming-kód szavainak listáját.

Példa:

Mivel prímhatvány alapszámú lineáris kód konstrukciójára még nem mutattunk példát, vázoljuk a kvaternáris ($q = 4$ alapszámú) Hamming-kód konstrukcióját. Az (5.2) szerinti generáló kódszavak

$$\begin{array}{lcl} h_1 & = & (0,0,1,1,1), \\ h_2 & = & (0,1,0,1,2), \\ h_3 & = & (1,0,0,1,3). \end{array} \tag{5.3}$$

Képezzük a h_1, h_2, h_3 vektoroknak az F_4-beli skalárokkal való szorzatát az 1.5. táblázat szorzótáblája szerint. A GF(4) test elemeivel megszorzott h_i vektorokat gyűjtsük össze az S_1, S_2, S_3 halmazokba, ily módon az alábbi halmazokat kapjuk:

$$S_1 = \begin{array}{l} \{\ 0h_1 = (0,0,0,0,0), \\ \quad 1h_1 = (0,0,1,1,1), \\ \quad 2h_1 = (0,0,2,2,2), \\ \quad 3h_1 = (0,0,3,3,3)\}, \end{array} \quad S_2 = \begin{array}{l} \{\ 0h_2 = (0,0,0,0,0), \\ \quad 1h_2 = (0,1,0,1,2), \\ \quad 2h_2 = (0,2,0,2,3), \\ \quad 3h_2 = (0,3,0,3,1)\}, \end{array} \quad S_3 = \begin{array}{l} \{\ 0h_3 = (0,0,0,0,0), \\ \quad 1h_3 = (1,0,0,1,3), \\ \quad 2h_3 = (2,0,0,2,1), \\ \quad 3h_3 = (3,0,0,3,2)\}. \end{array}$$

A h_1, h_2, h_3 vektorok által generált kód, vagyis a kvaternáris Hamming-kód kódszavait az

$$\{x + y + z : x \in S_1, y \in S_2, z \in S_3\}$$

halmaz vektorai adják. Ezek közül 10 kódszó a felírt S_i halmazok elemei, a többi kódszó pedig összeadással képezhető az S_i halmazok zéró vektortól különböző elemeiből, az

1.5. táblázat összeadótáblája használatával, így pl.

$$\begin{array}{rcl}
h_2+h_3 & = & (1,1,0,0,1),\\
h_2+2h_3 & = & (2,1,0,3,3),\\
h_2+3h_3 & = & (3,1,0,2,0),\\
 & & \\
2h_2+h_3 & = & (1,2,0,3,0),\\
2h_2+2h_3 & = & (2,2,0,0,2),\\
2h_2+3h_3 & = & (3,2,0,1,1),\\
 & & \\
3h_2+h_3 & = & (1,3,0,2,2),\\
3h_2+2h_3 & = & (2,3,0,1,0),\\
3h_2+3h_3 & = & (3,3,0,0,3).
\end{array} \tag{5.4}$$

Ezzel megvan már 19 kódszó. A még hiányzó 45 kódszót úgy kapjuk meg, hogy az utóbb felsorolt 9-hez, valamint $h_2,\ 2h_2,\ 3h_2,\ h_3,\ 2h_3,\ 3h_3$ mindegyikéhez, tehát 15 vektorhoz hozzáadjuk először h_1-et, utána $2h_1$-et és végül $3h_1$-et.

5.3.5. Nemlineáris perfekt kódok konstrukciója

Ismeretes, hogy tetszőleges q prím vagy prímhatvány és tetszőleges $n = \frac{q^h-1}{q-1}$ $(h \geq 2)$ esetén létezik a Z_q^n térben 1-hibajavító perfekt kód. Minden ilyen q, h, n esetén az ezen paraméterekhez tartozó egyik perfekt kód a Hamming-kód. Megmutatható, hogy ha $h \geq 3$ és $h + q \geq 6$, akkor a Hamming-kóddal azonos paraméterekkel rendelkező nemlineáris perfekt kód is létezik, amely nem is ekvivalens lineáris kóddal.

Az alább ismertetésre kerülő konstrukciót először, még csak a bináris esetre, Vasiliev [174] publikációjában jelent meg, amit később Schönheim [161] és Lindström [117] általánosított tetszőleges q-ra.

A konstrukció az eggyel kisebb h értékhez tartozó ismert perfekt kódra épül, amely lehet egy Hamming-kód, de lehet más lineáris perfekt kód is. Legyen $m = h - 1$, legyen továbbá $C \subseteq Z_q^n$ tetszőleges olyan perfekt lineáris kód, melyre $n = \frac{q^m-1}{q-1}$, ahol $m \geq 2$ és $m+q \geq 5$. Mivel a Z_q^n térben egy adott ponttal szomszédos (azaz 1 Hamming-távolságra lévő) pontok száma $n(q-1)$, ebből adódóan a perfekt C kód szavainak száma

$$M = \frac{q^n}{1 + n(q-1)} = \frac{q^n}{q^m} = q^{n-m}.$$

Rendezzük a C kód kódszavait és a $Z_q = \mathrm{GF}(q)$ test elemeit, mindkettőt a zéró elemmel kezdve, de egyébként tetszőleges módon:

$$C = \{c_0 = 0, c_1, c_2, \ldots, c_{M-1}\}, \;\; \mathrm{GF}(q) = \{0, \alpha_1, \alpha_2, \ldots, \alpha_{q-1}\}.$$

Most rendeljük hozzá a $c_0 = 0$ kódszóhoz a $\mathrm{GF}(q)$ test $f_0 = 0$ elemét, a további c_k $(k = 1, 2, \ldots, M-1)$ kódszavakhoz pedig tetszőleges módon a $\mathrm{GF}(q)$ test f_k elemét. Az így értelmezett $f_0, f_1, f_2, \ldots, f_{M-1}$ testelemek között azonosak is lehetnek, a legszélsőségesebb esetben valamennyien zérók, ám akkor (de nem csak akkor) az ismertetésre kerülő konstrukció lineáris kódot eredményez.

Legyen $c_k \in C$ egy tetszőleges kódszó, $x_i = (x_{i1}, x_{i2}, \ldots, x_{in})$ $(i = 1, 2, \ldots, q-1)$ pedig a Z_q^n tér tetszőleges pontjai. Fűzzük egymáshoz az $x_1, x_2, \ldots, x_{q-1}$,$c_k + \sum_{i=1}^{q-1} x_i$ vektorokat és végül az $f_k + \sum_{i=1}^{q-1} \alpha_i \sum_{j=1}^{n} x_{ij}$ skalárt. Az összefűzés eredményeként kapott vektorok koordinátáinak száma $N = nq+1$. Ha most $x_1, x_2, \ldots, x_{q-1}$ egymástól függetlenül végigfut a Z_q^n tér pontjain, c_k pedig a C kód szavain, akkor az összefűzött vektorok egy olyan C^* halmazt alkotnak, amely a Z_q^N tér $q^{n(q-1)} \cdot q^{n-m} = q^{nq-m} = q^{N-h}$ pontját tartalmazza, és amelyről megmutatható, hogy szintén perfekt kód. Az elemszám ismeretében ehhez csak azt kell bizonyítani, hogy C^* bármely két eleme legalább 3 Hamming-távolságra van egymástól.

Legyen $y = (y_1 \mid y_2 \mid y_3)$ és $y' = (y'_1 \mid y'_2 \mid y'_3)$ a C^* kód két különböző kódszava, ahol

$$\begin{aligned} y_1 &= (x_1 \mid x_2 \mid \ldots \mid x_{q-1}), \\ y_2 &= c_k + \textstyle\sum_{i=1}^{q-1} x_i, \\ y_3 &= f_k + \textstyle\sum_{i=1}^{q-1} \alpha_i \sum_{j=1}^{n} x_{ij}, \end{aligned}$$

és hasonlóan

$$y'_1 = (x'_1 \mid x'_2 \mid \ldots \mid x'_{q-1}),$$
$$y'_2 = c_{k'} + \sum_{i=1}^{q-1} x'_i,$$
$$y'_3 = f_{k'} + \sum_{i=1}^{q-1} \alpha_i \sum_{j=1}^{n} x'_{ij}.$$

E jelölésekkel a bizonyítás befejezése már kézenfekvő és a befejezést az olvasóra hagyjuk. Már csak annyit kell tenni, hogy a $d(y, y') = d(y_1, y'_1) + d(y_2, y'_2) + d(y_3, y'_3)$ összefüggés figyelembe vételével $d(y_1, y'_1)$ különböző lehetséges értékei szerint (0, 1, 2, ill. 2-nél nagyobb) csoportosítva vizsgáljuk a lehetséges eseteket.

Azt is könnyű belátni, hogy az f_k értékek megadhatók úgy, hogy C^* ne legyen lineáris altér, például úgy, hogy egy kivétellel minden c_k kódszóhoz az $f_k = 0$ értéket rendeljük hozzá.

7.1. Vegyes perfekt kódok konstrukciója

Perfekt kódok nemcsak a tiszta, hanem a vegyes kódok között is találhatók, de csak olyan vegyes Hamming-terekben ismerünk perfekt kódokat, melyekre az egyes koordinátákhoz tartozó kódábécék mérete ugyanannak a prímnek a hatványai. Az ilyen perfekt kódok a nem vegyes perfekt kódokhoz hasonlóan nagyon érdekes, szép konstrukcióval állíthatók elő, ezért a fejezetet az ilyen vegyes kódok konstrukciójának ismertetésével kezdjük Herzog és Schönheim [69], Lindström [118], valamint Östergård és Hämäläinen [143] publikációi alapján.

Herzog és Schönheim egyik szép tétele [69, Theorem 1] kimondja és bebizonyítja, hogy ha egy G Abel-csoport felbontható a $G_1, G_2, \ldots, G_n$ részcsoportjai egyesítésére oly módon, hogy azok páronként közös elemként csak a zéró elemet tartalmazzák, akkor e részcsoportok szorzatterében létezik 1-hibajavító perfekt kód. A szerzők egy ilyen perfekt kód konstrukcióját is megadják, megmutatva, hogy a szóban forgó szorzattér tetszőleges $(x_1, x_2, \ldots, x_n)$ pontját a G csoport $x_1+x_2+\ldots+x_n$ elemébe képező homomorf leképezés magtere 1-hibajavító perfekt kód. (Közérthetőbb kifejezéssel: a szorzattér azon pontjai, amelyekre $x_1 + x_2 + \ldots + x_n = 0$, perfekt kódot alkotnak.)

Lindström [118] cikke a Herzog–Schönheim-féle konstrukciót kifejezetten olyan esetben vizsgálja, amikor a G_i csoportok egy adott prím különböző hatványaihoz tartozó véges testek additív csoportjai. Lindström eredményeire támaszkodva Östergård és Hämäläinen a [143, Theorem 5] tételben az alábbi szükséges és elégséges feltételt fogalmazza meg:

Jelöljük $G(q)$-val a $\mathrm{GF}(q)$ *véges test additív csoportját. E jelöléssel egy $G(q^a)$-val izomorf G_1 csoport és további $(n-1)$ számú $G(q^b)$-vel izomorf $G_2, G_3, \ldots, G_n$ csoport esetén, ahol feltesszük még, hogy $a \geq b$, az e szakaszban tárgyalt perfekt kód konstrukció akkor és csak akkor alkalmazható, ha létezik olyan $r \geq a + b$ egész, melyre fennáll*

$$q^r = q^a + (n-1)(q^b - 1). \tag{7.1}$$

Példák a módszer alkalmazására:

Az alábbi példa mutatja, hogy $G^3(2)$ felbontható olyan G_1, G_2, G_3, G_4, G_5 csoportok egyesítésére, ahol ezek egyike $G(4)$-gyel, a további 4 pedig $G(2)$-vel izomorf. Konkrétan, a

$$G = G^3(2) = \{000, 001, 010, 011, 100, 101, 110, 111\}$$

csoport

$$\begin{aligned} G_1 &= \{000, 010, 100, 110\}, \\ G_2 &= \{000, 001\}, \\ G_3 &= \{000, 011\}, \\ G_4 &= \{000, 101\}, \\ G_5 &= \{000, 111\} \end{aligned}$$

felbontása megfelel az előbbi feltételeknek. A 7.1. táblázat bal oldali részén felsoroljuk a szorzattér mindazon pontjait, melyekre (bináris összeadással) fennáll az $x_1 + x_2 + x_3 + x_4 + x_5 = 0$ egyenlőség, jobbra pedig felsoroljuk az ily módon kapott vegyes perfekt $C \subset Z_4 Z_2^4$ kód megfelelő kódszavait a szokásos jelölésmóddal, vagyis a háromjegyű szimbólumokról egyjegyű szimbólumokra áttérve, a $G(4)$-gyel izomorf csoport elemeire a 0, 1, 2, 3 szimbólumokat, a $G(2)$-vel izomorf csoportok elemeire pedig mindenütt a 0, 1 szimbólumokat használva. (Algebrai tárgyú munkákban $G(4)$-re vonatkozóan az általunk alkalmazott 2, 3 szimbólumok helyett az α, β szimbólumokat szokták használni.)

x_1	x_2	x_3	x_4	x_5	C
000	000	000	000	000	(0,0,0,0,0)
000	001	011	101	111	(0,1,1,1,1)
010	000	000	101	111	(1,0,0,1,1)
010	001	011	000	000	(1,1,1,0,0)
100	000	011	000	111	(2,0,1,0,1)
100	001	000	101	000	(2,1,0,1,0)
110	000	011	101	000	(3,0,1,1,0)
110	001	000	000	111	(3,1,0,0,1)

7.1. táblázat. Perfekt vegyes kód konstrukciója

Az ismertetett módszer néhány további alkalmazása: A $G^4(2)$ csoportnak egy $G(4)$-gyel és 12 darab $G(2)$-vel izomorf csoportra történő felbontásával a $Z_4 Z_2^{12}$ térben, ugyancsak a $G^4(2)$ csoportnak egy $G(8)$-cal és 8 darab $G(2)$-vel izomorf csoportra történő felbontásával a $Z_8 Z_2^8$ térben tudunk 1-hibajavító perfekt kódot konstruálni. Az előbbi 1024, az utóbbi 128 kódszóból áll. Még több hasonló példát az (7.1) diofantoszi egyenlet vizsgálatával lehet keresni.