Golay-kód és Witt-design

Tétel: A C kódra teljesül, hogy a $\{0,1\}$ elemű ábécén 24 hosszú, 2^{12} elemű és bármely két eleme között legalább 8 távolság van, röviden egy $(24, 2^{12}, 8)_2$ paraméterű kód. Tegyük fel továbbá, hogy $\underline{0} \in C$. Ekkor pontosan egy ilyen C kód létezik.

Megjegyzés: Az egyértelműséget a koordináták permutációinak erejéig értjük.

Megjegyzés: Ezt a kódot G_{24} Golay-kódnak hívják.

Bizonyítás: Hagyjuk el az egyik koordinátát, mondjuk az utolsót (ezt hívják *lyukasztás*nak). Az így kapott kód 23 hosszú szavakból áll és 2^{12} eleme van, mivel két szó nem eshettet egybe az utolsó betű törlése után hiszen a minimális távolság 8 volt. Továbbá a kapott kódban legalább 7 a minimális távolság két szó között. Az így kapott kód perfekt, ugyanis teljesíti a Hamming-korlátot egyenlőséggel:

$$\frac{2^{23}}{1+\binom{23}{1}+\binom{23}{2}+\binom{23}{3}} = \frac{2^{23}}{2^{11}} = 2^{12}.$$

Tehát a kapott kód perfekt ami azt jelenti, hogy minden 23 hosszú $0-1$ sorozat pontosan egy kódszó körüli három Hamming-sugarú gömbben van benne. Jelölje A_i az i hosszú kódszavak számát, ekkor az előbbi észrevétel szerint

$$\binom{23}{i} = A_{i-3}\binom{26-i}{3} + A_{i-2}\binom{25-i}{2} + A_{i-1}\binom{24-i}{1} + A_i + A_{i+1}\binom{i+1}{1} + A_{i+2}\binom{i+2}{2} + A_{i+3}\binom{i+3}{3}$$

Ebből rekurziót kapunk A_i-re $A_0 = 1$-t felhasználva. Ebből kapjuk, hogy $A_0 = A_{23} = 1$, $A_7 = A_{16} = 253$, $A_8 = A_{15} = 506$ és $A_{11} = A_{12} = 1288$. Ebből az eredeti C kód súlypolinomhjának $\bar{A}_i$ együtthatói:

$$\bar{A}_0 = \bar{A}_{24} = 1 \qquad \bar{A}_8 = \bar{A}_{16} = 759 \qquad \bar{A}_{12} = 2576$$

(Az eredeti kódban nem lehet például 7 súlyú szó, mert akkor az egyik ilyen szó 1-est tartalmazó helyén lyukasztva a kapott 23 hosszú kódban lennének 6 súlyú szavak is. Hasonlóan $\bar{A}_9 = \bar{A}_{15} = \bar{A}_{17} = \bar{A}_{23} = 0$.)

Következő lépésként megmutatjuk, hogy $c_1, c_2 \in C$ esetén $(c_1, c_2) = 0$, ehhez meg kell mutatnunk, hogy $supp(c_1) \cap supp(c_2)$ páros. Ha $c_1 \in C$ akkor attérve a $C + c_1$ kódra a kapott kód kielégíti a feltételeket, így ebben is minden súly 4 osztható. Így 4 osztja $|supp(c_1)|+|supp(c_2)|-|supp(c_1+c_2)| = 2|supp(c_1)\cap supp(c_2)|$-t vagyis $|supp(c_1)\cap supp(c_2)|$ páros. Ebből következik, hogy C lineáris kód, ugyanis $|C| = 2^{12}$, így $\langle C\rangle$ legalább 12 dimenziós vagyis $C^\perp = \langle C\rangle^\perp$ legfeljebb 12 dimenziós, de ez az előbbiek szerint tartalmazza C-t vagyis pontosan 12 dimenziósnak kell lennie, így $\langle C\rangle$-nek is 12 dimenziósnak kell lennie vagyis meg kell egyeznie C-vel. Tehát C lineáris kód és $C = C^\perp$.

A következő cél C egy szép bázisát megadni. Legyen c_1 egy 12 súlyú szó és tegyük fel, hogy a koordináták úgy vannak permutálva, hogy a $2, 3, \ldots, 13$ helyen vannak a 0-k c_1-ben, a többi helyen vannak az 1-esek. A következő lépés a *reziduális képzés*: tekintsük minden kódszó $2, 3, \ldots, 13$ helyén levő betűit vagyis vetítsünk ezekre a helyekre. Az így kapott kód 12 hosszú. Tetszőleges $c \in C$-re c és $c + c_1$ vetítettje ugyanaz, másnak viszont nem lehet ugyanaz a vetítettje, ha ugyanis a $\underline{0}$ szót kapjuk akkor az eredeti c' nem lehet 8 súlyú, mert

akkor $c'+c_1$ 4 súlyú szó lenne, tehát csak 0 vagy 12 súlyú lehet vagyis $\underline{0}$ vagy c_1 maga. Tehát a kapott kód 11 dimenziós. A kapott kód minden szavának a súlya páros lesz, mert eredetileg is minden szó súlya páros volt és $(c, c_1) = 0$ minden $c \in C$-re. Tehát a kapott kód $[12, 11, 2]$ parameterű (legalább 2 a minimális távolság, több meg nem lehet), ez a kód egyertelmű: minden páros súlyú szót tartalmaz. Tehát választhatunk $c_2, c_3, \ldots, c_{12}$ kódszavakat, hogy c_i i.edik és 13. helyen 1-es áll, a vetítettje többi helyen pedig 0. Mivel c_i helyett $c_1 + c_i$-t is vehetünk azt is elérhetjük, hogy $c_2, \ldots, c_{12}$ első koordinátája 0 legyen. Az így kapott 12 vektor C bázisát adja, hiszen lineárisan függetlenek az első 12 koordináta miatt.

Most tekintsük $c_2, \ldots, c_{12}$ utolsó 11 koordinatáját, az így kapott 11 vektort jelöljük $a_2, \ldots, a_{12}$-vel. Mivel $w(c_i)$ legalább 8 így $w(a_i)$ 6 vagy 10-zel egyenlő. Ha $w(a_i) = 10$ lenne valamely $i \in \{2, \ldots, 12\}$ esetén akkor $w(c_1 + c_i) = 4$ lenne ami nem lehet, tehát $w(a_i) = 6$ $i \in \{2, \ldots, 12\}$ esetén. Vizsgáljuk $|supp(a_i) \cap supp(a_j)|$-t, jelöljuk ezt x-szel. Ekkor $w(c_i + c_j) = 2 + (6 - x) + (6 - x) = 14 - 2x$, így $x = 1$ vagy $x = 3$. Ha $x = 1$ lenne akkor $w(c + c_i + c_j) = 4$ lenne vagyis $x = 3$. Összefoglalva $supp(a_i)$ halmazok mindegyike egy 11 elemű halmaz 6 elemű részhalmaza és bármely kettő metszete 3 elemű. Megmutatjuk, hogy ez a rendszer létezik es egyértelmű.

Lemma: Egyértelműen létezik olyan $B_i \subset B$ halmazrendszer, ahol $|B_i| = 6$ $(i = 1, \ldots, 11)$, $|B| = 11$ és $i \neq j$ esetén $|B_i \cap B_j| = 3$.

Bizonyítás: Halmazrendszer létezése: legyen B_i az $\{i, i+1, i+3, i+4, i+5, i+9\}$ halmaz modulo 11 tekintve az elemeket. (Ez nem más, mint az $\{x^2 \mid x \in F_{11}\}$ halmaz eltoltjai.)

Halmazrendszer egyértelműsége: vegyük minden halmaz komplementerét: $A_i = B/B_i$, ekkor a kapott halmazrendszer minden halmaza 5 elemű és bármely kettő metszete két elemű. Először is megmutatjuk, hogy bármely két pont pontosan két A_i halmazban van benne. (Ez sokkal általánosabban igaz állítás szimmetrikus blokkrendszerekre, ebben a jegyzetben azonban próbálunk nem hivatkozni semmire.) Első lépésként megmutatjuk, hogy bármely két pont legfeljebb két halmazban van benne. Tegyük fel, hogy $p_1, p_2 \in A_1, A_2, A_3$, ekkor mivel bármely két halmaz metszete két elemű, így $A_i/|\{p_1, p_2\}$ halmazok diszjunktak. Tekintsünk egy A_4 halmazt. Mivel $|A_1 \cup A_2 \cup A_3| = 11$ így ha $A_4 \cap \{p_1, p_2\}| = k$ akkor $k = 0$ esetén A_4-nek 6, $k = 1$ esetén $1+3 = 4$ és $k = 2$ esetén 2 eleműnek kéne lennie, ellentmondás. Másrészt ha leszámoljuk a $\{(p_1, p_2, A_i)p_j \in A_i,\ p_1 \neq p_2\}$ halmaz elemszámát az egyrészt $11 \cdot 5 \cdot 4$ mivel 11 halmazból 5 illetve 4 féleképpen választhatjuk ki p_1, p_2-t, másrészt legfeljebb $11 \cdot 5 \cdot 4$, mert két pontot legfeljebb két halmaz tartalmaz. Mivel $11 \cdot 5 \cdot 4 = 11 \cdot 5 \cdot 4$, így minden pontpárt pontosan két halmaz tartalmaz.

Minden $p \notin A_1$ esetén definiálunk egy $\Gamma(p)$ gráfot A_1-n. Legyen $(x, y) \in E(\Gamma(p))$ ha x, y-re illeszkedő A_1-tól különböző halmaz átmegy p-n (minden pontpárra pontosan két halmaz illeszkedik!). Így kapunk hat darab gráfot, ezek a *Hussein-gráfok*. Minden $\Gamma(p)$ 2-reguláris gráf és $p \neq p'$ esetén $\Gamma(p) \cap \Gamma(p')$ pontosan két élt tartalmaz. Az első állítás abból következik, hogy $x \in A_1$ két szomszédja $|\Gamma(p)$-ben a p és x-re illeszkedő két halmaz A_1-gyel való metszete. A második pedig abból, hogy két pontot legfeljebb (pontosan) két halmaz tartalmazhat, így $\Gamma(p) \cap \Gamma(p')$ metszete nem más, mint a p, p'-re illeszkedő két halmaz metszete A_1-gyel. Másrészt a Hussein-gráfokból egyértelműen vissza lehet kapni a halmazokat: egy $x, y \in A_1$ pár meghatároz egy halmazt, az $\{x, y, p_1, p_2, p_3\}$ halmazt ahol $(x, y) \in \Gamma(p_i)$ $(i = 1, 2, 3)$. Tehát elég csak megmutatni, hogy a Hussein-gráfok rendszere egyértelmű. Mindegyik gráf 5 csúcson 2-reguláris vagyis egy 5-hosszú körnek kell lennie. Legyen a $\Gamma(p_1)$ az $\{(1, 2), (2, 3), (3, 4), (4, 5), (5, 1)\}$ élekből álló kör. A többi gráf ezekből pontosan két élet

tartalmaz, de ez nem lehet két szomszédos, mert akkor szükségszerűen tartalmazzák a két szomszédos éllel szemközti élet is. Tehát csak két nem szomszédos élet tartalmazhatnak, ezek már egyértelműen meghatározzák a többi gráfot: az $\{(1,3),(3,2),(2,5),(5,4),(4,1)\}$ gráf és elforgatottjai lesz a másik öt gráf. Ezzel bebizonyítottuk az egyertélműséget is.

Ezzel bebizonyítottuk a kód egyértelműségét. A halmazrendszer konstrukióját felhasználva megadhatjuk a kód egy szép bazisát is, ezt az alábbi mátrixban adtuk meg.

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

Állítás: Legyen $1, 2, \ldots, 24$ egy blokkrendszer pontjai és a blokkok $supp(c)$ ahol w(c)=8 valamely $c \in C$ kódra. Ekkor bármely 5 pontra illeszkedik pontosan egy blokk.

Bizonyítás: Bármely 5 pontra legfeljebb egy blokk illeszkedhet, mert ha valamely 5 pontra két blokk is illeszkedne akkor lenne $c_1, c_2 \in C$ kódok 8 súllyal, melyekre $c_1 + c_2$ súlya legfeljebb 6 lenne, ez pedig nem lehet, mert a Golay-kód lineáris kód, így minden nem $\underline{0}$ kódjának a súlya legalább 8. Most számoljuk meg kétféleképpen az (M, B) párokat, ahol $M \subset \{1, 2, \ldots, 24\}$ $|M| = 5$ es $M \subset B$ ahol B egy blokk. Mivel ezutóbbiak száma $\bar{A}_8 = 759$, így az ilyen párok száma $759 \cdot \binom{8}{5}$. Másrészt az ilyen párok száma legfeljebb $\binom{24}{5}$, mert minden 5 elemű halmazra legfeljebb egy blokk illeszkedik.

Mivel $759 \cdot \binom{8}{5} = \binom{24}{5}$ így minden 5 elemű halmazra pontosan egy blokknak kell illeszkednie.

Megjegyzés: Ezt a blokkrendszert Witt-designnak nevezik. Ennek van egy klasszikus Witt féle felépítése, amely egyesek szerint "hű, de tök jó", mások szerint "irtózatos munka" (én ezutóbbiak közé tartozom, így ezt a konstrukciót itt nem tárgyaljuk). Megmutatjuk, hogy egy fenti tipusú blokkrendszer létezéséből könnyedén következik a Golay-kód létezése, mivel ezutóbbi egyértelmű ebből kapjuk, hogy a kivánt tulajdonságú blokkrendszer egyértelmű.

A 5-(24,8,1) paraméterű blokkrendszer

Legyen B 8 elemű blokkok egy halmaza úgy, hogy az $\{1, 2, \ldots, 24\}$ minden 5 elemű halmaza pontosan egy blokkban van benne. Megmutatjuk, hogy ez csak az előbb megkonstruált Witt-design lehet. Néhány lemmára van szükségünk .

Lemma: Legyen $B, B' \in B$. Ekkor $|B \cap B'| \neq 3$.

Bizonyítás: Tegyük fel indirekt, hogy $|B \cap B'| = 3$. Legyen $B \cap B' = A$, legyen továbbá $A' \subset B$, melyre $A \subset A'$ es $|A'| = 4$. Bármely $p \in \{1, 2, \ldots, 24\}$ esetén létezik pontosan egy blokk amely tartalmazza A'-t és p-t. Mivel bármely két különböző blokk metszete legfeljebb 4 elemű, ezért ezen blokkok vagy megegyeznek vagy a metszetük pontosan A'. Tehát kaptunk 5 blokkot: $B = B_1, B_2, B_3, B_4, B_5$, hogy páronkénti metszetük pontosan A'. Ez a konstrukció még hasznos lesz, így nevet adunk neki: *teljes napraforgó*. Először is B' nem lehet eleme a teljes napraforgónak, mert B-vel való metszete csak 3 elemű, így B' különbözik B_2, B_3, B_4, B_5 mindegyikétől. Másrészt mivel $A \subset B'$ így $|(B_i/A') \cap B'| \leq 1$ (i=2,3,4,5) esetén, különben B_i és B'-nek legalább 5 közös eleme lenne. Ekkor viszont B'-nek legfeljebb 7 eleme lehet, mert B és B_i/A' lefedik az $\{1, 2, \ldots 24\}$ halmazt. Ez az elletmondás bizonyítja az allításunkat.

Lemma: Tegyük fel, hogy $B, B' \in B$ és $|B \cap B'| \neq 4$. Ekkor $(B \backslash B') \cup (B' \backslash B) \in B$.

Bizonyítás: Feltehető, hogy $B = \{1, 2, \ldots 8\}$, míg $B' = \{1, 2, 3, 4, 9, 10, 11, 12\}$. Tegyük fel indirekt, hogy $U = \{5, 6, \ldots 12\}$ nem blokk. Egyértelműen van egy blokk amely tartalmazza az $\{5, 6, 9, 10, 11\}$ halmazt, legyen ez S. Ekkor $S \neq B'$, de $|S \cap B'| \leq 3$. Ekkor az előző lemma szerint $|S \cap B'| = 4$. Két esetet különböztetünk meg aszerint, hogy mi $S \cap B'$ negyedik eleme.

1. eset: Nem a 12 a negyedik közös elem, hanem az $1, 2, 3, 4$ valamelyike, mondjuk az 1-es. Ekkor $|B \cap S| \geq 3$ az $1, 5, 6$ elemek miatt. Másrészt $B \neq S$, tehát van egy negyedik közös elemük. Ez azoban $2, 3, 4$ egyike sem lehet B' miatt így 7 vagy 8, mondjuk 7. Most tekintsük az $\{5, 8, 9, 10, 11\}$ halmazt, erre illeszkedik egy R blokk. $R \neq S$, mert S-ben nem volt benne a 8. Megint S-nek és B'-nek kell egy negyedik közös eleme, most nem lehet az $1, 2, 3, 4$ valamelyike, mert akkor az előzőekhez hasonlóan 6 vagy 7 eleme lenne R-nek, mert akkor mar $|R \cap S| \geq 5$ lenne, tehát csak 12 lehet $R \cap B'$ negyedik eleme. Most tekintsük a $\{7, 8, 9, 10, 11\}$ halmazt, ezt tartalmazza egy T blokk ami különbözik mind S, mind R-től. Most viszont már ellentmondást kapunk: $B' \cap T$ negyedik eleme sem 12 sem $1, 2, 3, 4$ valamelyike sem lehet, mert akkor $T \cap R$ vagy $T \cap S$ túl nagy lenne, utóbbi azért, mert akkor a látott módon 5 vagy 6-nak is T-hez kéne tartoznia.

2. eset: Akárhogy választunk ki két elemet az $5, 6, 7, 8$ elemek közül a $9, 10, 11$ halmaz mellé az ezt tartalmazó blokk tartalmazza 12-t, ekkor az előző eset $|R \cap T| \geq 5$ ellentmondását kapjuk ha $5, 6$ és $5, 7$-t választjuk ki $9, 10, 11$ mellé. Ellentmondás, tehát U-nak blokknak kell lennie.

Lemma: Minden B blokkhoz létezik B^*, B^{**} blokkok, hogy B, B^*, B^{**} páronkent diszjunktak.

Bizonyítás: Egeszítsük ki B-t egy teljes napraforgóva B_2, B_3, B_4, B_5 blokkokkal. Előbbi lemma szerint $B^* = (B_2 \backslash B_3) \cup (B_3 \backslash B_2)$ és $B^{**} = (B_4 \backslash B_5) \cup (B_5 \backslash B_4)$ is blokkok és a kivánt tulajdonságúak.

Lemma: Legyen $B, B' \in B$. Ekkor $|B \cap B'| \neq 1$.

Bizonyítás: Tegyük fel indirekt, hogy $|B \cap B'| = 1$. Egeszítsük ki B-t B^*, B^{**} blokkokkal, hogy B, B^*, B^{**} páronként diszjunktak legyenek. Mivel B' nem lehet B^*, B^{**} egyike sem, ezért mindegyiket legfeljebb 4 elemben metszi, de akkor az egyiket 4, a másikat 3 elemben metszi. Ez viszont ellentmondás, nem lehet két blokk metszete 3 elemű.

Következmény: Bármely két blokk metszete páros elemű.

Most már megkonstruálhatjuk a Golay-kódot. Legyen

$$V = \langle \underline{b} \mid \underline{b} \text{ egy blokk karakteriszikus vektora} \rangle$$

Mostantól meglehetősen pongyolák leszünk abban az értelemben, hogy egy blokkrol vagy a karakterisztikus vektorárol beszélünk.

Lemma: Minden $\underline{v_1}, \underline{v_2} \in V$ esetén $(\underline{v_1}, \underline{v_2}) = 0$, továbbá minden $\underline{v} \in V$ esetén $4 \mid w(\underline{v})$.

Bizonyítás: Az első állítás teljesül a blokkok karakterisztikus vektorára: $(\underline{b_i}, \underline{b_j}) = 0$, mert $|B_i \cap B_j| \in \{0, 2, 4, 8\}$. Így ez teljesül a generált altérre is.

A második allítás teljesül a blokkok karakterisztikus vektorára, továbbá ha teljesül $\underline{v_1}, \underline{v_2} \in V$-re akkor $\underline{v_1} + \underline{v_2}$-re is:

$$|supp(\underline{v_1} + \underline{v_2})| = |supp(\underline{v_1})| + |supp(\underline{v_2})| - 2|supp(\underline{v_1} \cap \underline{v_2})|$$

ahol $|supp(\underline{v_1} \cap \underline{v_2})|$ páros, mert $(\underline{v_1}, \underline{v_2}) = 0$. Tehát minden $\underline{v} \in V$ esetén $4 \mid |supp(\underline{v})| = w(\underline{v})$.

Lemma: Nincs 4 súlyú szó V-ben.

Bizonyítás: Tegyük fel, hogy $\underline{a} \in V$ az A karaketrisztikus vektora, ahol $|A| = 4$. Egeszítsük ki A-t teljes napraforgóva, hogy a $B_1, \ldots, B_5$ halmazok metszete A legyen. Válaszzunk ki minden B_i/A-ból egy pontot. Az így kapott 5 ponton van egy B blokk. Ekkor $B \cap (B_i/A)| \geq 1$ és $|B \cap B_i|$ páros, továbbá $|B \cap A|$ is páros, mert $(\underline{b}, \underline{a}) = 0$. Tehát $|B \cap (B_i/A)|$ is páros és így legalább 2 , de $8 = |B| \geq 5 \cdot 2 = 10$, ellentmondás. Tehát V-ben nincs 4 súlyú szó.

Lemma: V minden 8 súlyú szava egy blokk karakterisztikus vektora.

Bizonyítás: Tegyük fel, hogy $\underline{v} \in V$ es $w(\underline{v}) = 8$. Ekkor $\underline{v}$ 5 pontján át van B blokk, így $|\underline{b} \cap \underline{v}| \geq 5|$. Ekkor $|\underline{b} \cap \underline{v}|$ páros, így 6 vagy 8. Ha $|\underline{b} \cap \underline{v}| = 6$ akkor $w(\underline{b} + \underline{v}) = 4$, de ilyen nincs V-ben. Tehát $|\underline{b} \cap \underline{v}| = 8$ azaz $\underline{b} = \underline{v}$, így $\underline{v}$ egy blokk karakterisztikus vektora.

Nevezzük egy halmazt tucatnak ha megkapható két olyan blokk szimmetrikus differenciájaként, melyek metszete két elemű. Ekkor a tucat karakterisztikus vektora 12 súlyú és V-ben van: $\underline{t} = \underline{b_1} + \underline{b_2}$. Ennek a megfordítása is igaz.

Lemma: V minden 12 súlyú szava egy tucat karakterisztikus vektora.

Bizonyítás: T 5 pontjan van egy B blokk. Ha $|T \cap B| = 8$ akkor $w(\underline{t} + \underline{b}) = 4$ nem lehetséges, tehát $|T \cap B| = 6$ (páros és legalább 5). Ekkor $w(\underline{t} + \underline{b}) = 8$ így $\underline{t} + \underline{b} = \underline{b'}$, ahol $\underline{b'}$ egy blokk karakterisztikus vektora. Tehát $\underline{t} = \underline{b} + \underline{b'}$ azaz T tucat.

Lemma: Legyen B egy blokk és $U_i = |\{B' \mid |B' \cap B| = i\}|$. Ekkor

(i) Összesen 759 blokk van.

(ii) Minden pontot 253 blokk tartalmaz.

(iii) $U_8 = 1$, $U_1 = U_3 = U_5 = U_6 = U_7 = 0$ és $U_0 = 30$, $U_2 = 448$, $U_4 = 280$.

(iv) A tucatok száma 2576.

Bizonyítás: (i) Számoljuk meg a (H, B) párok számát, ahol $|H| = 5$, B blokk és $H \subset B$. Ez egyrészt $\binom{24}{5}$, mivel minden 5 elemű halmazt pontosan egy blokk tartalmaz, másrészt ez a blokkok száma szorozva $\binom{8}{5}$, így a blokkok száma 759.

(ii) Legyen p egy tetszőleges pont. Számoljuk le azon (H, B) párok számát, ahol $|H| = 5$, B blokk és $H \subset B$ és $p \in H$. H-t ki tudjuk választani $\binom{23}{4}$ féleképpen, a blokk mar egyértlemű. Mésrészt ez a p-t tartalmazó blokkok száma szorozva $\binom{7}{4}$, így a p-t tartalmazó blokkok száma 253.

(iii) Világos, hogy $U_8 = 1$, $U_1 = U_3 = U_5 = U_6 = U_7 = 0$. Szintén konnyű látni, hogy $U_4 = 280$, hiszen B egy 4 elemű részhalmazát kiválaszthatjuk $\binom{8}{4}$ féleképpen és minden 4 elemű halmazt B-n kivül még 4 blokk tartalmaz, a teljes napraforgó másik négy szirma. Számoljuk le a (p, B') párokat, ahol $p \in B \cap B'$. Egyrészt ez $8 \cdot 253$, mert B minden pontját 253 halmaz tartalmazza (ii) szerint, másrészt ez $2U_2 + 4U_4 + 8U_8$, ebből kapjuk, hogy $U_2 = 448$. Végül $U_0 = 759 - 1 - 280 - 448 = 30$.

(iv) Számoljuk le a (B_1, B_2) blokkok számát, ahol $|B_1 \cap B_2| = 2$. Ez egyrészt a blokkok száma szorozva U_2 vagyis $759 \cdot 448$. Másrészt ha $T = (B_1/B_2) \cup (B_2/B_1)$ akkor $|T \cap B_1| = 6$; T 5 pontjat kiválasztva egyértelműen van rajta egy blokk és ez meghatározza $T \cap B$ 6. metszéspontját ($T \cap B$ páros elemű, de nem lehet 8 elemű, mert nincs 4 súlyú szó V-ben), tehát a fenti párok száma egyenlő a tucatok száma szorozva $\binom{12}{5}\frac{1}{6}$. Innen kapjuk, hogy a tucatok száma 2576.

Tétel: V a Golay-kód.

Bizonyítás: V minden szava 4-gyel osztható súlyú, de 4 súlyú szavak nincsenek benne, így a legkisebb súlyú nem $\underline{0}$ szó 8 súlyú. V elemszáma $2 + 2 \cdot 759 + 2576 = 4096 = 2^{12}$ vagyis 12 dimenziós. Mivel a Golay-kód egyértelmű, ezért V a G_{24} kód .

Egyéb konstrukciók a G_{24} Golay-kódra

Tétel: Legyen N az ikozaéder gráfjának adjacenciamátrixa, J a csupa 1-esből álló mátrix. Ekkor az $(I_{12}, J - N)$ mátrix a G_{24} generátormátrixa .

Bizonyítás: Az ikozaéder minden csúcsának 5 szomszédja van, továbbá két átellenes csúcsának nincs, két nem átellenes csúcsának pontosan két közös szomszédja van. Ebből következik, hogy $H = (I_{12}, J-N)$ bármely sorában 8 darab 1-es van és bármely két sor merőleges egymásra . Ezutóbbiból következik, hogy ez bármely két kódszó is merőleges egymásra.

Így a kód minden szava 4-gyel osztható súlyú, ez teljesül C soraira és ha c_1, c_2-re teljesül, akkor $c_1 + c_2$-re is :

$$|supp(c_1 + c_2)| = |supp(c_1)| + |supp(c_2)| - 2|supp(c_1) \cap supp(c_2)|$$

hiszen $|supp(c_1) \cap supp(c_2)|$ páros, mert $(c_1, c_2) = 0$.

Az is világos, hogy a mátrix 12 dimenziós teret generál, hiszen az első 12 oszlop mutatja, hogy a 12 generáló vektor lineárisan független . Ebből következik, hogy a $C = C^{\perp}$. Ha C kódot a $H = (I, A)$ mátrix generálja akkor a $C^{\perp}$ altere $H^* = (-A^T, I)$ mátrix által generált altér. Most azonban $C = C^{\perp}$ 12 dimenziós, F_2 felett vagyunk és A szimmetrikus így C-t generálja a $(J - N, I_{12})$ mátrix is .

Most már bebizonyíthatjuk, hogy C nem tartalmaz 4 súly szót. Tegyük fel, hogy $c \in C$ es $w(c) = 4$. Írjuk fel c-t $c = (a, b)$ alakban ahol a és b két 12 hosszú vektor, $w(a)+w(b) = 4$. Ha $w(a) = 0$ akkor H mátrixbol látszik, hogy $c = 0$, ez nem lehet . Ha $w(a) = 1$ akkor szintén H mátrixból látszik, hogy c a H egyik sora, de ekkor $w(c) = 8$, ez sem lehet. Ha $w(a) = 3$ vagy $w(a) = 4$ akkor $w(b) = 1$ vagy $w(b) = 0$ és H helyett H^* mátrixot használva jutnánk ellentmondásra. Ha $w(a) = 2$ akkor c két bázis vektor összege, de a bizonyítás első mondatából következik, hogy ezen vektorok súlya 8 vagy 12 aszerint, hogy két nem átellenes vagy két átellenes csúcshoz tartozó vektorokról van szó. Tehát C-ben nincs 4 súlyú szó, de minden szó súly osztható 4-gyel, így a minimális súly 8. Mivel a kód 12 dimenziós, így a Golay-kód egyértelműségéből következik, hogy C a Golay-kód .

Tétel: A 24 hosszú $0 - 1$ sorozatokat rendezzük lexikografikusan, majd mohó módon válasszuk ki mindig az első $0-1$ sorozatot, amely legalább 8 távolságra van az addig kiválasztott sorozatoktól. Az így kapott kód éppen a G_{24} Golay-kód .