A Nilli vektorai:

p ptlan prím, $n := 4p$

$\mathcal{F} \subseteq \{-1,1\}^n$ így def, hogy $\underline{x} \in \mathcal{F}$ pontosan akkor ha $x_1 = 1$
és $|\{i : x_i = -1\}|$ = páros.

$\underline{x}$ és y merőleges, ha $\underline{x} \cdot y = 0$.

A Frankl-Wilson tétel helyébe a köv. lemma lép.

<u>Lemma</u>: Ha $\mathcal{G} \subseteq \mathcal{F}$-ben nincsenek merőleges vektorok, akkor

$$|\mathcal{G}| \le \sum_{i=0}^{p-1} \binom{n-1}{i}.$$

(Biz. ld. később.)

Ebből a Borsuk problémára így lesz ellenpélda:

<u>Def</u>: $\underline{x} \otimes \underline{x} = (x_1x_1, x_1x_2, \dots, x_ix_j, \dots, x_nx_n) \in \{-1,1\}^{n^2}$.

$\mathcal{S} := \{\underline{x} \otimes \underline{x} : \underline{x} \in \mathcal{F}\}$.

Mivel $(\underline{x} \otimes \underline{x}) \cdot (y \otimes y) = (\underline{x} \cdot y)^2$ — es egy könnyen látható azonosság —

$\mathcal{S}$-ben a legtávolabb eső vektorok (= legtávolabbi pontba mutatók) merőlegesek. [Ez megfelel az előbbi példa $\frac{n}{4}$-ekben metsző részhalmazokkal bíró teljes ps. gráfnak.] Tehát a lemma szerint $\mathcal{S}$-ből kisebb átmérőjű halmazban (~~mivel~~ használva, hogy $(\underline{x} \otimes \underline{x})$ és $(y \otimes y)$ pontosan akkor merőleges, ha $\underline{x}$ és y) legfeljebb $\sum_{i=0}^{p-1} \binom{n-1}{i}$ elem van. $|\mathcal{S}| = |\mathcal{F}| = 2^{n-2}$, tehát a kisebb átmérőjű

Ekkor azt is kihasználjuk, hogy mindegyik egyforma hosszú.

halmazokra való particionáláskor legalább

$$\frac{2^{n-2}}{\sum_{i=0}^{p-1}\binom{n-1}{i}}$$ partícióosztály kell.

Felhasználva, hogy $n=4p$ $\binom{n-1}{p-1} \sim 2^{n\,h\left(\frac{1}{4}\right)}$,

$\sum_{i=0}^{p-1}\binom{n-1}{i} < p\cdot\binom{n-1}{p-1} \sim p\,2^{n\,h\left(\frac{1}{4}\right)}$ azt kapjuk, hogy

a fenti tört még mindig exponenciális n-ben.

S dimenziója $\leq n^2$ (valójában $\binom{n}{2}$), így a szükséges

partícióosztályok száma nagy n-re messze több $(d+1)$-nél.

Kell tehát még a lemma bizonyítása. Ez jön.

Lemma biz.:

Egy észrevétel, ami kelleni fog: $\forall \underline{a}, \underline{b} \in \mathcal{F}$-re

1, $\underline{a}\cdot\underline{b}$ negatív koord. száma $\equiv$ $\underline{a}\cdot\underline{b}$ poz. koord. száma (mod 4) $\Rightarrow$

$\Rightarrow$ $\underline{a}\cdot\underline{b} \equiv 0 \pmod 4$

2, Az első koord. 1-re rögzítése miatt ($\underline{a} \in \mathcal{F} \Rightarrow -\underline{a} \notin \mathcal{F}$) $\Rightarrow$

$\Rightarrow$ $\underline{a}\cdot\underline{b} \equiv -4p$ nem fordulhat elő $\underline{a}, \underline{b} \in \mathcal{F}$-re.

1, + 2, -ből az adódik, hogy $\underline{a}\cdot\underline{b} \equiv 0 \pmod p$ $\Rightarrow$
$\underline{a}, \underline{b} \in \mathcal{F}$-re

$\Rightarrow$ $\underline{a} = \underline{b}$, vagy $\underline{a}\cdot\underline{b} = 0$. Ez volt az észrevétel.

Most legyen $\mathcal{G}$ a lemma szerinti és $\forall \underline{a} \in \mathcal{G}$-hez

definiáljunk egy $GF(p)$ feletti polinomot.

Az $\underline{a} \in \mathcal{G}$ -hez tartozó $GF(p)$ feletti polinom legyen

$$P_{\underline{a}}(\underline{x}) = \prod_{i=1}^{p-1} (\underline{a} \cdot \underline{x} - i) .$$

Az előbbi észrevétel alapján $\forall \underline{a}, \underline{b} \in \mathcal{G}$ $a \neq b$ -re $\underline{a} \cdot \underline{b} \equiv i \pmod{p}$ valamilyen $i = 1, 2, \dots, p-1$ -re, tehát

$P_{\underline{a}}(\underline{b}) = 0$. ($GF(p)$ -ben vagyunk!)

Másrészt $\underline{a} \cdot \underline{a} = kp$ ($=0$ $GF(p)$ -ben) $\forall \underline{a} \in \mathcal{G}$, így

$P_{\underline{a}}(\underline{a}) \neq 0$

Most kicsit módosítjuk $P_a(\underline{x})$ -et: kifejtés után egyszerűsítünk amíg lehet az $x_i^2 = 1$ azonosságot felhasználva (azaz: úgy tekintve, hogy van egy ilyen azonosságunk). Az eredmény legyen $\overline{P}_a(\underline{x})$. A fenti változtatás $\{-1, 1\}^k$ -beli vektorokra nem okoz változást, így a $\mathcal{G}$ -beli vektorokon $\overline{P}_a(\underline{x}) = P_{\underline{a}}(\underline{x})$, vagyis érvényben marad, hogy

$\overline{P}_{\underline{a}}(\underline{b}) = 0 \iff \underline{b} \neq \underline{a}$.

Ebből az következik, hogy ezek a polinomok ($\overline{P}_a$ -k) lineárisan függetlenek:

Ha $\sum_{\underline{a} \in \mathcal{G}} \lambda_{\underline{a}} \overline{P}_{\underline{a}}(\underline{x}) = 0$ akkor $\underline{x} = \underline{b}$ -t helyettesítve a fentiek alapján $\lambda_{\underline{b}} = 0$ adódik és ez eljátszható minden $\underline{b} \in \mathcal{G}$ -re.

E lineáris függetlenség miatt $|G|$ nem lehet nagyobb, mint az ilyen típusú polinomok terének dimenziója.

Mik az "ilyen" típusú polinomok?

Változóik száma $n-1$ (mert $x_1 = 1$-et van rögz.), mindegyik legf. elsőfokon szerepel és a fokszám legfeljebb $p-1$. ~~[illegible]~~ (minden változójában lineáris – ehhez kellett az $x_i^2 = 1$ helyettesítgetés).

Ekkor a ($GF(p)$ feletti) dimenzió

$\sum_{i=0}^{p-1}\binom{n-1}{i}$ és az állítás éppen ezt a korlátot adta $|G|$-re. □