Paley-gráfok és Hadamard-mátrixok

Hadamard-mátrix:. olyan ± 1-ekből álló $n \times n$-es mátrix, melyeknek a sorai páronként ortogonálisak: $HH^T = n \cdot I_n$.

Hadamard-mátrixok és kódok:. Egy $n \times n$-es ($n > 1$) Hadamard-mátrix sorai egy (általában nemlineáris) n jegyű, n kódszóból álló, $n/2$ távolságú kódot alkotnak (a $\{\pm 1\}$ ábécé fölött).

Feladat:. Tegyük föl, hogy $n > 2$-re létezik $n \times n$-es Hadamard-mátrix. Ekkor $4|n$.

Megoldatlan probléma:. Igaz-e, hogy tetszőleges $4|n$-re létezik $n \times n$-es Hadamard-mátrix.

Feladat:. Minden $n = 2^k$ alakú számhoz létezik $n \times n$-es Hadamard-mátrix.

Mostantól. q páratlan prímhatvány.

Négyzetek $\mathbb{F}_q^*$-ban:.

- $\mathbb{F}_q^*$ elemeinek fele (azaz $(q-1)/2)$) darab áll elő $\mathbb{F}_q^*$-beli elemek négyzeteként. ($\alpha \mapsto \alpha^2$ endomorfozmusa F_q^*-nak, a mag $\{\pm 1\}$.)
- -1 négyzet $\mathbb{F}_q$-ban $\Leftrightarrow 4|(q-1)$. ($\Rightarrow$: Ha -1 négyzet, akkor a négyzetek ellentett párokba sorolhatók, tehát $(p-1)/2$ páros. $\Leftarrow$: Ha $p-1$ osztható 4-gyel, akkor $\mathbb{F}_q^*$-nak van (2 darab) negyedrendű eleme.)

Paley-gráf:. $V = \mathbb{F}_q$. $(\alpha, \beta) \in E \Leftrightarrow \alpha - \beta$ négyzet $\mathbb{F}_q$-ban. Ha $4|q-1$, akkor ez egy irányítatlan gráfként fogható fel, ellenkező esetben pedig egy turnament. Minden pont ki- és befoka $(q-1)/2$.

Állítás:. $\alpha \neq \beta \in \mathbb{F}_q$ esetén

$$|\{\gamma \in \mathbb{F}_q | \gamma - \alpha \text{ és } \gamma - \beta \text{ egyaránt négyzetek vagy nemnégyzetek} \mathbb{F}_q^* \text{-ban}\}| = (q-3)/2.$$

Biz.: $(\gamma - \alpha)$ és $(\gamma - \beta)$ egyaránt négyzetek illetve nemnégyzetek $\Leftrightarrow (\gamma - \alpha)/(\gamma - \beta)$ négyzet. $\{(\gamma - \alpha)/(\gamma - \beta) | \gamma \in \mathbb{F}_q \setminus \{\alpha, \beta\}\} = \mathbb{F}_q^* - \{1\}$ (a $\delta = (x - \alpha)/(x - \beta)$ egyenlet milyen δ esetén oldható meg?), ez $q-2$ darab elem, melyek közül $(q-3)/2$ darab négyzet, és $(q-1)/2$ darab nem-négyzet.

Értelmezés:. Azon események (γ-ban), hogy $\gamma - \alpha$ illetve $\gamma - \beta$ négyzetek, lényegében függetlenek.

Hadamard-mátrix konstrukciója:. Legyen q egy $4k-1$ alakú prímhatvány és $\alpha, \beta \in \mathbb{F}_q$-ra

$$P_{\alpha,\beta} = \begin{cases} +1 & \text{ha } \alpha - \beta \text{ négyzet } \mathbb{F}_q^* \text{ban} \\ -1 & \text{egyébként} \end{cases}$$

Adjunk a P mátrixhoz egy-egy csupa 1-esből álló sort és oszlopot. A fenti állításból könnyen adódik, hogy Hadamard-mátrixot kaptunk.