Lösning till problem 8, övningstenta, vt 2004

• 8. Visa att för varje perfekt kod $\mathcal{C}$ gäller att minimalavståndet $d(\mathcal{C})$ är udda.

Repetition: För varje kod $\mathcal{C}$ av längd n och med minimalavstånd $d = d(\mathcal{C})$ gäller Hammings sfärpackningsolikhet:

$$(*) \qquad |F|^n \geqq |\mathcal{C}| \cdot \sum_{j=0}^{t} \binom{n}{j} (q-1)^j,$$

där F är vårt alfabete (så $\mathcal{C} \subset F^n$) och $t = [(d-1)/2]$. Beviset av denna olikhet bygger på att "bollarna"

$$S_t(v) = \{w \in F^n \mid d(w,v) \leqq t\}$$

är *parvis disjunkta* då v löper genom alla kodord, och

$$\big|S_t(v)\big| = \sum_{j=0}^{t} \binom{n}{j} (q-1)^j.$$

Kom nu ihåg att en kod kallas *perfekt* om *likhet* gäller i (*) ovan, dvs om och endast om hela mängden F^n *täcks* av dessa bollar.

Lösning till problemet: Antag att koden $\mathcal{C} \subset F^n$ är perfekt. *Antag att minimalavståndet $d = d(\mathcal{C})$ är jämnt.* Vi ska visa att detta leder till en motsägelse.

Tag två ord $w_1, w_2 \in \mathcal{C}$ med $d(w_1, w_2) = d$. Eftersom d är jämnt så finns det nu (minst) ett ord $w_3 \in F^n$ som uppfyller $d(w_1, w_3) = d(w_2, w_3) = d/2$. (Ett sådant ord kan skapas genom att man på rätt sätt ändrar w_1 i precis $d/2$ stycken av de d positioner där w_1 skiljer sig från w_2.)

Eftersom $\mathcal{C}$ är perfekt så täcks F^n av sfärerna $S_t(v)$ med $v \in \mathcal{C}$; speciellt täcks vårt ord w_3; dvs det finns ett kodord $v \in \mathcal{C}$ sådant att $w_3 \in S_t(v)$. Då är $d(w_3, v) \leqq t$. Kom ihåg att $t = [(d-1)/2]$, alltså $t = d/2 - 1$ eftersom d är jämnt. Alltså är

$$d(w_3, v) \leqq t < d/2 = d(w_1, w_3) = d(w_2, w_3),$$

så kodordet v *inte likamed* w_1 *eller* w_2*!*

Vi har också, enligt triangelolikheten:

$$d(w_1, v) \leqq d(w_1, w_3) + d(w_3, v) \leqq \frac{d}{2} + t = \frac{d}{2} + (\frac{d}{2} - 1) = d - 1 < d.$$

Detta är en *motsägelse* mot att koden $\mathcal{C}$ har minimalavstånd d och $w_1, v \in \mathcal{C}$ är olika kodord.

Alltså måste minimalavståndet $d = d(\mathcal{C})$ vara udda, vsb.