MATEMATIK
Chalmers Tekniska Högskola

Tentamen i TILLÄMPADE DISKRETA STRUKTURER
18/3 1997, kl 8.45–12.45

Hjälpmedel: Valfri miniräknare, men inga egna anteckningar.
Telefon: Jan Stevens, ankn 5345.

OBS! Linje och inskrivningsår samt namn och personnummer skall anges.

---

1. Låt C vara en kod som korrigerar 1 fel och som möjliggör att avgöra om precis 1 eller 2 fel har inträffat. Visa att $d(C) \geq 4$.
Låt A vara en paritetsmatris för en linjär kod med vikt $w \geq 3$ och bilda en ny matris A' genom att tilläga en rad bestående bara av 1-or. Visa att A' definierar en kod C' med $w(C') \geq 4$.

2. I en boolesk algebra $\mathcal{B}$ definieras en relation $\leq$ genom $x \leq y$ om $xy = x$ för $x,\ y \in \mathcal{B}$.
a) Visa att $\leq$ är en partiell ordning.
b) Visa att $x \leq y$ om och endast om $x + y = y$.
c) Visa att $x \leq y$ om och endast om $\overline{y} \leq \overline{x}$.

3. Skriv $(\mathbb{Z}_{60}^*, \odot)$ som produkt av mindre grupper. Bestäm alla delgrupper till $\mathbb{Z}_{60}^*$.
(8 p)

4. Visa att polynomet $p(X) = X^5 + X^2 + 1$ är primitivt i $\mathbb{Z}_2[X]$. Använd detta för att konstruera kodningspolynomet för en BCH-kod med vikt minst 5.

5. a) Bestäm kortaste perioden av rekurrensföljden $s_{n+3} = s_{n+1} + s_n$, $\overline{s}_0 = (1,1,1)$, över $\mathbb{Z}_3$.
b) Visa att polynomet $X^3 - X - 1 \in \mathbb{Z}_3[X]$ är irreducibelt men ej primitivt.

6. Låt $\mathcal{A}$ vara den linjära ändliga automaten med tillståndsmängd $S = \mathbb{Z}_2 \times \mathbb{Z}_2$, mängd av utsignaler $U = S$, mängd av insignaler $I = \mathbb{Z}_2$, utsignalfunktion $\tau(i,s) = s$ och nästa tillståndsfunktion $\sigma((s_0,s_1),i) = (s_1,i)$. Rita tillståndsgrafen för $\mathcal{A}$.
Vi återkopplar $\mathcal{A}$ genom att sätta $i = u_0 + u_1$. Bestäm den nya tillståndsfunktionen $\sigma' \colon S \to S$ och rita tillståndsgrafen för den återkopplade automaten.

7. Visa att $\omega = 3$ är en primitiv åttonde enhetsrot i $\mathbb{Z}_{41}$ med $\omega^4 = -1$ och använd snabb Fouriertransform baserad på ω för att beräkna

$$(5 + 7X + 9X^2 + 11X^3)(12 + 16X + 20X^2 + 30X^3)$$

i $\mathbb{Z}_{41}[X]$.

8. Vi definierar ett sk Hillkrypto över $\mathbb{Z}_{30}$. Vi koderar A–Ö som 1–28, utropstecken som 29 och punkt som 0. Matrisen $H = \binom{2\,1}{3\,5}$ definierar en linjär avbildning från $\mathbb{Z}_{30}^2$ till $\mathbb{Z}_{30}^2$ som används för att kryptera $\binom{x}{y} \in \mathbb{Z}_{30}^2$. Beräkna H^{-1} och dekryptera

$$\begin{pmatrix} \text{N} & \text{Ä} & \text{R} & \text{D} & \text{A} \\ \text{P} & \text{Ä} & \text{I} & \text{C} & \text{Ö} \end{pmatrix}.$$