MATEMATIK
Chalmers tekniska högskola

Lösningar tentan tillämpade diskreta strukturer 05 mars 2001

1. Observera att $\det H = -1$ (i $\mathbb{Z}_{29}$). Inversen beräknas som vanligt. Resultatet är att $H^{-1} = H$. Vi översätter matrisen och beräknar

$$\begin{pmatrix} 3 & 7 \\ 3 & 26 \end{pmatrix} \begin{pmatrix} 2 & 19 & 6 & 1 & 3 \\ 5 & 16 & 2 & 26 & 3 \end{pmatrix} = \begin{pmatrix} 12 & 24 & 3 & 11 & 1 \\ 20 & 9 & 12 & 12 & 0 \end{pmatrix}$$

som ger

$$\begin{pmatrix} \mathrm{L} & \mathrm{Y} & \mathrm{C} & \mathrm{K} & \mathrm{A} \\ \mathrm{T} & \mathrm{I} & \mathrm{L} & \mathrm{L} & ! \end{pmatrix}.$$

2. a) Matrisen

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

har ingen nollkolonn och alla kolonner är skilda från varandra, så koden med H som kontrollmatris korrigerar ett fel.
b) Felsyndromet för 111011 är $(1,1,0)^t$ och för 100111 $(0,1,1)^t$. Första ordet har ett fel på plats 3, andra på plats 6. De avkodas till 110011 respektive 100110.

3. Låt $f\colon \mathbb{Z}_{2001} \to \mathbb{Z}_{29} \times \mathbb{Z}_{23} \times \mathbb{Z}_3$, $n \mapsto (n \bmod 29, n \bmod 23, n \bmod 3)$. Vi har $f(29 \cdot 23) \equiv 2 \cdot 2 \equiv 1 \bmod 3$, alltså $f^{-1}(0,0,1) = 667$; $f(29 \cdot 3) \equiv 18 \bmod 23$, och med Euklides algoritm hittas inversen 9 till 18 (observera $-5 \cdot 9 = -45 \equiv 1 \bmod 23$). Därmed är $f^{-1}(0,1,0) = 783$. Vidare är $f(23 \cdot 3) \equiv 11 \bmod 29$, som har inversen 8 och $f^{-1}(1,0,0) = 552$.
Vi får $f^{-1}(20,0,1) \equiv 20 \cdot 552 + 667 \equiv 5 \cdot 2208 + 667 \equiv 5 \cdot 207 + 667 \equiv 1702 \bmod 2001$.

4. Först observerar vi att operationen $\oplus$ är kommutativ, ty $x \oplus y = x \cdot \bar{y} + \bar{x} \cdot y = \bar{x} \cdot y + x \cdot \bar{y} = y \cdot \bar{x} + \bar{y} \cdot x = y \oplus x$. Neutralt element är $0 \in \mathcal{B}$: $x \oplus 0 = x \cdot 1 + \bar{x} \cdot 0 = 1$. Inversen till x är $x$själva, ty $x \oplus x = x \cdot \bar{x} + \bar{x} \cdot x = 0$.
För att kolla associativet beräknar vi $(x \oplus y) \oplus z = (x \cdot \bar{y} + \bar{x} \cdot y) \cdot \bar{z} + \overline{(x \cdot \bar{y} + \bar{x} \cdot y)} \cdot z = x \cdot \bar{y} \cdot \bar{z} + \bar{x} \cdot y \cdot \bar{z} + (\bar{x} + y) \cdot (x + \bar{y}) \cdot z = x \cdot \bar{y} \cdot \bar{z} + \bar{x} \cdot y \cdot \bar{z} + \bar{x} \cdot \bar{y} \cdot z + x \cdot y \cdot z$ och samma resultat fås från $x \oplus (y \oplus z)$.

5. a) $SGD(r(X), p(X)) = 1$ omm det finns polynom $a(X)$ och $b(X)$ med $r(X)a(X) + p(X)b(X) = 1$, omm det finns $a(X) \in K[X]$ med $r(X)a(X) \equiv 1 \pmod{p}(X)$, d v s $[r(X)] \in K[X]/p(X)$ har en invers.
b) Ringen $K[X]/p(X)$ är en kropp omm varje element $r(X) \in K[X]/p(X) \setminus 0$, där $\mathrm{grad} r(X) < \mathrm{grad} p(X)$ har en invers, dvs $SGD(r(X), p(X)) = 1$. Men detta är så omm polynomet $p(X)$ är irreducibelt.

6. Polynomet $p(X) = X^5 + X^3 + 1$ har inga linjarfaktorer ty $p(0) = p(1) = 1$. Det är inte delbart med $X^2 + X + 1$ ty $SGD(X^5 + X^3 + 1, X^3 + 1) = SGD(X^3 + 1, X^2) = 1$. Därför är p irreducibelt. Eftersom multiplikativa gruppen i kroppen $\mathbb{Z}_2[X]/(p(X))$ har 31 element har $\alpha = [X]$ ordning 31 och $p(X)$ är primitivt i $\mathbb{Z}_2[X]$.
För en BCH-kod med vikt minst $5 = 2 \cdot 2 + 1$ behöver vi ett polynom med nollställen α, α^2, α^3 och α^4. Polynomet $g_1 := p$ har nollställen α, α^2 och α^4. Vi beräknar $\alpha^6 = \alpha + \alpha^4$, $\alpha^9 = 1 + \alpha^2 + \alpha^3 + \alpha^4$, $\alpha^{12} = \alpha + \alpha^2 + \alpha^3 + \alpha^4$ och $\alpha^{15} = \alpha + \alpha^2$. Man ser nu att α^3 uppfyller $g_3(X) = 1 + X + X^2 + X^3 + X^5 = 0$ och kodningspolynomet blir $g(X) = g_1(X)g_3(X) = 1 + X + X^2 + X^4 + X^5 + X^7 + X^{10}$.

7. Det karakteristiska polynomet $p(X) = X^3 - X + 1$ saknar nollställen ty $a^3 \equiv a \bmod 3$ for alla $a \in \mathbb{Z}$. Den kortaste perioden är nu ordningen av $\alpha = [X]$ i kroppen $\mathbb{Z}_3[X]/p(X)$. Den kan vara 2, 13 eller 26. Tydligen är $\alpha^2 \neq 1$. Vi beräknar $\alpha^9 = (\alpha^3)^3 = (\alpha - 1)^3 = \alpha^3 - 1 = \alpha + 1$ och $\alpha^{12} = (\alpha - 1)(\alpha + 1) = \alpha^2 - 1$, $\alpha^{13} = \alpha^3 - \alpha = -1$. Den kortaste perioden är alltså 26.

8. Vi har $\omega^0 = 1$, $\omega^1 = 2$, $\omega^2 = 4$, $\omega^3 = 8$, $\omega^4 = -1$, $\omega^5 = -2$, $\omega^6 = -4$, $\omega^7 = -8$ och $\omega^8 = 1$ i $\mathbb{Z}_{17}$. Vi beräkna FFTen genom att dela polynomet $f(X) = 3+3X+3X^2+3X^3$ med $X^4 - 1$, $X^4 + 1$, sen $X^2 - 1$, $X^2 + 1$, $X^2 - 4$, $X^2 + 4$ och sen med $X - 1$, $X + 1$, $X - 4$, $X + 4$, $X - 2$, $X + 2$, $X - 8$, $X + 8$. Vi får $-5\ 0\ 0\ 0\ -6\ 2\ 4\ -5$. Koefficientvis kvadratering ger $8\ 0\ 0\ 0\ 2\ 4\ -1\ 8$. Vi använder FFT met ω^{-1} (dvs vi dela med $X^4 - 1$, $X^4 + 1$, sen $X^2 - 1$, $X^2 + 1$, $X^2 + 4$, $X^2 - 4$ och sen med $X - 1$, $X + 1$, $X + 4$, $X - 4$, $X + 8$, $X - 8$, $X + 2$, $X - 2$) på $8 + 2X - X^{+}4X^5 + 8X^7$ med resultat $4\ -5\ -5\ 4\ 8\ 8\ -1\ 0$. Slutligen delar vi med 8, dvs multiplicerar med -2 och får 9 10 10 9 1 1 2 0. Kvadraten är alltså $9 + X + 10X^2 + 2X^3 + 10X^4 + X^5 + 9X^6$. Vi räknar också modulo 4: $(3+3X+3X^2+3X^3)^2 = 1+2X+3X^2+3X^4+2X^5+X^6$ och konstaterar att över $\mathbb{Z}$ gäller att kvadraten är $h(X) = 9 + 18X + 27X^2 + 36X^3 + 27X^4 + 18X^5 + 9X^6$. Eftersom `FF` $= p(4)$ sätter vi in $X = 4$ i $h(X)$. Detta ger:
`9+12·4+(1B+24·4)·10+(1B+12·4)·100+9000=51+AB0+6300+9000=FE01.`