KTH Matematik

5B1118 Diskret Matematik
Kontrollskrivning 5
Tisdagen den 18 May, 2004

- *Skrivtid:***09:15-10:15.**
- *Tillåtna hjälpmedel: Miniräknare med sifferdisplay.*
- *Motivering krävs!*
- *För godkänt resultat krävs minst 5 poäng.*

Personnummer:
Namn:

(1) (3p) Betrakta den linjra koden med checkmatris:

$$M = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

(a) Skriv alla ord i koden.
Ska lösa systemet:

$$\begin{array}{rcrcrcl} x_1 & + & x_4 & + & x_5 & = & 0 \\ x_2 & + & x_4 & + & x_5 & = & 0 \\ & & & & x_3 & = & 0 \end{array}$$

Orden är $\{00000, 11101, 11010, 00111\}$.

(b) Hur många fell kan koden rätta? $\delta(C) = 3$ då kan koden rätta ett fel.

(c) Rätta det felaktiga ordet 11001, om ett fel skedde. Låt $x = 11001$. Multiplicationen Mx ger kolumnen [001]. Ordet rättas som 11101.

(2) (3p) Skriv checkmatrisen av en kod av längd 7 som rättar precis ett fel.
$7 = 2^3 - 1$, så kan man skriva en Hamming kod med $r = 3$. Matrisen M har 3 rader och 7 kolumner, som består av alla ickenoll sekvenser av 3 element i $\mathbb{Z}_2$:

$$M = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

(3) (3p) Kryptera meddelandet 4 i ett RSA-system med krypteringsnyckel $n = 91$, $e = 47$.

2

Meddelandet 4 krypteras som 4^{47} mod 91.

$$47 = 2^5 + 2^3 + 2^2 + 2 + 1 \;\; 4^{47} = 4^{32} \cdot 4^8 \cdot 4^4 \cdot 4^2 \cdot 4$$

Man räknar att

$$4^4 = 256 \equiv_{91} 74 \; 4^8 = 5476 = 91 \cdot 60 + 16 \equiv_{91} 16 \; , 4^{16} = 16 \cdot 16 \equiv_{91} 74 \; 4^{32} \equiv_{91} 16$$

$$4^{47} = \equiv_{91} 16 \cdot 16 \cdot \cdot 74 \cdot 16 \cdot 44 \equiv_{91} 23$$