

**Svar och lösningsförslag till ks4, 9 april 2008,
i SF1610(/5B1118) Diskret matematik för CL**

1) (På a)–f) ger rätt svar $\frac{1}{2}$ p, inget svar 0p, fel svar $-\frac{1}{2}$ p.

Totalpoängen på uppgiften rundas av uppåt till närmaste icke-negativa heltal.)

	sant	falskt
a) Koden $\mathcal{C} = \{1010, 1101, 0111\}$ är 1-felsrättande. [Nej. Minimidistansen är 2.]		×
b) Koden $\mathcal{C} = \{00000, 11010, 10011, 01001\}$ är en linjär kod . [Ja, $a, b \in \mathcal{C} \Rightarrow a + b \in \mathcal{C}$.]	×	
c) I ett krypteringssystem med offentlig nyckel bör man ha en krypteringsfunktion E som saknar invers. [Nej, då kan man inte avkryptera.]		×
d) Om ett tal N klarar fermatetestet med bas ett primtal p , vet vi säkert att N är ett primtal. [Nej, just inte säkert.]		×
e) Den satslogiska sentensen $\neg(A \vee B) \rightarrow (A \rightarrow B)$ är en tautologi , dvs den är sann i alla tolkningar. [Ja, om $A \rightarrow B$ falsk är A sann, så $\neg(A \vee B)$ falsk.]	×	
f) Om $\mathcal{B}$ är en boolesk algebra och $p, q, r, s \in \mathcal{B}$ gäller $p \cdot q + r \cdot s = (p + r) \cdot (q + r) \cdot (p + s) \cdot (q + s)$. [Ja, visas med den ”konstiga” distributiva lagen.]	×	
g) Detta påstående är inte sant. [Lögnarparadoxen. Tydligen inte falskt och inte sant (så sant??).]	○	○

2a) (1p) Avgör om en linjär kod med kontrollmatrisen (checkmatrisen)

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

säkert kan rätta ett fel.

Om den kan det, rätta ordet 01111.

Om den inte kan det, ange ett ord med ett fel som inte kan rättas.

Lösning:

Alla kolonner olika och nollskilda, så koden kan rätta ett fel.

$H(01111)^T = (001)^T = H$:s fjärde kolonn, så fel i position 4.

Svar: Ja, koden rättar ett fel. Det rättade ordet är 01101.

b) (1p) A vill sända ett krypterat meddelande till B, som skall vara säker på att A skrivit det.

Hur kan A göra om de använder RSA-kryptering där person i har dekrypteringsfunktionen D_i och (den offentliga) krypteringsfunktionen E_i ($i = A, B$)?

Lösning:

Använd elektronisk signatur: A sänder $D_A(E_B(x))$ (eller $E_B(D_A(x))$), där x är meddelandet. B använder E_A och D_B för att avkryptera.

c) (1p) Låt $f(x, y, z)$ vara den booleska funktion som har $f(1, 1, 0) = f(1, 0, 1) = f(0, 0, 1) = 1$, alla övriga värden 0.
 Uttryck $f(x, y, z)$ på **disjunktiv normalform**.

Lösning:

Termerna i den disjunktiva normalformen är produkter av alla x, y, z , var och en med eller utan $\bar{}$. Precis de sådana termer tas med som ger 1 på rätt ställen.

Svar: $f(x, y, z) = xy\bar{z} + x\bar{y}z + \bar{x}\bar{y}z$.

3) (3p) Vilken är den minimala (ord)längden för en linjär, 1-felsrättande kod som innehåller 32 ord? (Tips: Vad är sambandet mellan antalet (linjärt oberoende) rader i kontrollmatrisen och ordlängden?)

Lösning:

Eftersom $32 = 2^5$ är kodens dimension 5, så om den sökta längden är n , skall antalet (linjärt oberoende) rader i kontrollmatrisen vara $r = n - 5$. Villkoret för att det skall vara möjligt med en 1-felsrättande kod är precis att det finns n stycken olika och nollskilda kolonner till kontrollmatrisen, dvs att $n \leq 2^r - 1 = 2^{n-5} - 1$. Prövning ger att det minsta möjliga värdet är $n = 9$.

Svar: Den minimala ordlängden är 9.

4) (3p) I ett RSA-system för kryptering används parametern $e = 15$ i krypteringsfunktionen.

Visa att precis ett av värdena 75, 85, 95 är möjligt för "det stora talet n " och ange det värdet.

Kan man för det n -värdet ta dekrypteringsparametern $d = 7$? Motivera.

Lösning:

Möjliga n -värden skall vara pq med p och q olika primtal, så att $\text{sgd}(e, m) = 1$, där $e = 15$ och $m = (p - 1)(q - 1)$. Man finner:

$n = 75 = 3 \cdot 5^2$ är inte en produkt av två olika primtal, så **75 är inte möjligt**.

$n = 85 = 5 \cdot 17$ ger $m = 4 \cdot 16 = 64$ och $\text{sgd}(e, m) = 1$, så **85 är möjligt**.

$n = 95 = 5 \cdot 19$ ger $m = 4 \cdot 18$ och $\text{sgd}(e, m) = 3 \neq 1$, så **95 är inte möjligt**.

Dekrypteringsparametern d till $n = 85$ skall uppfylla att $ed \equiv 1 \pmod{64}$, men $e \cdot 7 = 105 \equiv 41 \pmod{64}$, så d kan inte vara 7.

Svar: Enda möjliga n är 85. Motsvarande d är inte 7.

5) (3p) Uttryck den booleska funktionen

$$f(x, y, z, w) = xyzw + x\bar{z}\bar{w} + \bar{x}y\bar{w} + \bar{x}\bar{y}z\bar{w} + yz\bar{w}$$

på **minimal disjunktiv form**, dvs disjunktiv form med så få '.' och '+' som möjligt. ('.' skall förstås räknas även när de underförstås.)

Lösning:

Uttrycket för f ger karnaughdiagrammet härintill.

Genom att, som i fig., täcka 1:orna med så stora rektanglar som möjligt med sidlängder 1, 2 eller 4, får vi att $f(x, y, z, w)$ är ekvivalent med $xyz + y\bar{w} + \bar{z}\bar{w}$.

Svar:

Uttrycket blir $f(x, y, z, w) = xyz + y\bar{w} + \bar{z}\bar{w}$.

		zw			
		00	01	11	10
xy	00	1	0	0	0
	01	1	0	0	1
	11	1	0	1	1
	10	1	0	0	0