

KTH Matematik
B.Ek

Σ p	G/U	bonus

Efternamn	förnamn	pnr	program

**Kontrollskrivning 4, ti 28 april 2009, 15.05–16.00,
i SF1610(/5B1118) Diskret matematik för CL**

Inga hjälpmedel tillåtna.

Minst 8 poäng ger godkänt.

Godkänd ks n medför godkänd (3p) uppgift n vid tentor till (men inte med) nästa ordinarie tenta (högst ett år), $n = 1, \dots, 5$.

13–15 poäng ger ett ytterligare bonuspoäng vid samma tentor.

Uppgifterna 3)–5) kräver väl motiverade lösningar för full poäng.

Uppgifterna står inte säkert i svårighetsordning.

Spara alltid återlämnade skrivningar till slutet av kursen!

Skriv dina lösningar och svar på samma blad som uppgifterna, använd baksidan om det behövs.

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.)

Kryssa för om påståendena är sanna eller falska (eller avstå)!

poäng uppg.1

- a) Låt $\mathcal{C} = \{0000000, 1011001, 0101010, 1010101\}$. Med koden $\mathcal{C}$ kan ett fel i ett kodord säkert rättas.
- b) Om kontrollmatrisen H för en binär, linjär kod är av typ 5×12 , innehåller koden minst 128 olika ord.
- c) Låt $N \in \mathbb{N}$, $N > 2$. Om $2^{N-1} \equiv 1 \pmod{N}$ måste N vara **ett primtal**.
- d) Med ett RSA-system för kryptering kan parametrarna n , m och e offentliggöras. Bara d måste hållas hemlig.
- e) Om $\mathcal{B}$ är en **boolesk algebra** gäller för $a, b \in \mathcal{B}$ säkert att det finns ett $c \in \mathcal{B}$ med $a + c = b$.
- f) $\neg(p \rightarrow q) \equiv p \wedge \neg q$ gäller för alla satslogiska sentenser p och q . ($\equiv$ betecknar logisk ekvivalens).

sant	falskt

Namn	poäng uppg.2

2a) (1p) Den binära koden

$$\mathcal{C} = \{0000000000, 1100101000, 0110011010, 1011000101, \\ 1101011111, 0111101101, 1010110010, 0001110111\}$$

är **linjär** (det behöver du inte visa).

Vad är minimala avståndet (minimidistansen) δ för $\mathcal{C}$?

b) (1p) I ett (pytte-)RSA-system används "det stora talet" $n = 91 (= 7 \cdot 13)$. Ange för vart och ett av nedanstående tal om det är ett möjligt värde för krypteringsexponenten e eller inte.

2, 5, 12, 13, 35, 49

c) (1p) Låt $a, b \in \mathcal{B}$, en boolesk algebra.

Visa:

$$\text{om } \mathbf{a \cdot b = a} \text{ så } \mathbf{a + b = b.}$$

Namn	poäng uppg.3

3) En linjär kod $\mathcal{C}$ definieras av kontrollmatrisen (i boken kallad checkmatrisen)

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

a) (1p) Vilket eller vilka (om något) av följande är ord i koden $\mathcal{C}$?

0001101, 1110101, 0111001

b) (1p) Om man tar emot ordet **1010110** och högst ett fel har uppstått, vilket var det sända kodordet?

c) (1p) Finns det ord (binära, av längd 7) som varken tillhör $\mathcal{C}$ eller kan uppstå med ett fel i ett kodord? Motivera antingen varför inget sådant finns, eller ange ett.

Namn	poäng uppg.4

4) (3p) Vad blir (minsta icke-negativa) resten då 284^{2009} divideras med 7? Dvs finn x med

$$x \equiv 284^{2009} \pmod{7}, \quad 0 \leq x \leq 6.$$

Motivera ordentligt.

Namn	poäng uppg.5

5) (3p) Uttryck den booleska funktionen

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

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

Lösningar kommer att läggas ut på kurssidan efter skrivningen.