

B.Ek

Efternamn	förnamn	pnr	program

Kontrollskrivning 4, må 2 maj 2011, 9.00–10.00,
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) (För varje delfråga 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 **a)–f)** är sanna eller falska (eller avstå)!

poäng uppg.1	

	sant	falskt
a) Om det minimala avståndet (distansen) mellan ord i en binär kod är 6, kan man säkert rätta 3 fel med koden.		
b) En linjär kod av längd $n = 7$ och dimension $k = 3$ har precis 8 olika kodord.		
c) Om p och q är olika primtal och $r \equiv 1 \pmod{(pq - 1)}$ så är säkert $x^r \equiv x \pmod{(pq)}$ för alla $x \in \mathbb{Z}$.		
d) I ett RSA-system för kryptering med offentlig nyckel måste krypteringsexponenten e vara ett primtal eller en produkt av två primtal.		
e) Om $\mathcal{B}$ är en boolesk algebra gäller för $a, b, c \in \mathcal{B}$ säkert att $(a + b) \cdot \overline{a} \cdot \overline{c} = a + (b \cdot \overline{c})$.		
f) Om $f(x, y, z)$ är en boolesk funktion gäller säkert att $\overline{f(x, y, z)} = f(\overline{x}, \overline{y}, \overline{z})$.		

Σ p	G/U	bonus

Namn	poäng uppg.2

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

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

säkert kan rätta ett fel (dvs om man vet att det uppstått precis ett fel, kan man säkert avgöra vilket ordet var).

Om den kan det, rätta ordet 11101.

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

b) (1p) Formulera **fermattestet med bas b** (det som bygger på Fermats lilla sats) för att avgöra om talet N är ett primtal.

Ange noga vilka slutsatser som kan dras av olika utfall av testet.

c) (1p) Skriv upp värdetabellen för den booleska funktionen

$$f(x, y) = (\overline{x \cdot y}) \cdot (\overline{x \cdot y} + x).$$

Namn	poäng uppg.3

3) Den linjära binära koden $\mathcal{C}$ rättar (minst) 1 fel.

a) (2p) Finn det minsta möjliga värdet för $\mathcal{C}$:s längd (dvs längden av orden i $\mathcal{C}$), om den innehåller precis 16 ord, $|\mathcal{C}| = 16$.

b) (1p) Ange en möjlig kontrollmatris (checkmatris) H för koden $\mathcal{C}$.

Namn	poäng uppg.4

4) (3p) Vad blir (minsta icke-negativa) resten då $2^{5^{2011}}$ (dvs $2^{(5^{2011})}$) divideras med 13? Sökt är alltså x som uppfyller

$$x \equiv 2^{5^{2011}} \pmod{13}, \quad 0 \leq x \leq 12.$$

Motivera ordentligt.

Namn	poäng uppg.5

5) Betrakta den booleska funktion $f(x, y, z)$ som ges av värdetabellen

x	y	z	$f(x, y, z)$
1	1	1	1
1	1	0	1
1	0	1	1
1	0	0	0
0	1	1	0
0	1	0	1
0	0	1	1
0	0	0	0

a) (1p) Skriv $f(x, y, z)$ som ett booleskt uttryck (dvs ett uttryck med x, y, z och $+, \cdot, \neg$) på **disjunktiv normalform, dnf**.

b) (2p) Uttryck med hjälp av ett **karnaughdiagram** $f(x, y, z)$ som ett **minimalt** disjunktivt uttryck.