Matematiska Institutionen
KTH

Lösning till tentamensskrivning i Diskret Matematik för CINTE och CMETE, SF1610 och 5B1118, fredagen den 25 oktober 2013, kl 14.00-19.00.

Examinator: Olof Heden

Hjälpmedel: Inga hjälpmedel är tillåtna på tentamensskrivningen.

Betygsgränser: (**OBS:** Totalsumma poäng vid denna tentamensskrivning är **38p**.)

13	poäng totalt eller mer ger minst omdömet	Fx
15	poäng totalt eller mer ger minst betyget	E
18	poäng totalt eller mer ger minst betyget	D
22	poäng totalt eller mer ger minst betyget	C
28	poäng totalt eller mer ger minst betyget	B
32	poäng totalt eller mer ger minst betyget	A

Observera: Generellt gäller att för full poäng krävs korrekta och väl presenterade resonemang.

DEL I

Var och en av nedanstående uppgifter svarar mot en kontrollskrivning. Godkänt resultat på en kontrollskrivning ger automatiskt full poäng på motsvarande uppgift. Att lösa en uppgift som man på detta sätt redan har till godo ger inga extra poäng.

1. (3p) Bestäm den största gemensamma delaren till talen 498 och 713.

   Lösning: Vi använder Euklides algoritm:

$$\begin{aligned} 713 &= 498 + 215 \\ 498 &= 2\cdot 215 + 68 \\ 215 &= 3\cdot 68 + 11 \\ 68 &= 6\cdot 11 + 2 \\ 11 &= 5\cdot 2 + 1 \end{aligned}$$

   Den sista ickeförsvinnande resten är 1. Algoritmen ger då

   SVAR: 1.

2. (3p) Tio identiska bollar fördelas bland fyra barn. På hur många olika sätt kan detta ske. Svaret skall ges som ett heltal, dvs som något av talen 1, 2, 3, ...

   Lösning. Vi använder det kända sambandet att antalet sätt att fördela n identiska objekt i k olika lådor är

$$\binom{n+k-1}{k-1}$$

   så

   SVAR:

$$\binom{13}{3} = \frac{13\cdot 12\cdot 11}{1\cdot 2\cdot 3} = 286.$$

3. Betrakta gruppen $G = (Z_{21}, +)$.

(a) (1p) Bestäm en icke-trivial delgrupp H till G.

Lösning. Vi söker bland cykliska delgrupper. Den delgrupp som genereras av elementet 7, dvs

$$\langle 7\rangle = \{7, 14, 0\}$$

har varken ett eller 21 element och är då en icketrivial delgrupp.

(b) (1p) Vilka möjligheter finns det för ordningen av element i G.

Lösning. Ordningen av ett element $g \in G$ är lika med antalet element i den cykliska delgrupp $\langle g\rangle$ till G som genereras av elementet g. Antalet element i en delgrupp är enligt Lagranges sats en delare till antalet element i gruppen. Elementet 3 i vår grupp genererar en delgrupp med sju element. Delarna till 21 är 1, 3, 7 och 21. Sammanfattningsvis har vi alltså
SVAR: Ordningarna kan vara 1, 3, 7 eller 21.

(c) (1p) Bestäm ordningen av elementet 2 i G.

Lösning. Vi testar om ordningen av elementet 2 kan vara tre eller sju. Då $2 + 2 + 2 = 6 \neq 0$ och $2 + 2 + \cdots + 2 = 7 \cdot 2 = 14 \neq 0$ så är ordningen varken tre eller sju. Uteslutningsmetoden ger
SVAR: 21.

4. (3p) Ett RSA-krypto har de offentliga nycklarna $n = 85$ och $e = 13$. Kryptera medelandet 2, dvs bestäm E(2), och dekryptera meddelandet 3, dvs bestäm D(3).

Lösning. Då $n = 5 \cdot 17$ så är $m = (5 - 1)(17 - 1) = 64$. Vi söker den dekrypterande nyckeln d. Den satisfierar ekvationen $ed \equiv 1 (\text{mod } 64)$. Men med $e = 13$ gissar vi oss lätt fram till $d = 5$. Nu till kryptering och dekryptering: Vi finner att

$$2^{13} \equiv_{85} 2^8 \cdot 2^5 \equiv_{85} 256 \cdot 32 \equiv_{85} 1 \cdot 32 \equiv_{85} 32.$$

$$3^5 \equiv_{85} 3^4 \cdot 3 \equiv_{85} 81 \cdot 3 \equiv_{85} (-4) \cdot 3 \equiv_{85} 73.$$

Då

$$\mathrm{E}(3) = 3^e (\text{mod } n), \qquad \mathrm{D}(2) = 2^d (\text{mod } n)$$

så

SVAR: Talet 2 krypteras till talet 32 och talet 3 dekrypteras till 73.

5. (3p) För vilka hela tal n och m har den kompletta bipartita grafen $\mathrm{K}_{n,m}$ en Eulerkrets (sluten Eulerväg, alt. sluten Eulerpromenad), och för vilka hela tal n och m har den kompletta bipartita grafen $\mathrm{K}_{n,m}$ en Hamiltoncykel.

Lösning. En graf har en Eulerkrets om och endast om alla noder har jämn valens. Antalet grannar till noder i den kompletta grafen $K_{n.m}$ är antingen n eller m beroende på vilken del av den bipartita grafen noden tillhör. Således finns en Eulerkrets om och endast om både n och m är jämna hela tal större än noll.

För en cykel i en bipartit graf gäller att varannan nod tillhör ena delen av nodmängden och varannan nod den andra delen. Eftersom en Hamiltoncykel är en cykel som passerar varje nod måste då antalet noder i de bägge nodmängderna vara lika. Återstår att visa att om så är fallet så finns en Hamiltoncykel.

Låt ena nodmängden ha noderna $\{a_1, \ldots, a_n\}$ och den andra nodmängden noderna $b_1, \ldots, b_n$. Vi hittar nu Hamiltoncykeln

$$a_1 b_1 a_2 b_2 a_3 \cdots b_{n-1} a_n b_n a_1.$$

SVAR: Eulerkrets finns om och endast om både n och m är jämna tal större än noll. En Hamiltocykel finns om och endast om $n = m \geq 2$.

DEL II

6. (a) (1p) Skriv den Booleska funktionen $f(x,y,z,w) = (x\bar{y} + \bar{x})\bar{z}\bar{w} + \bar{y}(\bar{x} + z)$ på en disjunktiv normalform, dvs på d.n.f. .

Lösning. Gängse kalkyler i en Boolesk algebra ger att $f(x,y,z,w)$ är lika med

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

$$x\bar{y}\bar{z}\bar{w} + \bar{x}(y+\bar{y})\bar{z}\bar{w} + \bar{x}\bar{y}(z+\bar{z})(w+\bar{w}) + (x+\bar{x})\bar{y}z(w+\bar{w}) =$$

$$x\bar{y}\bar{z}\bar{w} + (\bar{x}y\bar{z}\bar{w} + \bar{x}\bar{y}\bar{z}\bar{w}) + (\bar{x}\bar{y}zw + \bar{x}\bar{y}z\bar{w} + \bar{x}\bar{y}\bar{z}\bar{w} + \bar{x}\bar{y}\bar{z}w) + (x\bar{y}zw + \bar{x}\bar{y}zw + \bar{x}\bar{y}z\bar{w} + x\bar{y}z\bar{w}) =$$

$$x\bar{y}\bar{z}\bar{w} + \bar{x}y\bar{z}\bar{w} + \bar{x}\bar{y}zw + \bar{x}\bar{y}z\bar{w} + \bar{x}\bar{y}\bar{z}\bar{w} + \bar{x}\bar{y}\bar{z}w + x\bar{y}zw + x\bar{y}z\bar{w},$$

vilket är den Booleska funktionen skriven på d.n.f. .

(b) (2p) Låt $f(x,y,z,w)$ vara som ovan och och låt $g(x,y,z,w) = \bar{y}(\bar{w}+z) + \bar{x}\bar{z}(\bar{y} + y\bar{w})$. Är $f(x,y,z,w)$ och $g(x,y,z,w)$ samma Booleska funktion.

Lösning. Vi skriver $g(x,y,z,w)$ på d.n.f. Om och endast om denna d.n.f överensstämmer med f:s d.n.f. så är f och g samma Booleska funktion. Vi får att

$$g(x,y,z,w) = (x+\bar{x})\bar{y}(z+\bar{z})\bar{w} + (x+\bar{x})\bar{y}z(w+\bar{w}) + \bar{x}\bar{y}\bar{z}(w+\bar{w}) + \bar{x}y\bar{z}\bar{w} =$$

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

så

SVAR: Ja, de beskriver samma funktion.

(c) (2p) Bestäm antalet Booleska funktioner $h(x,y,z,w)$ som är sådana att

$$|\{(x,y,z,w) \mid f(x,y,z,w) = 1\} \cap \{(x,y,z,w) \mid h(x,y,z,w) = 1\}| = 3.$$

Svaret får innehålla summor och produkter av tal.

Lösning. Funktionen $f(x,y,z,w)$ antar värdet 1 i åtta punkter eftersom dess dnf är en summa av åtta fundamentala konjunktioner. Funktionen $h(x,y,z,w)$ skall anta värdet 1 i precis tre av dessa åtta punkter och värdet 0 i de övriga fem punkter där f antar värdet 1. Dessa tre punkter kan väljas på $\binom{8}{3} = 56$ olika sätt. I övriga åtta punkter i definitionsområdet kan funktionen h anta värdet 0 eller 1, så antalet möjligheter där är totalt $2^8 = 256$. Multiplikationsprincipen ger nu

SVAR: $56 \cdot 256$.

7. Låt $\mathcal{S}_7$ beteckna mängden av alla permutationer av mängden $\{1,2,\ldots,7\}$, och låt ψ beteckna permutationen $\psi = (1\ \ 2\ \ 3\ \ 4)(5\ \ 6)(7)$ i $\mathcal{S}_7$.

(a) (2p) Bestäm en permutation φ i $\mathcal{S}_7$ sådan att permutationen $\psi\varphi$ har ordning 12.

Lösning. Vi tar $\varphi = (5\ \ 6)(5\ \ 6\ \ 7)$ och får då

$$\psi\varphi = (1\ \ 2\ \ 3\ \ 4)(5\ \ 6)(5\ \ 6)(5\ \ 6\ \ 7) = (1\ \ 2\ \ 3\ \ 4)(5\ \ 6\ \ 7),$$

vilket ju är en permutation av ordning 12, eftersom ordningen av en permutation är lika med minsta gemensamma multipeln av längderna hos de disjunkta cyklerna som beskriver permutationen.

(b) (2p) Bestäm antalet permutationer $\varphi \in \mathcal{S}_7$ sådana att permutationen $\psi\varphi$ har ordning 12. Lösningen skall motiveras och svaret ges i formen av ett heltal, dvs som något av talen 1, 2, 3, ...

Lösning. Låt γ vara en permutation, vilken som helst i $\mathcal{S}_7$, men av ordning 12. Låt φ vara den unika lösningen till ekvationen $\psi x = \gamma$, dvs

$$\varphi = \psi^{-1}\gamma.$$

Då gäller att $\psi\varphi$ har ordning 12, eftersom γ har det. Det sökta antalet permutationer φ är således lika med antalet permutationer γ av ordning 12 i $\mathcal{S}_7$. Enda sättet att skapa en permutation av ordning 12 i $\mathcal{S}_7$ är att kombinera två disjunkta cykler av längd 4 respektive 3. Vi beräknar nu antalet sådana kombinationer.
Det finns $\binom{7}{3} = 7\cdot 6\cdot 5/3! = 35$ olika sätt att välja tre element till 3-cykeln. Resterande element kommer till 4-cykeln. En cykel är en ordnad mängd, efter det att startpunkt valts i cykeln. Men startpunkt i given cykel kan väljas godtyckligt. Med given startpunkt, och given mängd av noder i en cykel kan man forma $3! = 6$ olika 4-cykler, och $2! = 2$ olika 3-cykler. Vi får då
SVAR:

$$\binom{7}{3} \cdot 3! \cdot 2! = 420.$$

8. (4p) Bestäm samtliga samanhängande grafer sådana att antalet noder av valens (grad) 2 är dubbelt så stort som antalet noder av valens (grad) 3, och antalet noder av valens (grad) 1 är tre gånger så så stort som antalet noder av valens (grad) 3. Grafen har inga noder av valens (grad) större än 3. Möjligheten att grafen skulle kunna ha multipla (parallella) kanter och loopar (öglor) är inte utesluten. (Vid poängsättningen av din lösning till denna uppgift kommer särskild vikt också att läggas vid att lösningen är så komplett och fullständig som möjligt.)

Lösning. Låt s beteckna antalet noder av valens 3. Då blir antalet noder av valens större än noll lika med

$$v = 3s + 2s + s = 6s$$

och antalet kanter

$$e = \frac{1}{2}(3s + 2\cdot 2s + 3s) = 5s,$$

eftersom summan av valenserna är två gånger antalet kanter. Varje sammanhängade graf har ett spännande träd. Då antalet kanter i ett träd är ett mindre än antalet noder så måste, för de grafer vi skall klassificera, antalet kanter vara minst $6s - 1$. Således

$$5s \geq 6s - 1,$$

varur $s \leq 1$. Ett fall är $s = 0$, som då med givna indata utgör en graf bestående av en nod med valens 0. Om $s = 1$ finns två möjligheter, noden med valens 3 har anting två grannoder med valens 2, eller en grannod med valens två. Med nodmängden $V = \{1, 2, 3, 4, 5, 6\}$, varav noden 1 har valens 3, och noderna 2 och 3 båda valenserna 2, så finns, upp till vilka grannar noderna 4, 5 och 6 skall ha, två möjligheter

1	2	3	4	5	6
2	1	1	2	3	1
3	4	5			
6					

1	2	3	4	5	6
2	1	2	3	1	1
5	3	4			
6					

SVAR: Varje graf med givna indata är **isomorf** men endera av de två graferna ovan, (eller består av en enda nod). (En miss av den sistnämnda triviala möjligheten ger inget poängavdrag.)

DEL III

Om du i denna del använder eller hänvisar till satser från läroboken skall dessa citeras, ej nödvändigvis ordagrant, där de används i lösningen.

9. *Vikten* av ett binärt ord definieras som antalet ettor i ordet. Vikten av ett ord $\bar{c}$ betecknas $\mathrm{w}(\bar{c})$. Ett binärt ord $\bar{c}$ har *jämn vikt* om $\mathrm{w}(\bar{c})$ är ett jämnt tal.

   (a) (1p) Den 1-felsrättande koden C har kontrollmatrisen (parity-check matrisen)

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

   Bestäm två ord $\bar{c}_1$ och $\bar{c}_2$, båda skilda från nollordet, sådana att $\bar{c}_1$ har jämn vikt och $\bar{c}_2$ inte har jämn vikt.

   Lösning. Ordet 0111000000 och 0000011101 är båda kodord, eftersom $\mathbf{H}$ multiplicerar transponatet av dessa kodord till nollkolonnen. Det ena ordet har udda vikt, det andra en jämn vikt.

   (b) (2p) Bestäm kontrollmatrisen till en 1-felsrättande kod C av längd 11 med 64 stycken ord, och sådan att samtliga ord i C har jämn vikt.

   Lösning. Kontrollmatrisen skall ha 11 kolonner, eftersom ordlängden är 11. Om matrisen har fem rader blir antalet kodord $2^{11-5} = 64$, vilket är antal ord i det sökta koden. Vi låter matrisen $\mathbf{H}$'s första rad bestå av enbar ettor. Det garanterar att alla ord har jämn vikt eftersom $\mathbf{H}$ multiplicerar alla kodord till nollkolonnen. Vi finner till exempel att

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

   också uppfyller kraven på att vara en kontrollmatris till en 1-felsrättande kod, dvs alla kolonner är olika och ingen kolonn är nollkolonnen.

   (c) (2p) Undersök om det finns någon 1-felsrättande kod av längd 15 med 2048 stycken ord, och sådan att samtliga ord i C har jämn vikt.

   Lösning. Vi observerar först det finns felkorrigerande 1-felsrättande koder som ej beskrivs av parity-checkmatriser, så vi kan inte förutsätta att en sådan finns.

   Om ordlängden är 15 så är antalet ord i sfärer med radien 1 runt kodord, inklusive kodordet i centrum, lika med 16 stycken ord. Totala antalet ord är $2^{15} = 16 \cdot 2048$, så om antalet ord i den 1-felsrättande koden är 2048 så tillhör varje möjligt ord $\bar{x}$ en unik 1-sfär runt ett kodord $\bar{c}$. Avståndet mellan $\bar{x}$ och $\bar{c}$ är då högst 1.

   Antag att alla ord i C har jämn vikt. Betrakta ett ord $\bar{x}$ på avstånd två från ett kodord $\bar{c}$. Eftersom minavståndet i koden är 3, så kan inte $\bar{x}$ vara ett kodord, men, enligt vad vi kom fram till i stycket ovan, befinner sig $\bar{x}$ på avståndet 1 från ett kodord $\bar{c}'$. Vi visar nu att $\bar{c}'$ har udda vikt.

   Låt kolonnen gjord av ett ord $\bar{y}$ betecknas med $\bar{y}^T$, dvs den transponerade matrisen. Vi inser att ett ord $\bar{y}$ har jämn vikt om och endast om

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \end{bmatrix} \bar{y}^T = \begin{bmatrix} 0 \end{bmatrix}$$

   när vi räknar modulo 2. Ordet $\bar{d} = \bar{x} - \bar{c}$ har precis två ettor, belägna i de positioner där orden skiljer, och ordet $\bar{d}' = \bar{c}' - \bar{x}$ precis en etta. Nu får vi

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \end{bmatrix} \bar{c}'^T = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \end{bmatrix} (\bar{d}' + \bar{x})^T =$$

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \end{bmatrix} (\bar{d}'^T + \bar{d}^T + \bar{c}^T) =$$

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \end{bmatrix} \bar{d}'^T + \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \end{bmatrix} \bar{d}^T + \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \end{bmatrix} \bar{c}^T =$$

$$\begin{bmatrix} 1 \end{bmatrix} + \begin{bmatrix} 0 \end{bmatrix} + \begin{bmatrix} 0 \end{bmatrix} = \begin{bmatrix} 1 \end{bmatrix},$$

   dvs ordet $\bar{c}'$ i C har en udda vikt.

10. Låt p och q vara två olika primtal och låt $n = p^2q^4$.

(a) (3p) Visa att antalet tal a i intervallet $1 \leq a \leq n$ som är relativt prima till n är lika med $p(p-1)q^3(q-1)$.

Lösning. Varje delare $d > 1$ till n innehåller antingen p eller q eller både p och q som faktor i en primtalsfaktorisering av d. Ett tal a är relativt primt med n om a saknar annan gemensam delare än 1 med n. Så a och n är relativt prima om och endast om inget av primtalen p eller q delar a. Vi använder nu inklusion exklusion för att bestämma antal tal a i intervallet $1 \leq a \leq n$ som är relativt prima med n.
Låt P beteckna mängden av tal x i intervallet $1 \leq x \leq n$ som är delbara med p och låt Q beteckna mängden av tal i detta intervall som är delbara med q. Antalet tal a i intervallet $1 \leq a \leq n$ som är relativt prima med n är då

$$n - |P \cup Q|.$$

Vart p:te tal är delbart med p, vart q:te tal är delbart med q och vart pq:te tal delbart med både p och q, så

$$|P| = \frac{n}{p}, \qquad |Q| = \frac{n}{q}, \qquad |P \cap Q| = \frac{n}{pq}.$$

Antalet tal i det givna intervallet som är relativt prima med n är då enligt inklusion exklusion lika med

$$n - (\frac{n}{p} + \frac{n}{q}) + \frac{n}{pq} = n(1 - \frac{1}{p} - \frac{1}{q} + \frac{1}{pq}) = p^2q^4\frac{pq - q - p + 1}{pq} = pq^3(pq - p - q + 1),$$

vilket ju är lika med det angivna uttrycket eftersom

$$(p-1)(q-1) = pq - q - p + 1.$$

(b) (2p) Visa att för varje inverterbart element a i ringen Z_n så gäller att

$$a^{p(p-1)q^3(q-1)} = 1.$$

Lösning. De inverterbara elementen i Z_n bildar en grupp G under operationen multiplikation i Z_n. Ett element a är inverterbart i Z_n om och endast om a är relativt primt med n. Från uppgift (a) har vi alltså att G har $pq^3(p-1)(q-1)$ element. Elementet a genererar en cyklisk delgrupp $\langle a \rangle$ med k element till G

$$\langle a \rangle = \{a, a^2, \ldots, a^k = 1\}.$$

Lagrange sats ger att $|\langle a \rangle|$ delar $|G|$, dvs

$$p(p-1)q^3(q-1) = dk.$$

Vi får nu

$$a^{p(p-1)q^3(q-1)} = a^{dk} = (a^k)^d = 1^d = 1$$