Matematiska Institutionen
KTH

Lösning till tentamensskrivning i Diskret Matematik för CINTE och CMETE, SF1610 och 5B1118, måndagen den 7 januari 2013, kl 14.00-19.00.

Examinator: Olof Heden

Hjälpmedel: Inga hjälpmedel är tillåtna på tentamensskrivningen.

Betygsgränser: (Totalsumma poäng är 36p.)

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

För godkänt resultat krävs också minst 12p på del I. 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 minsta postiva resten vid division av 2^{944} med 157.

   Lösning. Vi observerar att talet 157 är ett primtal p, vilket gör att vi kan använda Fermats lilla sats, dvs *om primtalet p inte delar talet a så gäller att* $a^{p-1} \equiv 1 (\mathrm{mod} \ \ p)$, vid våra beräkningar nedan:
   $$2^{944} \equiv_{157} 2^{6\cdot 156+8} \equiv_{157} (2^{157-1})^6 2^8 \equiv_{157} 1^6 \cdot 256 \equiv_{157} 99.$$
   Således har våra beräkningar gett att
   $$2^{944} = k \cdot 157 + 99$$
   för något heltal k. Eftersom dessutom $0 \leq 99 < 157$ så är vårt

   SVAR: 99.

2. (3p) Tolv röda och elva gröna, men för övrigt identiska, bollar skall läggas i påsar som barnen A, B, C och D skall få. Hur många möjliga fördelningar av bollarna finns om varje påse skall innehålla minst en boll av varje färg. Svara med ett heltal.

   Lösning. Placera först en boll av vardera färgen i varje påse. Återstår åtta röda och sju gröna men för övrigt identiska bollar att placera ut i fyra olika lådor, vilket kan ske på respektive
   $$\binom{8+4-1}{4-1}, \qquad \binom{7+4-1}{4-1}$$
   olika sätt. Dessa alla möjligher för respektive färg kan kombineras till ett

   SVAR:
   $$\binom{11}{3}\binom{10}{3} = \frac{11\cdot 10\cdot 9}{1\cdot 2\cdot 3}\cdot\frac{10\cdot 9\cdot 8}{1\cdot 2\cdot 3} = 11\cdot 5\cdot 3\cdot 10\cdot 3\cdot 4 = 10\cdot 10\cdot 11\cdot 9\cdot 2 = 19800.$$

3. (3p) Betrakta gruppen $G = (Z_3, +) \times (Z_3, +) \times (Z_3, +)$ som består av alla 3-tipplar (x_1, x_2, x_3), där $x_1, x_2, x_3 \in (Z_3, +)$ och där operationen är definierad genom komponentvis addition modulo 3, dvs

$$(x_1, x_2, x_3) + (y_1, y_2, y_3) = ((x_1 + y_1)(\text{mod } 3), (x_2 + y_2)(\text{mod } 3), (x_3 + y_3)(\text{mod } 3)).$$

(a) (1p) Bestäm ordningen av elementet $(1, 2, 0)$.

Lösning. Identitets elementet i den givna gruppen är $(0, 0, 0)$. Vi testar

$$(1, 2, 0) \neq (0, 0, 0), \quad (1, 2, 0) + (1, 2, 0) = (2, 1, 0), \quad (1, 2, 0) + (1, 2, 0) + (1, 2, 0) = (0, 0, 0)$$

så

SVAR: Ordningen är 3.

(b) (1p) Bestäm en icketrivial delgrupp till G.

Lösning. Vi kan t ex ta den delgrupp som genereras av elementet $(1, 2, 0)$ som

SVAR:

$$< (1, 2, 0) >= \{(1, 2, 0), (2, 1, 0), (0, 0, 0)\} =< (2, 1, 0) > .$$

(c) (1p) Hur många icketriviala delgrupper har G? (Ett korrekt svar utan motivering ger full poäng.)

Lösning. Gruppen G består av 27 element, vart och ett av dessa element, förutom identiteten, har ordning 3 och genererar en icke trivial delgrupp med tre element, vilken genereras av två element av ordning 3. Det finns också delgrupper med nio element. Eftersom inget element i G har ordning 9 så är en sådan delgrupp en kombination av två delgrupper med tre element vardera.

Som sammanfattning får vi:

Antalet delgrupper med tre element är lika med hälften av antal element av ordning 3, dvs $(27 - 1)/2 = 13$.

Antalet delgrupper med nio element är lite mer komplicerat att beräkna. En sådan grupp H har totalt $(9 - 1)/2 = 4$ olika delgrupper H_1 och H_2 med vardera tre element, och varje par av sådana delgrupper till G bestämmer en delgrupp H med nio element i G. Antalet delgrupper med nio element blir då

$$\frac{\binom{13}{2}}{6} = 13$$

eftersom det finns precis 6 par av delgrupper med tre element i en delgrupp med nio element.

SVAR: 26.

4. (3p) Bestäm kontrollmatrisen till en 1-fels-rättande kod C med $|C| = 32$ stycken ord av längd 9. När du gjort detta får du 1 poäng. Du får ytterligare 2 poäng om C är sådan att ordet 111111111 inte finns med i koden C men går att rätta till ett ord i C.

Lösning. Om kontrollmatrisen $\mathbf{H}$ har nio kolonner och fyra rader så blir $|C| = 2^{9-4} = 32$. Matrisen $\mathbf{H}$ multiplicerade med kolonnmatrisen bestående av nio ettor skall inte bli lika med nollkolonnen, men lika med en av matrisens kolonner för att ordet 111111111 skall kunna rättas. Vi ordnar detta genom att låta summan av de sju första kolonnerna bli lika med nollkolonnen och summan av de två sista kolonnerna bli lika med kolonn nummer ett. Så

SVAR:

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

5. (3p) Grafen G saknar multipla kanter och loopar (öglor), antalet noder med valens (grad) tre är fler än antalet noder med valens ett. Kan grafen G sakna cykler? (Ett svar utan motivering ger inga poäng.)

Lösning. Vi använder att summan av nodernas valenser är dubbelt så stort som antalet kanter, dvs

$$\sum_{v \in V} \delta(v) = 2|E|.$$

Vi tar först bort alla noder av valens 0, dvs isolerade noder. Låt V beteckna de noder som då finns kvar. Låt V_i beteckna mängden av noder med valensen i. Då gäller, emedan $3|V_3| \geq |V_1| + 2|V_3|$, att

$$2|E| = \sum_{i=1}^{\infty} i|V_i| \geq |V_1| + 2|V_2| + (|V_1| + 2|V_3|) + \sum_{i=4}^{\infty} i|V_i| \geq \sum_{i=1}^{\infty} 2|V_i| = 2\sum_{i=1}^{\infty} |V_i| = 2|V|.$$

Alltså gäller i den graf som återstår när noder med valens 0 plockats bort att antalet kaner är minst lika stort som antalet noder. En graf utan cykler är en skog med minst ett träd. Vare träd har fler noder än kanter. Således måste grafen ha minst en cykel.

DEL II

6. (4p) I en skola med fyra klasser med respektive 13, 14, 15 och 16 elever skall ett eleveråd utses om 12 elever och med minst en elev från varje klass. På hur många olika sätt kan detta ske? Svaret får innehålla uttryck som presenterats i kursen.

Lösning. Låt A beteckna de urval av 12 elever, bland skolans totalt 58 elever, som inte innehåller något barn från klassen med 13 elever, B de urval som saknar elever från klassen med 14 elever, samt C och D analogt. Vi får då att svaret ges av

$$\binom{58}{12} - |A \cup B \cup C \cup D|.$$

Vi använder principen om inklusion exklusion för att beräkna termen ovan. Om inget barn ur klassen med 13 elever väljs, skall 12 barn bland de återstående $58 - 13 = 45$ barnen väljas vilket kan göras på

$$|A| = \binom{58-13}{12} = \binom{45}{12}$$

olika sätt. På samma sätt får vi

$$|B| = \binom{44}{12}, \qquad |C| = \binom{43}{12}, \qquad |D| = \binom{42}{12}.$$

$$|A \cap B| = \binom{32}{12}, \qquad |A \cap C| = \binom{31}{12}, \qquad |A \cap D| = \binom{30}{12}$$

$$|B \cap C| = \binom{30}{12}, \qquad |C \cap D| = \binom{28}{12}, \qquad |B \cap D| = \binom{29}{12}$$

och

$$|A \cap B \cap C| = \binom{16}{12}, \qquad |B \cap C \cap D| = \binom{13}{12}, \qquad |A \cap C \cap D| = \binom{14}{12}, \qquad |A \cap B \cap D| = \binom{15}{12}.$$

SVAR:

$$\binom{58}{12} - (\binom{45}{12} + \binom{44}{12} + \binom{43}{12} + \binom{42}{12}) +$$

$$+(\binom{32}{12} + \binom{31}{12} + \binom{30}{12} + \binom{30}{12} + \binom{28}{12} + \binom{29}{12}) - (\binom{16}{12} + \binom{15}{12} + \binom{14}{12} + \binom{13}{12}).$$

7. (3p) Betrakta gruppen $\mathcal{S}_{12}$ av alla permutationer av elementen i mängden $\{1, 2, \ldots, 12\}$. Undersök om det finns permutationer φ, γ och ψ i $\mathcal{S}_{12}$ sådana att

$$\varphi^4 = \gamma^5 = \psi^6 = (1\ 2)(3\ 4)(5\ 6)(7\ 8)(9\ 10)(11\ 12).$$

Lösning. Varje 2-cykel δ har ordning 2, och då gäller för varje 2-cykel δ att

$$\delta^5 = \delta^2\delta^2\delta = \delta$$

Alltså om $\gamma = (1\ 2)(3\ 4)(5\ 6)(7\ 8)(9\ 10)(11\ 12)$, som ju är en produkt av disjunkta 2-cykler, så gäller

$$\gamma^5 = \gamma = (1\ 2)(3\ 4)(5\ 6)(7\ 8)(9\ 10)(11\ 12).$$

Vis av erfarenheten av räkningar med permutationer har vi att om ψ är en 12-cykel, så kommer ψ^6 att ha ordning 2, ty $(\psi^6)^2 = \psi^{12} = \text{id}$. Mer precist

$$(a_1\ a_2\ \ldots\ a_{12})^6 = (a_1\ a_7)(a_2\ a_8)\cdots(a_6\ a_{12}).$$

Enligt formeln ovan hittar vi den efterfrågade permutationen ψ, med $a_1 = 1$, $a_7 = 2$ etc:

$$\psi = (1\ 3\ 5\ 7\ 9\ 11\ 2\ 4\ 6\ 8\ 10\ 12).$$

Svårare med φ. Om φ^4 är en produkt av 2-cykler så gäller att $(\varphi^4)^2 = \text{id}$. Ordningen av elementet φ blir då 8, varför φ måste vara en produkt av enbart disjunkta 2-cykler, 4-cykler och 8-cykler. Minst en 8-cykel måste finnas med i denna produkt för att ordningen skall bli 8.

Men 2-cykler och 4-cykler "upphöjda" till 4 blir identiteten, och en 8-cykel upphöjt till 4 blir, i analogi med formeln ovan för 12-cykler, en produkt av fyra stycken 2-cykler. Vi kan således ej erhålla en produkt av sex stycken 2-cykler, eftersom sex inte är en jämn multipel av fyra.

SVAR: Endast γ och ψ finns, se ovan för dessa.

8. (a) (2p) Bestäm Booleska funktioner $f \neq 1$ och $g \neq 1$ sådana att ekvationen $f + x = g$ har precis fyra olika lösningar i en Boolesk algebra som du väljer själv.

Lösning. Vi betraktar Booleska funktioner i två variabler u och w. Låter vi

$$f = g = w,$$

så finns det precis fyra olika lösningar x till den givna ekvationen

$$x = w, \qquad x = 0, \qquad x = wu, \qquad x = w\bar{u}.$$

Det är enkelt, t ex med hjälp av ett Karnaugh-diagram, att övertyga sig om att inga andra lösningar finns.

SVAR: Se ovan.

(b) (2p) Kan en sådan ekvation, som den i föregående uppgift, ha precis fem olika lösningar? Motivera ditt svar.

Lösning. Antag att f, x och g är funktioner i n Booleska variabler. Om den givna ekvationen har minst en lösning finns tre slag av punkter:

1. Punkter, som vi betecknar $(x_1, x_2, \ldots, x_n)$, där både f och g antar värdet 1.
2. Punkter, som vi betecknar $(y_1, y_2, \ldots, y_n)$, där både f och g antar värdet 0.
3. Punkter, som vi betecknar $(z_1, z_2, \ldots, z_n)$, där f antar värdet 0 men g antar värdet 1.

Efersom $f + x = g$ måste dels

$$x(z_1, z_2, \ldots, z_n) = 1$$

i alla punkter av kategorin 3 och dels

$$x(y_1, y_2, \ldots, y_n) = 0$$

i alla punkter av kategorin 2.

För punkter $(x_1, x_2, \ldots, x_n)$ i kategorin 1 kan den Booleska funktionen x antingen anta värdet 0 eller värdet 1. Med m punkter i kategorin 1 finns då 2^m olika val av värden till funktionen x. Eftersom 5 inte är någon potens av 2 så blir vårt

SVAR: Nej.

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. Låt $\mathcal{A}$ vara ett alfabete med oändligt många men ett uppräkneligt antal bokstäver.

(a) (2p) Visa att mängden av ord av längd två som man kan bilda med hjälp av bokstäver från alfabetet $\mathcal{A}$ är en uppräkneligt oändlig mängd.

Lösning. Följer av lösningen till uppgift (b) eftersom mängden av ord av längd två är en delmängd till mängden av alla ord av ändlig längd. I uppgift (b) visas att denna sistnämnda mängd är uppräknelig och oändlig.

(b) (3p) Är också mängden av alla ord av ändlig längd, som man kan bilda med hjälp av bokstäver i $\mathcal{A}$, en uppräkneligt oändlig mängd?

Lösning. Vi gör först ett induktionsbevis där vi visar att mängden av ord av längd n, för varje givet n, är en uppräknelig mängd.

Varje ord av längd n är en sammansättning av ett ord a av längd $n-1$ med en bokstav b till ordet ab. Antag nu att orden av längd $n-1$ kan räknas upp

$$a_1, a_2, a_3, ...$$

och att bokstäverna i alfabetet har en uppräkning

$$b_1, b_2, b_3, ...$$

Vi kan då skapa en uppräkning av orden av längd n enligt följande diagonalmönster, vilket liknar uppräkningen av de rationella talen:

$$a_1b_1, \quad a_2b_1, a_1b_2, \quad a_3b_1, a_2b_2, a_1b_3, \quad ...$$

dvs vi räknar upp orden i indexsumma s ordning:

$$a_{s-1}b_1, a_{s-2}b_2, ..., a_1b_{s-1}.$$

Eftersom orden av längd 1 är uppräkneliga, de utgör ju bokstäverna i alfabetet, så följer av induktionsprincipen att alla ord av viss given längd n är uppräkneliga.

Låt nu orden av längd n ha uppräkningen

$$w_{1,n}, w_{2,n}, w_{3,n}, ...$$

Vi kan då som ovan få en uppräkning av alla ord av ändlig längd, nämligen

$$w_{1,1}, \quad w_{2,1}, w_{1,2}, \quad w_{3,1}, w_{2,2}, w_{1,3}, \quad w_{4,1}, ..., w_{1,4}, \quad w_{5,1}, ...$$

där vi alltså i tur och ordning räknar upp de ändligt många orden vars index summa är lika med s, för $s = 2, 3, \ldots$:

$$w_{s-1,1}, w_{s-2,2}, \ldots, w_{1,s-1}.$$

Så

SVAR: Ja de utgör en uppräknelig mängd.

10. (5p) I den bipartita grafen G med nodmängderna X och Y (så det finns inga kanter mellan noder i X och inga kanter mellan noder i Y) gäller att mängderna X och Y är ändliga och lika stora. Låt för varje delmängd A till X

$$R(A) = \{y \in Y \mid y \text{ granne till minst en nod i } A\}$$

och för varje delmängd B till Y

$$L(B) = \{x \in X \mid x \text{ granne till minst en nod i } B\}.$$

Visa att det finns en delmängd A till X med $|R(A)| < |A|$ om och endast om det finns minst en delmängd B till Y sådan att $|L(B)| < |B|$.

Lösning. Vi använder Halls bröllopssats som säger att *om och endast om* $|A| \leq |R(A)|$ *för varje delmängd* A *till* X *så finns en komplett matchning i den givna bipartita grafen*

Om $|B| \leq |L(B)|$ för alla delmängder B till Y finns, enligt Halls bröllopssats, en matchning i bipartita grafen där varje Y-nod är matchad med en X-nod. Eftersom antalet noder i X är lika med antalet noder i Y kommer då varje X-nod att vara matchad med en Y-nod. Då måste också $|A| \leq |R(A)|$ för alla delmängder A till X.

Detta visar att *om* $|R(A)| < |A|$ *för någon delmängd* A *till* X *så finns minst en delmängd* B *till* Y *sådan att* $|L(B)| < |B|$.

På samma sätt, byt X mot Y och A mot B, visas att *om* $|R(B)| < |B|$ *för någon delmängd* B *till* Y *så finns minst en delmängd* A *till* X *sådan att* $|L(A)| < |A|$.

Vi har nu visat påståendet i uppgiften.