Matematiska Institutionen
KTH

**Lösningen till tentamensskrivning i Diskret Matematik för CINTE och CMETE, SF1610 och 5B1118, torsdagen den 18 oktober 2012, kl 08.00-13.00.**

**Examinator:** Olof Heden

**Hjälpmedel:** Inga hjälpmedel är tillåtna på tentamensskrivningen.

**Betygsgränser:** (Totalsumma poäng är 37p.)

| | | |
|---|---|---|
| 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) Lös ekvationen $35x + 17 = 15$ i ringen $Z_{71}$.

   **Lösning:** Ekvationen förenklas till $35x = -2$. Söker invers till 35 i ringen $Z_{71}$ med hjälp av Euklides algoritm:
   $$71 = 2 \cdot 35 + 1$$
   vilket ger $1 = -2 \cdot 35 + 71$, varur $35(-2) = 1$ i ringen $Z_{71}$. Inversen till 35 i denna ring är alltså $-2$. Vi får nu
   $$35x = -2 \qquad \Longleftrightarrow \qquad (-2)35x = (-2)(-2) \qquad \Longleftrightarrow \qquad x = (-2)(-2) = 4.$$

   **SVAR:** $x = 4$.

2. (3p) Hur många olika ord av längd 9 kan man bilda med hjälp av bokstäverna A, A, A, B, B, B, C, C, C, dvs med hjälp av tre stycken A:n, tre stycken B:n och tre stycken C:n. För full poäng krävs att svaret ges i formen av ett heltal.

   **Lösning:** Vi skall tilldela bokstäverna A, B och C tre positioner vardera i ordet av längd nio. Mängden av de nio positionerna skall alltså delas in i tre etiktterade delmängder med vardera tre positioner. Antalet möjligheter för en sådan uppdelning ges av multinomialkoefficienten
   $$\binom{9}{3,3,3} = \frac{9!}{3! \cdot 3! \cdot 3!} = \frac{9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4}{6 \cdot 6} = 3 \cdot 4 \cdot 7 \cdot 5 \cdot 4 = 84 \cdot 20 = 1680$$

   **SVAR:** 1680.

3. (3p) Betrakta gruppen $G = (Z_{15}, +)$. Bestäm ordningen av elementen 10, 11 och 12.

**Lösning:** Ett elements ordning delar antalet element i gruppen, i detta fall blir då ordningen en delare till 15, dvs något av talen 1, 3, 5 eller 15. Vi finner att

$$1 \cdot 10 = 10 \neq 0, \qquad 3 \cdot 10 = 0,$$

så ordningen av elementet 10 är 3. Vidare

$$1 \cdot 11 \neq 0, \qquad 3 \cdot 11 = 3 \neq 0, \qquad 5 \cdot 11 = 10 \neq 0,$$

så elementet 11 har ordning 15. Tillslut $3 \cdot 12 = 6 \neq 0$, men $5 \cdot 12 = 0$ så 12 har ordning 5.

**SVAR:** 10 har ordning 3, 11 har ordning 15 och 12 har ordning 5.

4. Nedanstående matris $\mathbf{H}$ är kontrollmatrisen till en 1-felsrättande kod $C$.

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

(a) (1p) Bestäm två ord som tillhör koden $C$.

**Lösning:** Nollordet 0000000000 tillhör alltid en kod definierad genom en kontrollmatris. Summan av kolonnerna 1, 3, 4 och 5 blir nollkolonnen, varför ett ord med ettor i motsvarande positioner och noll i övriga positioner också tillhör koden.

**SVAR:** Till exempel 0000000000 och 1011100000.

(b) (1p) Bestäm antalet ord som finns i koden $C$.

**Lösning:** Antale kolonner är 10 och antalet rader är fyra, vilka är linjärt oberoende, så

**SVAR:** $|C| = 2^{10-4} = 64$.

(c) (1p) Undersök om ordet 0001110100 går att rätta. Rätta ordet om det går att rätta. Om du finner att ordet inte kan rättas skall du motivera varför så är fallet.

**Lösning:** Låt $\bar{x} = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$ och $\bar{x}^T$ det transponerade ordet. Då gäller att

$$\mathbf{H}\bar{x}^T = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

vilket är kolonn nummer fem i matrisen $\mathbf{H}$. Ett fel har då uppstått i position nummer fem.

**SVAR:** Ordet kan rättas till ordet 0001010100.

5. (3p) Kan det finnas någon planär sammanhängande graf med 38 kanter och 24 noder om alla grafens cykler har längd minst 5? (Ett svar utan motivering ger inga poäng.)

**Lösning:** Enligt Eulers formel blir antalet områden som uppstår vid en plan ritning lika med

$$r = e + 2 - v = 38 + 2 - 24 = 16.$$

Vi kommer att använda oss av att vid en plan ritning kommer varje område att omgärdas av en cykel av längd minst fem. Vi betraktar en incidensmatris $(\delta_{i,j})$ med 38 rader, svarande mot grafens kanter, och 16 stycken kolonner var och en svarande mot ett av de områden som skulle uppstå vid en plan ritning av grafen.

Låter vi

$$\delta_{i,j} = \begin{cases} 1 \text{ om kanten } e_i \text{ gränskant till området } r_j \\ 0 \text{ annars,} \end{cases}$$

kommer varje rad att innhålla högst två stycken ettor. Antalet ettor i matrisen blir då högst lika med $38 \cdot 2 = 76$. Å andra sidan kommer varje kolonn att innehålla minst fem stycken ettor, och därmed innehäller matrisen minst $16 \cdot 5 = 80$ ettor. Men 80 är inte mindre än 76, så en plan ritning av grafen existerar inte.

**SVAR:** Nej.

**DEL II**

6. (3p) En oändlig talföljd $a_0 = 5$, $a_1 = 2$, $a_3$, $a_4$, ... , definieras rekursivt genom

$$a_n = 2a_{n-1} + 8a_{n-2}$$

för $n = 2, 3, \ldots$ . Visa med ett induktionsbevis att $a_n = 3(-2)^n + 2 \cdot 4^n$ för alla naturliga tal $n$.

**Lösning:** Sätt $b_n = 3(-2)^n + 2 \cdot 4^n$. Vi visar att $a_n = b_n$ för $n = 0, 1, \ldots$.
För det första

$$a_0 = 5 = 3(-2)^0 + 2 \cdot 4^0 = b_0, \qquad \text{och} \qquad a_1 = 2 = 3(-2) + 2 \cdot 4 = b_1. \tag{1}$$

Nu visar vi

$$a_{n-2} = b_{n-2}, \quad \text{och} \quad a_{n-1} = b_{n-1} \qquad \Longrightarrow \qquad a_n = b_n. \tag{2}$$

Så antag $a_{n-2} = b_{n-2}$ och $a_{n-1} = b_{n-1}$. Då gäller att

$$a_n = 2a_{n-1} + 8a_{n-2} = 2(3(-2)^{n-1} + 2 \cdot 4^{n-1}) + 8(3(-2)^{n-2} + 2 \cdot 4^{n-2}) =$$

$$= 12(-2)^{n-2} + 32 \cdot 4^{n-2} = 3 \cdot (-2)^n + 2 \cdot 4^n = b_n.$$

Eftersom vi har visat att påståendena i ekvationerna (1) och (2) är sanna följer från induktionsaxiomet att $a_n = b_n$ för $n = 0, 1, 2, \ldots$ .

7. Låt $\mathcal{M} = \{1, 2, \ldots, 6\}$ och låt

$$\mathcal{S} = \{(1, 2), (3, 3), (3, 4), (6, 5), (5, 6)\}.$$

(a) (2p) Bestäm en ekvivalensrelation på $\mathcal{M}$ som innehåller $\mathcal{S}$.

**Lösning:** Varje ekvivalensrelation på en mängd $\mathcal{M}$ delar in mängden $\mathcal{M}$ i disjunkta ekvivalensklasser så att alla element i en ekvivalensklass är sinsemellan ekvivalenta, och element i skilda ekvivalensklasser är inte ekvivalenta. Omvänt gäller att varje sådan uppdelning av $\mathcal{M}$ på detta sätt definierar en ekvivalensrelation.
Den minsta uppdelningen som inte motsäger de givna ekvivalenserna i $\mathcal{S}$ är indelningen

$$\mathcal{M} = C_1 \cup C_3 \cup C_5,$$

där

$$C_1 = \{1, 2\}, \qquad C_3 = \{3, 4\} \qquad C_5 = \{5, 6\}$$

Alternativt kan man ge

**SVAR:** En ekvivalensrelation som uppfyller givna förutsättningar är

$$\{(1, 1), (1, 2), (2, 1), (2, 2)\} \cup \{(3, 3), (4, 4), (3, 4), (4, 3)\} \cup \{(5, 5), (6, 6), (5, 6), (6, 5)\}.$$

(b) (1p) Beskriv två andra ekvivalensrelationer på $\mathcal{M}$ som innehåller $\mathcal{S}$

**Lösning:** Vi kombinerar $C_1$ och $C_3$ ovan, resp för den andra ekvivalensrelationen $C_1$ och $C_5$ ovan, och får

**SVAR:** Till exempel de två ekvivalensrelationer som beskrivs av nedanstående uppdelningar i ekvivalensklasser:

$$D_1 = \{1,2,3,4\}, \qquad C_5 = \{5,6\}$$

resp

$$E_1 = \{1,2,5,6\}, \qquad C_3 = \{3,4\}$$

(c) (1p) Bestäm antalet ekvivalensrelationer på $\mathcal{M}$ innehåller $\mathcal{S}$.

**Lösning:** Den enda ekvivalensrelation som ger en uppdelning i tre ekvivalensklasser är den som presenterades i lösningen av uppgift (a). Det finns ytterligare en ekvivalensrelation som ger två ekvivalensklasser, förutom de som angavs i lösning till deluppgift (b), nämligen med ekvivalensklasserna $C_1$ och $F_3 = C_3 \cup C_5$. Det finns ingen ekvivalensrelation som innehåller den givna mängden $\mathcal{S}$ av relationer och som ger fler än tre ekvivalensklasser, men låter vi alla element vara ekvivalenta med varandra får vi en ekvivalensrelation med $\mathcal{M}$ som enda ekvivalensklass. Så om vi summerar de olika fallen ovan har vi

**SVAR:** $1 + 3 + 1 = 5$

8. (4p) Fem flickor och fem pojkar skall delas in i tre grupper på ett sådant sätt att varje grupp innehåller minst en pojke och minst en flicka. På hur många olika sätt kan detta ske? För full poäng krävs att svaret ges i formen av ett heltal.

**Lösning:** Vi delar först in pojkarna, respektive flickorna, i tre icketomma delgrupper, vilket i vart och ett av fallen går på $\mathrm{S}(5,3)$ olika sätt. Sedan kopplar vi ihop respektive grupper av flickor och pojkar, vilket går på $3!$ olika sätt.

Multiplikationsprincipen ger nu att total antalet möjligheter att fördela pojkar och flickor enligt givna specifikationer är

$$\mathrm{S}(5,3) \cdot \mathrm{S}(5,3) \cdot 3!.$$

Vi använder nu rekursionen $\mathrm{S}(n,k) = \mathrm{S}(n-1,k-1) + k\mathrm{S}(n-1,k)$ för att beräkna Stirlingtalet ovan:

$$\mathrm{S}(5,3) = \mathrm{S}(4,2) + 3\mathrm{S}(4,3) = (\mathrm{S}(3,1) + 2\mathrm{S}(3,2)) + 3(\mathrm{S}(3,2) + 3\mathrm{S}(3,3)) =$$
$$= (1 + 2\cdot 3) + 3(3 + 3\cdot 1) = 7 + 3\cdot 6 = 25,$$

eftersom det är lätt att direkt verifiera att $\mathrm{S}(3,2) = 3$.

**SVAR:** $6 \cdot 25^2 = 6 \cdot 625 = 3600 + 150 = 3750.$

## 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 $\mathcal{S}_n$, för varje naturligt tal $n$, beteckna den grupp som består av alla permutationer av de element i mängden $\{1,2,3,\ldots,n\}$.

(a) (2p) Bestäm den minsta delgrupp $\mathcal{T}_3$ till $\mathcal{S}_4$ som innehåller elementen $\tau_2$ och $\tau_3$, vilka i cykelnotation beskrivs $\tau_2 = (1\ 2)$ och $\tau_3 = (1\ 3)$.

**Lösning:** Vi visar att den minsta delgrupp till $\mathcal{S}_4$ som innehåller de givna permutationerna är den delgrupp som består av alla permutationer i $\mathcal{S}_4$ som fixerar elementet 4. Ty för det första observerar vi att generellt gäller

$$(i\ j)(i\ k)(i\ j) = (j\ k) \tag{3}$$

Således kommer $\mathcal{T}_3$ att förutom 2-cyklerna (1 2) och (1 3) också att innehålla 2-cyklen (2 3). Vi vet att samtliga $3! = 6$ permutationer av elementen 1, 2 och 3 kan beskrivas som en produkt av dessa 2-cykler. Alltså har vi nu

**SVAR:** $\mathcal{T}_3 = \{\mathrm{id}, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$.

(b) (2p) Bestäm samtliga delgrupper $H$ till $\mathcal{S}_4$ sådana att $\mathcal{T}_3 \subseteq H \subseteq \mathcal{S}_4$.

**Lösning:** Ett element $\varphi$ i $H$ som inte finns i $\mathcal{T}_3$ måste permutera 4 till något av elementen i mängden $\{1, 2, 3\}$. Skriver vi $\varphi$ som en produkt av disjunkta cykler

$$\varphi = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_c \tag{4}$$

så kommer precis en av dessa cykler, låt oss säga $\gamma_1$, att beröra elementet 4. De övriga cyklerna tillhör $\mathcal{T}_3$, eftersom de inte berör elementet 4. Multiplikation med inverserna till dessa cykler, som ju också tillhör $H$, leder till att

$$\gamma_1 = \varphi \circ \gamma_c^{-1} \circ \cdots \circ \gamma_2^{-1} \in H.$$

Vi kan anta att

$$\gamma_1 = (i_1\ \ldots\ i_k\ 4) = (i_1\ 4)(i_1\ i_k) \cdots (i_1\ i_2) \tag{5}$$

och efter multiplikation med de inverserna till de sista $k-1$ cyklerna i produkten ovan, som ju tillhör $\mathcal{T}_3$ och därmed också $H$, finner vi att

$$(i_1\ 4) \in H.$$

Vi använder nu sambandet i ekvation (3) med $k = 4$ och finner att alla 2-cykler i $\mathcal{S}_4$ kommer att tillhöra delgruppen $H$. Med hjälp av argument liknande de som gavs i deluppgift (a) inser vi att detta innebär att

**SVAR:** $H = \mathcal{S}_4$ om $\mathcal{T}_3 \subseteq H$ med $H \neq \mathcal{T}_3$.

(c) (2p) Går ditt resultat i uppgift (b) ovan att generalisera till fallet $\mathcal{S}_n$ och $\mathcal{T}_{n-1}$, och hur skulle i så fall en sådan generalisering se ut?

(Inga stringenta bevis krävs i svaret på denna deluppgift, men hur många poäng du får beror på hur du resonerar i ditt svar.)

**Lösning:** Låt $\mathcal{T}_{n-1}$ beteckna den minsta delgrupp som innehåller 2-cyklerna $(1\ 2), (1\ 3), \ldots,$ $(1\ n-1)$. Ekvation (3) ger då att $\mathcal{T}_{n-1}$ innehåller samtliga 2-cykler som inte berör elementet $n$, och därmed så består $\mathcal{T}_{n-1}$ av samtliga permutationer i $\mathcal{S}_n$ som fixerar elementet $n$.

Vi upprepar nu lösningen i deluppgift (b) men med 4 ersatt med $k$. Detta ger att

**SVAR:** De enda delgrupperna till $\mathcal{S}_n$ som innehåler $\mathcal{T}_{n-1}$ är dessa bägge grupper, dvs endast de triviala möjligheterna.

10. Betrakta följande två Booleska funktioner $f$ och $g$ i de fyra variablerna $x, y, z$ och $w$:

$$f(x, y, z, w) = xy + \bar{z}(xw + y), \qquad g(x, y, z, w) = xyw + z(w + \bar{y}).$$

(a) (1p) Bestäm två Booleska funktioner $h \neq 0$ och $k$ sådana att

$$fh + k = g.$$

där $f$ och $g$ är som ovan angivits. (Anm. $h = 0$ om $h(x, y, z, w)$ antar värdet 0 i samtliga punkter $(x, y, z, w)$.)

**Lösning:** Se nedan!

(b) (1p) Bestäm antalet par $(h, k)$ av Booleska funktioner $h$ och $k$ som löser den givna ekvationen ovan.

**Lösning:** Se nedan!

(c) (3p) Bestäm en generell formel för antalet par $(h, k)$ av Booleska funktioner i de $n$ variablerna $x_1, x_2, \ldots, x_n$ som löser en allmän ekvation $fh + k = g$, där $f$ och $g$ är två givna Booleska funktioner i variablerna $x_1, x_2, \ldots, x_n$.

**Lösning:** Vi definierar stödet till den Booleska funktion $f$, betecknas $\mathrm{supp}(f)$, från $B^n$ till $B$, där $B = \{0, 1\}$, som mängden av punkter $P$ i $B^n$ sådana att $f(P) = 1$. Till exempel gäller för de i deluppgift (a) givna funktionerna att

$$\mathrm{supp}(f) = \{1111, 1101, 1110, 1111, 1001, 0100, 0101\},$$

och

$$\mathrm{supp}(g) = \{0011, 0111, 1011, 1111, 1010, 0010, 1101\},$$

samt

$$\mathrm{supp}(fg) = \mathrm{supp}(f) \cap \mathrm{supp}(g) = \{1111, 1101\}.$$

Eftersom i den Booleska algebran $B = \{0, 1\}$ vi har att $1 + a = 1$ och $0a = 0$ alla $a \in B$ så får vi att paret $(h, k)$ av Booleska funktioner $h$ och $k$ löser en ekvation $fh + k = g$ om och endast om samtliga av följande fyra villkor är uppfyllda:

$$\begin{aligned}
P \in \mathrm{supp}(f) \cap \mathrm{supp}(g) \quad &\Longrightarrow \quad h(P) + k(P) = 1, \\
P \in \mathrm{supp}(f) \setminus \mathrm{supp}(g) \quad &\Longrightarrow \quad h(P) + k(P) = 0, \\
P \in \mathrm{supp}(g) \setminus \mathrm{supp}(f) \quad &\Longrightarrow \quad k(P) = 1, \\
P \in (\mathrm{supp}(f) \cup \mathrm{supp}(g))^C \quad &\Longrightarrow \quad k(P) = 0,
\end{aligned}$$

där vi med $A^C$ betecknar komplementet till mängden $A$ i universat $B^n$.

Till exempel har vi som svar på deluppgift (a) funktioner $h$ och $k$ med

$$\mathrm{supp}(h) = \{1111, 1101\}, \qquad \mathrm{supp}(k) = \{0011, 0111, 1011, 1010, 0010\}$$

Nu till deluppgift (b).

För punkter $P$ i $\mathrm{supp}(f) \setminus \mathrm{supp}(g)$ måste både $h$ och $k$ ges värdet 0.

För punkter $P$ i $\mathrm{supp}(f) \cap \mathrm{supp}(g)$ kan varken $h$ och $k$ ges värdet 0, så totalt 3 möjliga par av värden $(h(P), k(P))$ i var och en av dessa punkter $P$.

I övriga punkter finns bara ett möjligt värde som vi kan tilldela funktionen $k$ medan man i dessa punkter fritt kan välja mellan 0 och 1 som värde till $h$. Eftersom för de i uppgiften givna funktionerna vi har att

$$|\mathrm{supp}(f) \cap \mathrm{supp}(g)| = 2, \qquad |\mathrm{supp}(f) \setminus \mathrm{supp}(g)| = 5$$

så blir, enligt multiplikationsprincipen, antalet möjliga par av funktioner

$$2^{16-2-5}3^2,$$

dvs $9 \cdot 2^9$.

Generellt har vi också, vilket blir vårt svar på uppgift (c), och med motiveringar analoga med de ovan givna,

$$2^{(2^n - |\mathrm{supp}(f) \cap \mathrm{supp}(g)| - |\mathrm{supp}(f) \setminus \mathrm{supp}(g)|)}3^{|\mathrm{supp}(f) \cap \mathrm{supp}(g)|}.$$