Matematiska institutionen	Tentamensskrivning
Stockholms universitet	Kurskod: MM5013
Avd. Matematik	
Examinator: Olof Sisask	
Kursansvarig: Lisa Nicklasson	2020-05-28 09:00–14:00

Tentamen i Algebra och Kombinatorik

Lösningsförslag

1. Låt C vara koden som definieras av check-matrisen

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

(a) (1p) Hur många ord innehåller C?

(b) (1p) Vilka av orden 011110100, 101100100, 111100000 och 111111111 tillhör C?

(c) (2p) Hur många fel rättar C? (Kom ihåg att förklara varför just detta antal fel kan rättas, men inte fler.)

(d) (1p) Om några av orden i deluppgift (b) inte tillhör C: Rätta de som kan rättas.

Lösning: (a) Matrisen har fyra rader och kan alltså maximalt ha rang fyra. Vi kan se att den verkligen har rang fyra, eftersom t. ex. kolonn 1, 6, 7 och 9 är linjärt oberoende. Eftersom vi har 9 kolonner blir dimensionen av koden $9 - 4 = 5$ och koden har därför $2^5 = 32$ ord.

Alternativt kan vi tänka såhär. När vi löser ekvationsystemet blir det fem fria variabler, och var och en av dessa kan väljas som 0 eller 1. Alltså finns 2^5 ord.

(b) Orden 011110100, 101100100 tillhör koden, eftersom båda ger nollvektorn vid multiplikation med checkmatrisen.

(c) Eftersom matrisen inte har någon kolonn med bara nollor, och inga kolonner är lika rättar koden minst ett fel. De två ord som vi vet tillhör koden från deluppgift (b) har avstånd tre, så minimiavståndet i koden är högst tre. Det betyder att koden rättar högst ett fel. Vi kan därför dra slutsatsen att koden rättar precis ett fel.

(d) Eftersom

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

vilket inte är lika med någon kolonn i matrisen kan ordet 111100000 inte rättas. Däremot är

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

lika med kolonn 5 i matrisen. Ordet 111111111 rättas därför till 111101111.

2. Låt σ vara permutationen

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 6 & 8 & 7 & 4 & 2 & 3 & 1 & 5 \end{pmatrix}$$

   (a) (2p) Skriv σ och σ^{-1} som produkter av transpositioner.
   (b) (1p) Är σ^3 jämn eller udda? Är $(\sigma^{-1})^3$ jämn eller udda?
   (c) (2p) Finns det något k så att $\sigma^k(1) = 5$? Ange i så fall ett sådant k.

Lösning: (a) Vi börjar med att skriva σ som en produkt av disjunkta cykler, och därefter som en produkt av transpositioner. Det kan t. ex. se ut såhär

$$\sigma = (1\,6\,3\,7)(2\,8\,5) = (1\,6)(3\,6)(3\,7)(2\,8)(5\,8),$$

men kom ihåg att samma permutation kan skrivas som en produkt av transpositioner på flera olika sätt. Genom att sätta transpositionerna i omvänd ordning får vi σ^{-1} som

$$\sigma^{-1} = (5\,8)(2\,8)(3\,7)(3\,6)(1\,6).$$

(b) Eftersom σ kan skrivas som en produkt av fem transpositioner kan σ^3 skivas som en produkt av $3 \cdot 5 = 15$ transpositioner, och är därför udda. På samma sätt ser vi att även $(\sigma^{-1})^3$ kan skrivas som en produkt av 15 transpositioner, och därför är udda.

(c) Eftersom 1 och 5 sitter i olika cykler i $\sigma = (1\,6\,3\,7)(2\,8\,5)$ finns det inget k så att $\sigma^k(1) = 5$.

3. Låt G vara gruppen $(U(\mathbb{Z}_{16}), \cdot)$, där $U(\mathbb{Z}_{16})$ står för mängden av inverterbara element i $\mathbb{Z}_{16}$.

   (a) (1p) Lista alla element i G.
   (b) (1p) Är G cyklisk?
   (c) (3p) Vilka möjliga storlekar finns det för en delgrupp av G? Ge exempel på delgrupper av varje möjlig storlek.

Lösning: (a) De inverterbara elementen i $\mathbb{Z}_{16}$ representeras av de tal mellan 0 och 15 som är relativt prima till 16. Alltså är

$$U(\mathbb{Z}_{16}) = \{1, 3, 5, 7, 9, 11, 13, 15\}.$$

(b) Vi går igenom elementen och beräknar

$$\begin{aligned} &3^2 = 9,\ 3^3 = 11,\ 3^4 = 1, \\ &5^2 = 9,\ 5^4 = 9^2 = (3^2)^2 = 3^4 = 1, \\ &7^2 = 1, \\ &9^2 = 1, \\ &11^2 = (-5)^2 = 9,\ 11^4 = 9^2 = 1, \\ &15^2 = (-1)^2 = 1. \end{aligned}$$

Det finns alltså inget element som genererar hela G, och därmed är G inte cyklisk.

(c) Enligt Lagranges sats ska storleken på en delgrupp dela $|G| = 8$. Möjliga storlekar på delgrupper är därför 1, 2, 4 och 8. Av storlek 1 har vi delgruppen $\{1\}$, och av storlek 8 har vi G själv. Baserat på beräkningen i lösningen av (b) kan vi se att det finns cykliska delgrupper av storlek 2 och 4. Till exempel har delgruppen $\langle 7 \rangle = \{1, 7\}$ storlek 2, och delgruppen $\langle 3 \rangle = \{1, 3, 9, 11\}$ storlek 4.

4. (5p) Hur många ord med nio bokstäver kan vi bilda med hjälp av de tio bokstäverna `A A A B N N R S T U`, om orden inte får innehålla delorden `BANAN` eller `ANANAS`? (Svaret får uttryckas med hjälp av addition, subtraktion, multiplikation, division och fakultet.)

Lösning: Vi använder oss av principen för inklusion och exklusion för att lösa problemet.

Låt oss börja med att beräkna det totala antalet ord med nio bokstäver. Eftersom det finns tio bokstäver att tillgå blir det alltså en bokstav över när vi bildar ett ord. Vi tänker oss att vi ställer denna bokstav till höger om ordet. På så sätt får vi ett ord av tio bokstäver. Notera att alla ord av tio bokstäver kan fås på detta sätt. Vi kan också få tillbaka vårt ord med nio bokstäver genom att ta bort bokstaven längst till höger. Alltså är antalet ord med nio bokstäver lika med antalet ord med tio bokstäver. Eftersom vi har tre `A`, två `N`, och en var av `B, R, S, T, U` får vi att antalet ord är

$$\binom{10}{3,2,1,1,1,1,1} = \frac{10!}{3!2!} = 2 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10.$$

Låt oss nu beräkna antalet ord som innehåller delordet `BANAN`. Vi ska bilda ord som innehåller enheten `BANAN` och fyra av bokstäverna `A, R, S, T, U`. Vi väljer först bort en av de fem bokstäverna. Därefter kan vi bilda ett ord av `BANAN` och de fyra kvarvarande bokstäverna på 5! olika sätt. Antalet ord som innehåller `BANAN` är därför $5 \cdot 5!$.

Vidare ska vi beräkna antalet ord som innehåller delordet `ANANAS`. Dessa bildas av enheten `ANANAS` och tre av bokstäverna `B, R, T, U`. På samma sätt som i `BANAN`fallet väljer vi först bort en bokstav, och bildar därefter ett ord av fyra olika symboler. Detta ger att antalet ord som innehåller `ANANAS` är $4 \cdot 4!$.

Vi behöver också beräkna antalet ord som innehåller båda delorden `BANAN` och `ANANAS`. Detta är precis de ord som innehåller delordet `BANANAS`. Dessa bildas av enheten `BANANAS` och två av bokstäverna `R, T, U`. Samma resonemang som tidigare ger $3 \cdot 3!$ ord.

Sammantaget är antalet ord med nio bokstäver som inte innehåller delorden `BANAN` eller `ANANAS`

$$2 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 - 5 \cdot 5! - 4 \cdot 4! + 3 \cdot 3!.$$

5. (5p) En karusell med åtta säten ska målas om. Fyra av sätena ska målas svarta och fyra vita. På hur många sätt kan vi måla karusellen? Två målningar betraktas som samma, om vi kan få den ena från den andra genom att snurra på karusellen.

Lösning: Låt X vara mängden av målade fixerade karuseller, där vi inte räknar två målningar som lika om vi kan få den ena från den andra genom att snurra på karusellen. Eftersom det finns åtta platser varav fyra ska målas svarta, och övriga fyra vita är $|X| = \binom{8}{4} = 70$.

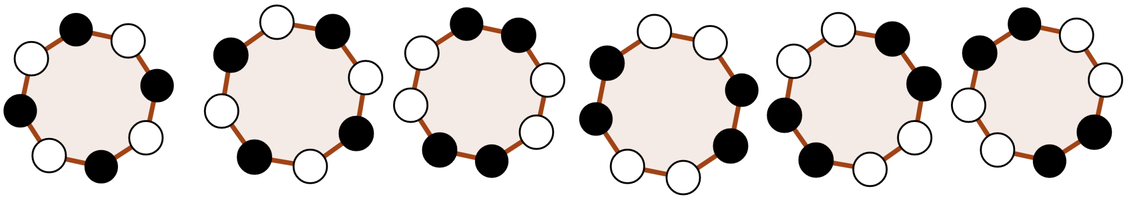
Låt α vara transformationen som roterar karusellen en åttondels varv. Då är $\alpha^8 = \mathrm{id}$, alltså transformationen som låter karusellen stå stilla. Vi låter G vara den cykliska gruppen $\langle \alpha \rangle$. Att en målad karusell i X kan fås från en annan är samma sak som att de två ligger i samma bana när vi låter G verka på X. Vi vill därför räkna ut antalet banor, och det gör vi med hjälp av Burnsides lemma.

Om en målad karusell ska vara fix under α måste varje säte ha samma färg som det framför. Men då måste alla säten ha samma färg, vilket inte går då vi ska ha fyra svarta och fyra vita. Alltså är fixpunktsmängden $F(\alpha)$ för α tom.

För en målad karusell som är fix under α^2 måste varje säte ha samma färg som det två steg framför. Det finns därför två målningar som är fixa under α^2, nämligen de där vartannat säte är svart och vartannat vitt.

För en målad karusell som är fix under α^3 måste var tredje säte ha samma färg. Detta leder till att alla säten måste ha samma färg, så $F(\alpha^3) = \emptyset$.

Det finns sex stycken målade karuseller som är fixa under α^4, nämligen



På liknande sätt bestämmer vi fixpunktsmängderna för α^5, α^6 och α^7, och får

$$|F(\alpha)| = |F(\alpha^3)| = |F(\alpha^5)| = |F(\alpha^7)| = 0, \ |F(\alpha^2)| = |F(\alpha^6)| = 2, \ |F(\alpha^4)| = 6$$

och

$$|F(\mathrm{id})| = |X| = 70.$$

Enligt Burnsides lemma är antalet banor, och därmed antalet sätt att måla karusellen, lika med

$$\frac{2+2+6+70}{8} = 10.$$

6. (a) (2p) Finns det ett $c \in \mathbb{Z}_7$ så att

$$(x+c)(x+1)(x+2)(x+3)(x^2+1) = (x^3 - x^2 - 3x - 1)(x^3 + x + 1) \ \text{ i } \mathbb{Z}_7[x]?$$

(b) (3p) Finns det ett $c \in \mathbb{Z}_{12}$ så att $(x+c)(x+2) = (x-4)^2$ i $\mathbb{Z}_{12}[x]$?

Lösning: (a) Eftersom $\mathbb{Z}_7$ är en kropp har vi unik faktorisering i $\mathbb{Z}_7[x]$. Faktorn x^3+x+1 är irreducibel, och förekommer i högerledet men inte i vänsterledet. Därför kan likheten inte gälla för något c. Hur vet vi då att x^3+x+1 är irreducibelt? Om det var reducibelt skulle det ha en faktor av grad 1, vilket skulle betyda att det finns ett nollställe. Men prövning av $x = 0, 1, 2, 3, 4, 5, 6$ visar att $x^3 + x + 1$ inte har något nollställe i $\mathbb{Z}_7$.

Alternativt kan vi lösa uppgiften genom att jämföra koefficienter. Vänsterledet har konstanttermen $6c = -c$, och högerledet har konstanttermen -1, så vi måste ha $c = 1$ för att det ska stämma. Därefter kan vi till exempel kolla på koefficientern för x^5. Då får vi $c + 6 = c - 1$ i vänsterled, och -1 i högerled. För att detta ska stämma måste $c = 0$ vilket motsäger $c = 1$. Det finns alltså inget c så att likheten är uppfylld.

(b) Eftersom $\mathbb{Z}_{12}$ inte är en kropp gäller inte resonemanget om unik faktorisering som i deluppgift (a). Utvecklar vi vänsterled och högerled får vi

$$(x+c)(x+2) = x^2 + (2+c)x + 2c$$

och

$$(x-4)^2 = x^2 - 8x + 16 = x^2 + 4x + 4.$$

Vi ser att dessa två polynom är lika om vi sätter $c = 2$.