

Lösningar till Inlämningsuppgifter på kursen Inledande Diskret Matematik

• TMV211 • Chalmers • HT 2020 •
Senast uppdaterad October 21, 2020

Den här texten innehåller lösningsförslag till inlämningsuppgifterna, filen kommer att uppdateras kontinuerligt under resten av kursen. Jag har försökt vara koncis men ändå ta med alla väsentliga detaljer. Man kan ofta lösa problemen på andra sätt. Poängen på inlämningsuppgifterna baseras också på presentationen, alltså hur tydliga dina lösningar är och hur lätt det är att följa dina argument.

1 Inlämningsuppgift 1

1.1 Logiska Argument

Ett logiskt argument är ett logiskt uttryck av formen $H_1 \wedge H_2 \wedge H_3 \rightarrow C$. Följande nota-

tion förekommer också för samma uttryck:

$$\frac{\begin{array}{c} H_1 \\ H_2 \\ H_3 \end{array}}{C}$$

Här kallas H_i för hypoteser (det behöver inte finnas exakt 3), och C för slutsatsen. **Ett logiskt argument kallas giltigt om det är en tautologi.** Argument kallas alltså giltiga om C alltid är sann när alla hypoteser är sanna. Avgör om vart och ett av följande logiska argument är giltiga, motivera dina svar ordentligt! Det kan hjälpa att införa mer symbolisk notation för meningarna.

- Alla vägar leder till Rom
1. $\frac{E4 \text{ är en väg}}{E4 \text{ leder till Rom}}$
 2. $\frac{\begin{array}{c} \text{Man kan inte lära en gammal hund att sitta} \\ \text{Håkan är en hund} \\ \text{Man kan inte lära Håkan att sitta} \end{array}}{\text{Håkan är gammal}}$
 3. $\frac{\begin{array}{c} \text{Newton väntade för länge} \\ \text{Den som väntar på nåt gott väntar aldrig för länge} \end{array}}{\text{Newton väntade inte på nåt gott}}$

Lösningsförslag

Man kan resonera på olika vis, exempelvis:

1. Argumentet är giltigt, detta är precis en tillämpning av Modus Ponens argumentet. Med $V(x) = "x \text{ är en väg}"$ och $R(x) = "x \text{ leder till Rom}"$ har argumentet formen $V(E4) \wedge \forall x : (V(x) \rightarrow R(x)) \rightarrow R(E4)$. Om $R(E4)$ skulle vara falsk blir vänsterledet också falskt, alltså är argumentet giltigt.
2. Argumentet är ogiltigt. Om Håkan är en ung hund som inte kan sitta kan alla hypoteserna vara sanna men slutsatsen ändå falsk.
3. Det kontrapositiva (och ekvivalenta) påståendet till "Den som väntar på nåt gott väntar aldrig för länge" är "Den som väntar för länge väntar inte på något gott". Så precis som i första uppgiften är detta Modus Ponens igen.

1.2 Omskrivning med negation och implikation

Vi har i veckan tittat på logiska uttryck som man kan få genom att kombinera ihop boolska variabler med parenteser och operationerna från mängden $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$. Visa att varje sådant logiskt uttryck är ekvivalent med ett uttryck som kan skrivas ned med endast boolska variabler, parenteser, och symbolerna ur mängden $\{\neg, \rightarrow\}$.

Lösningssförslag

För att visa att varje logiskt uttryck med $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$ kan skrivas med endast $\{\neg, \rightarrow\}$ så räcker det att visa att vart och ett av uttrycken $p \wedge q$, $p \vee q$, $p \leftrightarrow q$ kan skrivas med de två symbolerna. Då kan man substituera de olika delarna i det stora uttrycket.

Vi har

$$p \vee q \Leftrightarrow \neg p \rightarrow q$$

$$p \wedge q \Leftrightarrow \neg(\neg p \vee \neg q) \Leftrightarrow \neg(p \rightarrow \neg q)$$

$$p \leftrightarrow q \Leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p) \Leftrightarrow \neg((p \rightarrow q) \rightarrow \neg(q \rightarrow p)) \text{ vilket kan bekräftas genom att titta på sanningstabellerna.}$$

1.3 Antalet ekvivalenta uttryck

Det logiska uttrycket $(\neg p \wedge q) \rightarrow (r \vee p) \wedge (q \vee r)$ är ett exempel på ett uttryck i de tre boolska variablerna p, q, r . Ett annat exempel på ett uttryck i p, q, r är $p \wedge q$, även om det inte explicit beror på r .

a) Hur många olika sådana logiska uttryck kan man skriva ned med tre variabler p, q, r och alla möjliga logiska symboler? **Två uttryck betraktas som lika om de är ekvivalenta!** Motivera ditt svar.

b) Samma fråga om vi betraktar n boolska variabler $p_1, p_2, \dots, p_n$ istället.

Lösningssförslag

Två logiska uttryck är ekvivalenta om och endast om de har samma sanningstabell. Vi behöver därför bara räkna antalet sanningstabeller med n variabler. En sanningstabell har 2^n rader, och varje rad kan fyllas i på 2 sätt. Detta ger $2^{(2^n)}$ olika tabeller.

Slutsats: (b) Det finns $2^{(2^n)}$ olika logiska uttryck med n variabler.

(a) Med $n = 3$ får vi enligt ovan $2^{(2^3)} = 256$ olika uttryck.

1.4 Oändliga unioner och snitt

Betrakta den oändliga unionen av intervall: $I = \bigcup_{k=2}^{\infty} [\frac{2k+1}{k}, 5]$.

a) Mängden I kan faktiskt skrivas som ett enda intervall. Vilket? Och blir det öppet eller slutet? Motivera!

b) Skriv ned det slutna intervallet $[0, 1]$ som ett oändligt snitt av öppna intervall. (om du inte vet vad öppet/slutet intervall innebär: googla!)

Lösningssförslag

a) Låt $I_k = [\frac{2k+1}{k}, 5]$ så att $I = \bigcup_{k=2}^{\infty} I_k$. Man ser lätt att $I_{k+1} \supset I_k$, så det är en växande följd intervall, och därför är $\bigcup_{k=2}^N I_k = I_N = [\frac{2N+1}{N}, 5]$.

Vi påstår att $I = (2, 5]$. Det är klart att $2 \notin I$ eftersom 2 inte tillhör något I_k . Det vi behöver visa är att för varje $\epsilon > 0$ så har vi $2 + \epsilon \in I$, alltså att $\exists k : \frac{2k+1}{k} < 2 + \epsilon \Leftrightarrow \exists k : 2k + 1 < 2k + k\epsilon \Leftrightarrow \exists k : 1 < k\epsilon$ vilket är sant för varje fixt ϵ .

b) En liknande analys visar att vi har

$$[0, 1] = \bigcap_{k=1} \left(-\frac{1}{k}, 1 + \frac{1}{k}\right)$$

2 Inlämningsuppgift 2

2.1 Fermats stora sats modulo sju

Fermats stora sats är kanske den mest kända matematiska satsen. Den är enkel att förstå - den säger bara att ekvationen $x^n + y^n = z^n$ inte har några heltalslösningar med $n > 2$ och $x, y, z \neq 0$. Det är dock inte lika lätt att bevisa - det tog över 350 år och beviset är över 100 sidor. I den här uppgiften ska du bevisa Fermats sats - i en lite lättare version:

Bevisa att Fermats stora sats gäller i $\mathbb{Z}_7$ när $n = 3$. Bevisa alltså att $x^3 + y^3 = z^3$ saknar lösningar i $\mathbb{Z}_7$ när $x, y, z \neq 0$ i $\mathbb{Z}_7$.

Tips: Beräkna först a^3 modulo 7 för varje $0 < a < 7$.

Lösningsförslag

Vi följer tipset och ser att $a^3 \equiv \pm 1 \pmod{7}$ för alla heltal a som inte är delbara med sju, alltså som inte är lika med 0 i $\mathbb{Z}_7$.

Men ekvationen $\pm 1 \pm 1 \equiv \pm 1 \pmod{7}$ saknar lösningar (inga val av tecken ger en lösning då vänsterledet bara kan bli $-2, 0, 2$).

Därför saknar också ekvationen $x^3 + y^3 = z^3$ lösningar i $\mathbb{Z}_7$.

2.2 Misslyckad primtalsgenerering

I Euklides bevis för att det finns oändligt många primtal utgick han från motsatsen, att alla primtal som finns är $\{p_1, p_2, \dots, p_n\}$. Han konstruerade sedan talet $p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$ som också då blev ett primtal som saknades från listan - en motsägelse! Beviset tycks antyda en algoritm för att konstruera stora primtal: Definiera för varje $n > 0$ talet $q_n = (\text{produkten av de } n \text{ första primtalen}) + 1$.

a) Beräkna q_1, q_2, q_3, q_4

b) Är q_n ett primtal för varje n ? Bevisa eller motbevisa påståendet!

Lösningsförslag

a) Med definitionen i texten får vi

$$(q_1, q_2, q_3, q_4) = (3, 7, 31, 211)$$

b) Metoden garanterar att q_n inte är delbar med de första n primtalen, men det är inget som hindrar q_n från att vara en produkt av två högre primtal under q_n . Detta ser man om man provar ett par högre värden på n : q_5 är ett primtal, men $q_6 = 30031$ är sammansatt: $30031 = 59 \cdot 509$.

Argumentet fungerar alltså för att bevisa att det finns oändligt många primtal men inte för att generera primtal.

2.3 Linjär diofantisk ekvation i tre variabler

Ekvationen $6x + 10y + 15z = 1$ är en linjär diofantisk ekvation i tre variabler. Går ekvationen att lösa? Hitta alla lösningar **eller** motivera varför ekvationen måste sakna lösning.

Lösningsförslag

Vi ska lösa den linjära diofantiska ekvationen $(\star) : 6x + 10y + 15z = 1$, alltså hitta alla dess heltalslösningar.

Det finns olika trix man kan använda för att lösa en sådan ekvation. Ett är att dela upp den i två diofantiska ekvationer med bara två variabler var - sådana vet vi hur man löser.

Vi inför $w = 2y + 3z$. Ekvation $(\star)$ kan då skrivas $6x + 5w = 1$. Denna har en lösning $(x, w) = (1, -1)$ så alla dess lösningar kan skrivas $(x, w) = (1 - 5t, 6t - 1)$ där $t \in \mathbb{Z}$. Nu har vi hittat x och w , så för att hitta y och z behöver vi lösa $w = 2y + 3z \Leftrightarrow 2y + 3z = 6t - 1$. Eftersom $(y, z) = (-1, 1)$ löser $2y + 3z = 1$ så är $(y, z) = (-6t + 1, 6t - 1)$ en lösning till $2y + 3z = 6t - 1$ för varje fixt t .

Alla lösningar till $2y + 3z = 6t - 1$ ges därför av $(y, z) = (3s - 6t + 1, -2s + 6t - 1)$ för $s, t \in \mathbb{Z}$.

Vi har alltså visat att alla lösningar till $(\star)$ fås via

$$(x, y, z) = (1 - 5t, 3s - 6t + 1, -2s + 6t - 1) \quad s, t \in \mathbb{Z}.$$

Man kan enkelt testa att dessa verkligen är lösningar genom att sätta in uttrycken i $(\star)$. Samma lösningsmängd går att skriva på flera olika sätt, det kommer dock alltid att behövas två heltalsparametrar s, t .

3 Inlämningsuppgift 3

3.1 Slutsiffror

Beräkna de **tre sista siffrorna** i talet $6053^{1002537}$ genom att använda Eulers sats och metoden med successiv kvadrering. Alternativt kan du också ta hjälp av kinesiska restsatsen. Det är ok att använda dator/miniräknare till delstegen, men skriv ut hela din lösning!

Lösningsförslag

För att beräkna slutsiffrorna beräknar vi potensen i $\mathbb{Z}_{1000}$. Alla likheter nedan beräknas därför i $\mathbb{Z}_{1000}$. Vi har $x := 6053^{1002537} = 53^{1002537}$.

Eftersom $\varphi(1000) = \varphi(5^3)\varphi(2^3) = (125 - 25)(8 - 4) = 400$ och $\gcd(53, 1000) = 1$ så har vi enligt Eulers sats $53^{400} = 1$.

Därför har vi också $x = 53^{2506 \cdot 400 + 137} = (53^{400})^{2506} \cdot 53^{137} = 53^{137}$.

Nu har vi $53^{137} = 53^{128+8+1} = 53^{128} \cdot 53^8 \cdot 53$ som vi kan beräkna med successiv kvadrering. Vi får

$$(53^1, 53^2, 53^4, 53^8, 53^{16}, 53^{32}, 53^{64}, 53^{128}) = (53, 809, 481, 361, 321, 41, 681, 761)$$

så $x = 53^{128} \cdot 53^8 \cdot 53 = 761 \cdot 361 \cdot 53 = 213$ i $\mathbb{Z}_{1000}$. De sista siffrorna i talet $6053^{1002537}$ är alltså 213.

3.2 Kongruenssystemet med en parameter

För varje fixt heltal a betraktar vi följande system av kongruenser:

$$\begin{cases} ax \equiv 1 & (\text{mod } 12) \\ x \equiv a & (\text{mod } 13) \end{cases}$$

Om exempelvis $a = 0$ är det lätt att se att systemet saknar lösning. För vilka värden på heltalet a har systemet minst en lösning? Motivera ditt svar tydligt! Observera att du inte behöver hitta lösningarna för varje a för att kunna svara på frågan.

Lösningsförslag

Den övre ekvationen har en lösning om och endast om a är inverterbart modulo 12. Vi vet att detta sker om och endast om $\gcd(a, 12) = 1$ alltså om $a \equiv 1, 5, 7, 11 \pmod{12}$ eller med andra ord $a \equiv \pm 1 \pmod{6}$.

För sådana a kan systemet skrivas

$$\begin{cases} x \equiv a^{-1} & (\text{mod } 12) \\ x \equiv a & (\text{mod } 13) \end{cases}$$

och vi vet att detta system har en unik lösning modulo $12 \cdot 13$ enligt kinesiska restsatsen.

Slutsats: Systemet är lösbart precis för alla heltal a som uppfyller $a \equiv \pm 1 \pmod{6}$.

3.3 Kryptering med elliptiska kurvor

Den här uppgiften är ett förenklat mini-intro till kryptering med elliptiska kurvor (ECC). Uppgiften ser krånglig ut, men allt man behöver göra är att följa enkla instruktioner och kunna räkna i $\mathbb{Z}_5$.

Kurvan $y^2 = x^3 + x + 1$ i $\mathbb{R}^2$ består av ett antal punkter i (x, y) -planet. I ECC väljer man ett stort primtal q , och tittar på alla x, y som uppfyller samma ekvation fast i $\mathbb{Z}_q$! Eftersom man jobbar med heltal blir alla räkningar exakta. I vårt exempel nedan tar vi $q = 5$. I riktig ECC är q ett primtal med hundratals siffror. Alla räkningar nedan sker i $\mathbb{Z}_5$. Vi definierar $\Omega = \{(x, y) \in \mathbb{Z}_5 \times \mathbb{Z}_5 \mid y^2 = x^3 + x + 1\}$

Ω är en "Elliptisk kurva" över $\mathbb{Z}_5$ - den består alltså av alla punkter (x, y) där både x och y ligger i $\mathbb{Z}_5$ och där ekvationen $y^2 = x^3 + x + 1$ är sann i $\mathbb{Z}_5$. Punkten $(4, 2)$ tillhör t.ex. kurvan Ω eftersom ekvationen $2^2 = 4^3 + 4 + 1$ håller i $\mathbb{Z}_5$.

Uppgift (a): Skriv ned alla element i mängden Ω , visa hur du kom fram till svaret.

Antag nu att $P_1 = (x_1, y_1)$ och $P_2 = (x_2, y_2)$ är två punkter på kurvan Ω där $x_1 \neq x_2$. Då beräknar man punkternas "summa" $P_1 \oplus P_2$ så här:

Beräkna $\lambda = (y_2 - y_1) \cdot (x_2 - x_1)^{-1}$ (inversen beräknas alltså i $\mathbb{Z}_5$)

Beräkna $x = \lambda^2 - x_1 - x_2$

Beräkna $y = \lambda \cdot (x_1 - x) - y_1$

Då definierar vi $P_1 \oplus P_2 := (x, y)$. Detta blir en ny punkt på kurvan!

Uppgift (b): Beräkna $(2, 1) \oplus (4, 2)$ och verifiera att resultatet tillhör Ω , visa dina beräkningar.

Slutkommentar: ECC-kryptering bygger på det faktum att givet (Q, P, n) är det lätt att beräkna $R = Q \oplus nP := Q \oplus P \oplus P \oplus \dots \oplus P$ men givet samma (R, Q, n) är det mycket svårt att beräkna P .

Lösningsförslag

(a) Vi beräknar vänsterledet och högerledets värden i $\mathbb{Z}_5$ för $y^2 = x^3 + x + 1$:

a	a^2	$a^3 + a + 1$
0	0	1
1	1	3
2	4	1
3	4	1
4	1	4

(a) Vi ska alltså välja x, y så att motsvarande värden i kolonn 3, 2 blir lika. Vi får $\Omega = \{(0, 1), (0, 4), (2, 1), (2, 4), (3, 1), (3, 4), (4, 2), (4, 3)\}$

(b) Vi följer instruktionerna för att beräkna $(2, 1) \oplus (4, 2)$. Vi får $\lambda = 1 \cdot 2^{-1} = 1 \cdot 3 = 3$, och $x = 3^2 - 2 - 4 = 3$, och $y = 3 \cdot (2 - 3) - 1 = -4 = 1$.

Så enligt algoritmen blir $(2, 1) \oplus (4, 2) = (3, 1)$ vilket också tillhör Ω enligt (a).

4 Inlämningsuppgift 4

4.1 Övre begränsning för Fibonacci-följden

Kom ihåg att Fibonacci-talföljden kan definieras rekursivt av

$$F_1 = 1, F_2 = 1 \text{ och } F_n = F_{n-1} + F_{n-2} \text{ för } n > 2.$$

a) Visa att $F_n < 2^n$ för alla $n \geq 1$.

b) Använd induktion för att visa att $F_n < (\frac{7}{4})^n$ för alla $n \geq 1$.

Resultatet i a) följer direkt från resultatet i b), så om du gör uppgift b) behöver du inte göra uppgift a).

Lösningsförslag

Vi ska i (b) visa att $F_n < (\frac{7}{4})^n$ för alla $n \geq 1$. Vi gör detta med induktion:

Bassteg: Påståendet är sant för $n = 1$ och $n = 2$ eftersom $1 < \frac{7}{4}$ och $2 < \frac{49}{16}$.

Induktionssteg: Antag att påståendet är sant för alla n upp till och med k (får något $k > 1$). Vi ska visa att påståendet är sant också för $n = k + 1$ alltså att $F_{k+1} < (\frac{7}{4})^{k+1}$. Med hjälp av induktionsantagandena får vi $F_{k+1} = F_k + F_{k-1} < (\frac{7}{4})^k + (\frac{7}{4})^{k-1}$. Så vi behöver alltså visa att $(\frac{7}{4})^k + (\frac{7}{4})^{k-1} \leq (\frac{7}{4})^{k+1}$. Men här kan vi dividera med $(\frac{7}{4})^{k-1}$: $(\frac{7}{4})^k + (\frac{7}{4})^{k-1} \leq (\frac{7}{4})^{k+1} \Leftrightarrow (\frac{7}{4})^1 + 1 \leq (\frac{7}{4})^2 \Leftrightarrow \frac{11}{4} \leq \frac{49}{16} \Leftrightarrow 44 \leq 49$ vilket är sant. Enligt induktionsprincipen är därför alla $F_n < (\frac{7}{4})^n$. Eftersom $\frac{7}{4} < \frac{8}{4}$ har vi också visat det svagare påståendet i (a) gäller.

4.2 Den geometriska summan

a) Beräkna summan $\sum_{k=0}^7 2^k \cdot 5^{-\frac{k}{2}}$ (tips: den är faktiskt geometrisk!)

b) Beräkna $S_N = \sum_{k=0}^N 2^k \cdot 5^{-\frac{k}{2}}$ för varje naturligt tal N .

c) Vad händer med S_N då N blir stort? Vi definierar $\sum_{k=0}^{\infty} 2^k \cdot 5^{-\frac{k}{2}} = S$ om det finns ett tal S som S_N närmar sig när N blir större och större. Hitta S om ett sådant tal existerar, eller visa att ett sådant tal ej existerar.

d) Besvara samma fråga som i c) fast för summan $\sum_{k=0}^{\infty} 2^k \cdot 3^{-\frac{k}{2}} = T$ istället.

Lösningsförslag

(b och a) Med räkneregler och formeln för geometrisk summa har vi $\sum_{k=0}^N 2^k 5^{-\frac{k}{2}} = \sum_{k=0}^N (\frac{2}{\sqrt{5}})^k = \frac{(\frac{2}{\sqrt{5}})^{N+1} - 1}{(\frac{2}{\sqrt{5}}) - 1}$ för varje N . Speciellt får vi $S_7 = \frac{(\frac{2}{\sqrt{5}})^8 - 1}{(\frac{2}{\sqrt{5}}) - 1} = \frac{256 - 1}{(\frac{2}{\sqrt{5}}) - 1} = \frac{256 - 625}{\frac{2 - \sqrt{5}}{\sqrt{5}}} = \frac{269}{\frac{\sqrt{5} - 2}{\sqrt{5}}} = \frac{269\sqrt{5}}{625(\sqrt{5} - 2)}$.

(c) Vi har $S_N = \frac{(\frac{2}{\sqrt{5}})^{N+1} - 1}{(\frac{2}{\sqrt{5}})^{-1}}$. Eftersom $\sqrt{5} > 2$ så kommer täljar-termen $(\frac{2}{\sqrt{5}})^{N+1}$ att närma sig noll då N växer. Alltså kommer S_N att närma sig $S = \frac{-1}{(\frac{2}{\sqrt{5}})^{-1}} = \frac{\sqrt{5}}{\sqrt{5}-2} = 5 + 2\sqrt{5}$.

(d) Om vi ersätter $\sqrt{5}$ med $\sqrt{3}$ får vi summor $T_N = \frac{(\frac{2}{\sqrt{3}})^{N+1} - 1}{(\frac{2}{\sqrt{3}})^{-1}}$. Men $2 > \sqrt{3}$ så täljar-termen $(\frac{2}{\sqrt{3}})^{N+1}$ går mot oändligheten (växer utan gräns). Därför finns det inget sådant tal T som T_n närmar sig.

4.3 Lodjur och Harar

Här ska vi räkna på två talföljder som beror på varandra. Sådana kan användas för att beskriva populationsdynamik.



Snöskoharar jagas av Kanadensiska lodjur

Låt H_n och L_n beteckna antalet Harar respektive Lodjur år nummer n . (Man kan anta att H_n och L_n mäts i 100-tal djur, det spelar ingen roll för räkningen)

En grundläggande modell för populationerna är att de uppfyller rekursionsekvationerna

$$\begin{cases} H_n = \frac{5}{2}H_{n-1} - \frac{3}{2}L_{n-1} \\ L_n = \frac{1}{2}H_{n-1} + \frac{1}{2}L_{n-1} \end{cases}$$

a) Motivera varför modellen inte är helt orimlig - varför är t.ex. koefficienten framför H_{n-1} övre ekvationen > 1 ? Och varför är koefficienten framför L_{n-1} i övre ekvationen negativ?

b) Vad som händer med populationerna beror på startvärdena H_0 och L_0 . Beräkna de fem första elementen i talföljderna om $(H_0, L_0) = (4, 2)$.

c) Antag att lodjuren dör ut så att $L_n = 0$ för alla n . Vad händer då med har-populationen enligt den första ekvationen? Och tvärtom, vad händer om har-populationen dör ut?

d) Hitta explicita uttryck för de bägge talföljderna när $(H_0, L_0) = (3, 1)$. Vad blir kvoten $\frac{H_n}{L_n}$ de olika åren?

e) Hitta nollskilda värden på H_0 och L_0 som gör att populationerna blir stabila - samma antal harar varje år och samma antal lodjur varje år.

Lösningsförslag

(a) Att koefficienten framför H_{n-1} i uttrycket för H_n är > 1 säger att Har-antalet ökar exponentiellt i avsaknad av lodjur. Koefficienten för L_{n-1} är negativ eftersom lodjur äter harar.

(b) $\{(H_i, L_i)\}_0^4 = (4, 2), (7, 3), (13, 5), (25, 9), (49, 17)$

(c) Utan lodjur får vi $H_n = \frac{5}{2}H_{n-1}$ och $H_n = H_0(\frac{5}{2})^n$, en exponentiell ökning. Utan harar får vi på samma sätt $L_n = L_0(\frac{1}{2})^n$, en halvering av antalet lodjur varje år så lodjuren dör ut.

(d) Efter att ha satt in ett par värden ser det ut som att $(H_n, L_n) = (3 \cdot 2^n, 2^n)$ vilket kan verifieras med t.ex. induktion. Kvoten av populationerna blir $\frac{H_n}{L_n} = 3$, alltså konstant 3 oberoende av året - förhållandet bevaras men båda populationerna fördubblas vart år.

(e) Sätter vi in $H_n = H = H_{n-1}$ och $L_n = L = L_{n-1}$ i ekvationssystemet och förenklar så får vi $2H = 5H - 3L \wedge 2L = H + L \Leftrightarrow 3H = 3L \wedge L = H \Leftrightarrow H = L$. Så fort det finns lika många harar som lodjur förblir det alltså så varje år. Vi kan t.ex. ta $(H_0, L_0) = (100, 100)$ för att uppnå denna jämvikt.

5 Inlämningsuppgift 5

5.1 Kubfärgning

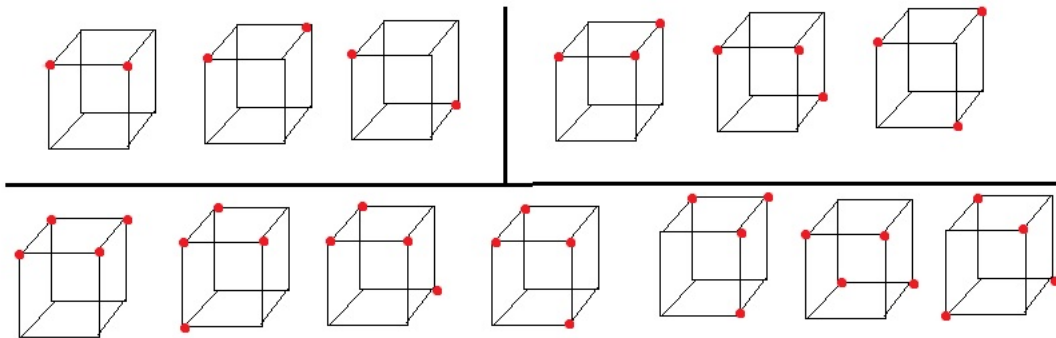
(a) På hur många olika sätt kan man färga de sex **sidorna** på en kub med två tillgängliga färger? Två färgningar räknas som lika om man kan få den ena från den andra genom rotationer. Motivera ditt svar!

(b) Samma förutsättningar som i (a) fast nu vill vi färga de åtta **hörn**en på kuben istället, på hur många olika sätt kan detta göras?

Tips: Falluppdelar!

Lösningsförslag

Vi ska färga kubens sidor i rött och blått (r,b). Vi falluppdelar med avseende på antal röda sidor. Noll eller en röd sida går på ett sätt vardera. Ska vi ha två röda sidor kan antingen sidorna dela en kant, eller vara motsående, två fall. Med tre röda sidor kan vi antingen ta tre sidor som alla delar ett hörn, eller ta två motsatta sidor och en sida till, två fall. Högre antal röda fås via symmetri. Med $(0, 1, 2, 3, 4, 5, 6)$ röda sidor fås alltså $(1, 1, 2, 2, 2, 1, 1)$ möjligheter, totalt 10 olika färgningar.



Vi betraktar nu hörnfärgningar istället. Med 0 och 1 rött hörn finns en möjlighet var. För två hörn har vi tre möjliga avstånd mellan hörnen, tre fall. Med tre röda hörn ligger antingen alla på en sida, eller så ligger två på samma kant, eller så ligger alla en sid-diagonal ifrån varandra. Med 4 röda hörn delar vi upp i delfall igen: Om tre hörn hör till samma sida finns det fem fall för det fjärde hörnet (två är spegelbilder av varandra men olika). Annars så ligger antingen två hörn på en kant och de två andra hörnen på diagonalt motsående kant, eller så ligger alla hörn symmetriskt med en sid-diagonals avstånd från varandra. Totalt sju fall med fyra hörna av varje färg alltså. Fallen med fler än fyra röda hörn följer av symmetrin. Med $(0, 1, 2, 3, 4, 5, 6, 7, 8)$ röda hörn får vi alltså $(1, 1, 3, 3, 7, 3, 3, 1, 1)$ fall, totalt 23 färgningar.

5.2 Heltalsmittpunkter

Två punkter (x_1, y_1) och (x_2, y_2) i planet $\mathbb{R}^2$ har mittpunkten $(\frac{x_1+x_2}{2}, \frac{y_1+y_2}{2})$

(a) Visa att givet fem punkter i $\mathbb{Z}^2$ (alltså punkter med heltalskoordinater) så finns det minst ett par av dem vars mittpunkt också ligger i $\mathbb{Z}^2$.

(b) Vi betraktar motsvarande fråga i $\mathbb{R}^3$. Hur många punkter i $\mathbb{Z}^3$ behöver jag ha för att vara säker på att minst ett par har en mittpunkt i $\mathbb{Z}^3$?

Tips: Använd postfacksprincipen!

Lösningsförslag

(a) Vi noterar att medelvärdet av två heltal är ett heltal omm heltalen är lika modulo 2. Vi definierar $f : \mathbb{Z}^2 \rightarrow \mathbb{Z}_2^2$ genom $f(x, y) = (x \pmod{2}, y \pmod{2})$. Vi får fyra möjliga funktionsvärden: $(0, 0), (1, 0), (0, 1), (1, 1)$. Dessa är våra "postfack", av fem punkter hamnar minst två i samma fack, och punkter i samma fack har en heltalsmittpunkt.

(b) Samma idé $f : \mathbb{Z}^3 \rightarrow \mathbb{Z}_2^3$ ger $2^3 = 8$ postfack, så med **nio punkter** får vi minst en heltalsmittpunkt.

5.3 Alfabetssträngar utan vissa ord

(a) På hur många sätt kan man skriva ned alla alfabetets 29 bokstäver så att inget av orden **GLAD**, **HÄST**, **PONKE** förekommer i textsträngen?

(b) Samma fråga fast med orden **VAKTHUND** och **MÅLVAKT**.

(Motivera ditt svar, det räcker att svara med ett korrekt uttryck, alltså utan att skriva ut hela talen)

Tips: Använd principen om inklusion och exklusion!

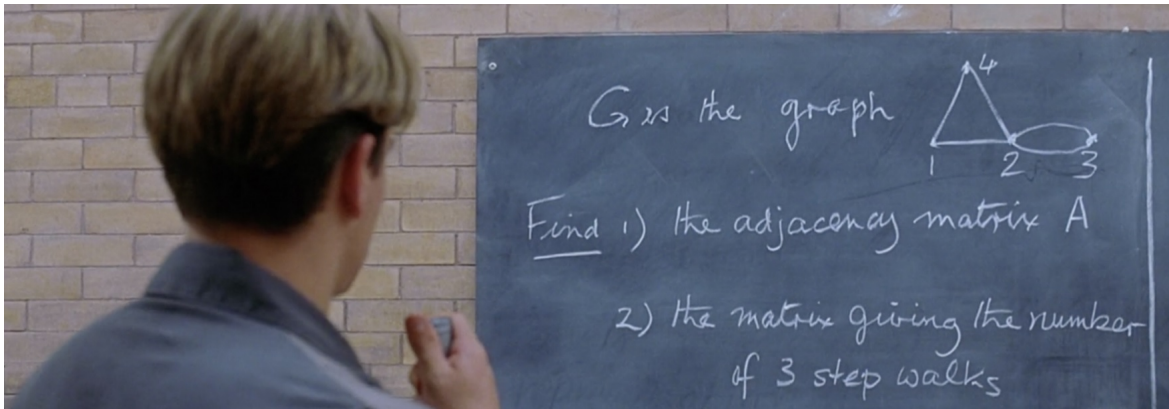
Lösningsförslag

(a) Låt A_1, A_2, A_3 vara mängderna ordsträngar som innehåller glad, häst, respektive, ponke. Varje ord i A_1 motsvaras av en permutation av de 26 symbolerna (glad),(b),(c), ..., (ö). Alltså är $|A_1| = 26!$ och på samma vis får vi $|A_2| = 26!$ och $|A_3| = 25!$. Ord i $A_1 \cap A_2$ motsvarar permutationer av symbolerna (glad),(häst),(b),(c), ..., (ö), så $|A_1 \cap A_2| = 23!$, på liknande vis blir $|A_1 \cap A_3| = 22! = |A_2 \cap A_3|$. Och analogt blir till slut blir $|A_1 \cap A_2 \cap A_3| = 19!$. Enligt principen om inklusion/exklusion blir $|A_1 \cup A_2 \cup A_3| = 26! + 26! + 25! - 23! - 22! - 22! + 19!$, och den sökta mängden textsträngar utan något av dessa ord blir därför $29! - 26! - 26! - 25! + 23! + 22! + 22! - 19! = 8840939927707301961626247168000$.

(b) Vi använder inklusion och exklusion som i (a). Det finns $23!$ ord med MÅLVAKT i och $22!$ ord med VAKTHUND i. Enda möjligheten att ett ord innehåller båda är att det innehåller ordet MÅLVAKTHUND, och det finns $19!$ sådana ord. Antalet strängar utan något av de två orden blir därför enligt principen om inklusion och exklusion $29! - 23! - 22! + 19! = 8841761966763806132981440512000$.

6 Inlämningsuppgift 6

6.1 Good Will Hunting



Du ska hjälpa Matt Damon att lösa problemet ovan från filmen "Good Will Hunting":

- 1) Hitta Grannmatrisen för multigrafen på bilden.
- 2) Skriv ned en 4×4 -matris där det på position (i, j) står antalet vandringar av längd tre från nod i till nod j .

(Här vill vi skilja på kanterna mellan 2 och 3: det finns exempelvis två olika 1-stegsvandringar från 2 till 3)

Lösningsförslag

- 1) Vi skriver på position (i, j) antalet kanter mellan nod i och nod j , då får vi grannmatrisen:

$$A = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 2 & 1 \\ 0 & 2 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

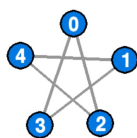
- 2) Låt B vara den sökta matrisen. Vi har $B_{1,1} = B_{2,2} = B_{4,4} = 2$, motsvarande två riktningar att gå runt triangeln, och $B_{3,3} = 0$. $B_{1,2} = 7$ - om vi går först till nod två finns totalt 6 tvåstegsvägar från 2 till 2, annars är enda möjligheten vägen $1 - 4 - 1 - 2$. Av symmetri blir också $B_{2,4} = 7$. $B_{1,3} = 2$ motsvarande $1 - 4 - 2 - 3$ där det finns två val för sista steget. Av symmetri blir också $B_{3,4} = 2$. $B_{1,4} = 3$ motsvarande $1 - 4 - 1 - 4$, $1 - 4 - 2 - 4$, $1 - 2 - 1 - 4$. Till slut har vi $B_{2,3} = 12$. Det finns $2^3 = 8$ vägar av formen $2 - 3 - 2 - 3$ och två vägar vardera av typ $2 - 4 - 2 - 3$ respektive $2 - 1 - 2 - 3$, totalt 12. Av symmetri har vi $B_{i,j} = B_{j,i}$ så nu har vi hela matrisen:

$$B = \begin{bmatrix} 2 & 7 & 2 & 3 \\ 7 & 2 & 12 & 7 \\ 2 & 12 & 0 & 2 \\ 3 & 7 & 2 & 2 \end{bmatrix}$$

Om man kan matrismultiplikation kan man alternativt beräkna $A^3 = B$.

6.2 Stjärnor

Vi definierar en (n, m) -stjärna som en graf med nodmängd $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ och kantmängd $\{\{x, x+m\} \mid x \in \mathbb{Z}_n\}$ (där summan beräknas i $\mathbb{Z}_n$).



En (5,2)-stjärna

- a) För vilka värden på $1 < m < 6$ blir en $(6, m)$ -stjärna en sammanhängande graf? Hur många sammanhängande komponenter får varje stjärna?
- b) För vilka $0 < m < n$ blir en (n, m) -stjärna sammanhängande? Hitta ett uttryck för antal sammanhängande komponenter i en (n, m) -stjärna.
- Motivera dina svar!

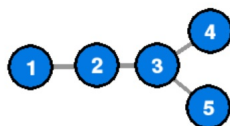
Lösningsförslag

- a) Ritar man upp stjärnorna ser man att då $m = (2, 3, 4, 5)$ får vi $(2, 3, 2, 1)$ komponenter.
- b) Vi betraktar komponenten som innehåller noden 0. Den består av noderna $0, m, 2m, \dots$ (modulo n). Att en fix nod c ingår i denna mängd betyder att $x \cdot m \equiv c \pmod{n}$, alltså att den diofantiska ekvationen $xm + yn = c$ har en lösning. Vi vet att detta händer då $\gcd(m, n) | c$. Vi inför $d = \gcd(m, n)$. Då blir alltså 0-komponenten $\{d, 2d, 3d, \dots, \frac{n}{d}d\}$. Av symmetri blir 1-komponenten $\{1, d+1, 2d+1, \dots\}$ och så vidare, vi får alltså d komponenter, varje komponent innehåller precis en av noderna $0, 1, \dots, d-1$.

Svar: En (n, m) -stjärna har $\gcd(n, m)$ stycken komponenter. Stjärnan blir alltså sammanhängande när m och n är relativt prima.

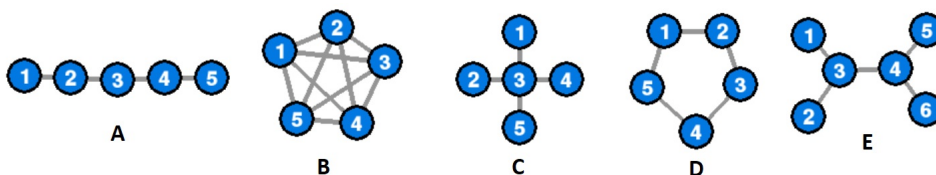
6.3 Automorfier - symmetrier i grafer

En **automorfi** för en graf är en isomorfi från grafen till sig själv. Identitetsfunktionen på grafens nodmängden är alltid en isomorfi, men det kan finnas flera. Antalet automorfier ger ett mått på hur symmetrisk grafen är.



Grafen ovan har t.ex. två automorfier: identitetsfunktionen, och funktionen som skiftar 4 med 5 (grafens är spegel-symmetrisk i x-axeln). Om vi skriver funktioner på nodmängden på formen $f = (f(1), f(2), f(3), f(4), f(5))$ så blir de två automorfierna $(1, 2, 3, 4, 5)$ respektive $(1, 2, 3, 5, 4)$.

- 1) Ange hur många automorfier som finns för var och en av nedanstående grafer A, B, C, D, E. Motivera dina svar!



- 2) Hitta en graf som har en enda automorfi! Svara med en bild (eller en bild med tecken om du kan göra den tydlig nog)

Lösningsförslag

(1) A har två automorfier, identitetsfunktionen och speglingen $(5, 4, 3, 2, 1)$.

B har $5! = 120$ automorfier. Eftersom grafen är komplett blir varje bijektion på nodmängden en automorfi.

C har $4! = 24$ automorfier. En automorfi måste skicka $3 \mapsto 3$, men sedan kan man fritt välja en bijektion på mängden $\{1, 2, 4, 5\}$.

D har 10 automorfier. Man kan rotera grafen på 5 sätt (inklusive identitets-rotationen). Var och en av dessa rotationer kan också speglas så vi får 5 till. De tio automorfierna blir explicit

$$(1, 2, 3, 4, 5), (2, 3, 4, 5, 1), (3, 4, 5, 1, 2), (4, 5, 1, 2, 3), (5, 1, 2, 3, 4) \\ (1, 5, 4, 3, 2), (2, 1, 5, 4, 3), (3, 2, 1, 5, 4), (4, 3, 2, 1, 5), (5, 4, 3, 2, 1)$$

E har 8 automorfier. Eftersom nod 3 och 4 har grad 3 måste en automorfi f uppfylla $f(3) \in \{3, 4\}$. Om $f(3) = 3$ blir $f(4) = 4$. Vi kan sedan välja om $1 \mapsto 1$ eller $1 \mapsto 2$, och oberoende välja om $5 \mapsto 5$ eller $5 \mapsto 6$. Fyra alternativ i detta fall alltså. Om istället $f(3) = 4$ får vi $f(4) = 3$ och fyra alternativ igen. De åtta automorfierna blir explicit

$$(1, 2, 3, 4, 5, 6), (2, 1, 3, 4, 5, 6), (1, 2, 3, 4, 6, 5), (2, 1, 3, 4, 6, 5) \\ (5, 6, 4, 3, 1, 2), (6, 5, 4, 3, 1, 2), (5, 6, 4, 3, 2, 1), (6, 5, 4, 3, 2, 1)$$

(2) Exempelvis kan vi skapa en trädgraf med sju noder och kanter

$\{(1, 2), (2, 3), (3, 4), (4, 5), (5, 6), (3, 7)\}$. Den har en central nod 3 och tre grenar av längd 1, 2, 3.

$$1 - 2 - 3 - 4 - 5 - 6 \\ \quad \quad \quad | \\ \quad \quad \quad 7$$

Det går också med 6 stycken noder, men då behöver man fler kanter.

En graf med endast en nod och inga kanter uppfyller tekniskt sett också villkoret.

7 Inlämningsuppgift 7

7.1 De två heltalsrelationerna

Vi definierar två relationer R_1 och R_2 på heltalen $\mathbb{Z}$ enligt följande:

$$xR_1y \Leftrightarrow x \equiv y \pmod{2}$$

$$xR_2y \Leftrightarrow x \equiv y \pmod{3}$$

Vilka heltal blir relaterade med varandra via den sammansatta relationen $R_1 \circ R_2$? Svara så explicit som möjligt och motivera ditt svar!

Lösningförslag

Om n är jämnt gäller nR_10 och nR_12 och nR_14 . Men eftersom 0, 2, 4 är kongruenta med 0, 2, 1 modulo 3 gäller att varje heltal x är relaterat till något av dessa tal via R_2 : $\forall x \in \mathbb{Z} : (0R_2x \vee 1R_2x \vee 2R_2x)$. Alltså gäller $\forall x : (nR_1 \circ R_2x)$ när n är jämnt. Å andra sidan, när n är udda gäller nR_11 och nR_13 och nR_15 och 1, 3, 5 är kongruenta med 1, 0, 2 modulo 3, och varje x är relaterad till någon av dessa via R_2 .

Slutsats: Alla heltal är relaterade till varandra via den sammansatta relationen. Med andra ord gäller $R_1 \circ R_2 = \mathbb{Z} \times \mathbb{Z}$.

7.2 Symmetrisk skillnad

Låt $U = \{1, 2, 3, 4, 5\}$. Då består $\mathcal{P}(U)$ av alla 32 delmängder av U .

Vi definierar följande binära operation Δ på $\mathcal{P}(U)$.

$$A\Delta B = (A \cup B) \setminus (A \cap B)$$

- Beräkna $\{1, 2, 3\}\Delta\{2, 3, 4\}$
- Har operationen ett identitetselement?
- Vilka element i $\mathcal{P}(U)$ har inverser?
- Är operationen associativ? *Tips: Rita Venn-diagram!*
- Lös ekvationen $(\{1, 2, 3\}\Delta X)\Delta\{1, 3, 5\} = \{4, 5\}$ i magman $(\mathcal{P}(U), \Delta)$

Lösningförslag

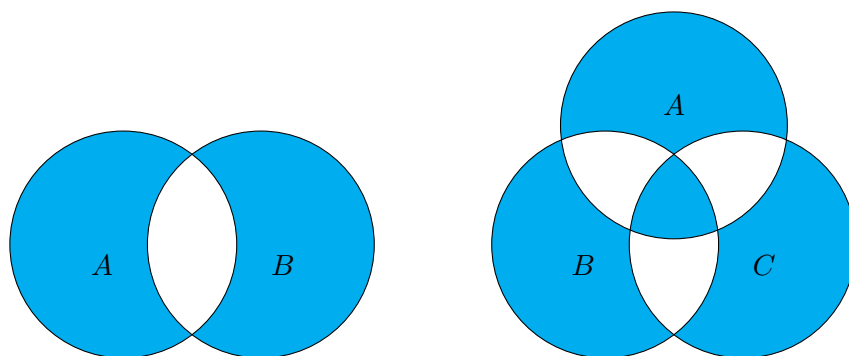
a) $\{1, 2, 3\}\Delta\{2, 3, 4\} = (\{1, 2, 3\} \cup \{2, 3, 4\}) \setminus (\{1, 2, 3\} \cap \{2, 3, 4\}) = \{1, 2, 3, 4\} \setminus \{2, 3\} = \{1, 4\}$

b) Ja, den tomma mängden $\emptyset$ är ett identitetselement eftersom $\emptyset\Delta X = X\Delta\emptyset = (X \cup \emptyset) \setminus (X \cap \emptyset) = X \setminus \emptyset = X$ för alla $X \in \mathcal{P}(U)$

c) Alla element har inverser. Varje element är sin egen invers eftersom $X\Delta X = (X \cup X) \setminus (X \cap X) = X \setminus X = \emptyset$ och $\emptyset$ är identitetselementet.

d) Ja, operationen är associativ. Till vänster i bilden nedan har vi skuggat mängden $A\Delta B$ som Venn-diagram. Ritar vi upp Venn-diagram för $A\Delta(B\Delta C)$ respektive $(A\Delta B)\Delta C$ får

vi samma bild, den till höger nedan.



Alternativt kan man resonera sig fram utan diagram, man kommer då fram till att $x \in (A \Delta B) \Delta C$ om och endast om x tillhör exakt en eller exakt tre av mängderna A, B, C . Samma villkor gäller om $x \in A \Delta (B \Delta C)$.

Alltså är operationen associativ. Vi har nu visat att $(\mathcal{P}(U), \Delta)$ faktiskt är en grupp!

e) Vi kan lösa ekvationen genom att multiplicera med inverser på bägge sidor, vi får då en ekvivalent ekvation. Eftersom operationen är kommutativ spelar det ingen roll om vi multiplicerar från vänster eller höger. Eftersom varje element är sin egen invers börjar vi med att applicera $\Delta\{1, 3, 5\}$ till både vänster och höger i uttrycket. Då kancellerar de två $\{1, 3, 5\}$ elementen från vänsterledet och vi får $\{1, 2, 3\} \Delta X = \{4, 5\} \Delta \{1, 3, 5\} = \{1, 3, 4\}$. Nu multiplicerar vi med $\{1, 2, 3\}$ på bägge sidor och får då $X = \{1, 2, 3\} \Delta \{1, 3, 4\} = \{2, 4\}$. Så $X = \{2, 4\}$ är ekvationens enda lösning.

7.3 Tabellen för den binära operationen

Nedan visas en delvis ifylld tabell för en binär operation $\star$ på mängden $M = \{a, b, c, d\}$. Fyll i resten av tabellen på så vis att $(M, \star)$ blir associativ, kommutativ, har ett identitets-element, och saknar nollelement. Detta går att göra på precis ett sätt. Blir $(M, \star)$ en grupp? Motivera dina slutsatser!

$\star$	a	b	c	d
a			a	
b	b			
c			a	c
d				

Lösningsförslag

Från tabellen framgår direkt att varken a, b, eller c är identitets-element. Alltså är d identitets-element och vi kan fylla i d's rad och kolonn i tabellen. Kommutativiteten säger också att tabellen ska vara symmetrisk med avseende på diagonalen. Vi fyller i detta och får

$\star$	a	b	c	d
a		b	a	a
b	b			b
c	a		a	c
d	a	b	c	d

Eftersom $\star$ är associativ har vi $a \star (c \star c) = (a \star c) \star c$ vilket enligt tabellen ger $a \star a = a$.

Vidare har vi via associativitet $(b \star a) \star c = b \star (a \star c)$ vilket ger $b \star c = b$ och därför också $c \star b = b$ och vi kan fylla i detta i tabellen. Nu återstår bara att hitta $b \star b$.

Associativiteten ger $(b \star b) \star a = b \star (b \star a) = b \star b$, vilket betyder att $b \star b$ måste vara a eller b . Men om $b \star b = b$ blir b ett nollelement i $(M, \star)$ så vi måste ha $b \star b = a$. Därmed är tabellen klar. $(M, \star)$ är inte en grupp, t.ex. saknar a invers eftersom ingenting multiplicerat med a blir identitets-elementet d .

Svar: $(M, \star)$ har följande tabell:

$\star$	a	b	c	d
a	a	b	a	a
b	b	a	b	b
c	a	b	a	c
d	a	b	c	d

Detta är inte en grupp.