Tentamen i CM1000 – Diskret Matematik, januari 2022 – Lösningar

1. Logik. Visa att nedanstående härledning är korrekt utan att använda sanningstabeller och redovisa i varje steg vilka slutledningsregler som används (*Modus Ponens*, *Modus Tollens*, etc.)

1. $p \to q$
2. $q \to p \vee r$
3. $r \to \neg(p \oplus q)$

$\therefore$ $p \leftrightarrow q$

Ledning: Utan motivation kan du använda att $p \oplus q \Leftrightarrow \neg(p \leftrightarrow q)$. Det är lättast att göra detta genom ett indirekt bevis, men även andra strategier fungerar. Var i vilket falls som helst mycket noggrann med den logiska strukturen och ange i synnerhet alltid om slutsatser vilar på antaganden.

Lösning: Vi gör ett motsägelsebevis och antar därför

4. $\neg(p \leftrightarrow q)$ *Antagande för indirekt härledning*

Enligt ledningen är detta ekvivalent med

5. $p \oplus q$ *(och 4)*

vilket ger oss

6. $\neg r$ *5, 3, Modus Tollens (och 4)*

Vi skriver nu om premiss 2 till

7. $\neg q \vee p \vee r$ *Omskrivning av 2 (och 4)*

och vi skulle här kunnat utelämna referensen till antagandet i 4, men vi låter ändå den följa med hela vägen. Nu använder vi 6 och 7 och får via disjunktiv syllogism

8. $\neg q \vee p$ *6, 7, Disjunktiv Syllogism (och 4)*

som kan skriva om igen till

9. $q \to p$ *Omskrivning av 8 (och 4)*

Och nu ser vi att 1, 9 kan skriva om till

10. $p \leftrightarrow q$ *Omskrivning av 1,9 (och 4)*

vilket ger oss en motsägelse:

11. $\bot$ *4, 10 (och 4)*

vilket gör att vi kan dra slutsatsen att antagandet i 4 måste vara falskt, det vill säga

12. $p \to q$ *4-11 och indirekt härledning.*

Beviset är klart.

Anmärkning: En lösning är godkänd även utan den löpande texten, det enda som behövs för att få godkänt är de rader med nummer. I den här lösningen väljer vi dock att vara extra utförliga eftersom det kan vara bra av pedagogiska skäl.

2. Mängdlära. Utan att använda Venndiagram, visa, för alla godtyckliga mängder A, B, C identiteten

$$(A \cup B \cup C) - (B \cap C) = (A - (B \cup C)) \cup (B \oplus C).$$

Här betyder $B \oplus C$ mängden $(B - C) \cup (C - B)$.

Ledning: Använd distributiva lagarna för mängder för att skriva om vänster och höger led men också uttrycket för $B \oplus C$.

Lösning: Vi skriver om både höger och vänster led i identiteten tills vi ser att de representerar samma mängd. Vi börjar att med hjälp av distributiva lagen konstatera att

$$B \oplus C = (B - C) \cup (C - B) = (B \cap C^c) \cup (C \cap B^c) = ((B \cap C^c) \cup C) \cap ((B \cap C^c) \cup B^c) =$$
$$(B \cup C) \cap (C^c \cup C) \cap (B \cup B^c) \cap (C^c \cup B^c)$$

och eftersom $(C^c \cup C) = (B \cup B^c) = U$, där U är universum och $(C^c \cup B^c) = (B \cap C)^c$ har vi identiteten

$$B \oplus C = (B \cup C) \cap (B \cap C)^c.$$

Vi skriver nu om mängddifferenserna i den ursprungliga identiteten som vi ska visa och använder det vi just funnit om $B \oplus C$ så att vi har

$$(A \cup B \cup C) - (B \cap C) = (A - (B \cup C)) \cup (B \oplus C)$$
$$\Leftrightarrow$$
$$(A \cup B \cup C) \cap (B \cap C)^c = (A \cap (B \cup C)^c) \cup ((B \cup C) \cap (B \cap C)^c).$$

Vi använder nu distributiva lagen på vänster led och skriver

$$(A \cup B \cup C) \cap (B \cap C)^c = (A \cup (B \cup C)) \cap (B \cap C)^c = (A \cap (B \cap C)^c) \cup ((B \cup C) \cap (B \cap C)^c)$$

vilket ju precis är samma mängd som representeras av högerledet. Beviset är klart.

3. Funktioner. Vi betraktar funktioner på mängden $\mathbb{R}^2$, det vill säga funktioner som tar punkter ur planet och avbildar på planet. Ett exempel på en sådan funktion som vi ska studera är

$$g(x, y) = (g_1(x, y), g_2(x, y)), \text{ där } g_1(x, y) = x + y \text{ och } g_2(x, y) = x - y.$$

Vi har då till exempel

$$g(1, 2) = (g_1(1, 2), g_2(1, 2)) = (1 + 2, 1 - 2) = (3, -1) \qquad g(2, 1) = (g_1(2, 1), g_2(2, 1)) = (2 + 1, 2 - 1) = (3, 1).$$

Låt nu a, b beteckna godtyckliga reella tal och studera funktioner $f : \mathbb{R}^2 \to \mathbb{R}^2$, där

$$f(x, y) = (f_1(x, y), f_2(x, y)) = (ax + by, bx + ay).$$

För varje var av två reella tal uppstår en sådan funktion. Finn nu alla tal a, b för vilka funktionen

$$h = f \circ g$$

är bijektiv.

Lösning: Vi ska alltså hitta alla tal a, b för vilka $h = f \circ g$ är bijektiv. Vi får en tydligare frågeställning om vi faktiskt räknar ut precis var h är för något. Vi har

$$h(x, y) = (f \circ g)(x, y) = f(g(x, y)) = f(g_1(x, y), g_2(x, y)) = f(x + y, x - y) =$$
$$(a(x + y) + b(x - y), b(x + y) + a(x - y)) = ((a + b)x + (a - b)y, (a + b)x + (b - a)y).$$

Detta kan uttryckas som ett matrissamband:

$$\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} a + b & a - b \\ a + b & -a + b \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}.$$

Att funktionen är bijektiv är, enligt teorin från den linjära algebran, precis samma sak som att matrisen är inverterbar som är samma sak som att determinanten är skild från noll. Determinantens värde är $-2 \cdot (a^2 - b^2)$, så vi har alltså att

$$h \text{ bijektiv} \Leftrightarrow -2 \cdot (a^2 - b^2) \neq 0 \Leftrightarrow a^2 \neq b^2 \Leftrightarrow |a| \neq |b|.$$

Så för alla val av a, b som har *olika absolutbelopp* blir funktionen $h = f \circ g$ bijektiv.

4. Inledande talteori. Visa, för alla heltal a, b, c att

$$\gcd(a, b) = \gcd(a + bc, a + b(c - 1)).$$

Ledning: Det går till och med att visa att detta gäller för en godtycklig gemensam delare. Gör det och dra sedan slutsatsen för största gemensamma delaren.

Lösning: Vi visar, för alla heltal a, b, c, att

$$d|a \wedge d|b \Leftrightarrow d|a + bc \wedge d|a + b(c - 1).$$

$\Rightarrow$: Antag att $d|a \wedge d|b$. Då gäller $a = k_1 \cdot d$ och $b = k_2 \cdot d$ så att vi har

$a + bc = k_1 \cdot d + k_2 \cdot d \cdot c = d \cdot (k_1 + k_2 c)$ $\quad$ $a + b(c - 1) = k_1 \cdot d + k_2 \cdot d(c - 1) = d(k_1 + k_2(c - 1))$.

Dessa båda identiteter visar att $d|a + bc \wedge d|a + b(c - 1)$.

$\Leftarrow$: Antag omvänt att $d|a + bc \wedge d|a + b(c - 1)$. Då finns k_1, k_2 så att $a + bc = k_1 d$ och $a + b(c - 1) = k_2 d$. Vi kan skriva om detta som

$$\begin{cases} a + bc = k_1 d \\ a + bc - b = k_2 d \end{cases}$$

Om vi subtraherar dessa ekvationer, led för led, från varandra får vi $-b = (k_2 - k_1)d$ vilket visar att $d|b$. Detta sätter vi in i den övre ekvationen som då får utseendet

$$a + bc = k_1 d \Leftrightarrow a = k_1 d - bc \Leftrightarrow a = k_1 d + c(k_2 - k_1)d = d(k_1 + c(k_2 - k_1))$$

vilket visar att $d|a$. Sammantaget har vi visat att $d|a \wedge d|b$

Slutsatsen blir att $d|a \wedge d|b \Leftrightarrow d|a + bc \wedge d|a + b(c - 1)$, det vill säga ett tal d är gemensam delare till a, b om och endast om det också är gemensam delare till $a + bc, a + b(c - 1)$, speciellt måste också detta gälla den *största* gemensamma delaren till a, b respektive $a + bc, a + b(c - 1)$ och dessa måste då alltså sammanfalla, det vill säga

$$\gcd(a, b) = \gcd(a + bc, a + b(c - 1))$$

vilket fullbordar beviset.

5. Relationer. Definiera relationen $\mathcal{R}$ på $\mathbb{Z}$ genom

$$x \mathcal{R} y \Leftrightarrow x \equiv y \pmod 2 \vee x \equiv y \pmod 3.$$

Ge en fullständig utredning som redovisar och motiverar vilka av egenskaperna reflexivitet, symmetri, antisymmetri och transitivitet som den här relationen har eller inte har. (För varje egenskap: motivera om den har egenskapen eller inte.)

Lösning: Relationen är reflexiv och symmetrisk, däremot varken antisymmetrisk eller transitiv.

Reflexivitet: Visa att $x \mathcal{R} x$ för alla $x \in \mathbb{Z}$. Detta är klart eftersom för varje x gäller både $x \equiv x \pmod 2$ och $x \equiv x \pmod 3$ (det hade räckt med att en av dessa alltid gällt) och därmed har vi för alla $x \in \mathbb{Z}$:

$$x \equiv x \pmod 2 \wedge x \equiv x \pmod 3 \Rightarrow x \equiv x \pmod 2 \vee x \equiv x \pmod 3 \Leftrightarrow x \mathcal{R} x$$

och eftersom x i detta resonemang kan vara godtyckligt är reflexiviteten visad.

Symmetri: På liknande sätt som relationen blir reflexiv eftersom kongruensrelationen är reflexiv så blir relationen också symmetrisk. Då gäller:

$$x \mathcal{R} y \Leftrightarrow x \equiv y \pmod 2 \vee x \equiv y \pmod 3 \Leftrightarrow y \equiv x \pmod 2 \vee y \equiv x \pmod 3 \Leftrightarrow y \mathcal{R} x.$$

och eftersom vi kan konstatera att detta håller för godtyckliga x, y är symmetrin visad.

Antisymmetri: Relationen är däremot inte antisymmetrisk eftersom vi till exempel har $2 \mathcal{R} 4 \wedge 4 \mathcal{R} 2$ (eftersom $2 \equiv 4 \pmod 2$ och $4 \equiv 2 \pmod 2$) men $2 \neq 4$.

Transitivitet: Slutligen finner vi x, y, z där vi har $x \mathcal{R} y$ och $y \mathcal{R} z$ men inte $x \mathcal{R} z$. Tre sådana tal är $x = 2$, $y = 4$ och $z = 7$. Här gäller

$$2 \mathcal{R} 4 \text{ (eftersom } 2 \equiv 4 \pmod 2) \qquad 4 \mathcal{R} 7 \text{ (eftersom } 4 \equiv 7 \pmod 3)$$

men vi har varken $2 \equiv 7 (\text{mod } 2)$ eller $2 \equiv 7 (\text{mod } 3)$ vilket betyder att vi *inte* har $2 \mathcal{R} 7$ och relationen kan därför *inte* vara transitiv.

6. Fördjupad talteori. Visa med hjälp av matematisk induktion att för varje heltal $n \geq 4$ gäller olikheten $4n^2 + 2^n \leq 3^n$.

Ledning: Om du gör ett konventionellt induktionsbevis kommer steg 2 att kräva att du kan visa en olikhet som ser ut ungefär så här: $8p + 4 + 2^p \leq 2 \cdot 3^p$. Du kan göra detta i ett separat extrainbäddat induktionsbevis i steg 2 (som en hjälpsats). Här får du utan motivering använda att funktionen $h(p) = 3^p - 2^p$ är växande för $p \geq 4$.

Lösning: Vi inför predikatet $A(n) \Leftrightarrow 4n^2 + 2^n \leq 3^n$ och vi ska med matematisk induktion visa $\forall n \geq 4 : A(n)$. I det följande skriver vi också VL_n för $4n^2 + 2^n$ respektive HL_n för 3^n. Då har vi $A() \Leftrightarrow VL_n \leq HL_n$. Vi tar nu de tre stegen i ett induktionsbevis.

Steg 1. Kontrollera att $A(4)$ är sann. Det betyder att vi ska se efter om $VL_4 \leq HL_4$. Därför beräknar vi VL_4 och HL_4:

$$VL_4 = 4 \cdot 2^2 + 2^4 = 80 \qquad HL_4 = 3^4 = 81$$

och eftersom $VL_4 = 80 \leq 81 = HL_4$ konstaterar vi att $A(4)$ är sann.

Steg 2. Vi ska nu visa att implikationen $A(p) \Rightarrow A(p+1)$ är sann för alla heltal $p \geq 4$ och därför gör vi det så kallade *insuktionsantagandet* och antar att för ett visst värde på p gäller $A(p)$, vi har alltså för detta p:

$$VL_p \leq HL_p \Leftrightarrow 4p^2 + 2^p \leq 3^p.$$

Med kraft av detta ska vi visa att även $A(p+1)$ är sann, det vill säga vi ska visa att

$$VL_{p+1} \leq HL_{p+1} \Leftrightarrow 4(p+1)^2 + 2^{p+1} \leq 3^{p+1}.$$

Vi studerar $VL_{p+1} = 4(p+1)^2 + 2^{p+1}$ och finner

$$VL_{p+1} = 4 \cdot (p^2 + 2p + 1) + 2 \cdot 2^p = 4p^2 + 8p + 4 + 2^p + 2^p = 4p^2 + 2^p + 8p + 4 + 2^p =$$

$$VL_p + 8p + 4 + 2^p.$$

Det är förstås tillåtet att snegla på vårt mål, vi vill att detta ska vara mindre än HL_{p+1} och vi kan komma en bit på vägen att visa detta genom att använda induktionsantagandet och uppskatta VL_p uppåt med $HL_p = 3^p$, sammanfattningsvis får vi

$$VL_{p+1} = VL_p + 8p + 4 + 2^p \leq HL_p + 8p + 4 + 2^p = 3^p + 8p + 4 + 2^p.$$

Vi önskar som sagt att detta i sin tur ska vara mindre än $HL_{p+1} = 3^{p+1} = 3 \cdot 3^p$, det vill säga vi vill kunna dra slutsatsen

$$3^p + 8p + 4 + 2^p \leq 3 \cdot 3^p \Leftrightarrow 8p + 4 + 2^p \leq 2 \cdot 3^p$$

och om detta gäller så har vi $A(p+1)$. Detta är i sin tur möjlig att visa genom ett extra induktionsbevis, vi inför nu därför predikatet

$$B(p) \Leftrightarrow 8p + 4 + 2^p \leq 2 \cdot 3^p$$

och vi ska visa $\forall p \geq 4 : B(p)$. Återigen kontrollerar vi att $B(4)$ stämmer:

$$B(4) \Leftrightarrow 8 \cdot 4 + 4 + 2^4 \leq 2 \cdot 3^4 \Leftrightarrow 32 + 4 + 16 \leq 2 \cdot 81 \Leftrightarrow 52 \leq 162$$

vilket uppenbart är sant. Steg 1 i detta inre induktionsbevis är allts klart. Nu ska vi visa att $B(p) \Rightarrow B(p+1)$ gäller så vi gör antagandet $B(p) \Leftrightarrow 8p + 4 + 2^p \leq 2 \cdot 3^p$. med kraft av detta ska vi visa att $B(p+1)$ gäller, det vill säga $8(p+1) + 4 + 2^{p+1} \leq 2 \cdot 3^{p+1} \Leftrightarrow 8p + 12 + 2 \cdot 2^p \leq 3 \cdot 3^p$. Vi studerar nu vänster led i denna olikhet och använder induktionsantagandet:

$$8p + 12 + 2 \cdot 2^p = 8p + 4 + 2^p + 8 + 2^p \leq 2 \cdot 3^p + 8 + 2^p.$$

Vi vill att detta uttryck ska vara mindre än eller lika med $3 \cdot 3^p$, det vill säga vi vill att

$$2 \cdot 3^p + 8 + 2^p \leq 3 \cdot 3^p \Leftrightarrow 8 + 2^p \leq 3^p \Leftrightarrow 3^p - 2^p \geq 8.$$

Funktionen $h(p) = 3^p - 2^p$ är växandet och $h(4) = 3^4 - 2^4 = 81 - 16 = 65 \geq 8$ vilket betyder att $h(p) \geq 8$ för alla $p \geq 4$, men det ger precis $3^p - 2^p \geq 8$ för alla $p \geq 4$ vilket är ekvivalent med $B(p+1)$. Sammantaget har vi alltså $B(p) \Rightarrow B(p+1)$ vilket tillsammans med att $B(4)$ är sann och principen för matematisk induktion att $B(p)$ är sann för alla $p \geq 4$. Detta i sin tur fastställer att $A(p+1)$ är sann, det vill säga vi har här fastställt att $A(p+1) \rightarrow A(p+1)$ gäller för alla $p \geq 4$.

Steg 3. Steg 1 och steg 2 samt induktionsaxiomet fullbordar beviset.

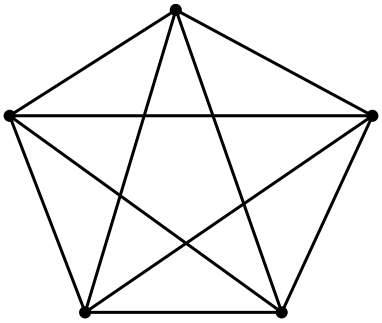
7. Grafteori. Rita en graf med följande egenskaper:

1. Den är sammanhängande.
2. Den har en delgraf som är isomorf med K_3.
3. Den har en delgraf som är isomorf med $K_{3,2}$.
4. Den har max 5 hörn och max 8 kanter.

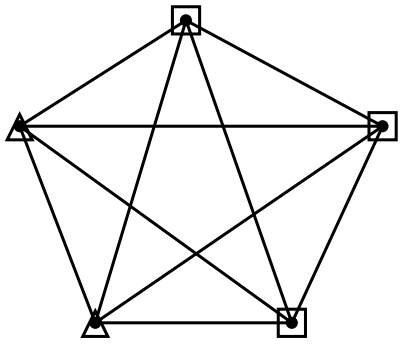
Ange *tydligt* de delgrafer som ska finnas i grafen som uppfyller krav 2 och 3. Använd *två* olika skisser för detta, en för att att visa att krav 2 är uppfyllt och en annan för att visa att krav 3 är uppfyllt.

Lösning: Vi utgår från K_5 som uppfyller de första tre kraven. K_5 har 10 kanter och 5 noder och uppfyller de första tre kraven men alltså *inte* det sista kravet. Om vi kan ta bort två kanter ur K_5 och få en ny graf som fortfarande uppfyller de första tre kraven så har vi funnit den graf som vi söker.

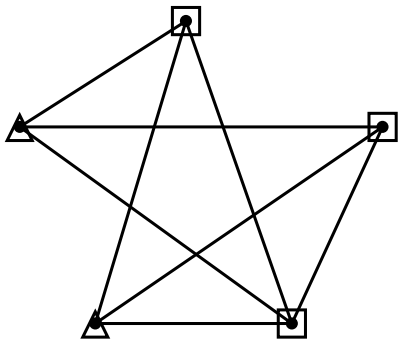
Betrakta alltså K_5:



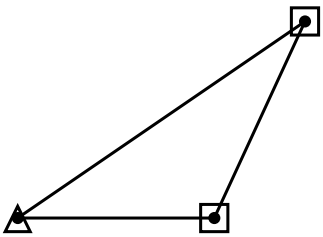
Vi behöver först välja de tre hörn som ska utgöra ena halvan av delgrafen som ska vara isomorf med $K_{3,2}$ och därmed fastställs också vilka två hörn som ingår i andra halvan av grafen som är isomorf med $K_{3,2}$. Vi illustrerar det valet genom att rita kvadrater runt de 3 hörn respektive trianglar runt två hörn:

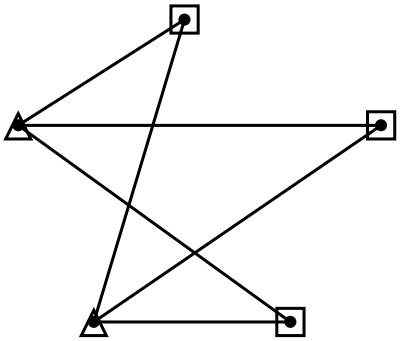


Vi ska nu se om vi kan ta bort kanter så att grafen uppfyller det sista kravet. Efter en del funderingar inser vi att vi kan ta bort kanten mellan de båda hörnen med trianglar ritade runt sig. Vi har fortfarande krav 1,2,3 uppfyllda. Vi måste ta bort en kant till. Någonstans ska även K_3 finnas inbäddad och det är frestande att låta K_3 vara inbäddad och utgöras av hörnen med kvadrater runt sig, MEN då blir det problematiskt att ta bort ytterligare en kant och uppfylla alla krav. Lösningen blir att vi anser att K_3 är inbäddad i två av hörnen med kvadrater, låt oss säga de till höger och ett av hörnen med trianglar, låt oss ta det nedre. Då finns både K_3 och $K_{3,2}$ i nedanstående graf:



Och en illustrationerna av följande delgrafer visar att grafen innehåller en delgraf isomorf med K_3 och en isomorf med $K_{3,2}$:





Anmärkning: Vi kan lösa detta med kravet 7 kanter också, kan du se vilken kant som vi också kan ta bort?

8. Kombinatorik. Låt $\Omega = \{1, 2, 3, \ldots, 1000\}$. Beräkna antalet element i mängden

$$M = \{x \in \Omega : \gcd(x, 999) = 1\}.$$

Lösning: Vi primfaktoriserar 999 enligt

$$999 = 3^3 \cdot 37.$$

Om vi inför $D_d = \{x \in \Omega : d|x\}$ så kan vi skriva

$$M = \Omega - (D_3 \cup D_{37})$$

och enligt principen för inklusion och exklusion har vi

$$|D_3 \cup D_{37}| = |D_3| + |D_{37}| - |D_3 \cap D_{37}| = 1000/3 + 1000/37 - 1000/(3 \cdot 37) = 333 + 27 - 9 = 351.$$

Här betyder $1000/3$, $1000/37$ respektive $1000/(3 \cdot 37)$ *heltalsdivisioner*, till exempel har vi

$$|D_{37}| = |\{1 \cdot 37, 2 \cdot 37, \ldots, 27 \cdot 37\}|$$

och 27 uppkommer alltså när 1000 heltalsdivideras med 37. Eftersom 3 och 37 är olika primtal har vi också $D_3 \cap D_{37} = D_{3 \cdot 37}$.

Sammantaget har vi alltså $|M| = |\Omega| - |D_3 \cup D_{37}| = 1000 - 351 = 649$.

9. Sannolikhetslära. Vi har tre urnor, U_1, U_2 och U_3. U_1 innehåller två blåa kulor. U_2 innehåller en blå och en gul kula och U_3 innehåller två gula kulor. Betrakta följande slumpprocess:

1. En av urnorna U_2 och U_3 väljs slumpmässigt.
2. En slumpvis i den valda urnan byter plats med en slumpvis vald kula i U_1.
3. En kula väljs slumpvis ur U_1

Beräkna sannolikheten att den slumpvis valda kulan ur U_1 är blå.

Ledning: Du kan förenkla formuleringen av problemet innan du inför händelser.

Lösning: Steg 1 och 2 är ekvivalent med att en kula ur U_1 byter plats med en slumpvis vald kula ur en större urna som innehåller alla kulor som U_2 och U_3 innehåller, vi kan kalla den urnan V och den innehåller då en blå och tre gula kulor.

Nu inför vi följande händelser:

$B =$ en blå kula ur U_1 byter plats med en blå kula ur V. Vi har $P(B) = 1/4$.
$G =$ en blå kula ur U_1 byter plats med en gul kula ur V. Vi har $P(G) = 3/4$.

I uppgiften söker vi sannolikheten av händelsen X som är att vi slutligen får en blå kula, enligt satsen om total sannolikhet har vi

$$P(X) = P(X|B) \cdot P(B) + P(X|G) \cdot P(G).$$

Här gäller $P(X|B) = 1$ eftersom vi bara har blåa kulor i U_1 om vi bytte plats med en blå kula ur V respektive $P(X|G) = 1/2$ eftersom vi hade haft en gul och en blå kula i U_1 om vi bytte plats på en blå ur U_1 och en gul ur V.

Sammantaget har vi

$$P(X) = P(X|B) \cdot P(B) + P(X|G) \cdot P(G) = 1 \cdot \frac{1}{4} + \frac{1}{2} \cdot \frac{3}{4} = \frac{5}{8}.$$

10. För C. *Kan även täcka delområde 4, inledande talteori.* Låt m vara ett positivt heltal och beteckna med $\overline{x}$ restklassen i $\mathbb{Z}_m$. Visa följande påstående:

$$m > 2 \Rightarrow |\{\overline{1^2}, \overline{2^2}, \ldots, \overline{m^2}\}| < m.$$

Lösning: Vi bildar alltså en mängd av restklasser

$$\{\overline{1^2}, \overline{2^2}, \ldots, \overline{m^2}\}$$

och vi ska visa att denna mängd har mindre än m element om $m > 2$. Ytligt sett ser det ut som om det finns m olika element i mängden, varje element uppstår som restklassen $\overline{i}$, där i antar de m olika värdena. Dock så räknar vi här modulo m och dessa m element är bara olika om vi inte kan hitta två *olika* i och j med $i^2 \equiv j^2 \pmod{m}$. Saken är den att förutsättningen $m > 2$ faktiskt möjliggör ett val av två olika tal i, j sådana att $i^2 \equiv j^2 \pmod{m}$, dessa tal är $i = 1$ respektive $j = m - 1$, vi har då

$$\overline{j^2} = \overline{(m-1)^2} = \overline{m^2 - 2m + 1} = \overline{1} = \overline{1^2} = \overline{i^2}$$

det näst sista elementet i listan på element i $\mathbb{Z}_m$:

$$\overline{1^2}, \overline{2^2}, \ldots, \overline{m^2}$$

som är $\overline{(m-1)^2}$ överensstämmer alltså med det första elementet som är $\overline{1}$. Alltså är antalet element i denna lista $< m$, eller med andra ord

$$|\{\overline{1^2}, \overline{2^2}, \ldots, \overline{m^2}\}| < m$$

vilket skulle bevisas. (*Anmärkning:* om vi inte hade $m > 2$, dvs om $m = 2$ så hade $i = 1$ och $j = m - 1 = 1$ variot samma element, det vill säga vi hade inte haft möjligheten att dra slutsatsen som baserade sig på att i och j var olika.)

11. För A. En så kallad differensekvation är en ekvation som definierar en talföljd $(a_n)_{n=0}^{\infty}$ rekursivt. Vi studerar en sådan av andra graden:

$$a_{n+2} = pa_{n+1} + qa_n$$

där a_0 och a_1 väljs som startvärden och som rekursivt definierar värdena på alla efterföljande a_n, $n = 2, 3, \ldots$. Vi har även $q \neq 0$ i de ekvationer vi studerar.

Visa följande påstående med stark matematisk induktion:

Om r_1, r_2 är lösningarna till den karakteristiska ekvationen

$$r^2 = pr + q$$

där $r_1 \neq r_2$ så finns konstanter C, D sådana att

$$a_n = Cr_1^n + Dr_2^n, n = 0, 1, 2, \ldots.$$

Lösning: Eftersom $q \neq 0$ så kan varken r_1 eller r_2 vara noll så därför kan vi skriva

$$\begin{cases} a_0 = Cr_1^0 + Dr_2^0 \\ a_1 = Cr_1^1 + Dr_2^1 \end{cases} \Leftrightarrow \begin{cases} a_0 = C + D \\ a_1 = Cr_1 + Dr_2 \end{cases} \Leftrightarrow \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ r_1 & r_2 \end{pmatrix} \cdot \begin{pmatrix} C \\ D \end{pmatrix}$$

Alltså ett ekvationssystem med de två obekanta C, D. Determinanten av koefficientmatrisen är $r_2 - r_1$ och eftersom $r_1 \neq r_2$ är den inte noll vilket innebär att ekvationssystemet har en entydig lösning i C, D dör varje val av a_0, a_1. Den här utredningen tjänar som första steget i induktionsbeviset.

Steg 2. Vi inför här ett predikat:

$$A(n) \Leftrightarrow a_n = Cr_1^n + Dr_2^n.$$

Om talföljden defineras rekursivt som beskrivits ovan ska vi nu visa

$$\forall n \geq 0 : A(n).$$

Vi har redan visat $A(0)$ och $A(1)$ i steg 1 ovan. Vi antar därför att $A(k)$ är sann för alla k, $k = 0, 1, \ldots, n, n+1$ och vi ska visa att $A(n+2)$ är sann. Eftersom $A(n)$ och $A(n+1)$ båda gäller så har vi

$$a_n = Cr_1^n + Dr_2^n \qquad \text{och} \qquad a_{n+1} = Cr_1^{n+1} + Dr_2^{n+1}$$

vi ska nu visa att $A(n+2)$ gäller, det vill säga $a_{n+2} = Cr_1^{n+2} + Dr_2^{n+2}$. Enligt den rekursiva definitionen och induktionsantagandet gäller

$$a_{n+2} = pa_{n+1} + qa_n = p(Cr_1^{n+1} + Dr_2^{n+1}) + q(Cr_1^n + Dr_2^n).$$

Om vi samlar alla r_1 i en term och alla r_2 i en term blir detta uttryck lika med

$$a_{n+2} = (pCr_1 + qC)r_1^n + (pDr_2 + qD)r_2^n = C(pr_1 + q)r_1^n + D(pr_2 + q)r_2^n.$$

Men eftersom r_1, r_2 är lösningar till ekvationen $r^2 = pr + q$ kan detta i sin tur skriva om som

$$a_{n+2} = Cr_1^2 \cdot r_1^n + Dr_2^2 \cdot r_2^n = Cr_1^{n+2} + Dr_2^{n+2}$$

men detta uttrycker precis att $a_{n+2} = Cr_1^{n+2} + Dr_2^{n+2}$ som är $A(n+2)$ vilket skulle visas. Steg 2 i induktionen är avklarat.

Steg 3: Steg 1 och steg 2 samt principen för stark matematisk induktion fullbordar beviset.

Den intresserade läsaren kan själv genomföra motsvarande bevis för sitationen då den karakteristiska ekvationen har en dubberot.