Lösningsförslag för TDDC75 - Lektion 7

Om du hittar ett fel i någon av uppgifterna eller i lösningsförslagen, skicka ett mejl till szilvia.varro-gyapay@liu.se.

- Obligatoriska uppgifter:

1. Låt P vara mängden av alla personnummer som någon har och $f : P \mapsto \mathbb{N}$ vara en funktion som anger ålder som hör till varje personnummer.
   (a) Är f injektiv?
   (b) Är f surjektiv?
   (c) Är f bijektiv?

   Lösning.
   (a) Nej. Två olika personer kan ha samma ålder: $x \neq y \wedge f(x) = f(y)$
   (b) Nej. Det finns ingen person x sådan att $f(x) = 300$.
   (c) Nej, ty den är varken injektiv eller surjektiv.

2. (Inspirerat av en tidigare tentauppgift.) Låt $f{:}\mathbb{N} \to \mathbb{N}$, en funktion som konverterar Celsiusgrader till Fahrenheit, vara definierad enligt $f(c) = FLOOR(c \cdot \frac{9}{5} + 32)$.
   (FLOOR avrundar ett tal till största heltalet mindre än eller lika med talet. Var uppmärksam på definitionsmängden och målmängden.)
   (a) Ange värdena f(0), f(1), f(5) och f(10).
   (b) Är f injektiv?
   (c) Är f surjektiv?
   (d) Är f bijektiv?
   (e) Låt oss ändra definitionsmängden till $\mathbb{Z}$. Blir den nya funktionen fortfarande en funktion? Om ja, är den nya funktionen injektiv, surjektiv, bijektiv?

   Lösningsförslag.
   (a) $f(-19) = FLOOR(-19 \cdot \frac{9}{5} + 32) = FLOOR(-2,2) = -3, f(0) = 32, f(1) = 33, f(5) = 41$.
   (b) f är injektiv eftersom värdedifferensen av två följande varandra heltal (märka att domän är mängd av heltal) $\frac{9}{5} = 1.8$ som är större än 1 som menar att om vi använder funktionen $FLOOR$ vi får ett annat heltal. Andra lösningen är: låt $x_1, x_2 \in \mathbb{Z}$ så att $f(x_1) = f(x_2)$ och vi bevisa att $x_1 = x_2$. $f(x_1) = f(x_2), FLOOR(x_1 \cdot \frac{9}{5} + 32) = FLOOR(x_2 \cdot \frac{9}{5} + 32) = n$.
   Det betyder att både $x_1 \cdot \frac{9}{5} + 32$ och $x_2 \cdot \frac{9}{5} + 32$ är mellan n och $n + 1$:
   $n \leq x_1 \cdot \frac{9}{5} + 32 < n + 1$,
   $n - 32 \leq x_1 \cdot \frac{9}{5} < n - 31$,
   $\frac{5}{9} \cdot n - \frac{5}{9} \cdot 32 \leq x_1 < \frac{5}{9} \cdot n - \frac{5}{9} \cdot 31$
   $\frac{5}{9} \cdot n - 17,77 \leq x_1 < \frac{5}{9} \cdot n - 17,22$
   Samma gäller för x_2. Eftersom differensen mellan två sidorna av likheten är ungefär $0,55$, det finns bara ett heltal mellan dessa tal. Så vi får att $x_1 = x_2$.
   (c) f är inte surjektiv eftersom funktionen är ökande och $f(1) = 33, f(2) = 35$ så det finns ingen heltal x för $f(x) = 34$.
   (d) f är inte bijektiv eftersom den är inte injektiv eller surjektiv.
   (e) Om vi definierar $f : \mathbb{R} \to \mathbb{R}$ som $f(x) = x \cdot \frac{9}{5} + 32$ får vi en surjektiv funktion eftersom det finns för alla $y \in \mathbb{R}$ an x så att $y = x \cdot \frac{9}{5} + 32, x = (y - 32) \cdot \frac{5}{9}$

3. Låt $A = \{x, y, z\}$, $B = \{0, 1, 2, 3\}$ och funktionerna $f : A \to B$ och $g : B \to A$ definieras som $f = \{x \mapsto 1, y \mapsto 2, z \mapsto 3\}$ och $g = \{0 \mapsto z, 1 \mapsto y, 2 \mapsto z, 3 \mapsto z\}$.
   (a) Vad blir sammansättningen $g \circ f$?
   (b) Vad blir sammansättningen $f \circ g$?

   Lösning.
   (a) $g \circ f : A \to A = \{x \mapsto y, y \mapsto z, z \mapsto z\}$
   (b) $f \circ g : B \to B = \{0 \mapsto 3, 1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 3\}$

4. Låt f vara en bijektiv funktion $f : A \to B$ med inversen $f^{-1} : B \to A$.

(a) Vad blir sammansättningen $f \circ f^{-1}$?
(b) Vad blir sammansättningen $f^{-1} \circ f$?

Inget lösningsförslag finns för denna uppgift.

5. Antag att $f: \mathbb{N} \to \mathbb{N}$ definieras enligt

$$f(n) = n + 1$$

och att $g: \mathbb{N} \to \mathbb{N}$ definieras enligt

$$g(n) = \begin{cases} 0 \text{ om } n \text{ är jämn,} \\ 1 \text{ om } n \text{ är udda.} \end{cases}$$

(a) Är f eller g injektiv och/eller surjektiv?
(b) Vad blir $(f \circ g)(n)$ för de fem minsta naturliga talen n?
(c) Vad blir på motsvarande sätt $(g \circ f)(n)$?
(d) Beskriv funktionen $(f \circ f)(n)$

Lösning.

(a) f är injektiv. Om $f(x) = f(y)$ så måste $x = y$. Men f är inte surjektiv eftersom det inte existerar något $x \in \mathbb{N}$ sådant att $f(x) = 0$. g är varken inektiv eller surjektiv eftersom $g(0) = g(2)$ samt att det inte existerar något $x \in \mathbb{N}$ sådant att $g(x) = 3$.
(b)
- $(f \circ g)(0) = 1$
- $(f \circ g)(1) = 2$
- $(f \circ g)(2) = 1$
- $(f \circ g)(3) = 2$
- $(f \circ g)(4) = 1$

(c)
- $(g \circ f)(0) = 1$
- $(g \circ f)(1) = 0$
- $(g \circ f)(2) = 1$
- $(g \circ f)(3) = 0$
- $(g \circ f)(4) = 1$

(d) $(f \circ f)(n) = n + 2$

6. Antag att vi har fyra *olika* funktioner f_1, f_2, f_3, f_4 där
   - f_1 är injektiv men inte surjektiv,
   - f_2 är surjektiv men inte injektiv,
   - f_3 är bijektiv, och
   - f_4 är varken injektiv eller surjektiv.

   Ge exempel på hur funktionerna f_1, f_2, f_3, f_4 kan se ut givet att funktionernas domäner och värdemängder kan väljas bland följande mängder:

$$A = \{a, b, c\} \quad B = \{0, 1, 2\} \quad C = \{0, 1\}.$$

Inget lösningsförslag finns för denna uppgift.

7. Låt $f : \mathbb{N} \to 2^{\mathbb{N}}$ vara en funktion definierad som $f(n) = \{i \in \mathbb{N} \mid i \leq n\}$ för alla $n \in \mathbb{N}$.
   (a) Ange funktionsvärdena för $f(0)$, $f(1)$, $f(2)$ och $f(5)$.
   (b) Är f injektiv?
   (c) Är f surjektiv?
   (d) Existerar den inversa funktionen $f^{-1} : 2^{\mathbb{N}} \mapsto \mathbb{N}$?

   Lösning.

   (a)
   - $f(0) = \{0\}$
   - $f(1) = \{0, 1\}$
   - $f(2) = \{0, 1, 2\}$
   - $f(5) = \{0, 1, 2, 3, 4, 5\}$

(b) Ja. Låt $x \neq y$ vara två olika naturliga tal. Vi kan utan begränsning anta att $x < y$. I så fall gäller att $y \in f(y)$ men $y \notin f(x)$, så $f(x) \neq f(y)$.

(c) Nej. Det existerar inget $x \in \mathbb{N}$ sådan att $f(x) = \{0, 2, 4\}$

(d) Nej eftersom f inte är bijektiv existerar inte dess invers.

8. Kryptering av ett meddelande kan modelleras som en funktion (encrypt) $e_K : A \to B$ där A är mängden av klartextmeddelanden, B är mängden av krypterande meddelanden och K är nyckeln. På motsvarande sätt finns en dekrypteringsfunktion $d_K : B \to A$, som för varje krypterat meddelande ger det ursprungliga meddelandet i klartext.

   (a) Uttryck funktionen d_K med hjälp av e_K.

   (b) Är e_K alltid, aldrig, eller ibland injektiv?

   (c) För att rent praktiskt kunna skapa krypterings och dekrypteringsfunktioner brukar meddelanden delas upp i *block* av en viss storlek, till exempel 128 bitar. Om elementen i A består av 128 bitars meddelanden, vad gäller då för storleken på elementen i B? Hur relaterar detta till huruvida e_K är injektiv och/eller surjektiv?

   Lösning.

   (a) $d_K(b) = e_K^{-1}(b)$ där $b \in B$ och e_K^{-1} betecknar inversen till krypteringsfunktionen.

   (b) e_K är alltid injektiv eftersom den har en invers. Om det fanns två meddelanden $m_1, m_2 \in A, m_1 \neq m_2$ sådana att $e_K(m_1) = e_K(m_2)$ så skulle det inte kunna finnas en dekrypteringsfunktion d_K som återställer båda till klartext.

   (c) Elementen i B måste vara minst 128 bitar eftersom det faktum att e_K är injektiv implicerar att $|A| \leq |B|$. Om e_K även är surjektiv så är e_K en bijektion så $|A| = |B|$ och elementen i B måste vara exakt 128 bitar långa. Om e_K inte är surjektiv kan de krypterade meddelandena vara längre.

9. Låt f vara $f : R_+ \to R_+$ och $g : R_+ \to R_+$ vara definierade genom $f(x) = x^2$ och $g(x) = \frac{1}{1+x}$ för $x \in R_+$.

   (a) Vad blir sammansättningen $f \circ g$?

   (b) Vad blir sammansättningen $g \circ f$?

   Lösning.

   (a) $(f \circ g)(x) = f(g(x)) = f(\frac{1}{1+x}) = (\frac{1}{1+x})^2 = \frac{1}{(1+x)^2}$

   (b) $(g \circ f)(x) = g(f(x)) = g(x^2) = \frac{1}{1+x^2}$

- Rekommenderade uppgifter:

1. En logisk grind (i digitaltekniken) med m st. ingångar $x_1, \ldots, x_m$ kan betraktas som en funktion $f : \{0, \ldots, 2^m - 1\} \mapsto \{0, 1\}$, där ingångarna betraktas som en binär kodning av ett naturligt tal. Bestäm för var och en av följande definitioner av f vilken typ av grind den motsvarar, eller om den inte motsvarar någon av de vanliga grindtyperna alls.

   (a) $f(n) = \begin{cases} 1, & \text{om } n = 2^m - 1 \\ 0, & \text{annars} \end{cases}$

   (b) $f(n) = \begin{cases} 0, & \text{om } n = 0 \\ 1, & \text{annars} \end{cases}$

   (c) $f(n) = \begin{cases} 1, & \text{om } n < 2^m - 1 \\ 0, & \text{annars} \end{cases}$

   Lösning.

   (a) Detta motsvarar en AND-grind med m ingångar. Endast om alla ingångar är 1 blir utsignalen 1.

   (b) Detta motsvarar en OR-grind med m ingångar. Om någon av ingångarna är 1 blir utsignalen 1.

   (c) Detta motsvarar en NAND-grind med m ingångar. Om alla ingångar är 1 blir utsignalen 0, annars blir den 1.

2. Låt F vara mängden av satslogiska formler (exempelvis gäller att $(p \wedge q) \in F$). Låt funktionen $f : F \times F \to \{0, 1\}$, vara definerad så att $f(F_1, F_2) = 1$ om $F_1 \Rightarrow F_2$ och $f(F_1, F_2) = 0$ annars.

(a) Avgör värdet av $f((p \vee q), (p \vee q \vee r))$.
(b) Är f surjektiv?
(c) Är f injektiv?
(d) Beskriv vilka element som finns i mängden $\{F_i \in F \mid f(1, F_i) = 1\}$ (de har en speciell benämning).

Lösning.

(a) Av regeln för disjunktiv förstärkning så vet vi att $(p \vee q) \Rightarrow (p \vee q \vee r)$. Därmed blir $f((p \vee q), (p \vee q \vee r)) = 1$.
(b) Målmängden för f är $\{0, 1\}$ och vi har redan visat att 1 är ett möjligt värde på f. Kvarstår att hitta två fromler F_1 och F_2 sådana att $f(F_1, F_2) = 0$. Om $F_1 = 1$ och $F_2 = 0$ så är $F_1 \nRightarrow F_2$, och därmed $f(F_1, F_2) = 0$. Alltså är f surjektiv.
(c) $f(0, 1) = 1 = f(0, p)$, men $1 \neq p$. Alltså är f inte injektiv.
(d) $\{F_i \in F \mid f(1, F_i) = 1\}$ är mängden av alla formler F_i sådana att $1 \Rightarrow F_i$. Det betyder alltså att de är sanna i alla tolkningar då 1 är sant (alltid). Sanningsvärdet för alla F_i är alltså 1. Dessa formler kallas tautologier.

3. Antag att $f : A \to B$ och $g : B \to C$. Visa eller motbevisa följande påståenden
   (a) Om $g \circ f$ är surjektiv så måste f och g vara surjektiva.
   (b) Om f och g är surjektiva så måste $g \circ f$ vara surjektiv.
   (c) Om $g \circ f$ är injektiv så måste f och g vara injektiva.

1. Om $g \circ f$ är surjektiv så måste f och g vara surjektiva.
   Motbevis: Låt $A = \{0, 1\}, B = \{2, 3, 4\}, C = \{5, 6\}$, och låt $f = \{0 \mapsto 2, 1 \mapsto 3\}, g = \{2 \mapsto 5, 3 \mapsto 6, 4 \mapsto 6\}$. Sammansättningen $g \circ f = \{0 \mapsto 5, 1 \mapsto 6\}$ är uppenbart surjektiv. Dock är f i detta exempel inte surjektiv.
2. Om f och g är surjektiva så måste $g \circ f$ vara surjektiv. *Bevis:* Låt z vara godtyckligt element i C. Eftersom g är surjektiv vet vi att det existerar ett element $y \in B$ sådant att $g(y) = z$. Dessutom vet vi att f är surjektiv, vilket innnebär att det existerar ett element $x \in A$ sådant att $f(x) = y$. Vi har alltså visat att för godtyckligt element $z \in C$ så existerar element $x \in A$ och $y \in B$ sådana att $f(x) = y$ och $g(y) = z$. Alltså $g(f(x)) = (g \circ f)(x) = z$, vilket visar att $(g \circ f)$ är surjektiv.
3. Om $g \circ f$ är injektiv så måste f och g vara injektiva. *Motbevis:* Låt $A = \{0\}, B = \{1, 2\}, C = \{3\}, f = \{0 \mapsto 2\}, g = \{1 \mapsto 3, 2 \mapsto 3\}$. Sammansättningen $(g \circ f) = \{0 \mapsto 3\}$ är injektiv, men g är inte injektiv eftersom $g(1) = g(2)$.

- Extra uppgifter. Visa att $f : \mathbb{N} \to \mathbb{N}$, $f(x) = |x - 1|$ är surjektiv.