Kapitel 5

Funktioner

Om du hittar ett fel i någon av uppfiterna eller i lösningsförslagen, skicka ett mejl till mikael.asplund@liu.se.

5.1. (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.

5.2. (a) $g \circ f : A \to A = \{x \mapsto y, y \mapsto z, z \mapsto z\}$

(b) $f \circ g : B \to B = \{0 \mapsto 3, 1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 3\}$

5.3. (a) f är injektiv. Om $f(x) = f(y)$ så måste $x = y$. Men f är inte surjektiv eftersom det inte existerar något $x \in \mathbf{N}$ sådant att $f(x) = 0$. g är varken inektiv eller surjektiv eftersom $g(0) = g(2)$ samt att det inte existerar något $x \in \mathbf{N}$ 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) $(f \circ f)(n) = n + 2$

5.4. Inget lösningsförslag finns för denna uppgift.

5.5. (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.

5.6. (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 $x \in \mathbf{N}$ sådan att $f(x) = \{0, 2, 4\}$

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

5.7. (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.

5.8. (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.

5.9. 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.
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.

(b) 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.

(c) 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 $g(1) = g(2)$.