Tentamen Diskret Matematik NV1 2006-12-14

Lösningar

1. *Avgör om utsagorna*

$$(p \vee q) \to r$$

och

$$(p \to r) \wedge (q \to r)$$

är logiskt ekvivalenta.

Sanningsvärdestabellen nedan visar att de är logiskt ekvivalenta.

p	q	r	$p \vee q$	$(p \vee q) \to r$	$p \to r$	$q \to r$	$(p \to r) \wedge (q \to r)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	F
T	F	T	T	T	T	T	T
T	F	F	T	F	F	T	F
F	T	T	T	T	T	T	T
F	T	F	T	F	T	F	F
F	F	T	F	T	T	T	T
F	F	F	F	T	T	T	T

2. *Ange antalet heltalslösningar till ekvationen*

$$x_1 + x_2 + x_3 + x_4 + x_5 = 13,$$

givet att $x_i \geq 0$, $i = 1, 2, 3, 4, 5$.

Varje lösning svarar till att ha valt $k = 13$ objekt, med upprepning tillåten ur en mängd med $t = 5$ distinkta element. Enligt sats går detta att göra på $C(k + t - 1, k) = C(17, 13) = \binom{17}{13}$ sätt.

3. *Bestäm koefficienten för termen* $x^4 z^{21}$ *i utvecklingen av*

$$(2x - 3z^3)^{11}.$$

Enligt binomialteoremet är

$$(2x - 3z^3)^{11} = \sum_{k=0}^{11} \binom{11}{k} (2x)^k (-3z^3)^{11-k}$$

Alltså fås den aktuella termen då $k = 4$ och ges av

$$\binom{11}{4}(2x)^4(-3z^3)^7x^4z^{21} = -\binom{11}{4}2^4 3^7 x^4 z^{21}.$$

Den sökta koefficienten är $-\binom{11}{4}2^4 3^7$.

4. *Ge ett exempel på, eller motivera varför det inte finns, en Eulercykel respektive en Hamiltoncykel, i graferna G_1 och G_2 nedan.*

   Ett exempel på en Eulercykel i G_1 är $(a, b, f, h, i, e, g, f, c, a, d, f, e, a)$. Det finns ingen Hamiltoncykel i G_1. En sådan skulle innehålla 9 kanter eftersom G_1 har 9 hörn. Endast två av dessa kan dock ha f som ändpunkt. 4 kanter går bort. Samma för a gör att ytterligare två kanter går bort, eftersom det inte finns någon kant mellan a och e. Återstår $13 - 4 - 2 = 7$ kanter. Det kan alltså inte finnas en Hamiltoncykel i G_1.

   Det finns ingen Eulercykel i G_2 eftersom exempelvis $\delta(E) = 5$. Ett exempel på en Hamiltoncykel i G_2 är $(A, B, C, I, H, F, E, D, G, A)$.

5. *Lös rekurrensrelationen*

$$a_n = 6a_{n-1} - 8a_{n-2},$$

   med begynnelsevärdena $a_0 = 2$, $a_1 = 12$.

   Karaktäristiska ekvationen ges av

$$t^2 - 6t + 8 = 0$$

   och har rötterna $r_1 = 2$, $r_2 = 4$. Den allmänna lösningen ges därför av

$$a_n = C_1 2^n + C_2 4^n.$$

   Begynnelsevärdena ger

$$a_0 = C_1 + C_2 = 2 \qquad (1)$$
$$a_1 = 2C_1 + 4C_2 = 12 \qquad (2)$$

   $(2) - 2 \cdot (1)$ ger $2C_2 = 8$, $\Rightarrow C_2 = 4$, insatt i (1) ger $C_1 = -2$. Alltså ges lösningen av

$$a_n = -2 \cdot 2^n + 4 \cdot 4^n = -2^{n+1} + 4^{n+1}.$$

6. *En något orutinerad krypterare har gjort en RSA kryptering med offentliga krypteringsnycklar $z = 35$ och $n = 5$.*

   a) Kryptera meddelandet $a = 9$.

   b) "Knäck krypteringen" och dekryptera det krypterade meddelandet $c = 12$.

   a) Krypteringen av a är $a^n \mod z = a^5 \mod 35$.

   $9^2 = 81 \equiv 11 \mod 35$.

   $9^4 \equiv 11^2 = 121 \equiv 16 \mod 35$

   $9^5 = 9 \cdot 9^4 \equiv 9 \cdot 16 = 144 \equiv 4 \mod 35$

   Krypteringen av 9 är alltså 4.

b) Eftersom 35 har primtalsfaktorisering $35 = 5 \cdot 7 = p \cdot q$, kan vi bestämma dekrypteringsnyckeln. $\phi = (p-1)(q-1) = 24$, söker $0 < s < 24$ så att $ns \mod \phi = 1$. Bestämmer s mha Euk. Alg.:

$24 = 4 \cdot 5 + 4$

$5 = 1 \cdot 4 + 1$

Euk. Alg. "Baklänges"

$1 = 5 - 1 \cdot 4 = 5 - (24 - 4 \cdot 5) = 5 \cdot 5 - 24$. Alltså är $s = 5$.

c kan dekrypteras genom $c^s \mod z = c^5 \mod 35$.

$12^2 = 144 \equiv 4 \mod 35$

$12^4 \equiv 4^2 = 16 \mod 35$

$12^5 \equiv 12 \cdot 16 = 192 \equiv 17 \mod 35$.

Dekrypteringen av c är alltså 17.

7. *a) Ge en optimal Huffmankod för tecknen A, B, C, D, E, F, G, med frekvenserna $A : 18$, $B : 13$, $C : 4$, $D : 9$, $E : 3$, $F : 12$, $G : 20$.*

   b) Hur många bitar (nollor och ettor) behövs för att skicka ett meddelande innehållande 18st A, 13 st B, 4st C, 9st D, 3st E 12st F och 20 st G med Huffmankoden från a)? Hur många hade krävts i en kod där varje tecken motsvaras av en binär sträng av fix längd?

   Följande steg

   $3, 4, 9, 12, 13, 18, 20 \rightarrow 3 + 4, 9, 12, 13, 18, 20$

   $7, 9, 12, 13, 18, 20 \rightarrow 7 + 9, 12, 13, 18, 20$

   $12, 13, 16, 18, 20 \rightarrow 12 + 13, 16, 18, 20$

   $16, 18, 20, 25 \rightarrow 16 + 18, 20, 25$

   $20, 25, 34 \rightarrow 20 + 25, 34$

   $34, 45$

   ger exvis nedanstående optimala Huffmankod.

   A 10

   B 000

   C 1110

   D 110

   E 1111

   F 001

   G 01

   b) I Huffmankoden i a) behövs $18 \cdot 2 + 13 \cdot 3 + 4 \cdot 4 + 9 \cdot 3 + 3 \cdot 4 + 12 \cdot 3 + 20 \cdot 2 = 36 + 39 + 16 + 27 + 12 + 36 + 40 = 206$st bitar. Med fix längd skulle varje tecken behöva beskrivas med 3 bitar. Alltså för hela meddelandet totalt $3 \cdot (18 + 13 + 4 + 9 + 3 + 12 + 20) = 3 \cdot 79 = 237$ bitar.

8. *a) Visa att om sammansättningen $g \circ f$ av två funktioner $f : X \rightarrow Y$ och $g : Y \rightarrow Z$ är injektiv så måste f vara injektiv.*

   b) Visa att om $g \circ f$ är surjektiv så måste g vara surjektiv.

   c) Ge ett exempel där $g \circ f$ är injektiv, men g inte är injektiv.

a) Antag att $g \circ f$ är injektiv, men att f inte är injektiv. Då finns $x_1 \neq x_2$ så att $f(x_1) = f(x_2)$. Då är även $g \circ f(x_1) = g \circ f(x_2)$, vilket motsäger att $g \circ f$ är injektiv.

b) Antag att $g \circ f$ är surjektiv, men att g inte är surjektiv. Då finns $z \in Z$ så att $g(y) \neq z$ för varje $y \in Y$. Då är även $g \circ f(x) \neq z$ för varje $x \in X$, vilket motsäger att $g \circ f$ är surjektiv.

c) Låt $X = \{a, b\}$, $Y = \{A, B, C\}$ och $Z = \{\alpha, \beta\}$. Definiera f genom $f(a) = A$ och $f(b) = B$. Definiera g genom $g(A) = \alpha$, $g(B) = \beta$ och $g(C) = \beta$. g är inte injektiv, men $g \circ f$ är injektiv.

9. *Bestäm ett minimalt uppspännande träd i grafen nedan mha Prim's algoritm.*

T_0 består enbart av hörnet a.

T_1 lägg till kanten (a, b) och hörnet b.

T_2 lägg till kanten (a, g) och hörnet g

T_3 lägg till kanten (g, c) och hörnet c

T_4 lägg till kanten (c, h) och hörnet h

T_5 lägg till kanten (b, f) och hörnet f (Här fanns flera alternativ)

T_6 lägg till kanten (f, k) och hörnet k

T_7 lägg till kanten (c, d) och hörnet d (Här fanns flera alternativ)

T_8 lägg till kanten (c, i) och hörnet i (Här fanns flera alternativ)

T_9 lägg till kanten (i, j) och hörnet j

T_{10} lägg till kanten (j, e) och hörnet e

T_{11} lägg till kanten (f, l) och hörnet l

T_{11} är ett minimalt uppspännande träd i grafen.